JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Implementing AMI Network using Riverbed OPNET Modeler for DDoS attack

Tejaskumar Bhatt[1*], Chetan Kotwal[2], Nirbhaykumar Chaubey[3]

[1,2]Dept. of Computer/IT Engg. Gujarat Technological University (GTU), Ahmedabad, Gujarat, India
[3]S.S.A.I. of Computer Science, Navasari Gujarat, India

DOI: https://doi.org/10.26438/ijcse/v7i2.569574 | Available online at: www.ijcseonline.org

Accepted: 24/Feb/2018, Published: 28/Feb/2019

***Abstract*-**Smart meter networks are the spine in distribution grid for smart electrical. Here, in smart Grid, and there are number of smart meters are interconnected and two-way information flows. The distribution side, the smart grid requires the integration of intellectual electronic devices such as Automatic Metering Infrastructure (AMI). This AMI needs wireless communication technology for relay information from the control centre to the energy meters. The flow of information and power in smart grids is bidirectional which is controlled with the help of software and supporting hardware. Optimized Network Engineering Tools (OPNET) Modeler is one of the most dominant simulation tools for the analysis of communication networks. In this paper, a number of models of dissimilar structured smart meter networks were developed with network parameters which were connected with different communication as wired and wireless in which order to compute database query, file transfer to server with respect to time where normal data transfer and DDoS attack to the network. Moreover, a security model that detects the DDoS attacks was mounted on AMI. The outcome of this paper provided a guideline to the future smart meter network developer so as to evade horrible challenges faced by some of the distribution companies. A scenario for the advanced metering infrastructure (AMI), which is one of the smart grid's application areas, was set up and the performance of the test bed was evaluated by implementing an able power management agent model. [1-5]

Keyword: Smart Grid OPNET, AMI, DDoS Attack

I. INTRODUCTION

The Institution of the smart grid, which is enables as an automatic and two-way communication between utilities and smart meters in AMI. It is a pioneering architecture. The empowered communications hardware, software, and its related data management systems networks can be defined as a network of smart meters, utilities, and authorized third-party operators, which can be metering data and other controls easy to evaluate information between these units. There are number of Smart meters are connected to the AMI network and can provide to the end user's with control over

Their energy consumption and also it can be making possible the integration of distributed energy resources. It comprises a covered communication network that is conscientious for the metering and billing of main household utilities such as electricity, water, and gas. [1, 2]

The AMI network includes three hierarchical layers: (i) home area network (HAN) or building area network (BAN), (ii) neighbourhood area network (NAN), and (iii) wide area network (WAN). Its operations are mainly reliant on the exploitation of smart meters. Its operations are mainly dependent on the use of smart meters. Smart meters are generally support in two way communications and it measure, store, and transmit energy consumption data to the AMI network and also make possible load control functionalities. The smart meters are located at customer site where such areas are typically considered as low trust environments. The Smart grid utilities are being able to perform some basis operational functions such as remote meter readings and leakage detections and other operations such as prepaid or time-of-use metering solutions. [1, 2,3, 4]

Beibei Li [3] et al represents the goal of an AMI is to offer the utility with near real-time power consumption data for pricing and billing purposes, and also allow customers to make informed choices about energy usage to improve energy competence and decrease energy budgets. Smart meters, the core intelligent electronic devices at the customer side in AMI, are capable of monitoring and precisely recording the energy usage data of the household appliances in real time bases.

The deployment of technologies such as the AMI as the electric power grid will elevate the responsibility of the grid and the cut costs of power delivery. AMI requires its assimilation with vital resources which make it a solemn target for cyber criminals with different spiteful intensions. Thus, cyber security solutions that will guard the entire AMI

against several attacks targeting its information infrastructures are not only pleasing but vital. [1, 2, 3]
Three main security objectives must be incorporated in the smart grid system: 1) Availability of uninterrupted power supply according to user requirements, 2) integrity of communicated information, and 3) confidentiality of user's data. [4]

J.T Agee et al [5], have questions about must be addressed in which order to the develop of general implementation and taking up of smart grid AMI concept include: (1) how can the other several intelligent electronic devices (IEDs) and the real-time data from smart meters that are crosswise the smart grid's AMI networks be managed wisely and powerfully ? (2) How can provide correct cyber security problems against different susceptibility attacks or cyber threats to targeting the AMI network which be designed and deployed at the proper places?

