Enhanced Lightweight Message Authentication Scheme for Smart Grid Communications in Power Sector

Research Thesis Submitted By

Fahim khan

(Reg#397-FBAS/MSCS/S08)

Supervisor

Prof. Dr. Muhammad Sher

HOD, DCS&SE, FBAS, IIUI

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING FACULTY OF BASICAND APPLIED SCIENCES INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD (2013).

1. Computer Software
2. Open Source Software

INTERNATIONAL ISLAMIC UNIVERSITY ISLAMABAD
DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

Dated: 22-03-2013

Final Approval

It is certified that we have examined the thesis titled "**Enhanced Lightweight Message Authentication Scheme for Smart Grid Communications in Power Sector**" submitted by Mr. Fahim Khan, Registration No. 397-FAS/MSCS/S08, and found as per standard. In our judgment, this research thesis is sufficient to warrant it as acceptance by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner

22-03-13

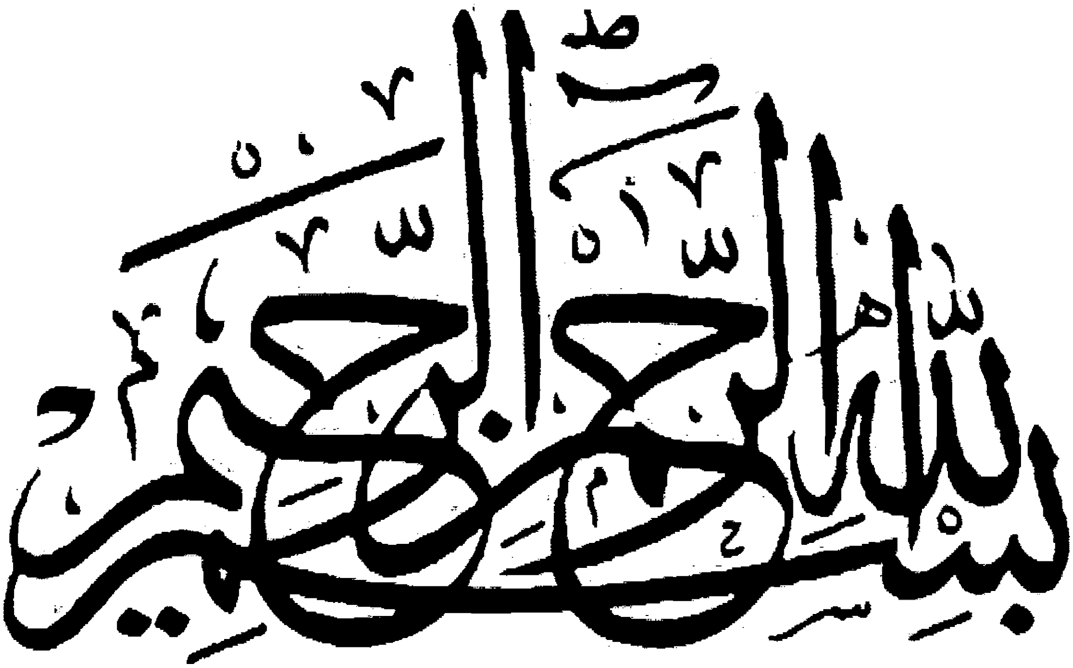
Dr. Nadeem Javaid
Assistant Professor
COMSATS Institute of Information Technology
Park Road, Chak Shahzad Islamabad

Internal Examiner

Syed Muhammad Saqlain
Assistant Professor
Department of Computer Science & Software Engineering
International Islamic University, Islamabad

Supervisor

Prof. Dr. Muhammad Sher
Chairman,
Department of Computer Science & Software Engineering/
Dean Faculty of Basic & Applied Sciences,
International Islamic University, Islamabad



With the name of ALLAH Almighty

The Most merciful and kind the most gracious and beneficent whose help and guidance always on me at every step and every moment

This technical report is submitted to Department of Computer Science and Software Engineering, International Islamic University Islamabad, as a partial fulfillment for the requirements of awarding Degree in Master of Science in Computer Science.

Dedication

I dedicate this work to my parents, sister and brothers whose love, support and prayers make this dream come true. I also dedicate this work to my all family members and to my current and past teacher whose help is always appreciated for my success in each and every field of life. To all my friends especially Shehzad Ashraf Ch for his kind helps, technical support, which gives me strength for achieving this difficult task.

Declaration

I Fahim khan S/O Yousaf khan declare that, this thesis as a part not as a whole is copied from any other source. I further declare that, this thesis and not a portion of this work are submitted by any other applicant/student in any other institution and educational organization for the award of degree at any level. This work is only submitted by me at IIUI for awarding of degree in MSCS.

Date: ____________________

Fahim Khan

(397-MSCS/FBAS/S08)

Acknowledgements

This thesis and all the efforts for completing this work is only done by the grace of Allah Almighty, the most Merciful and Beneficent, Who gave me the strength for completing this work with best abilities of my knowledge.

I would like to thanks my supervisor Prof. Dr. Muhammad Sher and my friend and teacher Mr. Shehzad Ashraf Ch for giving me all the knowledge, guidance and boosting my confidence and learning abilities for achieving this work to be done. I also like to thanks my parents, sister, brothers, nephew and all my family members for their support and prayers, which encouraged me for completing this work.

I also like to thanks my friends Sahibzada Nizamuddin, Ikram asghar, Anwar ghani for their encouragement and help in various phases of this work. I also like to thank my uncle Arshad Iqbal for his kind financial support.

I am very thankful to all my friends for encouraging me in achieving this difficult task.

Fahim khan

Abstract

Smart Grid is an update to the current electrical power grid. It is basically the integration of digital computation and communication technologies. The basic aim of Smart Grid is the secure and reliable delivery of electricity to consumers more intelligently. In the last decade Smart grid got significant attentions from researchers and engineers both in electric power generation and communication areas. Smart Grid allows two-way communication between consumers and utility provider. Consumers play an active role for adjustment of their electrical power usage and communicate back and forth with utility provider for this purpose. IP-Based communication technologies are used for setting Smart Grid communication network, but they are challenged by huge volume of delay sensitive data and control information between consumers and the utility provider. It is also challenged by the number of security attacks namely, man-in-the-middle attack, reply attack due to the resource limitation problem in Smart meters specially related to privacy concerns.

Different authentication schemes were proposed for addressing these problems, which are not suitable for these resource constrained devices. They results to high communication, computation overhead and latency. Designing a security mechanism must consider the resource constrained nature of these devices and focus on an authentication technique which is light weight enough so as to be suitable for Smart Grid. In this way these resource constrained devices will not be over burden.

The proposed scheme is a light weight authentication scheme which uses the well-known Diffie-Hellman approach for session key generation. It is basically a hybrid approach of AES and RSA. To ensure message integrity the proposed scheme exploits the advantages of HMAC technique. The proposed scheme provide security by achieving mutual authentication, thwarting reply and man-in-the-middle attacks in the key generation phase and also achieves integrity of message through HMAC.

The simulation showed that the proposed scheme is suitable for smart grid communication, which results in low computation, communication overhead and latency. The overall results show 49% low communication overhead, 35% low computation overhead than schemes presented by fouda [2] and sule [33] and also 32% lighter in latency than the schemes of fouda and sule.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1. Introduction

Electric power grid is an electrical infrastructure whose aim is to produce and distribute the electric power to consumers in a more reliable manner in order to maintain reliability and efficiency in distribution, but the current electric grid is out-dated. So Smart Grid (SG) is the update to current electric power grid, which fulfill the current and future electric power requirements of the consumers in a most reliable and intelligent way [1].

In recent year's SG got attention from researchers and also from engineers in electric power generation and communication areas [2]. Smart Grid is the important component of U.S power system modernization, which has different names in the literature like, "power grid", "intelligent grid", "grid wise", "modern grid", "perfect grid" and "Grid of the future" [3].

SG which is also referred as grid of the future is an enhancement of the current electrical power grid, by integrating digital computation and also communication technologies for providing secure, efficient and reliable delivery of electricity and exchange of information between power generators, utility companies and consumers of the electric power [4].

SG is an electrical infrastructure whose aim is to make suitable and correct decisions about the state of electric power system and maintain a stable environment intelligently. SG provides all the functionalities provided by current electric grid with some new functionalities, which is described below [1].

a. **Self healing**

   If the electrical transmission path is interrupted then, the smart grid can automatically redirect and adjust the flow of electric power by using alternative path (i.e. with the help of intermediate nodes, if the primary link is interrupted then there is secondary path installed and the power is directed to that path, which reduce the frequency and duration of outage [5]).

   In short, it is the ability of detecting the fault rapidly, analyzing it and responding to it intelligently by taking appropriate action to recover from the fault [6].

   It was estimated that, the major blackout from U.S. to Canada in August 14, 2003 had a social cost of $10 billion [37].

b. Motivate and include the consumers

In current electrical power grid the consumers are not provided with more information about their electrical power, but smart grid provide more options and information to consumers about their current consumption of electrical power, so as to do better decision about power utilization which enables the consumer cost effective utilization of resources.

c. Resist attack

SG resists to both physical and also to cyber attacks.

d. Increase in power quality

SG provides increase in power quality by maintaining constant voltage. In short the quality of the power must fulfill the consumer's demands [6].

e. Accommodate all sources of generations and storage options

Smart grid supports new energy sources along with the traditional power sources. As the conventional electric power grid has a broadcast model and designed to allow a one-way flow of power from a single generated source to many consumers. So smart grid can accommodate the distributed generation of power and efficiently distribute the power to many consumers with no issue.

SG adapts new technologies such as green power with no issues [6]. Smart grid also adopts wind power generation and distributes the power to consumer with no issues. In Sweden 20% of the electricity demands are fulfilled with wind power [7].

In Germany, the consumers using solar power panel experienced issues related to their power grid. Consumers of the solar panel can overload the power grid when a huge power comes from solar panels [38].

f. Enables electrical markets

Smart grid encourages competition among electrical power suppliers in electrical market to develop cheaper and efficient means of power generation. The suppliers provide electricity on a low price to consumers in order to compete the competitors in the electrical market. Smart grid support distributed power sources, which promote new electric power suppliers and service providers to enter the market. By which the consumers have supplied the electric power on much low cost.

g. Optimizing assets and operate efficiently

The smart grid automatically assists the equipment conditions and also manages its configuration, by reducing the cost as compared to conventional electrical grid. Smart grid incorporates new technologies by reducing energy loss during electrical transit and increase efficiency of the electrical power grid.

Thus SG is an electrical power infrastructure with smart capabilities by allowing power providers, power distributors and power consumers to maintain one another operating requirements and capabilities in a near-real-time and also with these capabilities SG produce, distribute and consume the power in efficient and intelligent way [2]. The SG provides the power to consumers in a stable and also in a reliable way, whereas the conventional grid will not provide it in future [2] [8].

The SG allows two-way communications among consumers and provider of electrical power, this two-way communications enable consumers to effectively identify their power requirements to utility provider by which they play an active role and efficiently minimize their current consumption level [2]. Thus through this ability the consumers can efficiently minimize their energy consumptions by communicating back and forth with the providers of the electricity. Whereas the conventional grid broadcast the electricity in one-way fashion and the consumers are not actively participate, and neither have they minimized their consumption level.

The demand response capability for the load management can efficiently reduce the load in an emergency situation or in high price situation, so the consumers can reduce their consumption level in these situations accordingly [9]. It was estimated in [39] that, the demand response in non emergency situation can reduce the price from 5% to 15% in peak load.

In SG, a number of sensing devices, smart meters and control-systems lies in the path between provider and consumers of electric power for facilitating this two-way communications [2][8][10]. The sensing devices are capable of malfunctions detection and also operations normal ranges deviation, it require a proper response from control center, while these responses are converted to control messages and send to SG segments [2][10]. For this purpose, the SG communication framework and its functionality must be characterized in order to allow active consumers participation and facilitate resiliency to various security threats. In SG the consumers have smart meters, by which they are capable of identifying their consumption of power in most efficient way as compared to conventional energy meters [2].

The smart meters normally collect the electrical consumptions information of smart home, which is then collected by utility company (i.e. for monitoring and billing purposes). Consumers also access his/her smart meter for checking their consumption level and adjust the power usage accordingly (i.e. less usage of electricity during peak hours for saving money) [2][8][10]. For this purpose smart meter sends messages to the utility provider periodically for adjusting their power usage and participate actively for their power usage adjustment with in SG dynamically. The utility provider can also send some special offers by sending messages to smart meters, by which the consumers can save money and adjust their usage accordingly.

During peak electrical hours if all the appliances are switched on and the smart grid are going to an emergency situation then the utility provider send messages to all consumers by using smart meters to notify about the emergency event and to adjust consumption level accordingly, by which the consumers thwart the situation by shutting down some appliances and participate to the stable environment actively [11]. Whereas the conventional power grid didn't have such functionality. The smart meters can efficiently communicate with their appliances and collect the energy requirements from all appliances i.e. smart appliance [8].

The smart grid communication infrastructure consist homes, buildings and large neighborhoods, in order to facilitate smart grid communication the Internet Protocol (IP)-based communications network technologies are the suitable choice for setting up IP-based SG communications. The smart meters and smart appliances (i.e. heater, dishwasher, washing machine, air conditioner, tube light, television etc) must have a unique IP addresses for supporting SG communication and support standards of standards of IETF (Internet Engineering Task Force) for remote management of smart meters located at different places in the hierarchy [2][8][10].

The electric utilities itself turn off loads remotely in peak hours demands and they can also manage integration to their distribution systems of power generation, like solar and wind for load balancing [12].

The remote management allows the power provider to efficiently collect metering data from Smart meters for monitoring and billing purposes and they also send some control messages which contains some special offers and error events [40].

1.1. SG communication system model

In current decade smart grid got attentions from researchers in both distribution and communication sectors, for this purpose different communication models are presented in the literature [3][9][13][14][15]. The communication model which is adopted here is presented in [2] [8][10] with a miner enhancement, by replacing wimax technology through optical fiber for long distance communication between control centers and buildings feeders shown in figure 1.1.

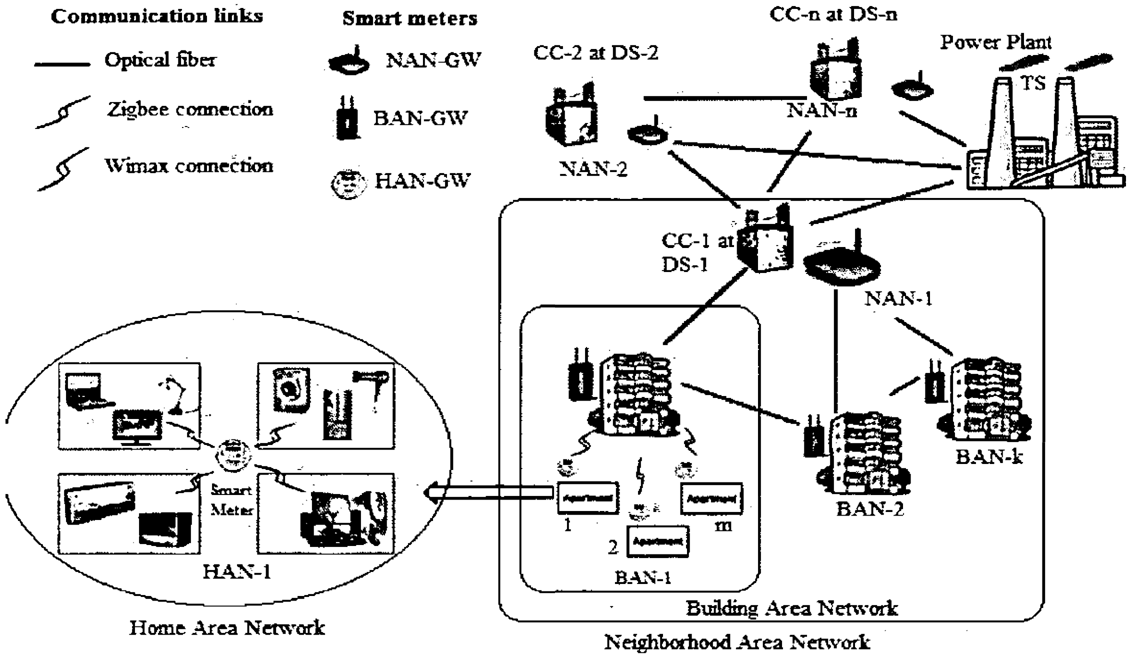


Figure 1.1: SG communications Framework

The authors in [2][8][10] proposed the communication model for SG, in which they separate transmission and distribution system of the power from communication.

The distribution network (DN) delivers electric power from power plants to consumers by the following two primary systems; 1) Transmission Substation (TS) at power plant, 2) one or many distribution substations (DSs) [2][3][8][10]:

The TS's delivers the electrical power from power generation plants through higher voltage transmission lines (230KV's) to DS's resides at different regions. They then transforms this high voltage power to a medium voltage power and distributes it to feeders resides at buildings, the feeders at buildings then transforms medium voltage to a lower voltage, which is then used by smart home appliances [2].

The "handoff" between transmission substation to distribution substation of high voltage and the conversion process of this high voltage to medium voltage is done in DS. So in short the transmission substation delivers the electric power from power plant to distribution substation whereas the distribution substations delivers the medium level voltage electric power from distribution substations to feeders, which convert it to lower level voltage and is then consumed by consumers appliances [41].

In [3] the author said that, the distribution of the electric power starts at distribution substation and ends with consumer electric meter.

The authors in [8] stated that, for communication purpose the above scenario is not applicable, because the requirements of communication links are different than power lines. In [2][10] they divide the smart grid communication network to a number of hierarchal networks, the TS's and control centers(CCs) of the DS's are linked to one another by mashed network by using optical fiber. Optical fiber is chosen for two reasons; 1) suitable for mesh network [2] and 2) least possible communication latency [3].

