Indian J.Sci.Res. 14 (1): 318-325, 2017 ISSN: 0976-2876 (Print)
ISSN: 2250-0138 (Online)

# DEFENDED DATA TRANSMISSION SCHEME BASED RELIABLE METERING FOR SMART GRID APPLICATIONS

**K. VEDAVALLI[a1] AND N. MURUGANANTHAM[b]**

[ab]Department of EEE, PMU, Vallam, Thanjavur, Tamil Nadu, India

## ABSTRACT

**To expand the usage, reliability, availability of power resources and some distribution system must be met which is conceivable by the support of present day information technologies. This paper concentrates on client support and electricity distribution, where payment of electric bills (counting energy utilization every month or year and association points of interest) should be possible with online arrangements. It is proposed a protected and reliable solution which combines the elements of the electrical system with the network systems to give better execution on information issues, which is done on a given demand location. The electrical readings of the client will be upgraded each month in the database which is kept up in the distributed storage. The client will be furnished with security keys to see the perusing values and perform payment of bills. To make the solution more available, the dynamic information will be kept up on different servers in various areas of the cloud, and there will be a service supplier who deals with the service request. The hardwired electric meter transmits the electrical reading, which in turn accesses the particular service to make an entry for the specific association at the cloud. The usage data will be kept up at various areas of the cloud, which is accessible with security. The customer availability is controlled with Supervisory Control and Data Acquisition Systems (SCADA).**

**KEYWORDS:** Smart Meter; Smart Grid; Cloud Storage; Energy Utilization; Utility.

Smart Grids (SG) have several applications with various methodologies, yet utilizing them to support the mains is somewhat new. In this paper, the control and observing of a Lighting Smart Grid (LSG) are amplified using a communication model. The objective is to have a higher and more precise control of the LSG while keeping a robust and self-sufficient foundation. Moreover, this power inject some vital components to these micro grids: the ability to exchange energy flows with different buses or the mains going to financial or strategical reasons, e.g. injecting energy to the grid in case of a shortage or smoothing the demand curve of the system improving the stability of the network.

The significance of the Demand Side Management can be found in the literature. The uniqueness in this proposal is that the control would be produced using the grid side. This new point of view is named as Grid Side Management (GSM). GSM approach is legitimate since this LSG on which this paper is centered around are expected to substitute the general open lighting framework, so the grid would have a huge number of these micro grids accessible to obtain or inject energy from them. A control strategy to accomplish this task on a Lighting Smart Grid (LSG) with power generation and storage capability is proposed. Several advantages of distributed control in AC and DC micro grids using control techniques highlighting its robustness and simplicity.

Fig. 1 outlines the high-level scheme of the typical structure of the street light system. These are the principle obstructs that are incorporated in the framework: A 48 VDC BUS. LED load with 18 independent loads with different capability and remote communications (120 W). Wind energy generation such as Vertical axis wind turbine (VAWT) with its related Maximum Power Point Tracker (MPPT) and 3 to 9 Photovoltaic Panels (PV) with its associated MPPTs.

An energy storage system composed of several modules of 3 LiFePo4 batteries. Each module has its own particular BMS with a limit of 140Wh. A little power inverter is associated with the grid systems. Besides, a communication model between the several modules inside the micro grid is exhibited with a specific end goal to expand its abilities.

This new approach depends on a past plan yet with some necessary improvements. A backbone communication between the LED Load driver, the BMS and the inverter with a lightweight protocol over an RS-485 BUS is proposed. Communications outside the framework are accomplished with IPV6 over low-power personal area network (6LowPan) or Zigbee.