Bou-Harb et al [5, 6] considered this cyber terrorization as two categories: (a) connection-based (b) device-based threats or vulnerabilities. According to the study [6], the connection-based, attacks which are the protocols and use the vulnerabilities existing within the communication channel. Examples such as: jamming, eavesdropping, jamming and message injection or modification attacks. In the device-based attacks, it usually exploits flaws and vulnerabilities on the devices to perform malicious activities and they include such as: denial of service (DoS/DDoS), man-in-the-middle, and metering data tampering/falsification. The focus of this study is on mitigating the effect of distributed denial of service attack (DDoS) on an AMI network.

Section II contains an overview of DDoS attacks. Section III is progress of Smart Meter Network Using OPNET Modeler. Section IV has a brief review on related research works. In section IV as design methodology of the grid OpenFlow firewall is described. In Section V contains the simulation results and analysis. Finally section VI provides the conclusion for our study.

II. OVERVIEW OF DDOS ATTACK

Yonghe Guo et al [5, 7] , in distinction to the traditional DoS attack which uses a single source of attack, DDoS attack which is a single source of attack and it increase across several nodes thereby amplifying its harmful effect and making defence more complex. These attacks can downtime the networks for several hours, days or weeks via cyber criminals and these is the main weapon as attack for the cyber criminals for targeting to the any organizations or companies. Several times, DDoS attack in which this is avoid the traditional target web applications, application database of any organizations and network defenses. DDoS attacks is to do as trying behave as it is regular web traffic thus initiating requests and difficult to detected by traditional firewall and other network gateway securities to detect. The below diagram is for the conceptual model of distributed denial of service (DDoS) attack in AMI network was given in fig.1.

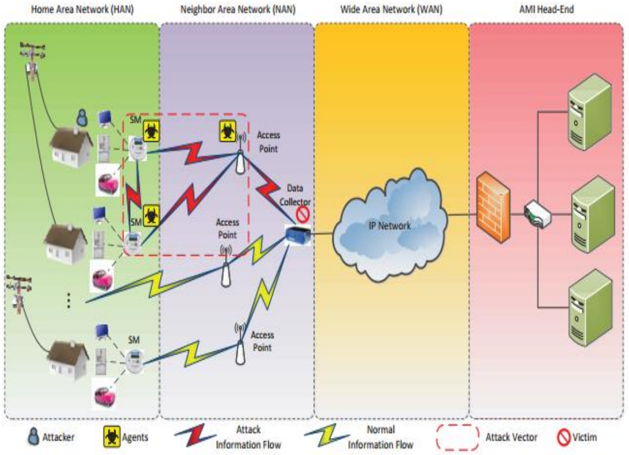

Figure 1: DDoS in AMI network [7]

A DDoS attack is basically initiated by an attack agent targeting to exploit system vulnerabilities that will affect the availability of network service and devices. According to the model, the attacker's main objective is to exhaust the bandwidth and processing power of its vulnerable victims which can be smart meters or other edge devices connected to the AMI network. The discovery of vulnerable devices is the first stage in launching a DDoS attack in AMI network. This stage is then followed by an attack stage. In an AMI network, three types of attack have been identified. They include: attacks targeting network protocols, attack on network infrastructures, and attacks on network bandwidth. [5, 6, 7]