In [8] the author describes the real life scenario of a city, having many neighborhoods and a neighborhood contains many buildings and a building contains many apartments. So by taking in mind this real life scenario the lower distribution network is constructed.

The authors in [2][8][10] divide the lower level distribution network (from control centers to onward) to a number of hierarchal networks and named him Neighborhood Area Network (NAN), Building Area Network (BAN), and Home Area Network (HAN). They said that, each DS only covers one neighborhood area, and one NAN contains a number of BANs, and one BAN have multiple HANs as shown in above figure 1.1.

In figure 1.1, n DS's covering n neighborhood, so each DS have one NAN and each NAN have k BANs and each BAN have m HANs. The smart meters shown in figure 1.1 are responsible for allowing the two-way communication among consumers and provider of electricity, the smart meters comprises two interfaces, one is used for power reading and another is used like gateway (GW) for communication purpose [2][8][10].

The smart meters located at different places in the hierarchy shown in figure 1.1 are named as NAN-GW, BAN-GW and HAN-GW, through these smart meters/GWs consumer can check their current consumption level of the electrical power and adjust their consumption by shutting/ running some appliances[2][8][10].

The MSP430F571xx microcontroller in smart meter is able to operate as a communication HAN-GW, which consists 16 MHz of CPU, 120 KB of flash memory, 8KB of Ram, programmable gain amplifiers (PGAs), real time clock (RTC), 160-segment Liquid digital converters (LCD), 16-bits of analog to digital converter's (ADCs), and 32 x 32 hardware multiplier (32*32) for calculation of energy measurement [42].

The author in [2] states that, fully functional BAN-GW is not yet released in the market, but they assume that BAN-GW must be ten times greater in computation as compared to HAN-GW, so the smart meter in BAN will have BAN-GW with the following specification, by having CPU of 160MHz, 128 KB of RAM and 1 MB of flash memory. They assumed that the NAN-GW be a Personal computer with core i7 CPU and 6GB of RAM because it is not released yet in the market.

In the proposed communication model, the difference in the specification of the smart meters in the hierarchal network is made to the reason, because lower level consumers in SG results lower traffic and having a budget constraints (e.g. how much the consumers wants to pay for his/her smart meter), whereas the NAN-GW on CC can easily use one or more PCs for dealing with a huge amount of traffic which is originated by consumers in the neighborhood [2].

The IP-based communication networking technologies are suitable choice for connecting HANs, BANs, NANs, CCs and TS because it provide a virtual effortless connection between them [2][3].

The HAN, BAN and NAN are described in the coming subsections.

1.1.1. Home Area Network (HAN)

Home area network is on the lowest level of the hierarchy in the communication model shown above in figure 1.1, which is on a consumer end. In home area network the consumers can efficiently manage their consumption level by switching on/off some appliances respectively [10]. In figure 1.1 the HAN-1 connects the appliances (i.e. oven, television, washing machine, hair drier, computer, tube-lights etc., these appliances have their own IP addresses in a smart home) to HAN-GW at HAN-1 [2].

The authors in [10] adopted, Smart Energy Profile (SEP) version 1.5 for HAN as a communication protocol, which use ZigBee radio communications, and efficiently connect smart meter with smart appliance in smart home, so ZigBee is the appropriate communication medium for home area network.

The author in [8] compare wireless technologies and suggested that, ZigBee is the best choice for HAN than (IEEE 802.11) WiFi and (IEEE 802.15.1) Bluetooth, because it provide a higher communication rage from 10-100 meters, maintain lower power requirements from 1-100 nW and having low cost, and having simple network configuration and management than Bluetooth and WiFi.

The HAN-GW at HAN-1 in figure 1.1 is also connected to BAN-GW at BAN-1 for communication purpose, the power requirement messages is send by using HAN-GW at HAN-1 to BAN-GW at BAN-1, which is then forward to NAN-GW at NAN-1 and the CC-1 of the utility provider take an appropriate action on the requested messages accordingly [2].

1.1.2. Building Area Network (BAN)

Building Area Network (BAN) resides at the middle level in the hierarchal network. In a real life example, a city is made of a number of neighborhoods and each neighborhood contains a number of buildings and each building contains a number of homes, so BAN in the considered communication model contains multiple HANs.

The equipment on building feeder is a BAN smart meter, which act as a BAN-GW and its functionality is monitoring of power requirement needs and usage of residents at that building, in-short the BAN-GW at BAN-1 in above figure 1.1 monitors the flow of power and also power consumption needs of the residence of smart homes in that building [10].

BAN to HANs communications is allowed by using WiMax technology, which normally cover more area than WiFi and ZigBee, the choice of WiMax against WiFi and ZigBee is made on the reason that the distance between the BAN-GW and a particular smart home maybe hundred or more meters, so for this reason WiMax is suitable than ZigBee and WiFi and accommodate more HANs to a specific BAN and provide communication between BAN and multiple HANs [2].

1.1.3. Neighborhood Area Network (NAN)

Neighborhood Area Network is at the top of the smart grid communication hierarchy i.e. it resides at the CC of the distribution substation shown above in figure 1.1.

The smart meter installed at the CC act as NAN-GW, by which utility company can monitors that, how much of power is currently distributed to neighborhood by CC at DS [2][8][10].

The NAN consist a number of BANs and to facilitate communication between NAN-BANs we adopt Optical fiber instead of WiMax and 3G. The Optical fiber framework in SG is used for communication only and here it does not provide other services like internet, its only function is to provide communication between NAN-BANs.

The author in [3] stated that, Optical fiber installation cost is inexpensive for the utility provider, the error rate in Optical fiber is low, increased transmission speed, short communication delay [15], provide high scaling i.e. accommodating more consumers to smart grid and also provide accommodation of more messages i.e. high bandwidth (several hundred of gigabits per second) than WiMax and 3G. So for that reasons we adopted Optical fiber for NAN-BANs communication in smart grid instead of WiMax.

1.2. Security in Smart Grid

IP-based smart grid communication make use of IP-based communication network technologies, which has a problem of large volume of delay-sensitive data and control information and also vulnerable to different attacks like reply, eaves dropping, denial-of-services, man-in-middle, in short attacks of wired and wireless networks are also applicable to IP-based SG communication network [2][10].

As SG networking combines different components of electrical power system to work together and interact with one another, which require interaction between these different technologies to work effectively by introducing different security risks [1].

The higher degree of interconnection between different components of smart grid introduces new security vulnerabilities [16]. Electric Power Research Institute (ERPI) stats the main issue of SG development concerning to cyber security, and states in their report that, "Cyber security becomes a critical component for smart grid due to various cyber-attacks and incident which disconnect the smart grid network. Cyber security not only address deliberate attacks (i.e. form disgruntled employee, industrial espionage, and also from terrorists) but also a compromise to information infrastructure caused by user errors, failure of equipment and natural disasters. The attackers exploit these vulnerabilities and get access to control software easily and alter the load conditions by destabilizing the grid in an unpredictable way" [43]. The author in [17] states that, the availability, confidentiality and integrity were the only security objectives of the conventional power grid.

The existing smart meter technology is centralizing the consumer's consumption information, which leads to privacy concerns [15]. This power reading is send back to power suppliers on regular intervals for billing and monitoring purposes, which also give a SG with a feedback mechanism to model the power usage requirement in a much more detail level than what is currently possible [2][8][10]. In 2009, The Netherland Parliament pass a bill in which, privacy issues are made mandatory while using smart meters [18]. The National Institute of Science and Technology (NIST) has identified that, privacy is the main concern while using smart meters in SG [19]. NIST stated in U.S. that, SG must have a "*privacy for design*" approach [44]. The utility provider can read power usage efficiently many times hourly by using smart meters and demand response requests from consumers, but creating privacy concerns for the consumers of electric power [20].

The conventional electric grid only focus on physical security but smart grid also focus on cyber security due to the use of smart meters which are connected to one another on a broadband network and contain consumers personal data and also the consumption information of the smart homes. So, privacy of the consumer credentials including the electrical consumption information is necessary.

1.3. Importance of Security in Smart Grid

The SG communication network is IP-based, which provide connectivity between the components of the smart grid, which allow two way communication among these components but will introducing new security risks, in short all the security threats are also applicable to Smart Grid, by which the attackers can easily exploit smart grid by gaining access to smart grid environment [1][2].

In smart grid the consumers of smart homes are equipped with smart meters, which collect the consumers consumption information and these smart meters send these information to utility provider on regular interval for monitoring and billing purposes. So the security of the smart meters is important. Some means of security mechanisms must be presented to thwart attackers from gaining access to smart meters located at various locations of smart grid communication hierarchy.

In [45] the attackers with basic electrical background and equipment's can easily get command on smart grid communication system bilaterally, and cause the blackout by one of the two ways: 1) shutting down the smart meters after getting control on them. 2) Disturbing the load balance of the local system by increasing or decreasing the demand of electric power suddenly.

In smart grid, not all the entities are trusted; in this case there should be a proper authentication mechanism which must verify the authenticity of both parties involved in communication [10].

The altered readings from a smart meter can lead to incorrect billings and also leads to false approximation of the power usage [1]. From US power system, $6 billions of worth of power was stolen [21]. As the smart meter readings are send back to power provider, so it is necessary that these reading must not be modified. The smart grid important security aspects are integrity and confidentially. The authors in [22] [23] built tools to profile the electric usage readings of the consumers to determine which appliance is being used and which is not, it is then used by different individuals and companies and will lead to privacy concerns.

In [14] the author categorize the security attacks in to three types base on their desire goal, named 1) network availability, 2) data integrity and 3) information privacy, the availability of network can be compromised by denial-of-service attack by delaying, blocking or corrupting the transmission to make the network resources unavailable to smart meters, when they want to exchange information in the smart grid, where as attacks(less brute force) on data integrity focuses on accessing consumer information such as account information and their current balance, or operational information of the network such as voltage readings and status of the smart meters etc, the main concern of these attacks is to modify the actual reading of critical information which is shared between smart meters in the smart grid, the attacks on information privacy only eavesdropping the information which is being exchanged between smart meters and utility provider but does no modify it, their main focus is on collecting consumers account number and their current electric usage.

In [24] propose a *"false data injection"* attacks whose purpose is to inject the state of the estimation of the power grid, they supposed that the attacker have already compromised one or many smart meters and they taking advantage of the power system configuration by injecting false data to monitoring center, which bypass data integrity checks of the current power grid system.

The authors in [2] states that, 'the SG communication framework must consider an efficient authentication mechanism by which the attackers cannot compromise the secrecy or privacy of the information which is exchanged among consumers and utility provider of the electric power. They suggested that, smart meters authentication will resolve privacy concerns, but smart meters have limited resource (i.e. it contains low memory and have lower computation capacity), so the authentication mechanisms should be designed on a light weight way such that, they should not situate too much burden to smart meter resources.

To address the privacy concern in using smart meters the message authentication algorithms must be designed on a light way manner such that, it will not results to high computation cost, latency and only few signals messages will be exchanged in authentication phase. It is the most interesting question, if SG is an IP-based then why the existing authentication suites of security are not applicable in IP-based smart grid network, the answer to this question is very simple, because the smart meters are resource constrained (i.e. limited computational and communication capacity and having low memory), so the existing authentication mechanisms didn't work efficiently and will lead to scalability issues i.e. multiple requests are not processed at the same time and will increase the communication latency and produce delay in providing service to all consumers. For this purpose the researchers are trying to develop the authentication mechanisms in a light-weight way, so that they do not put too much burden on the existing constrained devices in terms of exchanging few messages and does not contribute high computation complexity and communication latency [2][8][10].

1.4. Research objective

As the smart grid devices (i.e. smart meters) have low computation capabilities, so the authentication techniques for addressing privacy concerns are needed to be designed in a lightweight manner i.e. they seems to be acceptable in-terms of communication and computation overhead. The proposed authentication scheme use Diffie-Hellman key establishment protocol with both RSA and AES suites for session key establishment and HMAC for message integrity and results into low computation and communication overhead with low delay and latency. Proposed scheme will also achieve mutual authentication in session key establishment phase and also thwart man-in-the-middle attack and reply attack. Proposed scheme will also achieve authenticity of user and integrity of message.

1.5. Thesis organization

The rest of the report is organized as follows:

- Chapter 2 covers the literature review of the selected studies and also formalizes the problem statement.
- Chapter 3 describes the two way communication flow and proposed authentication scheme and also its security analysis.
- Chapter 4 describes the simulation setup and performance metrics and also describes results comparisons with existing techniques by using performance metrics.
- Chapter 5 concludes the thesis and mentioned future work.

Chapter 2

Literature review

2.1. Selected studies for literature review

The following section presents the systematic literature review of different research articles, which form the base of this research study. After a careful investigation of 120 research articles in smart grid, only 14 research articles are selected for systematic literature review. Each of the selected articles is considered one by one and explained with the help of following three criteria's named Motivation, Contribution and Limitation. List of papers is given bellow:

- **P1→** IEEE P2030 Draft Guide.
  Available at: http://grouper.ieee.org/groups/scc21/2030/2030 index.html.
- **P2→** A. Hamlyn, H. Chaung, R. Cheung, T. Mander, C. Yang and L. Wang, "Network Security Management and Authentication of Actions for Smart Grids Operations", in proc.IEEE Electr, Power conf, pp.31-36, Oct, 25-27, 2007 Montreal, QC, Canada.
- **P3→** G.N. Ericsson, "Cyber security and power system communication-essential parts of a Smart Grid infrastructure", IEEE Trans, Power Del., vol.25, no.3, pp.1501-1507, Jul, 2010.
- **P4→** A.R. Metke and R.L. Eki, "Security Technology for Smart Grid Networks", IEEE TRANSECTION ON SMART GRID, Vol. 1, NO.1, PP.99-107, ISDN, June, 2010, IL, USA.
- **P5→** K. Kursawe, G. Danezis and M. Mohlwieiss, "privacy friendly aggregation for the smart grid", Microsoft Research.
  Available at: http://research.microsoft.com/apps/pubs/?id=146092.
- **P6→** D. Chung, M.H. Dwijaksara, J. Kim, K. Kim and Y. Park, "An efficient and privacy-preserving authentication protocol for HAN", Symposium on Cryptography and Information Security (SCIS 2011), Jan, 25-28, 2011, kokura, Japan.
- **P7→** D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid", IEEE Transaction on Smart Grid, Vol.2, No.2, pp.375-381, Jun, 2011, FL, USA.
- **P8→** G. Cao and Q. Li, "Multicast Authentication in the Smart Grid with One-Time Signature", IEEE TRANSECTION ON SMART GRID, VOL.2, NO.4, pp 686-696, Dec, 2011, PA, USA.
- **P9→** T.W. Chim, L.C.K. Hui, V.O.K. Li and S.M. Yiu, "PASS: Privacy-preserving Authentication scheme for Smart Grid Network", IEEE Conference on Smart Grid communications (SmartGridCom), pp. 196-201, Oct, 17-20, 2011, Hong Kong, China.
- **P10→** J. Choi, C. Li, J. Seo and I. Shin, "An Efficient Message Authentication for Non-

repudiation of the Smart Metering Service", ACIS/JNU Conference on Computer networks (CNSI), pp. 331-333, May, 23-25, 2011, Daejeon, South Korea.

- **P11→** E. Ayday and S. Rajagopal, "Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks", IEEE Conf on Communications and Networking (CCNC), pp. 1161-1165, Jan, 9-12, 2011, Atlanta, GA, USA.
- **P12→** M. Kgwadi and T. Kunz, "Security RDS Broadcast Messages for Smart Grid Applications", in proc.6th int. wireless commun. Mobile comput. Cont., France, Jun, 2010.
- **P13→** M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu and X. Shen, "A Lightweight Message Authention Scheme for Smart Grid Operations", IEEE Transactions on Smart Grid, vol. 2, no.4,PP. 675- 685, ISSN: 1949-3053 Dec 2011.
- **P14→** R. Sule, R.S. Katti and R.G. Kavasseri, "A Variable Length fast message authentication code for secure communication in smart grids", IEEE Conf. on Power and Energy society, pp. 1-6, Jul, 22-26, 2012, Fargo, ND.

2.2. The Detailed Summery of the selected studies

The detailed summary of the selected studies are discussed below.

- **P1 →** IEEE P2030 Draft Guide. Available at: http://grouper.ieee.org/groups/scc21/2030/2030 index.html [46].

Motivation:

For fulfilling the requirements of Smart Grid (SG) and for the enhancement of the current electrical power grid to SG, many standards should be taken into account. For that reason Institute of Electrical and Electronics Engineering (IEEE) launches IEEE P2030 group to define standards for SG environment, which provides the SG functionality.

Contribution:

They established three taskforces to formulate the SG agenda. These taskforces are taskforce 1, taskforce 2 and taskforce 3.

The taskforce 1 was assigned on power engineering technologies. Their objectives was defining boundaries on the generation of power, transmission of the generated power and efficient distribution of the power while keeping in mind the consumers i.e. the consumers will get the electric power in a more efficient and reliable manner with low cost. This taskforce takes into account conventional generation of electric power with renewable generation sources of the electric power and combines it in a way to entertain consumers with a constant voltage in a more intelligent and reliable way to thwart blackouts caused in the near past.

The taskforce 2 was assigned to deal with information technology. Their work focused on identifying security technologies for maintaining information about distributed environment, so information technologies actually securing SG communication digitally. They investigated various issues like privacy, interfaces, data integrity and interoperability with in the SG. They designed various system protection and communication policies to allow the functionality in SG with certain considerations in mind. They also defined various procedures to thwart various security threats against SG.

The taskforce 3 was assigned to deal with communication technologies. They identified efficient communication technologies for allowing two-way communication among consumers and utility provider in a more reliable and intelligent way with in SG.

Limitation:

The policies designed by these taskforces have a broad-nature and be coarse in design and are difficult for security enforcement in SG [25].