[1]Corresponding author

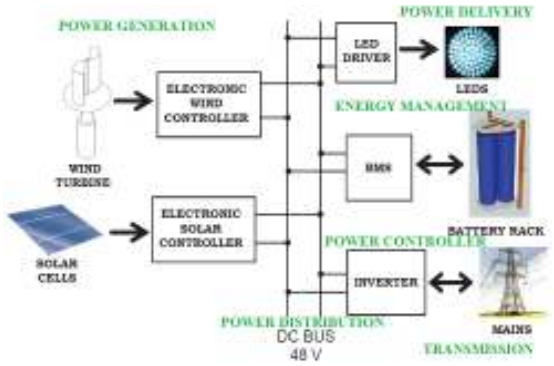



**Figure 1: Conventional Architecture**

## RESEARCH BACKGROUND

The authors briefly discuss the latest developments in domestic electricity metering and then discuss meter communications systems for local, remote, and automatic meter reading. They describe optical links, pilot wire systems, power line carrier methods, telephones, and radio. The suitability and advantages of each type of system are discussed.

Data integrity and confidentiality of end-to-end information have been concentrated widely on the Internet. Be that as it may, most plans, for example, TLS, expect the gadgets have copious memory and computational energy to perform costly cryptographic operations. In smart frameworks, then again, reporting devices have restricted memory with a moderate CPU. Traditional web security conventions are in this manner not appropriate for information accumulation in Smart Grids. Distributed Network Protocol (DNP3) is a standard communications convention utilized as a part of supervisory control and information obtaining, the information gathering subsystem of power grids.

It accepts all segments are inside the security edge of the administrator and is not intended to ensure information sent by the DC as in our circumstance. The following standard for substation computerization is the IP-based the International Electro technical Commission (IEC) 61850 Yet, IEC 61850 was also initially designed without security mechanisms. It is thus generally agreed by the experts that new security protocols for data collection and command delivery of Smart Grids need to be developed. Our proposed approach comprises security aspect of the Smart Grid data collection as well as the time minimization. In what follows, we provide synopses of related work from these aspects as well as on a variety of other relevant subtopics of our holistic approach.

Gathering information by the method for transport layer conventions from many users has been contemplated in the literature. Kim et al. concentrated how to lessen the capacity required when the control focus needs to set up numerous sessions with the Grids. Long-term Joint keys are produced by a position so that the control focus just needs to remember the ability however not individual keys. By the by, the key built up along these lines is not extremely secure. Additionally, the convention is not appropriate for the various leveled information accumulation design. Information collection through a Data Center is considered in.

The creators propose to keep up two separate transmission control protocol (TCP) associations, and the two associations can be secured utilizing distinctive components autonomously. In any case, the Datacenter (DC) is thought to be dependable, that is, it can read the information sent by the Grid. Another critical part of secure data accumulation is worried about key administration. Numerous expect trusted DC, that is, they don't consider concealing the information from the DCs, for example. Wu and Zhou connected the elliptic bend open key procedure to perform essential administration. Typical validation between various substances is concentrated. All things considered, there is no exchange on the most proficient method to secure the information reported by a sensor.

Law et al. described how to establish keys and secure unicast and multicast communications. Kim et al. proposed long-term keys to be given to the different parties for protecting messages. Fouda et al. described how to apply the Diffie–Hellman (DH) mechanism to establish a Joint key for data authentication between two parties. Reference, on the other hand, relies on identity-based cryptography. All these mechanisms cannot be applied in the hierarchical data collection model because the PO and the MDs cannot establish a direct connection. Nicanfar and Leung depicted how a gadget builds up Joint keys with various controllers at different progressive levels.

Be that as it may, it is accepted that a key exists between two adjoining controllers. Another approach exhibited in depends on symmetric cryptography to give information secrecy and validation amongst sensors and the base station. Once more, an ace key is expected with a pre-agreed on pseudo-arbitrary capacity in the plan. Another classification for giving security and protection misuses the complete insights of the detected information, for example, summation, reasonable, least, most extreme, and so forth. It is apparently found that the system has a

problem of service selection in all the above approaches when there is a large number of customers from a different location. Hence a new secure service communication method is proposed in this paper.

## PROPOSED METHODOLOGY

The principle target of the proposed Reliable Smart Grid Communication (RSGC) model and its energy control in a smart home/ public street lighting framework is appeared in Fig. 2. Dependable Energy Management models are improved in Smart Grid communications both inside and outside the Smart Grid.