III. DEVELOPMENT OF SMART METER NETWORK USING RIVERBED OPNET MODELER

The origin of OPNET Modeler and IT Guru products, which are getting the spotlight as the best communications and networks simulation solutions, can be trace back the network simulator carried forward as part of the project which was ordered by the Department of Defence to MIT in 1986 and have reached their present forms as a result of continuous efforts and studies by the participating developers. OPNET solutions have been used and verified over 20+ years, and with the established trust, they are expanding their scope of application to the areas of Network Capacity Planning, Network Engineering, Network Management, etc. OPNET Modeller provides robust platform to design and analyse systems and networks. It incorporates a lot of already-prepared simulation models of standard communication equipment and protocols for wired, radio and optical transmission mediums. To model a specific component rarely appearing in real network, the components are to be modelled using an object oriented approach. OPNET has been used to model smart meters and develop a smart meter network by deploying smart meters, Ethernet switches, routers, firewalls and servers. To model a smart meter network with OPNET, the works were divided into four parts—model design, applying statistics, run simulation and then view and analyze the results. If the results are not satisfactory, then the network has to be re-modelled and then new statistics applied. The basic work flow of OPNET can be seen in fig 2. [8, 9, 10]

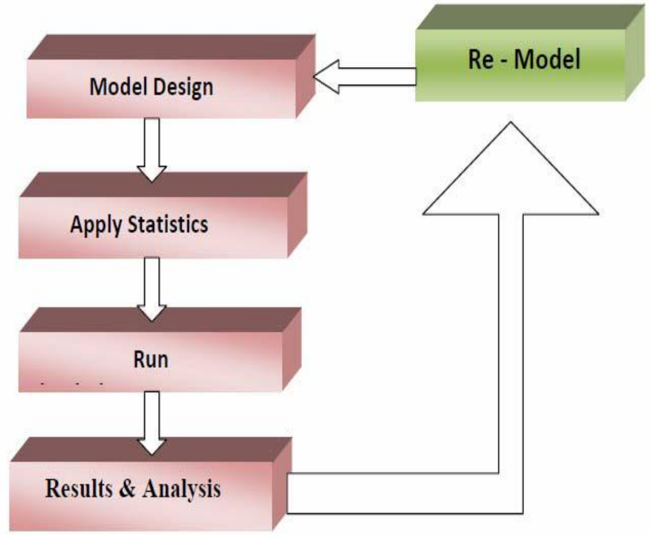

Figure 2.Workflow with OPNET [8]

IV. A DEVELOPMENT OF SMART METER NETWORK USING OPNET

A smart meter network is dependable for data access between smart meters and the server. The communication with meters needs the creation of topology to bond them with the server. To develop a appropriate model of a smart meter network, three different models were developed within OPNET environment to analyze network performances. The developed models based on OPNET have the capability to manufacture vast amounts of output data throughout simulations. The simulation models allow fast assessment of important recital measures such as network delay, database query response time and server utilization. Simulation sets were defined by selecting the network model by using required network entities, such as Application Configuration, Profile Configuration, Virtual Private Network Configuration (VPN), Server, Nodes to be executed and then specifying values for input parameters. Application Configuration: The applications, namely FTP (medium), FTP(low), HTTP(heavy browsing), HTTP (light browsing), Email(medium), Email(low), Database (medium) and Database(low) were adopted to specify the required applications in the simulation models of smart meter network. Profile Configuration: Eight profiles, namely FTP medium), FTP low), HTTP heavy browsing), HTTP light browsing), Email medium), Email low), Database medium), and Database low) are used to create user profiles and these profiles can be specified on different nodes in the network design to generate the application traffic. Virtual Private Network Configuration (VPN): VPN was arranged to offer a secure communication of information over the network. VPN increases packet latency by the addition of encryption and decryption, as well as wrapping and unwrapping packets at each end of the tunnel this has been specifically examined in this paper. Server: This is a WLAN server with applications over a protocol such as TCP/IP. In server, the supported services can be defined based on the user profiles that may support FTP (medium), FTP (low), HTTP (heavy browsing), HTTP (light browsing), Email (medium), Email (low), and Database (medium), Database (low) on the client.

Nodes: Nodes includes smart meters (two way communication devices), Ethernet switches, Ethernet hubs, routers, and firewalls running over TCP/IP protocol that support underlying WLAN connection. Apply statistics of smart meter network: Statistics that need to be applied for designed models are basically two types—global or scenario-wide statistics and object statistics. Global statistics could be collected from the de- signed network model and the object statistics could be accumulated over nodes [8, 9, 10, 11]

V. IMPLEMENTATION OF SMART METER NETWORK IN RIVERBED OPNET SIMULATOR

There are different cases with different scenarios were considered while analyzing the smart meter network as smart meters are wired and wireless connections with others networks elements as Nodes , Routers, Switches and Servers through Cloud environment.