- **P2 →** A. Hamlyn, H. Chaung, R. Cheung, T. Mander, C. Yang and L. Wang, "Network Security Management and Authentication of Actions for Smart Grids Operations", in proc.IEEE Electr, Power conf, pp.31-36, Oct, 25-27, 2007 Montreal, QC, Canada [26].

Motivation:

The authors identified that, due to micro gird developments the operations of the electric power grid are more crucial and must be authenticated, because any security and authorization violation will affect the micro grid performance and results to false billing.

Contribution:

They proposed their scheme in which they designed strategies and procedures for security checks and authenticate commands requests for operations in host Area Electric Power System (AEPS) and also from interconnected neighboring AEPS. They also mentioned that, only a trained staff can get access to a utility computer network. The designed policies must be followed by trained staff to thwart authorization violations. The security management architecture is shown in figure 2.1.

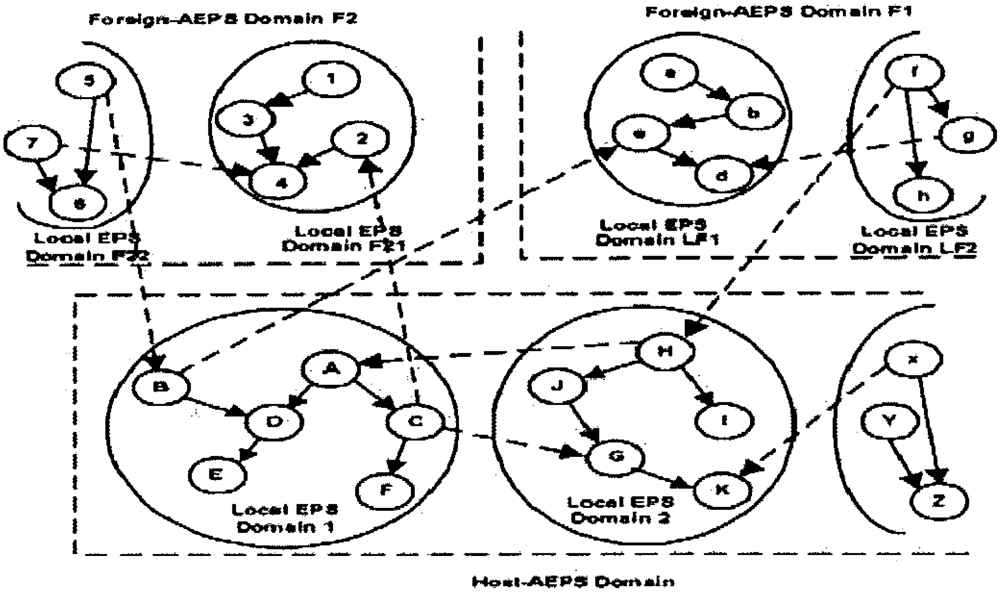


Figure2.1: Power Grid Security Management Architecture [26]

The host AEPS domain contains one network control center and many local EPS domains, the network control center act as administrator for its local domains and communicates with other AEPS domains and also defines a host-AEPS role hierarchy, whereas each local domain is a micro grid having some distributed resources. In figure 2.1 a role is defined as a collection of privileges, which must be executed by authorized users in the AEPS. The privilege is performed on objects like monitoring performance of power system, operating substation equipment, trading of electricity etc. The foreign users request can be authenticated by validating foreign users access polices.

The authentication of smart grid operations on role-based is described below.

Authentication w.r.t role constrains: They grouped a role constraint to cardinality, separation-of-duty and prerequisite constrains. In cardinality constraints they assigned a role to limited users. They managed separation-of-duty constraint by enforcing conflict of interest policies by network controller. They also mentioned that, in prerequisite constraint a user can perform a prerequisite operation if and only if he has a membership in prerequisite role.

***Authentication w.r.t Foreign Domain Interfacing*:** They authenticate users from foreign domain by establishing access policies for foreign-users and by them they verified the authenticity of users from host-domains and also users from foreign-domains. They did this by using digital credentials and verify foreign domain users by digital credential verification.

They also specified the security management for procedure pre-execution and suggested that only appropriate users can gain access to procedures, which have gained access to prior one.

Limitation:

The main shortcoming of this approach is that, it allows limited authentication between host-AEPS and electric circuits i.e. authentication is done only on host-AEPS [2].

- **P3 →** G.N. Ericsson, “Cyber security and power system communication-essential parts of a Smart Grid infrastructure”, IEEE Trans, Power Del., vol.25, no.3, pp.1501-1507, Jul, 2010 [7].

Motivation:

The author identified the two important and critical components of smart grid, which are 1) power system communication and 2) digital security, for Smart grid deployment they both must be considered deeply, because they both are important for proper electric transmission and infrastructure of information. They also identified that, development of communication capabilities to electric grid start moving electric power system from “island of automation” to totally integrated computer environment, which open ways to new security vulnerabilities.

Power system communication capabilities connect Supervisory Control and Data Acquisition (SCADA) systems and substations to other systems over dedicated lines or over internet. This introduce digital security issues, which must be solved for smart grid communications e.g. combining SCADA/EMS (Energy Management System) to information technology networks will open several new security threats like, intrusion etc.

Contribution:

The author identified different access points to a SCADA system, shown in figure 2.2.

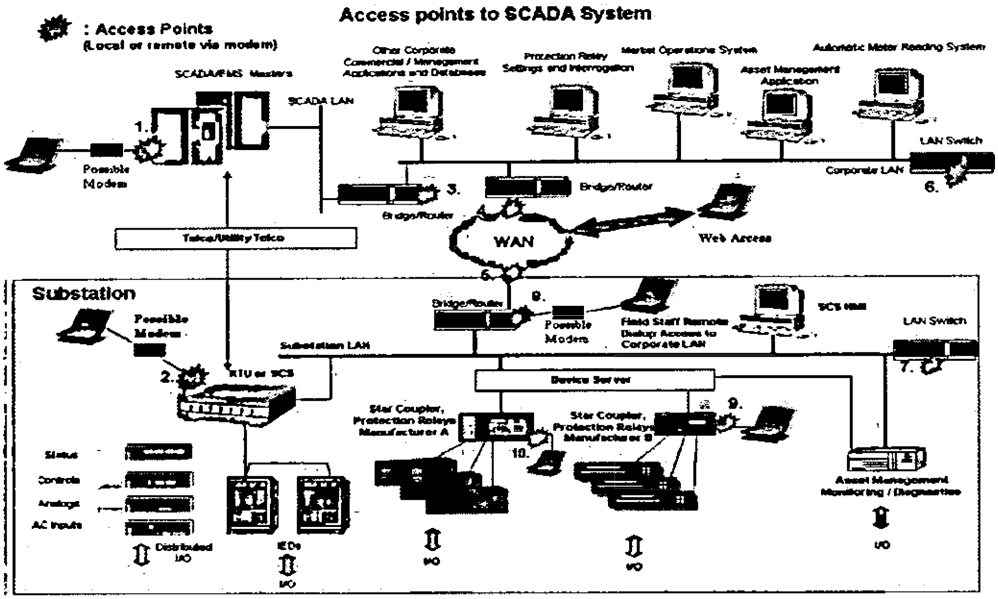

Access points to SCADA System
: Access Points
(Local or remote via modem)
SCADA/EMS Masters
SCADA LAN
Other Corporate Commercial / Management Applications and Databases
Protection Relay Settings and Interrogation
Market Operations System
Asset Management Application
Automatic Meter Reading System
LAN Switch
Corporate LAN
1.
Possible Modem
3.
Bridge/Router
Bridge/Router
6.
Telco/Utility Telco
4.
WAN
Web Access
Substation
6.
Bridge/Router
8.
Possible Modem
Field Staff Remote Dialup Access to Corporate LAN
SCS HMI
LAN Switch
Possible Modem
Substation LAN
7.
2.
RTU or SCS
Device Server
Star Coupler, Protection Relays Manufacturer A
Star Coupler, Protection Relays Manufacturer B
9.
10.
Status
Controls
Analogs
AC Inputs
Distributed I/O
IEDs
I/O
I/O
I/O
Asset Management Monitoring / Diagnostics
I/O

Figure 2.2: Access points to SCADA system [7]

The author also mentioned that, by using a broad band internet technologies the intruders can easily get access to smart meters and also to a central system through which they can collect information (i.e. meter data), which contains consumers personal information, account information. This is breach of privacy. The utility provider can directly access the smart meter data without consumer's permission through broadband network technologies, which is used for monitoring and billing purposes.

Suggestion:

For the above problems they suggested that, for thwarting the security vulnerabilities, authentication of smart grid operations in necessary [2].

- **P4 →** A.R. Metke, R.L. Eki, "Security Technology for Smart Grid Networks", IEEE TRANSECTION ON SMART GRID, Vol. 1, NO.1, PP.99-107, ISDN, June, 2010, IL, USA [16].

Motivation:

The authors described that, adding new capabilities to current power grid will introduce new security vulnerabilities and thus SG development must fulfill the requested security requirements. They stated that, all the standard bodies have restricted on one thing i.e. SG security is only depends on, Authorization, Authentication and privacy technologies.

Contribution:

They considered strong authentication techniques, which are necessary for all users and devices in smart grid environment and discussed Public Key Infrastructure (PKI) and trusted computing for SG environment. Their proposed PKI solution is shown in in figure 2.3.

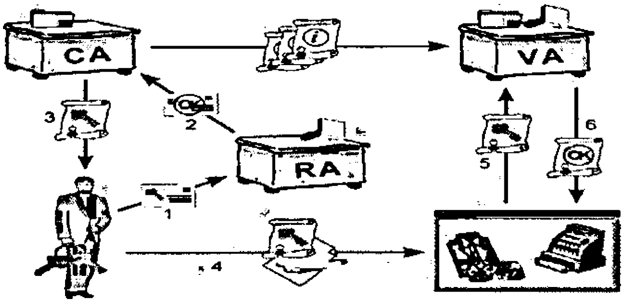


Figure 2.3: Basic PKI procedure [16]

The figure 2.3 shows the basic steps of utilization of the PKI. The sender willing to communicate with receiver simply sends a Certificate Signing Request (*CSR*) to registration authority (*RA*). The *RA* then signs *CSR* and will forward it to Certificate Authority (*CA*) and *CA* issue a certificate. Sender simply sends the certificate to receiver. The receiver validates the certificate from Validation Authority (*VA*) and gets a positive reply from him.

They also stated that, PKI is more efficient than shared keys for connection setting and maintaining for a large system and suggested that, each entity is configured with its own certificate.
The complexity of PKI can be reduced by including the following elements.

1. ***PKI standards***: Standards for establishing the requirements of PKI operations in energy service providers and manufacturers of the SG devices.
2. ***Automated trusted anchor security***: Every operator must support their own PKI hierarchy by using trusted anchor (*TA*) at the top of that hierarchy and is ensured that every secure device will have the valid *TA* information.
3. ***Certificate attributes***: The authentication of SG devices and verification of authorization can be done by using certificate policies attributes locally, without reaching to backend server.
4. ***Smart Grid PKI tools***: The vendor can simply build the PKI tools in SG devices which work

same like PKI tools.

They also mentioned that, demand response introduce malware attacks, which initiate an instantaneous drop in demand and causing damage to distribution, transmission and generation facilities of the SG. They suggested that, smart grid must have a comprehensive plan to deal with these attacks, so one component of the plan is trusted computing shown in figure 2.4.

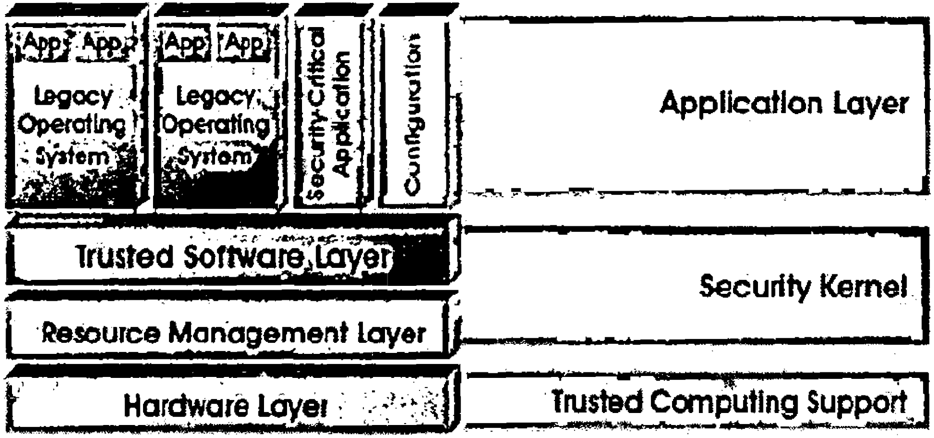


Figure 2.4: Trusted Computing Model [16]

They dealt malware protection problem by validating the software by using High Assurance Boot (HAB) technique, which resides in secure hardware for validation boot-block code. This code validates the Operating System (OS), and OS validate Application Software's, which are performed by using public key or preinstalled key in a secure hardware. They validate continuous running devices by using a background task called device attestation, which is manufactured in smart grid devices and authenticate continuous running devices periodically. For general purpose computing devices they used antivirus to detect malware, because antivirus use "signature" dictionary as a tool to detect and prevent malware.

Claims:

Based on SG security requirements, the utilization of PKI technologies along trusted computing and also with other architectural elements are proper choice for smart grid.

Limitations:

The main shortcoming of strong authentication based on PKI is that, as the users and devices in smart grid are very large in numbers, so strong authentication techniques are not fastest one and also raised a scalability issue in SG. The trust management and key scalability between utility provider and consumers are the main concerns in Smart Grid [2].

- **P5 →** K. Kursawe, G. Danezis and M. Mohlwieiss, "privacy friendly aggregation for the smart grid", Microsoft Research.
  Available at: http://research.microsoft.com/apps/pubs/?id=146092 [19].

Motivation:

They identified the importance of the fraud detection and privacy concerns by using smart meters in SG, and also the need and importance of aggregation of data securely which are taken form smart meters.

Contribution:

They proposed four protocols for data aggregation named as "interactive protocol", "Diffie-Hellman key-exchanged protocol", "Diffie-Hellman and bilinear-map protocol" and "low-overhead protocol", which is discussed below.

- ***Interactive protocol*:** this protocol used additive secret sharing, in every round i of measurement a subset of smart meters choose a leader and computes random secrete shares and encrypt them and send to leader. The leader simply compute the final shares by taking sum of all the shares equal to zero. The K_j is the private key of home, and $PK_1 ... PK_n$ are the public keys of other homes. Each home j then generate masking values by computing p random values $(s_{j,1}, ..., s_{j,n})$. they also computes leader identities $l_1, ..., l_p$ for p leaders and then encrypt $s_{j,k}$ with PK_{lk}, $1 \leq k \leq p$. they sends the p encrypted shares to aggregator, which send the corresponding values to each leader. Every leader l_k then collects $n-1$ shares $s_{j,k}$,$1 \leq j \leq n$, $j \neq l_k$, and also computes its own share $s_{l_k,k}$ such that sum of shares results to zero. At the end all parties sum their shares $s_{j,1}, ..., s_{j,p}$ and derive s_j. When smart meter send reading $c_{i,j}$, they compute $b_{i,j} = c_{i,j} + s_{i,j} \ mod \ 2^{33}$. The aggregator then collect all the reading and compute $\sum_i b_{i,j} = \sum_i c_{i,j}$.
- ***Diffie-hellman Key-exchanged Based protocol*:** Each smart meter j has private and public keys i.e. X_j and Pub_j. For every round i, $g_i = H(i)$ is a "Diffie-hellman" group generator. Each home computes round specific public key $Pub_{i,j} = g_i{}^{X}{}_j$, and distribute it to other members of aggregation set, after receiving these values the home verify public key $Pub_{i,1}, ... Pub_{i,n}$. The

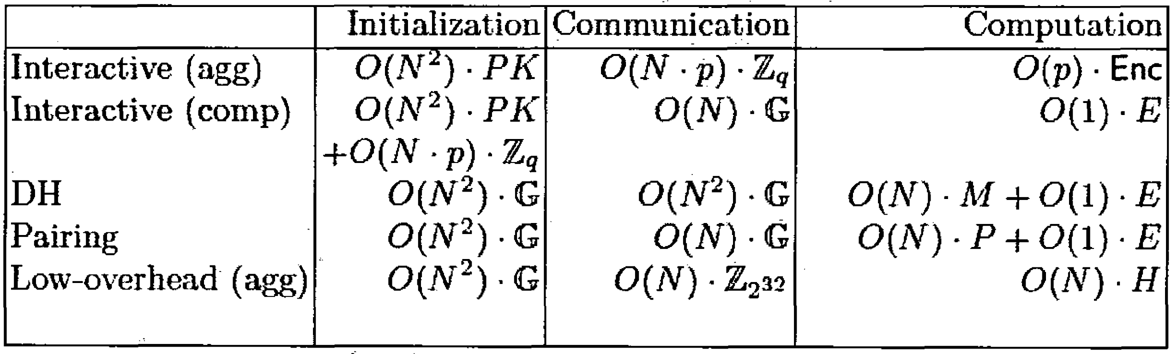
home compute $g_i{}^x{}_j = \prod Pub_{i,k}{}^{(-1)^\wedge k<j\, X_j}$ $k \neq j$. At last each meter compute $g_{i,j}$, like $g_{i,j} = g_i{}^{ci,j} . g_i{}^{x_j} = g_i{}^{c_{i,j} + x_j}$. $g_{i,j}$ is used for comparison in this protocol.