The proposed RSGC framework is situated in two different measures, a wired one for the data streams inside the small scale grid and a remote system between inter-grid communication control and management from SCADA.

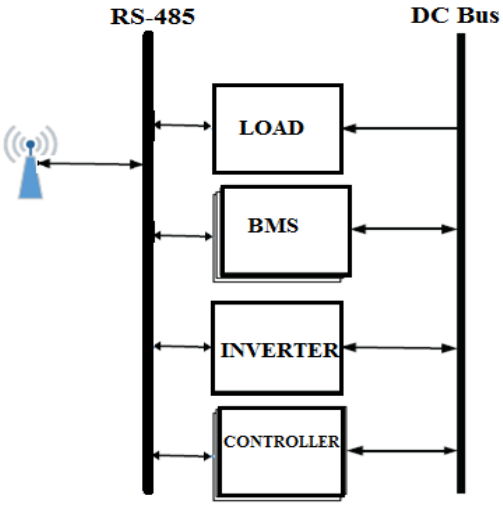



**Figure 2: Proposed Reliable Smart Grid Communication Model**

### Internal Communications

RS-485 is suggested as it is the facto standard for industrial applications. A custom yet first convention will be actualized on top of it. The principle attributes of RS-48 5 systems are:

Up to 256 gadgets with addressing.

Master/slave topology.

Transmission speed up to 35 Mbit/s

### Intergrid Communications Reliable Mesh Network

Every one of the information originating from the Smart meter is burrowed into a remote channel. Two individual choices for the correspondence with the SCADA station have been executed, both based on IEEE 802.15.4. This convention based solid work organized topology is shown in Fig. 3. This protocol works as an adjustment layer amongst IPV6 and the MAC layer, managing directing, neighbor discovery, header compression, and security. Its principle favourable position is the interoperability with IPV6, so the hubs are associated with the internet. The preferred fundamental standpoint of this innovation is its effortlessness and vigour and consistent quality.

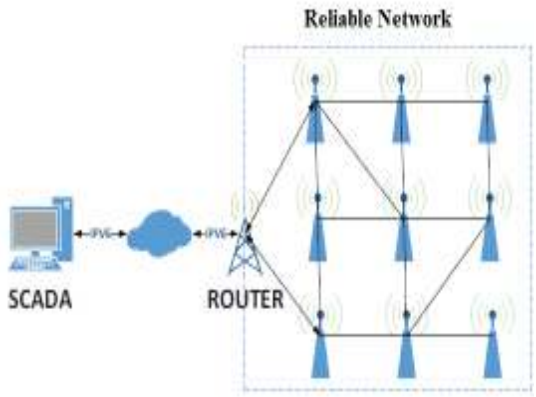



**Figure 3: Proposed Network Architecture**

### Reliable Communication Service and Security

The proposed Smart Grid is intended to substitute the model smart home/open road lighting framework; the system will be usually presented to obstruction and channel meddling. To manage these issues, a Defended Data Transmission (DDT) calculation will be actualized on top of the physical layer as proposed in the system. Proposed DDT offers a great exchange off between packet conveyance rate and reduced duty cycle alongwith great clamor versatility that makes it perfect for data communication.

Besides having problem maintaining Quality of Service (QoS) of the system, another issue is the security. Henceforth the proposed DDT based digital strategy convention will be presented to many conceivable attackers and all sorts of interruptions.

## DEFENDED DATA TRANSMISSION (DDT)

The proposed scheme has different stages, to be specific; Chiper Key Generation, Reliable OTP Verification, Reliable data mapping and smart metering selection and Composition. We talk about each of them in the accompanying.

### Cipher Key Generation

The proposed framework has various customers, and each of them are in different parts and the proposed approach produces the one time key and

circulate to them. For a general client, the key is created at every charging period, while for another client the key is produced just once. The key generation mechanism utilizes a randomization strategy to process the key for the clients. The randomization system uses a blend of group id, user id, and an arbitrary number to create the key. For instance, for a client with user id "U001" and with cluster id "C01", the irregular number of the scope of 100000 as 68124 is chosen to register "C01U00168124". The produced key will be encoded with the group key which is unmistakable for the particular group id and will be sent to the users. By getting the key, the client could decode the key utilizing the group key which will be used for further correspondence.