Case1:- This case shows as wired connection system having different-different scenarios for different AMI network. Scenarios-1 as normal AMI network with 20 smart meters are connected as wired connections with network elements as Nodes, Routers and server and all connected with 100BaseT link through a cloud environment shows in figure 3. In which 10 smart meters are connected with a Switch and created an AMI network, in which multiple AMI networks are connected with a network connecting device as a Router and a router is connected to the Utility server through a cloud environment.

In this Scenario-2, there are number of AMI networks are connected to the utility server through a router and cloud environment and in this network, a malicious nodes tried to attack on utility centre. The attack is nothing but it is the DDoS attack in which it is jamming the whole system, shows in figure 4.

In this Scenario-3, we have to keep firewall for protecting the system from DDoS attack, shows in figure-5.

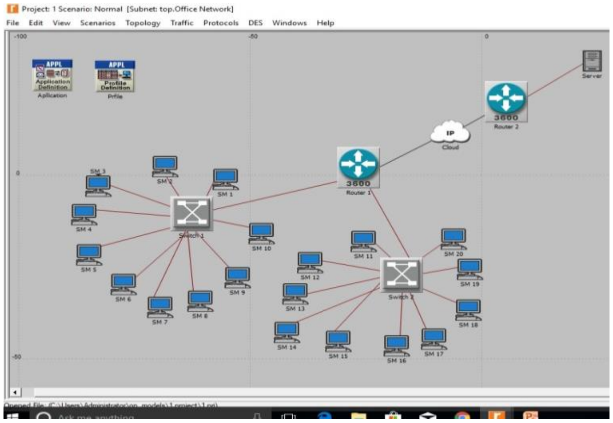

Figure 3. AMI network

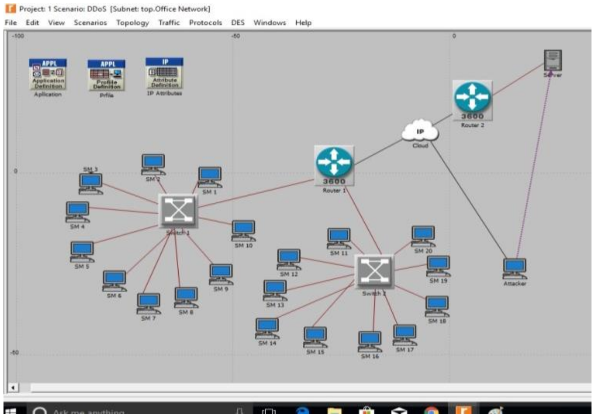

Figure 4. AMI network with DDoS Attack

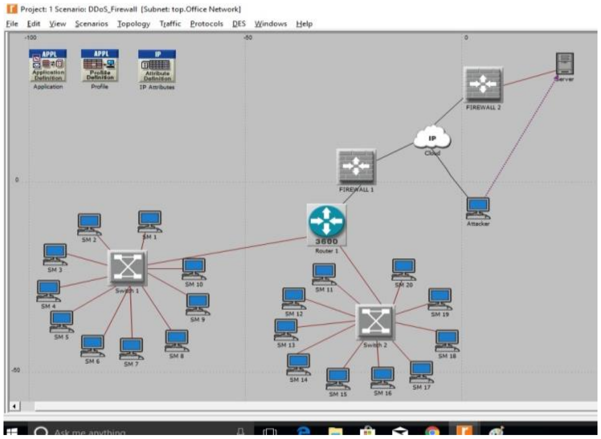

Figure 5. AMI network with Firewall

VI. RESULTS OF SMART METER NETWORK IN RIVERBED OPNET SIMULATOR

In this section, we have discussed about results for Riverbed Opnet Simulation as FTP, Database, and HTTP request to the server by any Smart Meter. From below figure are shows that the attacker attacks on to the system.