- ***Diffie-Hellman and Bilinear-map Based protocol***: for every round i, each home computes $\hat{g}_i$ $=H(i)$ and $g_i = e(\hat{g}_o, \hat{g}_i)$ and then compute $g_i{}^{x_j} = (\prod e\ (Pub_k, \hat{g}_i)^{(-1)k<j})^{X_j}$, where $k<j$ are variables having values 1 or 0 depends upon the comparison results, and the sum of all x_j be 0. Each meter compute $g_{i,j}$, $g_{i,j} = g_i{}^{c_{i,j}} . g_i{}^{x_j} = g_i{}^{c_{i,j}+x_j}$, which is a comparison protocol value.
- ***Low-overhead protocol***: in this protocol all meters have a fixed $Pub_j = g^{X_j}$, where g is fixed globally known generator. In first step each meter initiate the public keys of other meters and calculate shared keys, $K_{j,k} = H(Pub_k{}^{X_j})$ where $k \neq j$, after generating shared key they discard the public keys of all other meters. For every round i, meter j generate the masking values as $x_{i,j} = \sum(-1)^{k<j}\ H(K_{j,k}\ \mathrm{I}\ i)$. Only 32 bits of $x_{i,j}$ is needed and calculate $b_{i,j} = c_{i,j} + x_{i,j} \bmod 2^{32}$, the aggregator simply calculate sum of all the outputs $\sum_j c_{i,j} = \sum_j b_{i,j} \bmod 2^{32}$.

Results:

The author also compared these protocols and gives the computation and communication overhead in a table 2.1.

Table 2.1: Performance comparison of the concrete protocols [19]



	Initialization	Communication	Computation
Interactive (agg)	$O(N^2) \cdot PK$	$O(N \cdot p) \cdot \mathbb{Z}_q$	$O(p) \cdot \mathsf{Enc}$
Interactive (comp)	$O(N^2) \cdot PK$ $+O(N \cdot p) \cdot \mathbb{Z}_q$	$O(N) \cdot \mathbb{G}$	$O(1) \cdot E$
DH	$O(N^2) \cdot \mathbb{G}$	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot M + O(1) \cdot E$
Pairing	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot \mathbb{G}$	$O(N) \cdot P + O(1) \cdot E$
Low-overhead (agg)	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot \mathbb{Z}_{2^{32}}$	$O(N) \cdot H$

The table2.1 shows that the variants of the Diffie-Hellman based security aggregation protocols have low overhead on smart meters.

Limitation:

The main shortcoming of this work is that, the researchers did not consider the smart meter authentication [8].

- **P6 →** D. Chung, M.H. Dwijaksara, J. Kim, K. Kim and Y. Park, "An efficient and privacy-preserving authentication protocol for HAN", Symposium on Cryptography and Information Security (SCIS 2011), Jan, 25-28, 2011, kokura, Japan [27].

Motivation:

The authors in this paper stated that, an attacker can easily access the consumer private information by using eavesdropping, by which they try to find which appliance is currently on and which is off, and compromise the smart meter easily because it is located outside the home.

Contribution:

They proposed a protocol in which they used a member ship verification method for appliance verification in home area network. Their protocol has four main phases which is described below.

1. ***Appliance registration phase***: in this phase, the home server issues $E\ [-r,\ PK_{BGN},\ G]$ and R_{HS} to appliance for the membership verification.
   Home server ----------------- $E[-r,\ PK_{BGN}, G] \mid R_{HS}$ -------------------→Appliance.

2. ***Appliance authentication phase***: in this phase, the appliances authenticate itself by using $E[-r,\ PK_{BGN}, G]$ and generate a fresh session key $K_{SM,APP}$. After that, smart meter can check the authenticity of the smart appliances by calculating $C^{SK_{BGN}}$ and authenticate if the calculated value is same to the previous one. The smart meter can then simply send *res* to appliance.
   Smart Meter---- $res = H(R_{SM} \mid E\{MSG\_ACK \mid R_{SM} \mid R_{APP} + 1, K_{SM,APP}\}$---→Appliances.
3. ***Power request phase***: after the appliance authentication, they send their required power requirement *request* to smart meter.
   Appliance-------$request = R_{APP} \mid E\ \{MSG\_REQ \mid R_{SM}+1 \mid R_{APP},\ K_{SM,APP}\}$-→Smart Meter.
   The smart meter decrypt the encrypted request packet by using $K_{SM,APP}$. Extract the nonce R_{APP}, and then smart meter verifies $R_{SM}+1$ and send the *result* message to appliance after a valid verification.
   Smart Meter----- $result = E\{MSG\_ACK \mid R_{SM}+2, K_{SM,APP}\}$------------- →Appliance.

4. ***Report phase***: home server then collects the requested power usage information from smart meter and it is then viewed by consumer. The consumer can simply view its consumption level by

accessing home server. The home server can get the consumption information from smart meter by using $K_{SM,HS}$, the smart meter then replied to request if and only if R_{SM} is correctly verified and send *ack* to home server.

Home Server----$R_{SM}|E\ \{MSG\_REPORT|R_{SM}|E\ [-r,\ PK_{BNG}, G], K_{SM,HS}\}$→Smart meter.

The smart meter then calculate R_{SM} by using $K_{SM,HS}$ and verify the received one and send ack to home server.

Smart meter----- $ack = R_{SM}|E\ \{MSG\_ACK|R_{SM}+2|E_{APP}, K_{SM,HS}\}$-------→Home server.

Claims:

They claimed that, their approach provides confidentiality, integrity and also mutual authentication between smart appliances and smart meter and by using nonce they also thwart reply attack.

Limitations:

The only consider a home area network in smart grid and did not consider building area network and smart meter on building feeders. This scheme requires 7 steps for performing authentication.

- **P7** → D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid", IEEE Transaction on Smart Grid, Vol.2, No.2, pp.375-381, Jun, 2011, FL, USA [28].

Motivation:

They identified the reply and man-in-middle attacks in the existing key management protocols for Smart Grid, which only provide key management and does not consider authentication of devices in SG. They also given example of successive reply attack in which they showed that, how successfully the reply messages are accepted as a fresh message.

Contribution:

They proposed a key management scheme by using "*symmetric*" and "*elliptic curve*" key techniques for dealing with the above problems. The symmetric key scheme is based on "*needham-schroeder*" authentication protocol. Their scheme perform authentication on three different components listed below.

- ***Mutual authentication between an aggregator and collector:*** the *A* sequence messages from *A1* to *A6* is used for performing *mutual authentication* among collector and an aggregator. The collector initiates authentication process with trusted anchor by simply sending message *A1* to him. Trusted anchor sends *A2* in response which contain symmetric key. For obtaining session key the same procedure of *"needham-schroeder"* is used, collector firstly sends *A3* message to trust anchor, which replies with *A4*, collector then send *A5* to generator and it replies to collector with *A6*.
- ***The mutual authentication between aggregators across realms:*** the *B* sequence message from *B1* to *B6* is used for performing *mutual authentication* among aggregators across the realms. The authentication process is initiated by aggregator, which sends *B1* message to trust anchor in same realm, the trust anchor replies with *B2* message containing symmetric key for aggregator. The session key is obtained by using *"needham-schroeder"* protocol, the aggregator sends *B3* message to trust anchor which resides in another realm. Trust anchor with *B4* message replies. Aggregator then send *B5* message to aggregator residing in other realm, which replies with *B6* message to aggregator of the requested message.
- ***The mutual authentication among sensor and collector:*** the *C* sequence message from *C1* to *C6* is used for performing *mutual authentication* among sensor and collector. The *C1* and *C6* messages are used for trust request and verification, *C2* and *C3* for symmetric key and *C4*, *C5* are used for delivery of session key.

Claims:

They claimed that, their approach have these advantages over the existing ones.

1) Key management at trust anchor is simple and did not maintain shared symmetric keys.
2) Key request response is fast i.e. the trust anchor assign the key request to other trust anchor for session key issuance.
3) Allows high level of fault tolerance.

Limitations:

This scheme provide mutual authentication between various components of a key management system, but this authentication is not enough for a real SG scenario.

The elliptic curve cryptography has high computational complexity and cost [11].

- **P8 →** G. Cao and Q. Li, “Multicast Authentication in the Smart Grid with One-Time Signature”, IEEE TRANSECTION ON SMART GRID, VOL.2, NO.4, pp 686-696, Dec, 2011, PA, USA [29].

Motivation:

The authors identified the importance of multicast communication in SG applications such as wide area protection, demand-response and protection of substation operations. They observed that, the current existing techniques are not suitable for a resource and computationally constraint devices of SG. They identified the importance of multicast in the case when, utility center multicast the demand-response command to a very large number of homes for turning off their appliances in peak hours or in emergency situation.

Contribution:

In their proposed scheme, they combine Heavy Signing Light Verification (HSLV) and Light Signing Heavy Verification (LSHV) and get Tunable Signing and Verification (TSV). This scheme divides elements of signature to groups by their position in signature, the TSV mechanism is as follows.

- ***Key generation***: in this phase, they generate t random l-bit string $(s_1,s_2,...s_t)$. Now for each s_i generate one-way chain $s_i \rightarrow f(s_i)......f^w(s_i)$ of length $w+1$. This t chain forms a private key SK, whereas public key is generated as $PK = (v_1,..,v_t)$, where $v_i=f^{w+1}(s_i)$.
- ***Signing***: in this phase, for signing a message m, $h = H(m/c)$ is computed, where c is counter with initial value 0. Now $SPLIT(h)$ is called, where all i_j from $SPLIT(h)$ must be different and must be stored in a decreasing order in same group. The signature of m is generated by repeating the above process $(c, f^{w-w_q}{}_1(s_{i1}), ...,f^{w-w_q}{}_t(s_{ik}))$.
- ***Verification***: the signature $(c', (s'_1,...,s'_k))$ on message m is verified by computing $h = H(m/c')$. Call $SPLIT(h)$, and check 1) for all i_j from $SPLIT(h)$ are different. 2) i_j from the same group are stored in decreasing order. 3) Check $f^{w_q}{}_j^{+1}(s'_j) = v_{ij}$ for each j.

TSV is configured on two vectors $n = (n_1,...,n_g)$ and $w = (w_1,..,w_g)$ and the proposed TSV is represented by TSV (g,n,w).

They adapted heuristic solution for reducing the computational cost (signing and verification cost) by simply reducing the signature cost. The steps are given below.

1. Initializing $n_0 = k$, and $n_r = 0$ $(r=1,..,k-1)$
2. For step $1,...,C$ do
3. Go through $n_{0,...,}n_{k-1}$ and find smaller r which satisfies for all $r' \neq r$, $n_r/(n_{r+1}+1) \geq n_r'/(n_r'_{+1}+1)$;
4. Update $n_r = n_r - 1$ and $n_{r+1} = n_{r+1} + 1$.
5. End for
6. The output is $([n_0,..,n_{k-1}],[0,1,...,k-1])$.

Here n_r and n_{r+1} represent the size of the groups and the time complexity is $O(kC)$, where is $C<k(k-1)/2$ and the space complexity is $O(k)$.

Their multicast authentication protocol is based on TSV and for dealing with public key distribution problem in One-Time Signature (OST)-based they used one-key chain to distribute public keys efficiently. Their protocol starting from t random values of $s_{<1,1>},....,s_{<1,t>}$, the sender now generate one-way of t chains having length $d+1$ and stores this series of keys and generate $PK_0 = (s_{<d+1,1>,..,}s_{<d+1,t>})$. The receiver can also refresh and update it private and public keys by replacing the old values to the new ones.

Limitations:

The main limitation of this approach is that, multicast authentication provides security on one-time signature but with increased computational cost of verification and generation of signature. One-time signature generation for each multicast slow the performance of the overall SG environment.

- **P9 →** T.W. Chim, L.C.K. Hui, V.O.K. Li and S.M. Yiu, "PASS: Privacy-preserving Authentication scheme for Smart Grid Network", IEEE Conference on Smart Grid communications (SmartGridCom), pp. 196-201, Oct, 17-20, 2011, Hong Kong, China [30].

Motivation:

The authors identified two problems 1) how to validate a coming message request, i.e. *weather* it comes from a valid user or not? , 2) analyzing the electricity usage pattern can be used for revealing the consumers daily habits, when he is at home and when he is outside from his home.

Contribution:

They dealt the above two problem and proposed their scheme. They divide the smart grid network into three layers i.e. Power Operator (Control Center), Substations, Smart meters and Smart appliances at consumers side. The smart appliances communicate with smart meter, the smart meter also communicate with substation and forward the real-time demand information to control center. The information sent by smart appliances can determine the electricity requirement for a certain time period by which the power generator, generate electricity to fulfill the requirements of appliances. The identity of the sender must be ensured by using authentication. For this purpose, their scheme focused substation to consumer subsystem only.

Their proposed PASS scheme uses Public Key Infrastructure (PKI) for signature generation and verification, the scheme is given below.

1. ***Preparation mode***: each smart appliance is attached with tamper-resistance device, which is responsible for generation of the pseudo identities and also signature of the message. The control center have public and private key Pub_{cc} and Pri_{cc} , ST_r represents substation at region R_r, SID_r is substation identity at region, now the control center generated initial system key s_r saves it to tamper-resistance device at R_r and also to ST_r for verification of signature and then store $< SID_r, s_r >$ to its local-database. The CC assign a real identity RID_i to each smart appliance A_i and load it to tamper-resistance device securely, Pub_i and Pri_i are the private and public keys of appliance A_i at that region. The control center stores $<RID_i, Pub_i>$ to its local-database.

2001

2. ***Pseudo identity generation module***: for electricity request from control center, the tamper-resistance device at A_i generates pseudo identity PID_i, $PID_i = ENC_{Pubcc} (RID_i|r)$, r is random nonce used in each session.
3. ***Signing module***: M_i represent request of electricity amount, A_i tamper-resistance device generate signature on message M_i as $\sigma_i = HMAC_{sr} (PID_i||ENC_{Pubcc} (M_i)||T_i)$, where T_i is time stamp of the tamper-resistance device clock and s_r is a region system key. Now A_i sends $< PID_i, ENC_{Pubcc}(M_i), T_i, \sigma_i >$ to CC by using smart meter and regional substation.
4. ***Verification module***: when the substation ST_r at region r receives message from A_i $< PID_i', ENC_{Pubcc}(M_i)', T_i', \sigma_i >$ can drop the message if T_i' is not valid, which reduce the impact of reply attack. After that, substation verify the signature by calculating $HMAC_{sr} (PID_i' ||ENC_{Pubcc} (M_i)' ||T_i')$. If it is not equal to the arrived one then drop the message and if valid then simply

forward it to control center.

5. ***Tracing module***: the control center firstly reveals the real identity RID_i of A_i which is based on pseudo-identity PID_i by decrypting the message on its private key Pri_{cc} and recovers r and updates the current supply rate of electricity to fulfill A_i requirement.

Claims:

Their scheme fulfill all the security requirements, because the message encryption is done by using CC public key and also pseudo-identities of smart appliances are used which are generated by tamper-resistance device and the requested message is delivered to control center in the original form.

Results:

They gave a simulation results in case of average delay VS smart appliances as shown in figure 2.5.

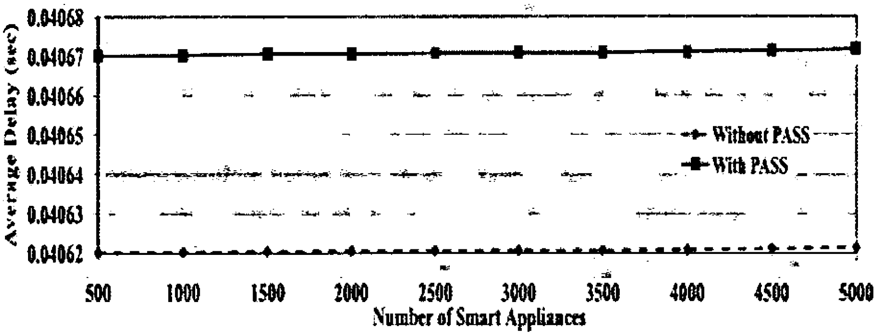


Figure 2.5: average delay vs. No's of smart appliances [30]

Limitation:

Their approach is based on PKI, which are not fast for smart grid environment, because the smart meters and smart appliances have limited resources and results in high communication and computation overhead [2]. They use tamper-resistance devices attached to smart appliances which generated signature but this will increase the cost of smart appliances, weather the consumers are willing to pay extra money for installing these devices to smart appliances is also an issue. Mutual authentication between subsystems and smart meters are not provided in this scheme.

- **P10 →** J. Choi, C. Li, J. Seo and I. Shin, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service", ACIS/JNU Conference on Computer networks.

(CNSI), pp. 331-333, May, 23-25, 2011, Daejeon, South Korea [31].

Motivation:

They stated the effect of non-repudiation and tempered-data attacks in smart grid while in billing phase.

Contribution:

They proposed their authentication scheme for addressing non-repudiation of smart meter data, which is used for billing purpose and to thwart tempered-data attack. For this purpose the smart meter release secrete key α_2 to AMI server and also AMI server releases secrete key β_2 to smart meter. Their proposed scheme is shown in figure 2.6 below.