Algorithm:

Input: Cluster ID, User ID sets, group Key Gk.

Yield: Chiper Key Ck, Keyset Pk

For every client Ui

Recognize Cluster ID CID.

Register user id Uid.

Register number of users in the cluster

NuC = ∫ Max(Cid.Uid) +1

Create random number R = ∫ (Nuc,Nuc+10000)

Create key k = ∫ (CID+UID+R)

Create chiper key Ck = K/(Group key)

Insert to key set Pk = ∑ Ck+Cki

Send to User

End

**Reliable One Time Pin (OTP) Verification Scheme**

The smart grid network performs responsible energy management utilizing the cipher key presented by the client. The client gives the cipher key to the Smart network with the group key. The grid framework and the group key distinguish which group the client belongs to and if the customer client is identified, then the key submitted is decrypted with the group key and after that it is contrasted and the first key is made accessible.

Algorithm:

Input: Cipher key Ck, Group key gk, key set ks

Yield: Access flag

Step1: Check the gk with the key set and recognize the cluster id

Step2: Decrypt the cipher key utilizing group key

Step3: Compare the cipher key Ck in the key set ks

Step4: stop

**Reliable Energy Management Based Service Selection And Composition**

The strategy keeps up the history of information getting to be performed by the client and set of services are made accessible. Those histories are utilized to choose the service, from the history the set of services is recognized. For every service available, service access rate is processed and completeness is measured to rank the services. From the positioned services top services are chosen to composite the service. The selected services are composed to form a complete service and will be given to the user.

Algorithm:

Input: Access History Ah

Yield: Selected service S

Step1: Select Distinct services from Ah

DS = ∫ ∑ Distinct(services)

Step2: for each service Si from Ds

Compute service access rate SAR = (Number of time service invoked)/(Total number of records in Ah)

Compute service weight sw = SAR×CM

End

Step3: Select most weighted service S $= \int_{1=1}^{N} Max(sw)$

Step4: perform service composition

Step5: stop

The operation of a basic situation with two different

$$BMS = 3/2\ (V\text{-}V_{ref}) \quad (1)$$

$$BMS = \begin{cases} \frac{-1}{2}(V - Vref)^2 \text{ if } V < Vref \\ \frac{1}{2}(V - Vref)^2 \text{ if } V > Vref \end{cases} \quad (2)$$

Reliable Power Management Control profiles in a similar Smart Grid is created by Battery Management System (BMS) and a grid inverter. The Voltage on the transmission bus through time and the current on the bus when the Battery Management

System (BMS) are set up with conditions (1) and (2) separately. An operating current means the BMS are charging the batteries while a negative one shows the energy is streaming to the inverter. The control capacities appear.

The BUS and the various components are monitored, and errors are accounted for the SCADA continuously. Current and voltage are measured in the BUS and additionally on each module. A change on a proposed Control profile or in the Bus voltage may bring about changes in the current on the BUS, so this variation into the record was searching for the anomalous conduct of the framework. The SCADA would need to check the state of charge (SOC) of the batteries, the power generation capacity (in spite of the fact that on account of some renewable vitality sources like wind this is genuinely erratic), and after that the control station will send the request to those request coordinating the lively necessities.

## RESULTS AND DISCUSSION

The proposed DDT calculation based proposed metering gadget is actualized in Matlab Environment with different situations and some smart meter nodes with various transmission range and power. Every technique is tried for its productivity taking into consideration various factor of quality of service. The simulation has created three different clouds, and each of them keeps running in different areas. The electric meter is connected to the remote device to empower communications. Additionally, a web interface is considered, utilizing which payment can be made.

The power utilization Estimation for every client in the Grid range computed in based on hourly requests. Fig. 4 & Fig. 5 demonstrates the Mean and variance of the Average power consumption (W) of each time interval (Hour) by utilizing the proposed data simulation procedure.