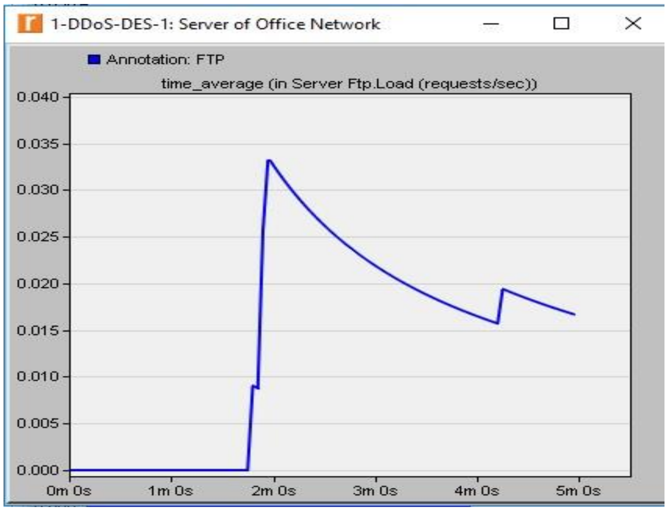

Figure 6. FTP request to server without Firewall

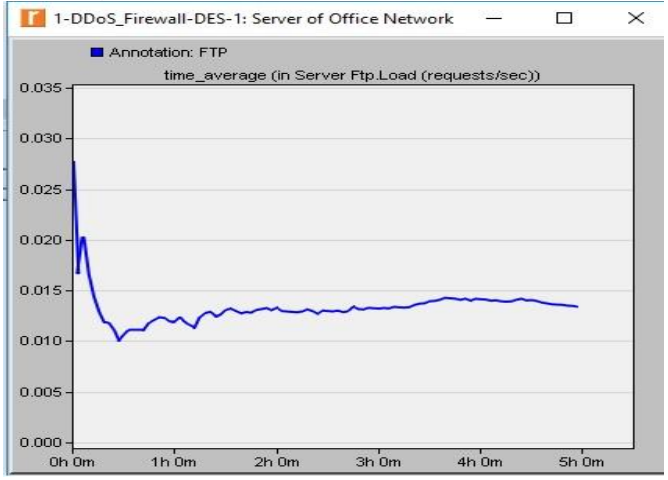

Figure 7. FTP request to server without Firewall

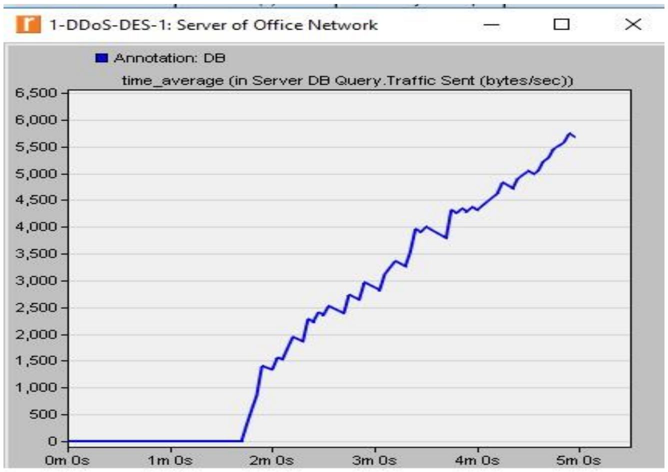

Figure 8. DB request to server without Firewall

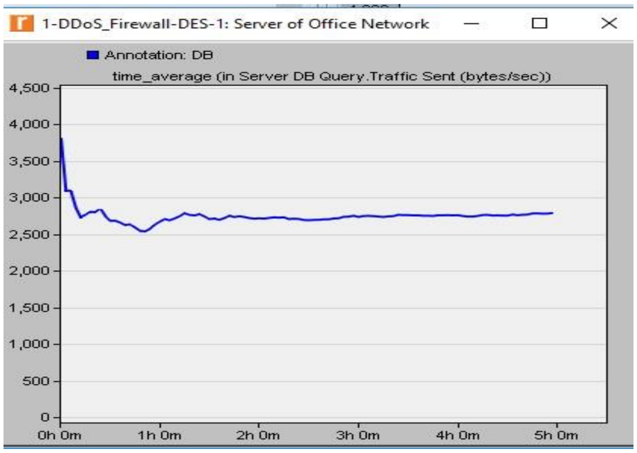

Figure 9. DB request to server with Firewall

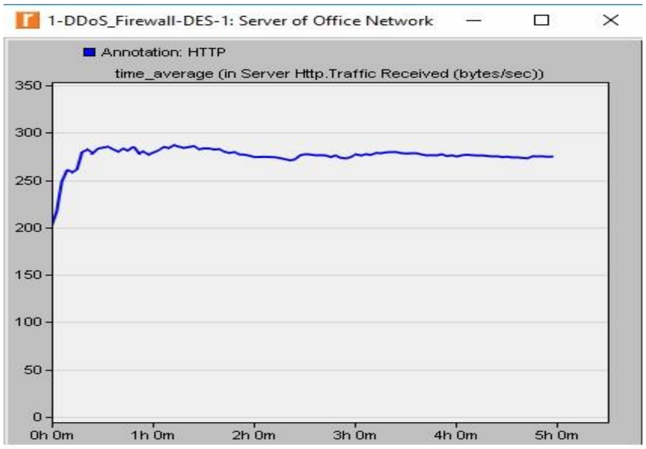

Figure 11. HTTP request to server with Firewall

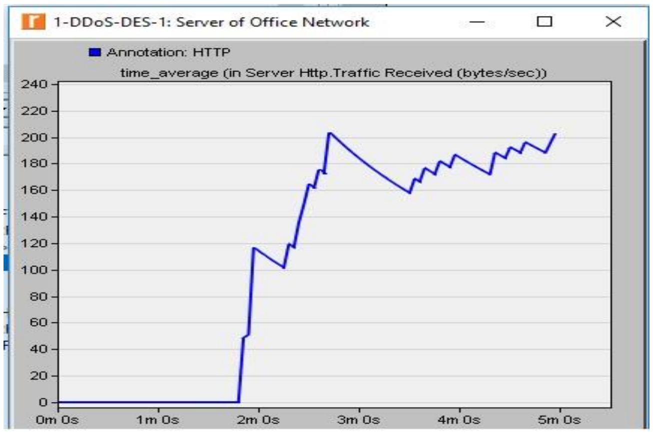

Figure 10. HTTP request to server without Firewall

VII. RESULT ANALYSIS

Table 1. Summary of simulation Average result without Firewall and With Firewall**.**

Different structured smart meter network	Database query request time in server		HTTP request received in server		FTP request response in server	
	Without Firewall (bytes/ sec) in 5 minute	With Firewall (bytes / sec) in 5 hour	Without Firewall (bytes / sec) in 5 minute	With Firewall (bytes/ sec) in 5 hour	Without Firewall (request / sec) in 5 minute	With Firewall (request / sec) in 5 hour
Smart meter network (as shown in **Figure 4 & 5**) consists of two LANs Network in which each LAN comprises of twelve smart meters and an Ethernet switch, routers, a server, a firewall and a cloud server	5500	2700	270	240	0.017	0.013

VIII. FUTURE WORK

Here we can use different cases with different scenarios were considered while analyzing the smart meter network as smart meters with wireless connections with others networks elements as Nodes , Routers, Switches and Servers through Cloud environment. Same as wired network, create a wireless AMI network with network connecting devices to connect with utility server through cloud environment. With the Riverbed Opnet Simulation, we can get the results for FTP, Database, and HTTP request to the server by any Smart Meter.

IX. CONCLUSION

Here with Riverbed Opnet modeler simulator was used to develop both smart meter and smart meter network models for AMI. Simulated with different scenarios were developed and the developed models can measure the performance of smart meter network accurately.

As discussed in the details of each case, the AMI network without Firewall and with Firewall smart meter network in a distribution system. From the simulations results are carried out as security is required in smart meter when transmit valuable information from devices to the utility centre as central server.
In this paper, we tried to develop a smart meter network model which can analyze for how providing security based on this research paper.