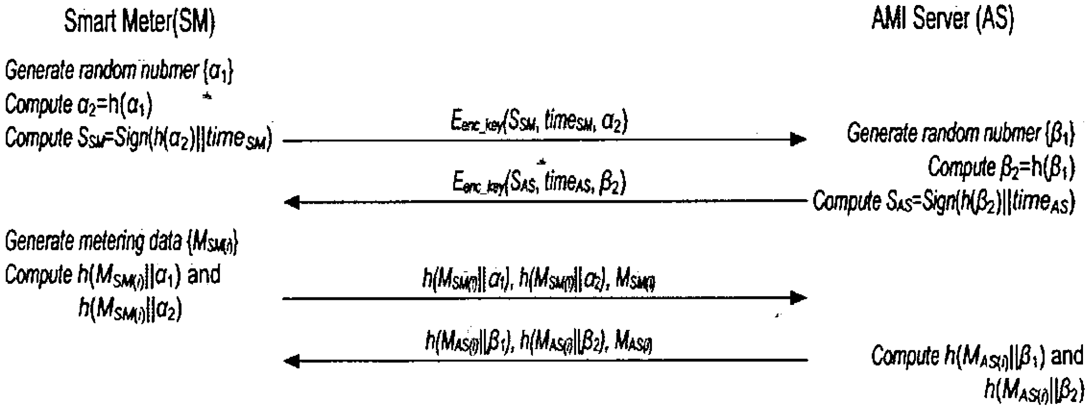

Smart Meter(SM)
AMI Server (AS)
Generate random nubmer {α_1}
Compute α_2=h(α_1)
Compute S_{SM}=Sign(h(α_2)||time$_{SM}$)
$E_{enc\_key}(S_{SM}, time_{SM}, \alpha_2)$
Generate random nubmer {β_1}
Compute β_2=h(β_1)
$E_{enc\_key}(S_{AS}, time_{AS}, \beta_2)$
Compute S_{AS}=Sign(h(β_2)||time$_{AS}$)
Generate metering data {$M_{SM(i)}$}
Compute h($M_{SM(i)}$||α_1) and h($M_{SM(i)}$||α_2)
$h(M_{SM(i)}||\alpha_1), h(M_{SM(i)}||\alpha_2), M_{SM(i)}$
$h(M_{AS(i)}||\beta_1), h(M_{AS(i)}||\beta_2), M_{AS(i)}$
Compute h($M_{AS(i)}$||β_1) and h($M_{AS(i)}$||β_2)

Figure 2.6: the proposed scheme message flow [31]

Figure 2.6 shows the procedure of monitoring the electricity usage and its transmission to AMI server.

They also given the case of non-repudiation where the smart meter denies on smart meter data $M_{SM(j)}$. The AMI Server search for α_2 and $M_{SM(j)}$ and $MAC1_{SM(j)}$, the smart meter sends α_1 to AMI Server, Now the AMI Server compute α_2 by taking hash on α_1 and then perform verification of $MAC1_{SM(j)}$ on metering data $M_{SM(j)}$. The smart meter can perform the same in case when AMI Server denies about the generated information.

Claims:

Their scheme provides non-repudiation, authentication of messages among smart meter and AMI Server. Their scheme reduces power consumption while exchanging metering data among AMI server and also reduces digital signature quantity for performing operations for non-repudiation.

Limitations:

The limitation of their scheme is that, they used a pre shared secrete key i.e. *enc_key*, which is not established for a certain session and will be used for the whole time, if this key is compromised by an attacker, which effect the performance of the overall system. This scheme only focused on non-repudiation problem.

- **P11 →** E. Ayday and S. Rajagopal, "Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks", IEEE Conf on Communications and Networking (CCNC), pp. 1161-1165, Jan, 9-12, 2011, Atlanta, GA, USA [32].

Motivation:

The author identified that, Home Area Network is a critical part of SG because the utility have no direct control on it. So due to that reason the attackers can easily exploit it by launching a *man-in-the-middle* and *impersonation* attacks. Which cause great impact on smart grid availability of electricity by shutting down all the appliances and cause blackout or overcharged the user in his/her electric bills.

Contribution:

They thwart *man-in-the-middle* attack and *impersonation* attack during authentication phase in their proposed scheme. The schemes are described below.

- ***Authentication between Smart Meter and Gateway***: they state that a compromise gateway cause a serious damage to a network by launching *man-in-the-middle* attack during authentication process between gateway and smart meter. Due to this attack the attacker send incorrect billing or control messages to gateway and cause blackout by shutting down all the appliances. The smart meter(SM) and gateway initiate the process by sending authentication and acknowledge message to one another. After that, both send authentication messages to trust center (Cloud/Utility), the authentication message contains their *ID's* and *IP* address of the trusted center. The cloud maps *ID* of SM (ID_M) and finds its location in his database and verifies its location by using *IPS* by submitting IP, now the cloud verify the location of SM by using ISP and submit IP_G and $Location_M$ to *IPS.* The *ISP* gives response in a true/false pattern. In case of true from *ISP* the cloud generate a pair-wise key $K_{G,M}$ between gateway and SM and send it to gateway $\{E_{KG,U}(K_{G,M},ID_M),MAC(K_{G,U},E_{KG,U}(K_{G,M},ID_M)),IP_G\}$, and this to SM $\{ E_{KM,U}(K_{G,M},ID_G), MAC(K_{M,U},E_{KM,U}(K_{G,M},ID_G)),IP_M\}$. After successful arrival of these messages to gateway and smart meter, they both decrypt the messages with the keys shared with the cloud and get a pair-wise key $K_{G,M}$.

This scheme requires 9 steps for performing the authentication between gateway and SM.

- ***Authentication between the Smart Appliances (SA's) and HAN***: in this scheme the SA can communicate with a Cloud by using gateway, which is more vulnerable to man-in-the middle attack. The detailed steps are shown in figure 2.7.

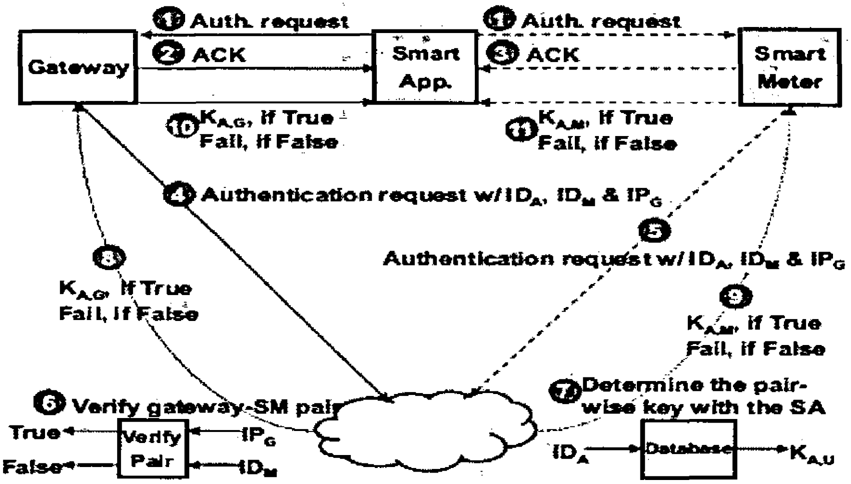

1 Auth. request
1 Auth. request
Gateway
2 ACK
Smart App.
3 ACK
Smart Meter
10 K_{A,G}, If True Fail, If False
11 K_{A,M}, If True Fail, If False
4 Authentication request w/ ID_A, ID_M & IP_G
5 Authentication request w/ ID_A, ID_M & IP_G
8 K_{A,G}, If True Fail, If False
9 K_{A,M}, If True Fail, If False
6 Verify gateway-SM pair
True
False
Verify Pair
IP_G
ID_M
7 Determine the pair-wise key with the SA
ID_A
Database
K_{A,U}

Figure 2.7: Authentication mechanism between SA and HAN [32]

The cloud then send $\{E_{KG,U}\ (E_{KA,U}\ (K_{A,G},ID_G),MAC(K_{A,U},E_{KA,U}(K_{A,G},ID_G)),K_{A,G}),MAC(K_{G,U},E_{KG,U}(E_{KA,U}(K_{A,G},ID_G),MAC(K_{A,U},E_{KA,U}(K_{A,G},ID_G)),K_{A,G})),IP_G\}$ to a gateway.

It then send message $\{E_{KM,U}\ (E_{KA,U}\ (K_{A,M},ID_M),MAC(K_{A,U},E_{KA,U}(K_{A,M},ID_M)),K_{A,M}),MAC(K_{M,U}, E_{KM,U}(E_{KA,U}(K_{A,M},ID_M),MAC(K_{A,G},E_{KA,U}(K_{A,M},ID_M)),K_{A,M})),ID_M\}$ to SM.

The gateway send the messages $\{E_{KA,U}\ (K_{A,G},ID_G),MAC(K_{A,U},E_{KA,U}(K_{A,G},ID_G)),ID_A,\ ID_G\}$ to SA, and SM send message $\{E_{KA,U}\ (K_{A,M},ID_M),MAC(K_{A,U},E_{KA,U}(K_{A,M},ID_M)),\ ID_A,ID_M\}$to SA. The SA then verifies the integrity of these messages from gateway and SM and authenticates them.

This scheme requires 11 steps for performing the authentication between SA an SM in HAN.

- ***Authentication between the transit devices (TD's) and HAN***: they assumed that TD can communicate with its own home gateway. The detailed authentication steps are described below. TD sends $\{Auth_Req, ID_{T}, ID^{T}_{M}, M\}$to visiting gateway and also to visiting SM and initiate authentication process. Here $M=\{E_{K_{T,U}}(ID_T, Seq.No), MAC(K_{T,G}, E_{K_{T,G}}(ID_T,\ Seq.No))\}$. If TD is authenticated by another SM in HAN, then the user can manually enter to visiting gateway and duration of authentication through UI (User interface). The cloud map the *ID* of TD (ID_T) to a pair-wise key $K_{T,U}$ between TD and cloud and then forward the message $\{E_{K_{HG,U}}(M), MAC(K_{HG,U}, E_{K_{HG,U}}(M))\}$ to the home gateway of the TD to thwart impersonate attack. The cloud send messages to home gateway and the home gateway send it to TD, the message is $\{E_{K_{T,U}}(K_{T,G}, ID_G), MAC(K_{T,U}, E_{K_{T,U}}(K_{T,G}, ID_G)), ID_{T}, ID_G\}$.

The cloud then send it to visiting SM and it then forwards it to TD. The message is $\{E_{K_{T,U}}(K_{T,M}, ID_M), MAC(K_{T,U}, E_{K_{T,U}}(K_{T,M}, ID_M)), ID_{T}, ID_M\}$.

This scheme is resilient against to *impersonation* attack and this scheme requires 14 steps for providing authentication between TD and HAN.

Limitations:

For achieving authentication the proposed schemes require many steps, which results to high communication cost and latency. These schemes only consider HAN and do not consider other elements of SG i.e. Building Area Network etc. These schemes do not consider smart meter to smart meter authentications i.e. mutual authentication.

- **P12 →** M. Kgwadi and T. Kunz, "Security RDS Broadcast Messages for Smart Grid Applications", in proc.6th int. wireless commun. Mobile comput. Cont., France, Jun, 2010 [11].

Motivation:

They identified the problems in the Demand Responds (DR) facility, which is provided in RDS (Radio Data System) network. RDS is a one-way broadcast wireless technology. They also states that, wireless nature of RDS is more vulnerable to security risks like the attacker can easily compromise the overall system performance by using a compromised wireless transmitter and can produce fake messages or canceling some price events in network.

Suggestion:

They dealt the above problem by suggesting that, the receiver must authenticate the messages i.e. they performed source authentication.

Contribution:

They proposed and compared three methods for performing source authentication named as "Bins and Balls (BiBa)", "Hash to Obtain Random Subsets Extension (HORSE)" and "Elliptic Curve Digital Signature Algorithm (ECDSA)", which are discussed below.

1. ***BiBa Signature Protocol***: they proposed two instances of the conventional BiBa protocol i.e. long-term BiBa instances are used for signing short-term BiBa instance public keys and short-term BiBa instances sign application messages. The sender generates long-term BiBa instances and uses it as a public key. The generation process is given below.
   Sender divide time to equal duration and generate t chains of *SElf* Authenticating values (*SEALs*) like $S_{<1,i>},..,S_{<t,i>}$ and *Salt* chain. For signing message m at i time interval the sender perform hash on m, $h=H\ (m/c)$, c is counter and h is a generated signature. The sender then use hash function $G_h()$ and input *t-SEALs* to it and observe k-way collisions, i.e. $S_{<1,i>} \neq S_{<2,i>}, \ldots, S_{<t,i>}$ such that $G_h\ (S_{<1,i>}) = \ldots. = G_h\ (S_{<t,i>})$. And then send *k-SEALs* together with message m to receiver, $(<S_1, \ldots, S_k> \mathrm{l} m)$. The receiver authenticates the received message if $G_h\ (S_1) = \ldots.. = G_h\ (S_k)$ for all $S_1 \neq \ldots \ldots \neq S_k$.
2. ***HORSE Authentication Protocol***: they proposed the two instances of HORSE like BiBa approach. The initial public key of a new short-term HORSE instance is send by using the long-term HORSE instance, when previous one expires. The sender maps a message m to k-elements of t-element subset T by using Collision-resistance Hash H. for $m_1, \ldots, m_r$ it is infeasible to get $H\ (m_r) \subseteq U^{r-1}{}_{i=1}\ H(m_i)$. The sender generate secrete key $SK = (s_1, \ldots, s_t)$ and public key $PK = (v_1, \ldots, v_t)$ of random t values with $v_i = f(s_i)$, $1 \leq i < t$. the generated signature is subset of $SK = (s_{j,1}, \ldots, s_{j,k})$ and send it to receiver with message m. The receiver simply verify the signature $(\acute{s}_1, \ldots., \acute{s}_k)$ and compute $h = H(m)$ and verifies $v_i = f(\acute{s}_i)$, if same like the received one then verifies it otherwise reject it. This approach repeatedly make use of hash function on t random values $s_{<0,1>}, \ldots, s_{<0,t>}$ for generation of chains of d length. The keys are used in reverse order of generation and the initial secrete key $SK_0 = (s_{<d-1,1>}, \ldots., s_{<d-1,t>}) = (s_1, \ldots, s_t)$, such that $s_{<i,j>} = H^i(s_{<0,j>})$, and the initial public key $PK_0 = (v_1, \ldots, v_t)$i.e. $v_i = f(s_i)$ for all $s_i \in SK_0$.
3. ***Elliptic Curve Signature***: Both sender and receiver agreed on common base point P over finite field F_P. x is sender private key and $Q = xP$ sender public key, where a, b, P, q, F_P are known to

receiver. The sender generate random number $k \in [1, n\text{-}1]$ and compute $kP=(x_1,y_1)$, it then convert x_1 to $\bar{x}_1$. It now compute $r=\bar{x}_1$ mod n and repeat the same until $r\neq 0$. The sender now computes k^{-1}mod n and then computes $SHA\text{-}1(m)$ and converts the output to integer e. It then computes $s=k^{-1}(e+dr)$ mod n. and send (r,s) to receiver, which is a signature. The receiver verifies the signature $r,s \in [1,n\text{-}1]$ and compute $SHA\text{-}1(m)$ and convert the output to integer e. it then compute $w= s^{-1}$mod n, after that compute $u_1= ew$ mod n and $u_2= rw$ mod n. The receiver also calculate $X = u_1P+u_2Q$. The x coordinate of X is converted to integer $\bar{x}_1$ and v is computed as $v=\bar{x}_1$ mod n. The receiver then accept signature when $v=r$.

Results:

They provided a simulation result in which they observed that ECDSA offer high security than BiBa and HORSE with increased computation cost on the receiver side with high communication overhead given in table 2.2.

Table 2.2: comparing BiBa and HORSE with t=512, k=4 and ECDSA used SHA-1 [11]

Security scheme	Overhead	95% service availability (KM)	security level	computational effort (at receiver)
ECDSA	133.33%	120	2^{-80}	High
HORSE	41.32%	130	2^{-35}	Low
BiBa	30.08%	120	2^{-35}	Low

Limitation:

These approaches are designed for one-way communication and for that reason they only provide source authentication and do not provide mutual authentication [2].

- **P13 →** M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu and X. Shen, "A Lightweight Message Authention Scheme for Smart Grid Operations", IEEE Transactions on Smart Grid, vol. 2, no.4,PP. 675- 685, ISSN: 1949-3053 Dec 2011 [2].

Motivation:

The authors discussed the problems faced in Smart Grid implementation, as smart grid allow two-way communication between consumers and control center, by which the consumers can actively participate for the adjustment of their current power usage. They also stated that, IP-based networking technologies are used for setting up this environment, but they are challenged by larger volume of delay-sensitive data and vulnerable to many security threats like replay, denial of service, traffic analysis attacks etc. They also described that, the smart meters have also a privacy concern. They also stated the importance of lightweight operations in SG.

Contribution:

For these problems their proposed scheme provides mutual authentication among smart meters resides at different locations in a hierarchal network. Their proposed scheme achieved a secure channel for late transmission. The mutual authentication is done on Diffie-Hellman key establishment protocol while authentication of message is done by using key based HMAC technique. The proposed scheme is shown in figure 2.8 below.

$$\begin{array}{lcr} \text{HAN GW } i & & \text{BAN GW } j \\ a \in \mathbb{Z}_q^*, g^a \in \mathbb{G} & \xrightarrow{\{i||j||g^a\}_{\{encr\}Pub_{BAN\_GWj}}} & \\ & \xleftarrow{\{i||j||g^a||g^b\}_{\{encr\}Pub_{HAN\_GWi}}} & b \in \mathbb{Z}_q^*, g^b \in \mathbb{G} \\ K_i \leftarrow H(i||j||(g^b)^a) & \xrightarrow{g^b} & K_i \leftarrow H(i||j||(g^a)^b) \\ & \xrightarrow{\{M_i||T_i||HMAC_{K_i}\}_{\{encr\}K_i}} & \end{array}$$

Figure 2.8: proposed lightweight message authentication scheme [2]

HAN GW i chose a random number *a*, and calculate g^a and encrypt g^a by using the RSA algorithm and public key of *BAN GW j* and send it to *BAN GW j*. The *BAN GW j* then select a random number *b* and calculate g^b and decrypt the packet by using its private key and store g^a and then encrypt the message $(i|j|g^a|g^b)$ by using the public key of *HAN GW i* by using RSA algorithm and send it *HAN GW i*. The *HAN GW i* decrypt the message by using its private key and compared the received g^a to its calculated one, if they both are same then *BAN GW j* is authenticated *by HAN GW i*. The *HAN GW i* stores g^b and also send g^b to *BAN GW j* in a plain text. After getting g^b, it authenticate *HAN GW i*. they calculate session key K_i by taking Hash on message $(i|j|(g^b)^a)$ in *HAN GW i* and Hash on $(i|j|(g^a)^b)$ in *BAN GW j*. The *HAN GW i* then calculate Hash-based Message Authentication Code

(HMAC) of message M_i by using session key K_i and concatenate it to M_i and recorded time instance T_i and encrypt the whole by using AES algorithm and shared session key K_i and send it to *BAN GW j*. here T_i is used to thwart reply attack and $HMAC_{Ki}$ is used for message integrity. The BAN GW j then decrypt the message by using AES algorithm and key K_i and authenticated the *HAN GW i* and send the authenticated message to CC of the *NAN GW*.