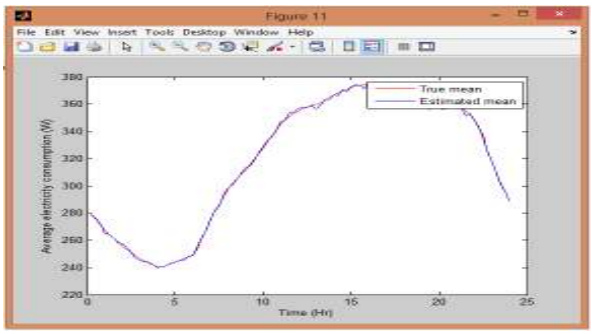



**Figure 4: Mean of the Average power consumption (W) of each time interval (Hour) for the individual user**

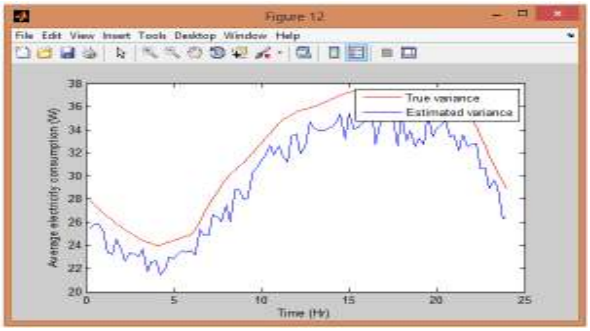



**Figure 5: The variance of the Average power consumption (W) of each time interval (Hour) for the individual user**

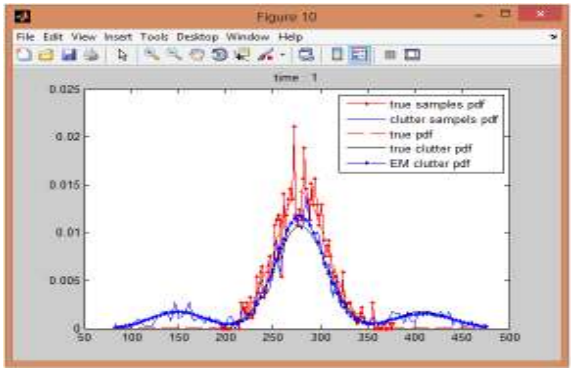



**Figure 6: Probability Distribution Function of Smart meter; true report (strong blue line); proposed strategy ensured report (dark dash-dab line); Existing technique secured report (blue spots line); Estimated distribution from the secured release (strong red line); estimated distribution from existing method secured report (red dabs line).**

The Probability Distribution Function (PDF) results of Smart Meter (SM) demonstrates the estimation precision of a given Smart grid arranged after applying protection methods. In Fig. 6, we can see that both the proposed strategy and existing technique change the good dispersion of SM. Remarkably, the progressions presented by the proposed method just happen at the lower and upper finishes of the actual conveyance. It can be translated that our technique devotes to ensure these clients who truly should be secured. The proposed calculation adequately explains these disadvantages inside existing methods. Hence we presume that the proposed calculation outflanks the current method.

**Table 1: Simulation Parameters**

| Parameters | Value |
|---|---|
| Tool | Matlab |
| Area | 1000m x 1000m |
| Transmission Range | 250 m |
| Packet size | 512 bytes |
| Laxity Time | 100-500 Sec. |
| Number of service providers | 2 |
| Number of Customers | 1 million |

To assess the execution of the proposed arrangement, the accompanying measurements are measured, in particular, Availability Ratio, Security Value, and time complexity. Availability is the proportions of aggregate requests submitted and add up to demands handled. Security level is measured by total solicitations produced and finished. The execution of the proposed technique is contrasted and five well-known scheduling strategies for the grid environment, to be specific: Security of Real Time Data Intensive Applications on Grids (SARDIG), SAREC: a security-aware scheduling strategy for real-time applications on clusters and Earlier Deadline First (EDF) algorithms.