REFERENCES

[1]. R.C Diovu and J.T Agee " *Quantitative Analysis of Firewall Security under DDoS Attacks in Smart Grid AMI Networks*" 2017 IEEE 3rd International Conference on Electro-Technology for National Development pg no. 696-703

[2]. Md. Mahmud Hasan , Hussein T. Mouftah "Cloud-Centric Collaborative Security Service Placement for Advanced Metering Infrastructures" IEEE TRANSACTIONS ON SMART GRID 2017

[3]. Beibei Li, Rongxing Lu, and Gaoxi Xiao " HMM-Based Fast Detection of False Data Injections in Advanced Metering Infrastructure" 2017 IEEE

[4]. Tejaskumar Bhatt, Dr. Chetan Kotwal, Dr.Nirbhaykumar Chaubey "Survey on Smart Grid: Threats, Vulnerabilities and Security" IJEECS ISSN 2348-117X Volume 6, Issue 9 September 2017

[5]. C Diovu and J.T Agee "*A Cloud-Based Open flow Firewall For Mitigation Against DDoS Attacks In Smart Grid Ami Networks*" 2017 IEEE PES-IAS Power Africa pg no.28-33

[6]. E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication Security for Smart Grid Distribution Networks," IEEE Communication Magazine, vol. 51, no. 1, pp. 42-49, 2013.

[7]. Yonghe Guo, Chee-Wooi Ten, Shiyan Hu and Wayne W. Weaver, "*Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure*" Innovative Smart Grid Technologies Conference (ISGT) 2015 IEEE Power and Energy Society, pp. 1-5.

[8]. M. Rahman, Amanullah Mto "*Investigation of Bandwidth Requirement of Smart Meter Network Using OPNET Modeler"* Smart Grid and Renewable Energy, 2013, 4, 378-390

[9]. Opnet Modeler, OPNET Technologies Inc. http://www.opnet.com

[10]. Jun-Ho Huh , Seung-Mo Je , Kyungryong Seo "*Design and Simulation of Foundation Technology for Zigbee-based Smart Grid Home Network System using OPNET Simulation*" Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology Vol.5, No.4, August (2015), pp. 81-89

[11]. K. Brown and L. Christianson, "*OPNET Lab Manual to Accompany Business Data and Communications*," 2005

[12]. D. Bian, Y. Wu, "*Real-time Co-simulation Platform using OPAL-RT and OPNET for Analyzing Smart Grid Performance*" 2015 IEEE

[13]. Jun-Ho Huh, Kyungryong Seo "*Smart Grid Framework Test Bed Using OPNET and Power Line Communication"* 2016 IEEE DOI 10.1109/SCIS&ISIS.2016.192

About Authors

Tejaskumar P Bhatt, Assistant Professor Department of Computer Engineering.SVIT Vasad-388306,Gujarat. He has obtained his B.E.in Computer Engineering in 2007 ,Master degree in Computer Science and Engineering in 2013 . He has published 8 research Papers in peer reviwed internatinal Journals and conferences.his research area of interest is Smart Grid , Cloud Computing mobile Ad-hoc Network and wireless communication.

Chetan D. Kotwal, is a Professor at Department of Electrical Engineering, SVIT, Vasad, Gujarat, India. He received his B.E. and M.E. degrees from M.S. University of Baroda, Vadodara. He obtained his PhD. from Indian Institute of technology, Roorkee, India. His research interests are in Power Electronics applications to Power System, FACTS controllers and Power System Dynamics, Smart Grid, Swarm Intelligence, Cyber Physical Security, Cloud Computing. Email: chetan.kotwal@gmail.com, M – 9909006055.

Nirbhay Chaubey Associate Professor and Director, S.S. Agrawal Institute of Computer Science. Navsari affiliated to GTU Gujarat India Before joining as Associate Professor, he was working as an Assistant Professor and Head of MCA Department, at Institute of Science & Technology for Advanced Studies & Research (ISTAR), Vallabh Vidyanagar, Gujarat for about 12 years. He has completed his Ph.D. in Computer Science from Gujarat.
In computer science from Gujarat University, Ahmedabad in Year 2014. His research interest lie Protocol Design, QoS, Routing,
Mobility, and Security, cloud Computing and sensor network etc. and Security), Cloud Computing and Sensor Network etc

.