Claims:

They claimed that, their approach did not results to high latency and few signal messages are exchanged in key generation phase. They also claimed that their scheme provide mutual authentication, forward secrecy and provide a secure channel for late transmission by using secrete session key K_i.

Results:

They also give the simulation result in which they compare their approach to ECDSA and get good result in number of HANs per BAN given bellow in figures 2.9, 2.10.

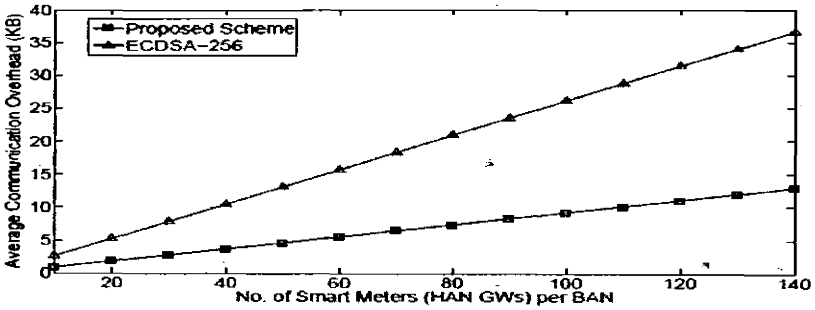


Figure 2.9: Average communication overhead on BAN [2]

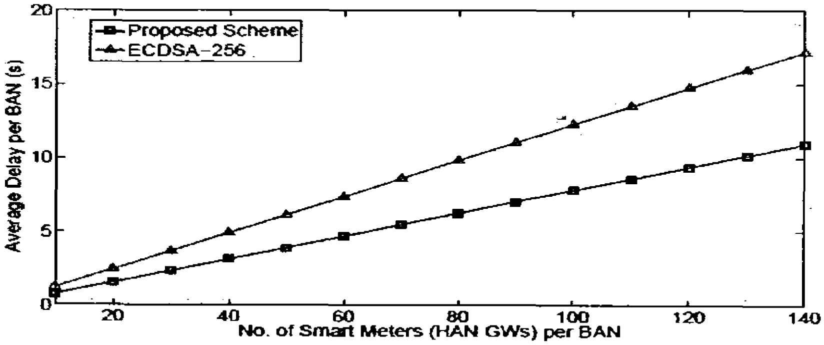


Figure 2.10: Average delay at BAN [2]

Limitations:

For session key establishments all the encryption and decryption is done by using RSA algorithm, which require high computational cost as compared to symmetric one (i.e. AES), also the communication overhead is high because huge size of bytes are traveling between both HAN and BAN.

- **P14 →** R. Sule, R.S. Katti and R.G. Kavasseri, "A Variable Length fast message authentication code for secure communication in smart grids", IEEE Conf. on Power and Energy society, pp. 1-6, Jul, 22-26, 2012, Fargo, ND [33].

Motivation:

The author in this paper identified the problems in HMAC$_{Ki}$ scheme, and said that the HMAC$_{Ki}$ is slow and required high computation cost and verification time. This will affect the overall performance of the smart grid operations.

Contribution:

For addressing these problems, they proposed a variable length message authentication code, which used multiple inputs shift registers (MISR) for compressing the message for authentication. They also used pseudorandom function AES-128 which took compressed message as an input and generate tag as a MAC code. Their scheme is shown in figure 2.11.

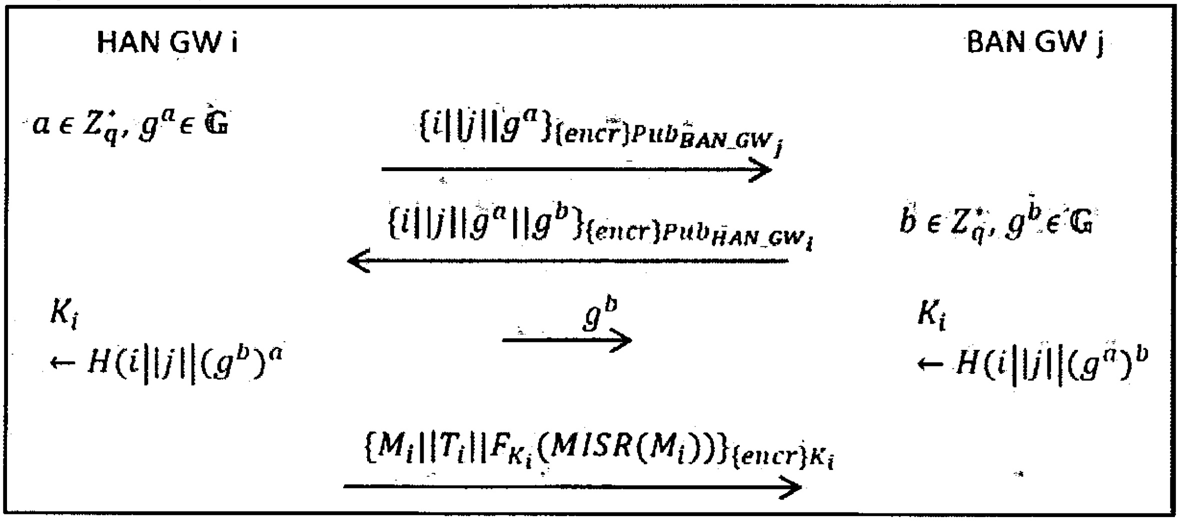

HAN GW i
BAN GW j
$a \in Z_q^*, g^a \in \mathbb{G}$
$\{i||j||g^a\}_{\{encr\}Pub_{BAN\_GW_j}}$
$\{i||j||g^a||g^b\}_{\{encr\}Pub_{HAN\_GW_i}}$
$b \in Z_q^*, g^b \in \mathbb{G}$
$K_i \leftarrow H(i||j||(g^b)^a$
g^b
$K_i \leftarrow H(i||j||(g^a)^b$
$\{M_i||T_i||F_{K_i}(MISR(M_i))\}_{\{encr\}K_i}$

Figure 2.11: their proposed authentication scheme [33]

For a message M of length d check d mod (L) = 0, where L=1024. If it is not then simply pad $[d/(L)]L\text{-}d\text{-}log_2d$ bits of zero and append to M, which becomes $M^{P}=[M\|0^{-}\|(d)_{b}]$ and M^{P} is parsed to $L/8= l = 128$ blocks of size $s = [M^{P}]/l$, and then input to *MISR*. The tag of l messages is computed by $F_k(R)$, where R is reminder. Where $F_k(R)$ is a pseudorandom function, where F: $\{0, 1\}n\times\{0, 1\}n \rightarrow \{0, 1\}n$ is length preserving, efficient and keyed function, for each distinguisher D it have a negligible function *negl(.)* such that, $[(Pr[D^{(Fk(.))}(n)] = 1\text{-}(Pr[D^{f\,(.)}(n)] =1)| \leq negl(n)$. They used Block Cipher AES-128 as a pseudorandom function.

The construction of $\Pi(Gen, Mac, Vrfy)$ is given bellow.

i. ***Gen:*** on n input, K_i is obtained, and secrete irreducible $g(x)$ on $GF(2)$ of m degree is also obtained. Here $n=l$ which is kept fixed. They select $g(x)$ only once and calculate the key which is $(K_i,g(x))$.
ii. ***Mac:*** on the input $k=K_i$ a message M is checked and pad with 0 bits, then parse M_p into l blocks having length s like $M_p=\{m_1,...,m_n\}$. They input m_i's to *MISR* for calculating tag $t= F_k(R)$.
iii. ***Vrfy:*** it will then output 1 if $t=F_k(MISR(M))$.

Claims:

The authors claimed that their proposed MAC is faster than HMAC$_{Ki}$ in terms of low computation cost, authentication and verification delays and also accommodates large volume of messages for MAC generation.

Results:

They also give a simulation results in which they compare their proposed MAC to HMAC, shown below in figures 2.12.

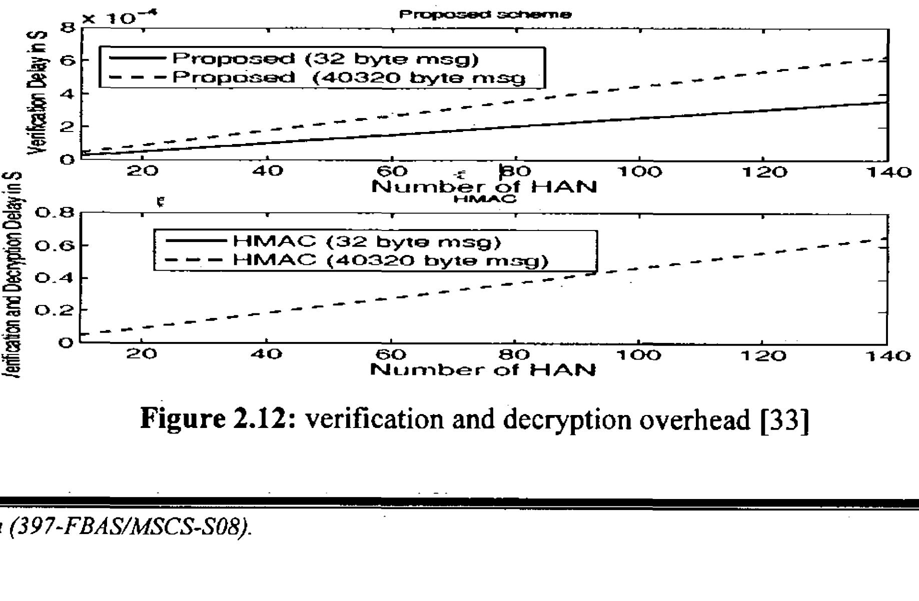


Figure 2.12: verification and decryption overhead [33]

Limitation:

For session key establishment they used the same approach as used in [2].

2.3. Problem Statement

The existing authentication schemes being used in smart grid are based on PKI, which have high computational, communication overhead and latency [2].

The authors in [34] stated that, Smart Grid communications depends on 1) Communication latency, 2) large volume of messages. They suggest that, the authentication techniques must be designed in a way that, they did not produce large volume of messages and having less communication overhead with less latency.

The existing techniques make use of PKI based signature, these signature generation and verification require high computation cost and the communication overhead is high for this signature generation and also for their verification [2].

Previous techniques of fouda [2] and sule [33] have a communication overhead of 1024 bytes and 234 milli seconds of computation overhead in handshaking. The total time (latency) taken for authentication in fouda is 260 milli seconds.

PKI-based scheme required high computation cost, communication overhead which also resulted to high latency, for that reason they did not seems too fast for SG constrained environment [10].

Some authentication schemes requires too much steps for achieving authentication, which also resulted to high communication overhead and high latency. The authentication schemes must be designed in a manner such that it will achieve authentication in few signal message [2][8][10]. The asymmetric algorithms were proved to be computationally slower than symmetric ones [35].

Chapter 3

Proposed Authentication Scheme

3.1. Two way communication flow

The on demand request of the consumer of Home Area Network (HAN-1) is fulfilled in the following manner as given in figure 3.1.

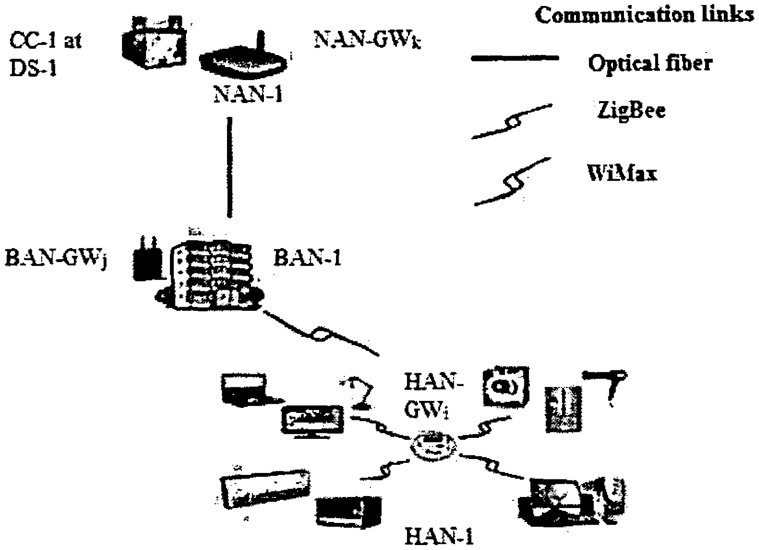


Figure 3.1: Two-way communication between consumers and Control center

During peak hours the consumer at HAN-1 wants to adjust its electric power usage, so the HAN-GW$_i$ at HAN-1 can send the request to power provider and the power provider take appropriate actions and adjust the electric power of HAN-1 in a corresponding Neighborhood, the steps are given below.

- The HAN-GW$_i$ first send authentication request to BAN-GW$_j$ at BAN-1 as shown in figure 3.1. They both can authenticate one another and generate a secret session key K$_i$.
- After successful authentication the HAN-GW$_i$ at HAN-1 can generate HMAC$_{Ki}$ of the message and concatenate it to the message and recorded time instance and encrypt the whole by using a secrete session key and send it to BAN-GW$_j$ at BAN-1.
- The BAN-GW$_j$ then decrypts the message and verifies the integrity of the message and authenticity of sender and forwards the authentic message to NAN-GW$_k$ at NAN-1.
- The CC-1 of the NAN-GW$_k$ of NAN-1 will then take appropriate action and adjust the electric power to HAN-1 of the corresponding BAN-1 of the NAN-1.

In above figure 3.1, the HAN-GW$_i$ of HAN-1 and BAN-GW$_j$ of BAN-1 are connected to one another by using WiMax technology whereas the BAN-GW$_j$ of BAN-1 and NAN-GW$_k$ of NAN-1 are connected by using optical fiber, because optical fiber are best for long distance communication and have a least possible communication delay. The on-demand request travel from bottom to up and the response travels from up to bottom.

The author in [3] suggested that, the control center is connected to 10,000 feeders (i.e. BAN-GWs) and 100,000 servers (i.e. HAN-GWs). In hot summer these servers generate one message per seconds so the total messages are 100,000 and the feeders also send messages to control center and also to one another, so the required transmission bandwidth with 100bye of packet is 800Mbps.

So for that reason authors in [2] suggested that, the operation must be light weight for avoiding possible communication delay and also reducing the computation overhead by cutting unnecessary signal messages.

The proposed scheme provide all the functionalities provided in [2], by having low computation cost. The proposed scheme makes use of the variants of Diffie-Hellman algorithm with both asymmetric Algorithm (RSA) and symmetric algorithm (AES) for the generation of secret shared session key. This hybrid approach can efficiently produce the secrete session key with few signal messages and does not contribute to high computation cost, high communication overhead and latency between smart meters residing at different location of hierarchal network. This secret session key provide a secure communication channel for late transmission between smart meters, through which authenticity of the sender and integrity of the message is verified.

The proposed scheme is a lightweight scheme which leads towards low computation cost, minimum latency and authenticate the smart meters in a fastest way, which also improves the scalability in SG environment as computation is fast so more HAN-GWs can be processed.

3.2. Proposed scheme

The author in [34] stated that, SG communication is strongly depended on these two requirements 1) communication latency and 2) large volume of messages. So the authentication techniques do not produce large volume of messages and also the communication overhead will be less. As the CC take decisions on consumers on-demand requests so the messages generated from consumers of HAN will not be modifies and deliver in its original form for the correct decisions of CC, because incorrect or modified messages will affect the overall system performance and will cause blackouts. For keeping these considerations in mind, we propose an Enhance Light Weight Message authentication Scheme for SG Communications in Power Sector. The proposed scheme achieves all the goals which are achieved in [2] but in a more light weight manner i.e. low computation cost and communication overhead. The table 3.1 shows the list of abbreviations used in the scheme.

Table 3.1: List of abbreviations used in the proposed scheme

Abbreviation	Description
HAN-GW$_i$	The gateway of the Smart meter on Home Area Network 1.
BAN-GW$_j$	The gateway of the Smart meter on Building Area Network 1.
i and j	Id's of HAN-GW$_i$ and BAN-GW$_j$
priBAN-GWj	Private key of BAN-GW j.
PubBAN-GWj	Public key of BAN-GW j.
E	Encryption algorithm.
D	Decryption algorithm.
H	Cryptographic Secure Hash function.
HMAC$_{Ki}$	Key based Hash Message authentication code of the message M$_i$.
T$_i$	Recorded time on HAN-GW i.
M$_i$	The on-demand message of the smart appliances power requirement of HAN-GW i.
NAN-GW$_k$	The gateway of the Smart meter on Neighborhood Area Network 1.

3.2.1. Detailed Description of the Proposed Scheme

The public key of BAN-GW$_j$ is stored in Corresponding HAN-GW's, whereas the private key of BAN-GW$_j$ is stored in BAN-GW$_j$.

The variant of the Diffie-Hellman protocol [36] is used for initial handshake, which is a hybrid approach by using both symmetric (AES) and asymmetric (RSA) algorithms for session key generation. The proposed scheme is shown below in figure 3.2.