Table 2 demonstrates the simulation results of the security esteem for the four calculations. Security esteem is figured utilizing the aggregate number of requests submitted and some requests endless supply of clients present in the system. The proposed calculation demonstrates preferable security esteem over alternate calculations as the quantity of customers or jobs increases.

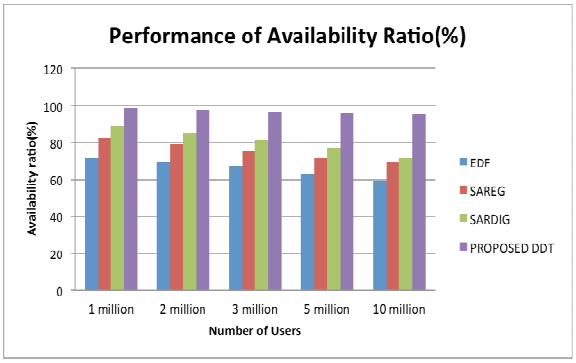
**Table 2: Shows the Comparison Results of Security Level**

| Security Level Value | | | | |
|---|---|---|---|---|
| No. of Users | EDF | SAREG | SARDIG | Proposed DDT |
| 1million | 0.89 | 0.92 | 0.95 | 0.99 |
| 2 million | 0.83 | 0.85 | 0.90 | 0.96 |
| 3 million | 0.77 | 0.79 | 0.86 | 0.93 |
| 4 million | 0.61 | 0.72 | 0.82 | 0.91 |
| 5 million | 0.55 | 0.65 | 0.77 | 0.89 |

**Table 3: Shows the Comparison Result of Service Availability**

| Availability Ratio % | | | | |
|---|---|---|---|---|
| No. of Users | EDF | SAREG | SARDIG | Proposed DDT |
| 1 million | 72 | 82 | 89 | 98.7 |
| 2 million | 69 | 79 | 85 | 97.6 |
| 3 million | 67 | 75 | 81 | 96.6 |
| 5 million | 63 | 72 | 77 | 95.8 |
| 10 million | 59 | 69 | 72 | 95.1 |

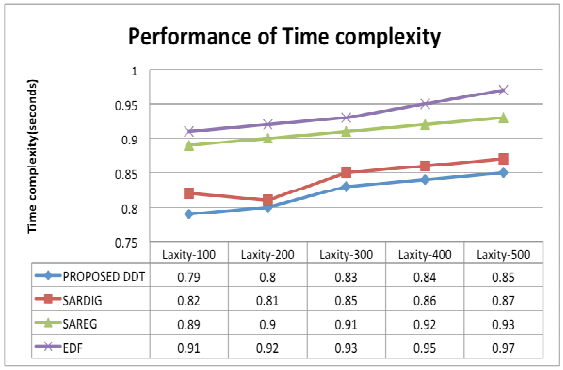
**Graph 1: Explains the Comparative Results of Availability Rat Under Different Users**




The time complexity is ϕ (N×M), where N-is the quantity of areas where the service is accessible, and M-is, the number of providers available. The general time complexity is registered as: Time complexity Tc = N × Log (M)

The Graph 2 shows the time complexity of different methods to access the service where the service and data are available in various locations of the region.

**Graph 2: Shows the Time Complexity of Different Approaches**




## CONCLUSION

This paper has proposed a Defended Data Transfer service for reliable access to the communication network services in the smart grid. The reliable energy management scheme can be implemented by collecting and analyzing customer energy data, making energy saving suggestions, and applying real-time pricing. The proposed strong power management consists of the smart meter, Data Server storage unit and a group of cluster units which are interfaced by the smart metering approach. The smart grid node is to trust the reliability and independence of few groups in the grid networks. Also, the consumers

will be restricted to access the service a few time periods only and secure the whole system from flooding attacks. The proposed method has produced higher quality results and quality of assurance.

## REFERENCES


Kayastha N., Niyato D., Hossain E. and Han Z., 2012. "Smart grid sensor data collection, communication, and networking: A tutorial," Wireless Commun. Mobile Comput., **14**(11):1055–1087.