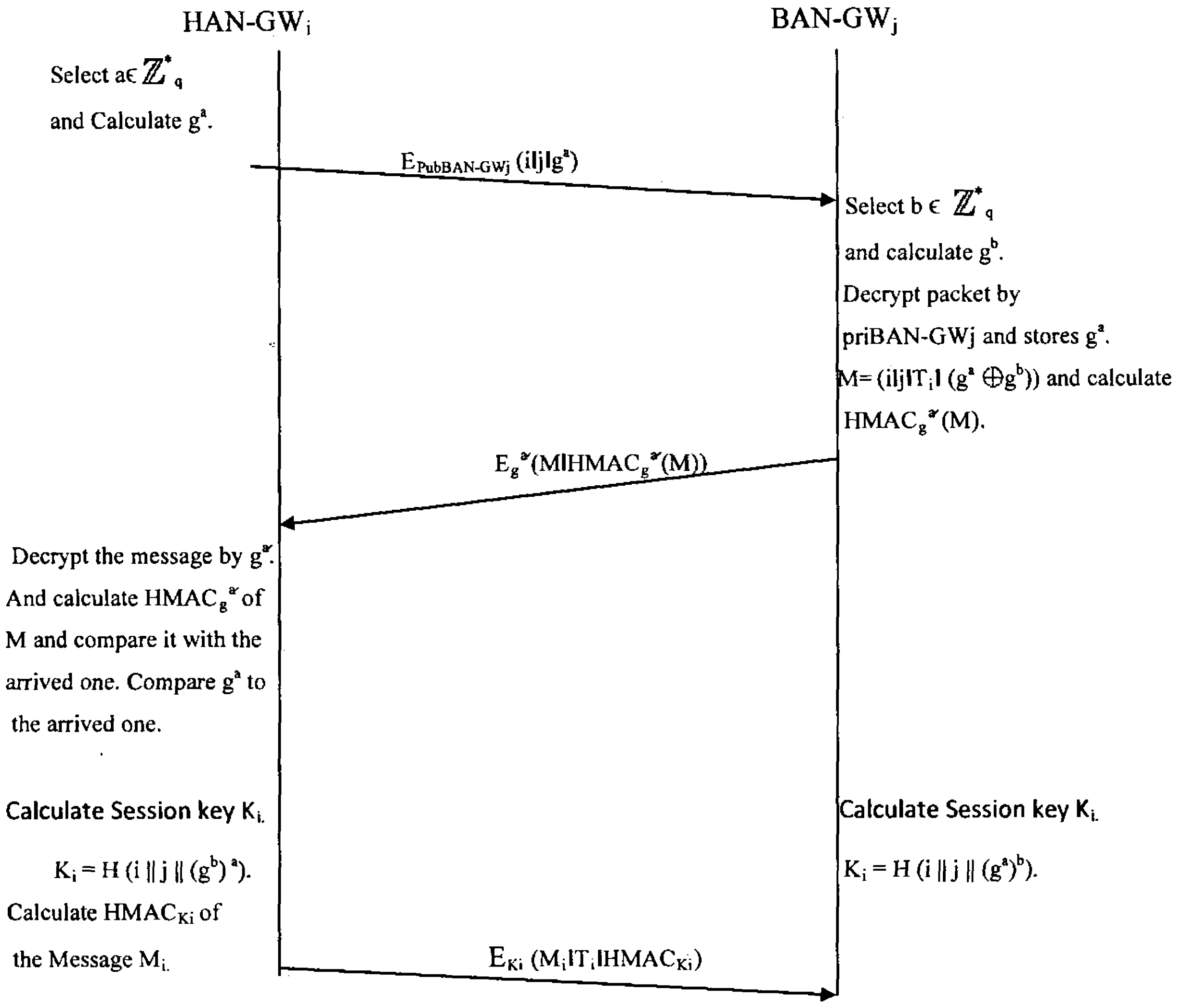

HAN-GW$_i$
BAN-GW$_j$
Select a$\in \mathbb{Z}^*_q$
and Calculate g^a.
E$_{PubBAN-GWj}$ (i|j|g^a)
Select b $\in$ $\mathbb{Z}^*_q$
and calculate g^b.
Decrypt packet by
priBAN-GWj and stores g^a.
M= (i|j|T$_i$| (g^a $\oplus$g^b)) and calculate
HMAC$_g$^{ar}(M).
E$_g$^{ar}(M|HMAC$_g$^{ar}(M))
Decrypt the message by g^{ar}.
And calculate HMAC$_g$^{ar}of
M and compare it with the
arrived one. Compare g^a to
the arrived one.
Calculate Session key K$_i$.
K$_i$ = H (i || j || (g^b) ^{a}).
Calculate HMAC$_{Ki}$ of
the Message M$_i$.
Calculate Session key K$_i$.
K$_i$ = H (i || j || (g^a)^b).
E$_{Ki}$ (M$_i$|T$_i$|HMAC$_{Ki}$)

Figure 3.2: the proposed authentication scheme

Let $\mathbb{G}$ = <g> is a group on large prime order on q, which satisfies computational Diffie-Hellman (*CDH*) assumption i.e. if both g^a and g^b are given to an adversary and he does not know a,b$\in\mathbb{Z}^*_q$, it is computationally hard for adversary to calculate $g^{ab} \in \mathbb{G}$. The authentication starts when the consumer wants to adjust his electric power usage by sending the on-demand power list to Control Center for electric current.

The detailed steps of the proposed scheme for session key establishment are discussed below.

Step 1: the HAN-GW$_i$ of the consumer select a random number a $\in \mathbb{Z}^*_q$, which is selected from a positive integer on large prime order q. The HAN-GW$_i$ then calculates g^a, which is 1024 bits of length and it stores g^a to its memory. The HAN-GW$_i$ then concatenates i, j and g^a and encrypt the whole concatenated packet by using public key of BAN-GW$_j$ through RSA algorithm. It sends the encrypted packet to BAN-GW$_j$. the size of the packet is 384 bytes.

HAN-GW$_i$ $\longrightarrow$ BAN-GW$_j$: $E_{PubBAN\text{-}GWj}$ (i || j || g^a).

As shown in figure 3.3.

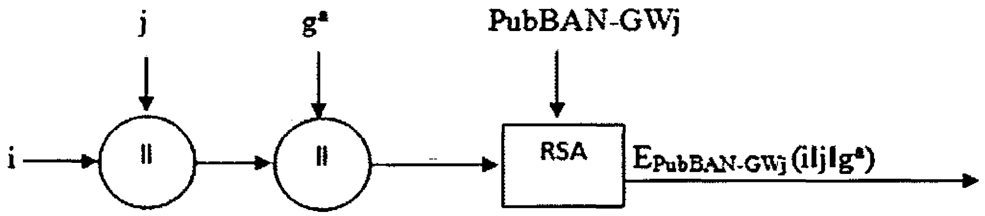


Figure 3.3: Operations performed on HAN-GW$_i$

Step 2: when the BAN-GW$_j$ receives the encrypted packet, it simply decrypts the packet by using its private key priBAN-GWj on RSA algorithm i.e. $D_{priBAN\text{-}GWj}$ (i I j I g^a) and then store g^a. now the BAN-GW$_j$ select the rightmost 128 bits of g^a as an encryption key (i.e.$g^{a'}$), which is used as a key for Encryption on AES and also for generation of HMAC.

The BAN-GW$_j$ then select a random number b $\in \mathbb{Z}^*_q$ and calculate g^b. It then takes the XOR of g^a and g^b and then concatenates i, j, T$_i$ to the XOR of g^a and g^b i.e. M = i I j I T$_i$ I ($g^a \oplus g^b$). Here T$_i$ is a recorded time instance. The BAN-GW$_j$ then calculates the HMAC on M by using $g^{a'}$as a key and then concatenates it to M and encrypts the whole packet by using AES on $g^{a'}$ and sends it to HAN-GW$_i$.

BAN-GW$_j$ $\xrightarrow{\hspace{2cm}}$ HAN-GW$_i$: $E_{g}^{a'}(M \mathbf{I} HMAC_{g}^{a'}(M))$.

As shown in figure 3.4 below.

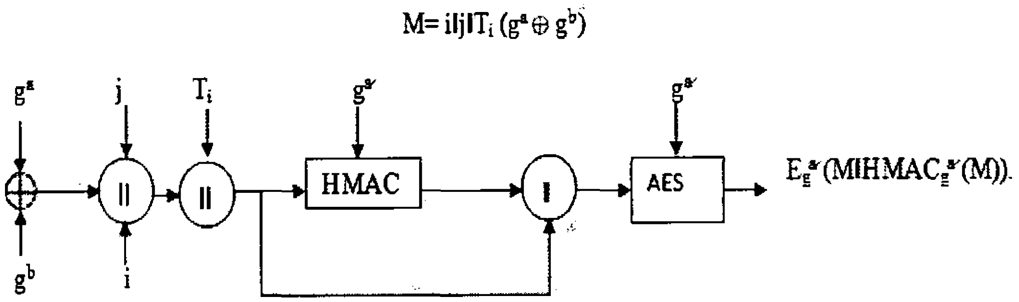

M= iljlT$_i$ ($g^a \oplus g^b$)
g^a
j
T$_i$
$g^{a'}$
$g^{a'}$
||
||
HMAC
I
AES
$E_g^{a'}$(MIHMAC$_g^{a'}$(M)).
g^b
i

Figure 3.4: Operations performed on BAN-GW$_j$

In this step 156 bytes of data travel from BAN-GW$_j$ to HAN-GW$_i$. In this step the HAN-GW$_i$ is authenticated by BAN-GW$_j$ because, HAN-GW$_i$ is the only one having g^a and take g^b by taking XOR to received (g^a XOR g^b), so only a HAN-GW$_i$ with correct g^a can recover g^b.

Step 3: When the HAN-GW$_i$ receives the encrypted packet from BAN-GW$_j$, it simply decrypt the message by using AES algorithm and key $g^{a'}$(taking rightmost 128 bits of g^a as a key) i.e. $D_g^{a'}(M \mathbf{I} HMAC_g^{a'}(M))$. The HAN-GW$_i$ first calculate the $HMAC_g^{a'}(M)$ and compare it with the arrived one, it then take XOR with g^a and recover g^b and also recover g^a and compare g^a to its stored one. If they are equal then they authenticate one another. The HAN-GW$_i$ then calculate the session key by computing $(g^b)^a$ and concatenate it to i and j after this HAN-GW$_i$ take a cryptographic secure hash on the concatenated packet, which compute a secure session key K$_i$ for late successive transmission.

$K_i = H(i \| j \| (g^b)^a)$. Here $H: \{0, 1\}^* \xrightarrow{\hspace{1cm}} \mathbb{Z}^*_q$, is a cryptographic secure hash function.

As shown in figure 3.5 below.

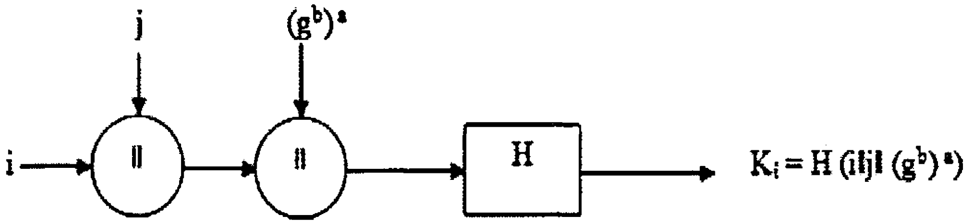


Figure 3.5: Session key generation on HAN-GW$_i$

The BAN-GW$_j$ also compute $(g^a)^b$ and concatenate it to i and j and then take a cryptographic secure hash H on the concatenated packet, which generate the session key K$_i$. Both the generated session keys are same as achieved in Diffie-Hellman key establishment protocol. The generation of session key by BAN-GW$_j$ is given bellow.

$K_i = H(i \,||\, j \,||\, (g^a)^b)$. Here $H: \{0, 1\}^* \longrightarrow \mathbb{Z}^*_q$, is a cryptographic Secure hash function.

As shown in figure 3.6.

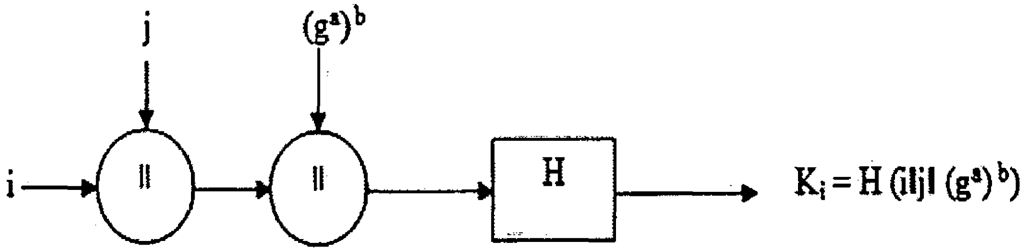


Figure 3.6: Session key generation on BAN-GW$_j$

3.2.1.1. Message transmission

The session key K$_i$ provides a secure channel for late transmission between HAN-GW$_i$ and BAN-GW$_j$. To ensure message integrity the HAN-GW$_i$ simply generate message authentication code by using Hash-based Message authentication code (HMAC) algorithm by using session key K$_i$. The on-demand request message M$_i$ which contains the electricity requirements of the smart appliances for certain period of time is passed from HMAC$_{Ki}$, which generate message authentication code of the message M$_i$. The HAN-GW$_i$ then concatenate M$_i$, T$_i$ and HMAC$_{Ki}$ and then encrypt the whole packet by using AES algorithm and secret session key K$_i$. The HAN-GW$_i$ then sends the encrypted packet to BAN-GW$_j$. Here T$_i$ is the recorded time instance and it is used for thwarting possible reply attack. The HAN-GW$_i$ sends the encrypted packet to BAN-GW$_j$.

$\text{HAN-GW}_i \longrightarrow \text{BAN-GW}_j$: $E_{Ki}(M_i \,||\, T_i \,||\, HMAC_{Ki})$.

As shown in figure 3.7 on next page.

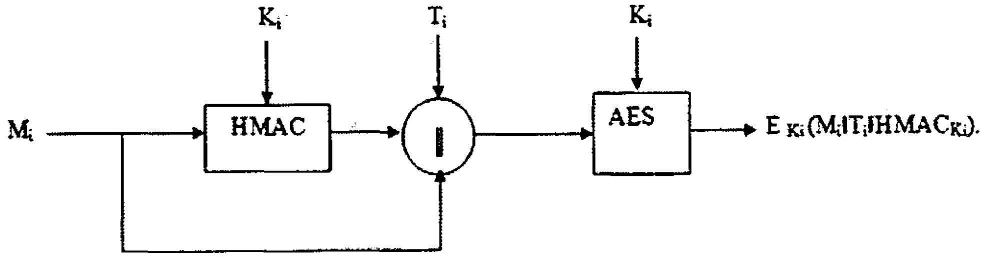


Figure 3.7: HMAC generation and encryption of concatenated packet on HAN-GW$_i$

When BAN-GW$_j$ receives the encrypted packet form HAN-GW$_i$, it first decrypt it by using session key K$_i$ (i.e. D_{Ki} (M_i | T_i | $HMAC_{Ki}$)). The BAN-GW$_j$ verifies the authenticity of the HAN-GW$_i$, because K$_i$ is shared only between them and also verifies the integrity of the message by calculating HMAC$_{Ki}$ of the message. After this the BAN-GW$_j$ simply forwards the authenticated messages to NAN-GW$_k$.

3.3. Security Analysis of the Proposed Authentication scheme

The proposed scheme provides.

1. **Mutual authentication is provided by proposed scheme:**

   As in step 1 g^a is encrypted by using public key of the BAN-GW$_j$ and recovered only by BAN-GW$_j$ private key. When the BAN-GW$_j$ recovers g^a, it simply computes g^b and take XOR with g^a, with this BAN-GW$_j$ simply authenticate the HAN-GW$_i$ at step 2. At step 3 HAN-GW$_i$ recover the encrypted packet by using $g^{a'}$ as key and compare the received g^a to the stored one, if they both are same then HAN-GW$_i$ also authenticated a BAN-GW$_j$. So they both get mutual authentication in step 3 and the proposed scheme provide mutual authentication.

2. **The proposed scheme thwart man-in-middle and reply attack in secrete key generation phase:**

   In step 1 HAN-GW$_i$ encrypt g^a by using BAN-GW$_j$ public key, so the private key of BAN-GW$_j$ is only known to BAN-GW$_j$ and he is the only one to decrypt the encrypted message by using RSA algorithm and its private key in step 2 and attacker cannot get g^a. In step 2 as g^a and also $g^{a'}$ are only known to BAN-GW$_j$, which then use $g^{a'}$ as a key for AES algorithm and it then encrypt the concatenated packet by using $g^{a'}$ and send it to HAN-GW$_i$ in step 2. The HAN-GW$_i$ in step 3 decrypts the encrypted message, because $g^{a'}$ is stored in his memory, and only he is able to decrypt the

message. So the proposed scheme thwarts a man-in-the-middle attack and also a reply attack by using T_i.

3. **The proposed scheme also provide forward secrecy:**

   As the semantic-secure shared key holds *CDH* assumption and it is hard for attacker by using chosen-plaintext attack to calculate the actual key and also to achieve mutual authentication when either HAN-GW_i or BAN-GW_j is compromised. Security of the previous session keys is not affected by the private key of BAN-GW_j, because HAN-GW_i didn't use private and public keys. So the shared session key provide perfect forward secrecy for late transmission.

4. **The propose scheme also provide secure and authenticated channel for late successive transmission:**

   As session key K_i is only shared among HAN-GW_i and BAN-GW_j, which is in late transmission E_{Ki} $(M_i||T_i||HMAC_{Ki})$ not only provide confidentiality but also provide authenticity and integrity of user and message. The $HMAC_{Ki}$ is used for verifying integrity of the message, whereas Ti is used for thwarting possible reply attack. The encryption of the whole packet by using AES algorithm and session key K_i is used for sender authenticity verification.