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, Smart Grid Interoperability Panel (SGIP), NIST Standard 1108R3, Oct. 2013.

Fang X., Misra S., Xue G. and Yang D., 2012. "Managing smart grid information in the cloud: Opportunities, model, and applications," IEEE Netw., **26**(4):32–38.

Bera S., Misra S. and Rodrigues J., "Cloud computing applications for smart grid: A survey," IEEE Trans. Parallel Distrib. Syst., to be published.

Tabassum R., Nahrstedt K., Rogers E. and Lui K.S., 2013. "SCAPACH: Scalable password-changing protocol for smart grid device authentication," in Proc. 22nd Int. Conf. Comput. Commun. Netw., Nassau, pp. 1–5.

The Transport Layer Security (TLS) Protocol Version 1.2, RFC Standard 5246, 2008.

Kim Y.J., Kolesnikov V. and Thottan M., 2011. "Resilient end-to-end message protection for large-scale cyber-physical system communications," in Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm), Tainan, Taiwan, 2012, pp. 193–198. DNP3 Secure Authentication Version 5, IEEE Standard 1815-2012.

IEC Power Utility Automation, Technical Committee 57 (TC57), IEC Standard 61850, 2003.

Vaidya B., Makrakis D. and Mouftah H.T., 2011. "Device authentication mechanism for smart energy home area networks," in Proc. IEEE ICCE, Las Vegas, USA, pp. 787-788.

Kim Y.J., Kolesnikov V., Kim H. and Thottan M., 2011. "SSTP: A scalable and secure transport protocol for smart grid data collection," in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), Brussels, Belgium, pp. 161–166.

Khalifa T., Naik K., Alsabaan M., Nayak A. and Goel N., 2010. "Transport protocol for smart grid infrastructure," in Proc. IEEE Int. Conf. Ubiquitous Future Netw., Jeju Island, Korea, pp. 320–325.

Crossley D., 2008. "The role of advanced metering and load control in supporting electricity networks," Tech. Rep. No 5 Task XV, International Energy Agency Demand Side Management Programme. Energy Futures Australia PTY LTD, Australia.

Mathieu J.L., et al., 2011. "Examining uncertainty in demand response baseline models and variability in automated responses to dynamic pricing," in Decision and Control (CDC), 50th IEEE Conf. on, pp. 4332–4339.

Roozbehani M., et al., 2010. "On the stability of wholesale electricity markets under real-time pricing," in Decision and Control (CDC), 2010 49th IEEE Conf. on, pp. 1911–1918.

Ustun T.S., 2013. Fault current coefficient and time delay assignment for micro grid protection system with central protection unit, IEEE Transaction on Power systems, **28**(2):598-606.

Ziari S., 2013. Optimal distribution network reinforcement considering load growth, line loss, and reliability, IEEE Transaction on Power systems, **28**(2): 587-597.

Shenghan S., 2013. Development of physical-based demand response-enabled residential load models, IEEE Transaction on Power systems, **28**(2): 607-614.

Lianordi B., 2013. An approach for real time voltage stability margin control via reactive power reserve sensitivities, IEEE Transaction on Power systems, **28**(2): 615-625.

Shaaban M.F., 2013. DG allocation for benefit maximization in distribution networks, IEEE Transaction on Power systems, **28**(2):639-649.

Stankovic J.A., et al., 1998. GC. Deadline Scheduling for Real-Time Systems: EDF and Related Algorithms. Kluwer: Dordrecht.

Xie T., et al.,2005. SAREC: a security-aware scheduling strategy for real-time applications on clusters. In Proceedings of the 34th

International Conference on Parallel Processing, Oslo.

Islam M.R., et al., 2011. An architecture and a dynamic scheduling algorithm of grid for providing security for real-time data-intensive applications, international journal of network management, Int. J. Network Mgmt., **21**(5):402–413.

Maxwell J.C., 1892. A Treatise on Electricity and Magnetism, 3rd ed., Oxford: Clarendon, **2**:68-73.