The proposed scheme is secure and more suitable candidate for allowing two-party SG communication.

Chapter 4

Results comparison and discussion

4.1. Simulation Setup and performance metrics

The proposed solution in analyzed and verified mathematically, also it is simulated in C# on core i-3 processor having 2.4GH core, 2 GB RAM. The results of the proposed scheme are compared with existing techniques of fouda and sule.

The proposed scheme is analyzed by these three performance matrices which are given bellow.

1. **Computation cost**: The time taken on each HAN-GW$_i$ and BAN-GW$_j$ for performing asymmetric encryption, asymmetric decryption, symmetric encryption, symmetric decryption, hash generation and verification, HMAC generation and verification in a handshake process.
2. **Communication overhead**: In termed to be the extra bytes traveled within HAN-GW$_i$ and BAN-GW$_j$ in each handshake step.
3. **Delay and Latency**: The total time taken for authentication.

These three performance metrics are considered for comparing the proposed scheme with the scheme presented by fouda and sule.

4.2. Results Comparison and Discussion

This main section is dedicated to the results of the proposed approach achieved and comparison of these results with other well-known approaches. The proposed approach is compared to two other techniques presented by fouda and sule with respect to the most important factors given below. Any security technique should not overload a system with heavy communication since it is known that, one operation over a network is many times more expansive than a local computation. If a security technique has high communication overhead it means that this approach will also contribute to the total system delay and latency negatively. Similarly a security mechanism aim for light weight devices with limited computation and power sources must not be computationally expansive. Therefore this section, will take into account these three important factors while comparing the proposed scheme with the other mentioned approaches presented by fouda and sule.

1. Communication overhead.
2. Computation overhead (i.e. time for performing major operations in handshaking process).

3. Delay and latency (i.e. the total time taken for authentication).

The comparison of the proposed scheme with the schemes of fouda and sule for the above performance metrics is described below.

1. Communication overhead

The main overhead in communication of the proposed approach comes from the handshaking process. This is the only difference with the other approaches since the rest of the communication of the proposed as well as the other approaches are the same. The communication overhead for handshake process in proposed scheme and the schemes presented by fouda and sule are shown in table 4.1.

Table 4.1: Communication overhead between HAN-GW$_i$ and BAN-GW$_j$ in each handshaking step

Technique	**Step no. 1**	**Step no. 2**	**Step no. 3**	**Overall data.**
Proposed scheme	384 *bytes*	156 *bytes*	Nil	540 *bytes*
Scheme of fouda	384 *bytes*	512 *bytes*	128 *bytes*	1024 *bytes*
Scheme of sule	384 *bytes*	512 *bytes*	128 *bytes*	1024 *bytes*

The table 4.1 shows the improvement of the proposed scheme in terms of communication overhead than schemes of fouda and sule. In first step the proposed scheme and schemes presented by fouda and sule sends 384 bytes of data, because all the schemes are using RSA algorithm in first step. In second step, the proposed scheme only sends 156 bytes of data by using AES algorithm whereas the schemes of fouda and sule sends 512 bytes of data because they both use RSA. In step 3 the proposed scheme sends nothing whereas the schemes of fouda and sule send 128 bytes of data in a plaintext form. The proposed scheme decreases the communication overhead in handshake up to 49%, with low communication latency because the less bytes of data is traveled among HAN-GW$_i$ and BAN-GW$_j$ in handshake process, due to that reason the proposed scheme have low communication overhead than schemes of fouda and sule.

2. Computation overhead

The computation cost analysis is based on major operations performed during handshake process, these major operations include asymmetric encryption, asymmetric decryption, symmetric encryption, symmetric decryption, HMAC generation and verification, Hash generation and verification at each HAN-GW$_i$ and BAN-GW$_j$.

The computation overhead for handshake process in proposed scheme and the schemes presented by fouda and sule are shown in table 4.2.

Table 4.2: Overall computation overhead for handshaking in both HAN-GW$_i$ and BAN-GW$_j$

Technique	**RSA** (Enc) in milli sec	**RSA** (Dec) in milli sec	**AES** (Enc) in milli sec	**AES** (Dec) in milli sec	**HMAC** (gen & ver) in milli sec	**Hash** (gen) in milli sec	**Total time for Handshaking in milli sec**
Propose scheme	58	52	12	10	4	4	150
Scheme of fouda	58*2	52*2				4	234
Scheme of sule	58*2	52*2				4	234

The table 4.2 specifies the computation time taken by major operations while performing handshaking for session key establishment. The overall time taken for handshaking process in proposed scheme is 150 milli sec, whereas the schemes of fouda and sule took 234 milli seconds in handshaking phase.

By using a hybrid approach of RSA and AES algorithms, the proposed scheme results to a low computation cost, by achieving 35 % of low computation overhead as compared to the schemes of fouda and sule. The proposed scheme is suitable in terms of computation overhead.

3. Delay and latency

The total time taken for authentication in the proposed authentication scheme and the schemes presented by fouda and sule is given in table 4.3 in next page.

Table 4.3: Total time taken for authentication in both HAN-GW$_i$ and BAN-GW$_j$

Technique	**RSA** (Enc) in milli sec	**RSA** (Dec) in milli sec	**AES** (Enc) in milli sec	**AES** (Dec) in milli sec	**HMAC** (gen & ver) in milli sec	**Hash** (gen) in milli sec	**Total time for authentication in milli sec**
Proposed scheme	58	52	12	10	4	4	176
Scheme of fouda	58*2	52*2	12	10	4	4	260
Scheme of Sule	58*2	52*2	12	10	2	4	258

The table 4.3 specifies the total time taken for authentication between HAN-GW$_i$ and BAN-GW$_j$. The proposed scheme results to 176 milli seconds for handshaking and authentication of message and authenticity of user, whereas the scheme proposed by fouda took 260 milli seconds and sule 258 milli seconds for achieving the same objectives. The proposed scheme is more than 32% lighter than the scheme of fouda and sule, while achieving message integrity and user authenticity. The proposed scheme results to low communication delay and latency.

Delay and latency is the total time taken for authentication i.e. in both session key establishments and also in late successive transmission.

Chapter 5

Conclusion and Future work

5. Conclusion and Future work

The two-way communication among consumers and control centers of the utility provider in SG has been presented in this thesis. IP-based communication facility as well as the error prone nature of the wireless communication makes SG more vulnerable to security threats. Especially devices like smart meters are more vulnerable to different security threats and there are different privacy concerns due to the resource limitation problem for example the low computational capabilities.

The proposed authentication scheme is based on Diffie-Hellman key establishment protocol. For session key establishment it uses the well-known algorithms RSA and AES. To provide message integrity it exploits the advantages of the HMAC technique. The results of this study show that, the proposed technique is lightweight and is suitable for use in resource constrained devices such as smart meters in the Smart Grid environment. It has also been proved by the security analysis of the proposed scheme that, the proposed scheme is secure and more reliable for SG communication.

A comparison of the proposed technique simulation results for handshaking process with the existing well-known approaches presented by fouda and sule has been presented. It is clear from the results that the proposed technique has 49% low communication overhead than schemes of fouda and sule, which ultimately also resulted in a low system delay.

Similarly the results comparison for computation overhead of the proposed scheme with those of the schemes of fouda and sule, show that the proposed technique has achieved 35% improvement in lowering the computation overhead in handshaking process.

All these improvements collectively affect the overall system positively. Therefore the overall time taken for authentication of the proposed scheme is lower than fouda and sule schemes, which also positively affect the overall latency of the whole system in SG.

The focus of the proposed scheme is only addressing the privacy concerns, achieving mutual authentication, thwart reply and man-in-the-middle attack. Further improvements need to be done in the area of security against different attacks like Denial-of-Service thereby providing a more resource efficient solution for the Smart Grid environment.

Appendix A

References and Web links

References:

[1] T. Baumeister, "Literature Review on Smart Grid Cyber Security", Collaborative Software Development Laboratory Department of Information and Computer Sciences, University of Hawai'i, Dec, 2010.

[2] M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu and X. Shen, "A Lightweight Message Authention Scheme for Smart Grid Operations", IEEE Transactions on Smart Grid, vol. 2, no.4, PP.6 75- 685, ISSN: 1949-3053, Dec 2011.

[3] A. Aggarwal, S. Kunta and P.K. Verma, "A Proposed Communications Infrastructure for the Smart Grid", in innovative Smart Grid Technologies (ISGT), pp.1-5, Jan. 19-21, 2010, Univ. of Oklahoma-Tulsa, Tulsa, OK, USA.

[4] Office of the National Coordinator for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards, release 1.0", *NIST Special Publication 1108*, 2009.

[5] T.M. Overman and R.W. Sackman, "High Assurance Smart Grid: smart grid control systems communications architecture", IEEE Conf on Smart Grid Communications, pp.19-24, Oct. 4-6, 2010. Sunnyvale, CA, USA.

[6] R. Hasan and G. Radman, "Survey on Smart Grid", IEEE SoutheastCon (SoutheastCon), pp. 210-213, Mar. 18-21, 2010.

[7] G.N. Ericsson, "Cyber security and power system communication-essential parts of a Smart Grid infrastructure", IEEE Trans, Power Del., vol.25, no.3, pp.1501-1507, Jul, 2010, Sundbyberg, Sweden.

[8] M.M. Fouda, Z.M. Fadlullah, N. Kato, A. Takeuchi, N. Iwasaki and Y. Nozaki, "Towards Intelligent Machine- to Machine Communication in Smart Grid", IEEE communication, magazine, vol.49, no.4, pp.60-65, Apr. 2011.

[9] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid", IEEE TRANSACTIONS ON SMART GRID, VOL. 1, NO. 1, pp.57-64, JUNE 2010, Santa Clara, CA, USA.

[10] M.M. Fouda, Z.M. Fadlullah, N. Kato, R. Lu and X. Shen, "Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid communications", proc. IEEE INFOCOM'11, pp. 1035-1040, ISBN: 978-1-4577-0249-5, Shanghai, China, Apr, 2011.

[11] M. Kgwadi and T. Kunz, "Security RDS Broadcast Messages for Smart Grid Applications", in proc.6th int. wireless commun. Mobile comput. Cont., France, June, 2010.

[12] K. Kowalienko, "Smart Grid projects pick up speed", IEEE, The Institute, Standards, Article 06, Aug. 2009.

[13] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data", IEEE International Conf on Smart Grid Communications (SmartGridCom), pp.238-243, Oct. 4-6, 2010, Bristol, UK.

[14] X. Lu, Z. Lu, C. Wang and W. Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid", Military Communications Conference (MilCom), pp.1830-1835, Oct, 31 to Nov, 3, 2010, NC, USA.

[15] W. Wang, Y. Xu and M. Khanna, "A Survey on the communications architectures in smart grid", Conference on Communication networks 55, pp.3604-3629, Jul.27, 2011, NC, USA.

[16] A.R. Metke and R.L. Eki, "Security Technology for Smart Grid Networks", IEEE TRANSECTION ON SMART GRID, Vol. 1, NO.1, PP.99-107, ISDN, June, 2010, IL, USA.

[17] H. Khurana, D.A. Frincke, M. Hadely and N. Lu, "Smart-grid Security issues", IEEE magazine on Security and Privacy, Vol. 8, No. 1, pp. 81-85, Jan, 2010, IL, USA.

[18] C. Cuijpers, B.J. Koops and H. Wetsvoorstal, "Slimme Meters": Een Privacytoets op Basis Van art. 8 Evrm. Tilburg, the Netherlands: Tilburg Univ., Oct. 2008.

[19] K. Kursawe, G. Danezis and M. Mohlwieiss, "privacy-friendly aggregation for the smart grid". Microsoft Research.

[20] S. Clements and H. Kirkham, "Cyber-Security Considerations for the Smart Grid", IEEE Conference of Power and Energy, pp.1-5, Jul.25-29, 2010, WA, USA.

[21] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the Smart Grid", IEEE security privacy Magazine, vol.7, no. 3, pp.75-77, 2009, PA.

[22] G.W. Hart, "Nonintrusive appliance load monitoring", Proceedings of the IEEE, vol. 80, no. 12, pp. 1870-1891, Dec,1992, NY, US.

[23] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford and P. Armstrong, "Power signature analysis", IEEE Power and Energy Magazine, vol. 1, no. 2, pp. 56-63, Apr, 2003.

[24] Y. Liu, P. Ning and M. Reiter, "False data injection attacks against state estimation in electric power grids", in Proc. of ACM Conference on Computer and Communications Security *(CCS '09)*, ISBN: 978-1-60558-894-0, pp. 21-23, Sept. 2009.

[25] M.M. Fouda, Z.M. Fadlullah and N. Kato, "Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications", Proc. of the 6th IEEE International Conference on

Computer Engineering and Systems (ICCES'10), Cairo, Egypt, pp. 245 - 250, Nov 30 - Dec. 2, 2010.

[26] A. Hamlyn, H. Chaung, R. Cheung, T. Mander, C. Yang and L. Wang, "Network Security Management and Authentication of Actions for Smart Grids Operations", in proc.IEEE Electr, Power conf, pp.31-36, Oct, 25-27, 2007 Montreal, QC, Canada.

[27] D. Chung, M.H. Dwijaksara, J. Kim, K. Kim and Y. Park, "An efficient and privacy-preserving authentication protocol for HAN", Symposium on Cryptography and Information Security (SCIS 2011), Jan, 25-28, 2011, kokura, Japan.

[28] D. Wu and C. Zhou, "Fault-Tolerant and Scalable Key Management for Smart Grid", IEEE Transaction on Smart Grid, Vol.2, No.2, pp.375-381, Jun, 2011, FL, USA.

[29] G. Cao, and Q. Li, "Multicast Authentication in the Smart Grid with One-Time Signature", IEEE TRANSECTION ON SMART GRID, VOL.2, NO.4, pp 686-696, Dec, 2011, PA, USA.

[30] T.W. Chim, L.C.K. Hui, V.O.K. Li and S.M. Yiu, "PASS: Privacy-preserving Authentication scheme for Smart Grid Network", IEEE Conference on Smart Grid communications (SmartGridCom), pp. 196-201, Oct, 17-20, 2011, Hong Kong, China.

[31] J. Choi, C. Li, J. Seo and I. Shin, "An Efficient Message Authentication for Non-repudiation of the Smart Metering Service", ACIS/JNU Conference on Computer networks (CNSI), pp. 331-333, May, 23-25, 2011, Daejeon, South Korea.

[32] E. Ayday and S. Rajagopal, "Secure, Intuitive and Low-Cost Device Authentication for Smart Grid Networks", IEEE Conf on Communications and Networking (CCNC), pp. 1161-1165, Jan, 9-12, 2011, Atlanta, GA, USA.

[33] R. Sule, R.S. Katti and R.G. Kavasseri, "A Variable Length fast message authentication code for secure communication in smart grids", IEEE Conf. on Power and Energy society, pp. 1-6, Jul, 22-26, 2012, Fargo, ND.

[34] C.H. Hauser, D.E. Bakken, A. Bose, I. Dionysiou, K.H. Gjermundrod, J. Halkey and V.S. Irava, "security trust, and QoS in next generation control and communication for large power systems", int., j.crit, infrastrust, vol.4, no.1/2, pp.3-16, 2008.

[35] S.M. Seth and R. Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology (IJCST), ISSN: 0976-8491, Vol. 2, No. 2, pp. 292-294, Jun, 2011.

[36] D.R. Stingson, "Cryptography: Theory and Practice", 3rd ed. Boca Raton, FL: CRC, 2005.

Related Web links:

[37] DOE, Final Report on the August 14, 2003 Blackout in the United States and Canada. U.S.-Canada Power System Outage Taskforce, 2004.
Available online at: https://reports.energy.gov/BlackoutFinal-Web.pdf
Access on: 14, April, 2012.

[38] NewScientist, "Solar power could crash Germany's grid", Oct, 27, 2010.
Available online at: http://www.newscientist.com/article/mg20827842.800-solar-power-could-crash-germanys-grid.html.
Access on: 15 Oct, 2012.

[39] Harnessing the power of demand-How ISOs and RTOs are integrating demand response into wholesale electricity markets, Markets Committee of the ISO/RTO Council, Oct, 16, 2007.
Available online on ISO/RTO : http://www.isorto.org/atf/cf/%7B5B4E85C6-7EAC-40A0-8DC3-003829518EBD%7D/IRC_DR Report_101607.pdf.
Access on: 20 Oct, 2012.

[40] DOE-Office of the Electricity delivery and Energy reliability, "Demand Response".
Available online: http://energy.gov/oe/technology-development/smart-grid/demand-response.
Access on: 22 Oct, 2012.

[41] DOE-Office of Electricity Delivery and Energy Reliability. GridWorks: Overview of the Electric Grid. Available in archive form on:
http://sites.energetics.com/gridworks/gridworks_pdfs.zip.
Access on: 13, Mar, 2012.

[42] MSP430 for utility Metering Applications.
Available online at: http://focus.ti.com/mcu/docs/mcuorphan.tsp?contentid=31498
Access on: 25, Oct, 2011.

[43] Report to NIST on the Smart Grid Interoperability Standards Roadmap, Jun, 2009.
Available online at:
http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf
Access on: 20, Oct, 2011.

[44] "The Smart Grid interoperability panel cyber security working Group: Smart Grid cyber security strategy and requirements", U.S. National Institute of Standards and Technology (NIST).

Available at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

Accessed On, 15, May 2012.

[45] Clemente, J., "The Security Vulnerabilities of Smart grid", Journal of Energy Security, Jun, 18, 2009.

Available online at:

http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345.

Access on: 15 march, 2011.

[46] IEEE P2030 Draft Grid.

Available: http://grouper.ieee.org/groups/scc21/2030/2030_index.html.

Access on: 14, Nov, 2011.