

Implementing and Examination of EIGRP OSPF RIP Routing protocol in AMI Network for DDoS attack using OPNET

Tejaskumar Bhatt, Chetan Kotwal, Nirbhaykumar Chaubey

Abstract: A Smart Grid is the advancement for power matrix with utilization of correspondence innovation with number of powerful meters which are interconnected and two-way data / information flows and has the main goals is to the active participants of consumers to improve quality and reliability of energy usage as for reducing energy consumption and provide increasing reliability as communication between smart meters and consumers. Basically, Smart Grid is working with distributed system manner, and create a network infrastructure as Advanced Metering Infrastructure (AMI) with number of different smart meter. This AMI network includes NAN (Neighbourhood Area Network), have connected with number of smart meters (as wired / wireless) connections with repeater / router as commonly name as Gateway collector which collects the all the consumers information's and send to the Utility centre. The flow of information as energy usages and power in smart grids is bidirectional which is controlled with the help of software and supporting hardware.

Here, with using of Optimized Network Engineering Tools (OPNET) Modeler is one of the most dominant simulation tools for the analysis of communication networks. In this paper, the number of smart meters is connected and create an AMI networks were developed with network parameters which related to different communication as wireless for the compute the different network parameters with respect to the time where data transfer and DDoS attack to the network. The security aspect as detect the DDoS attack to the AMI network and provide a guideline to the future of AMI network where escape strange challenges faced by Distribution companies. Here, in this paper the progressed metering foundation (AMI), which is one of the savvy framework's application regions where make a proving ground and arrangement in the OPNET for assessed the exhibition and power the board model for the framework.

Keyword: Smart Grid OPNET, AMI, DDoS Attack.

I. INTRODUCTION

The customary power frameworks have a few constraints for that its being moved up to turn into the Smart Grid framework. The savvy lattice framework is fundamentally coordination with custom power network framework with correspondence framework and it improved the different ways for overseeing and controlling various assets of the power framework for the executives and power stream. In the Smart Grid conveys the power between the shoppers and specialist organizations with two-way computerized innovation to control keen apparatuses at customers home or working to spare vitality,

lessen cost and increment dependability, proficiency and transparency.[1]

The Institution of the brilliant framework, which is empowers as a programmed and two-route correspondence among utilities and keen meters in AMI. The enabled correspondences equipment, programming, and its related information the executive's frameworks systems can be characterized as a system of shrewd meters, utilities, and approved outsider administrators, which can be metering information and different controls simple to assess data between these units. There are number of Smart meters are associated with the AMI organize and can furnish to the end client's with authority over their vitality utilization and furthermore it tends to make conceivable the incorporation of appropriated vitality assets. It has secured correspondence organize that is intensive for the metering and charging of principle family unit utilities, for example, power, water, and gas. [2, 3]

The AMI system incorporates three progressive layers: (I) home territory organize (HAN) or building region arrange (BAN), (ii) Neighborhood region organize (NAN), and (iii) wide region organize (WAN). Its tasks are basically dependent on the abuse of shrewd meters. Its tasks are primarily subject to the utilization of savvy meters. Brilliant meters are by and large help in two manner correspondences and it measure, store, and transmit vitality utilization information to the AMI system and furthermore make conceivable burden control functionalities. The savvy meters are situated at client site where such regions are normally considered as low trust conditions. The There are some utilities being perform for Smart grid as 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 [4] et al speaks to the goal of an AMI is to offer the utility with near steady power use data for esteeming and charging purposes and empower customers to pick or instructed choices going to improve and decrease imperativeness spending plans. Splendid meters, the middle insightful electronic contraptions at the customer side in AMI, are fit for checking and completely recording the imperativeness use data of the family mechanical assemblies ceaselessly bases.. The organization of innovations, for example, the AMI as the electric power network will host the obligation of the lattice and the cut expenses of intensity conveyance. AMI requires its digestion with indispensable assets which make it a grave objective for digital hoodlums with various angry intensions. [2,3,4] J.T Agee et al [5], have inquiries regarding must be

Revised Version Manuscript Received on 16 September, 2019.

* Correspondence Author

Tejaskumar Bhatt¹, Chetan Kotwal², Nirbhaykumar Chaubey³

S.V.I.T. VASAD, GUJARAT1,

2, U.V.Patel,GV, GUJARAT3

tended to in which request to the create of general execution and taking up of shrewd lattice AMI idea include:

(1) in what manner can the other a few savvy electronic gadgets (IEDs) and the continuous information from keen meters that are across the brilliant matrix's AMI systems be overseen carefully and intensely ? (2) How can give right digital security issues against various powerlessness assaults or digital dangers to focusing on the AMI organize which be structured and sent at the best possible spots?

Bou-Harb et al [6,7] considered the two different of categories for cyber-attack as (a) connection-based (b) device-based threats or vulnerabilities.

There are various sorts of digital assault conceivable to brilliant lattice framework as sticking, listening in, sticking and message infusion or adjustment assaults. In the gadget-based assaults, it more often than not adventures imperfections and vulnerabilities on the gadgets to perform malignant exercises and they incorporate, for example, renouncing of organization (DoS/DDoS), man-in-the-middle, and metering data changing/corruption. The point of convergence of this examination is on mitigating the effect of passed on refusal of organization surprise attack (DDoS) on an AMI sort out.

Segment II contains an outline of DDoS assaults. Area III is progress of Smart Meter Network Using OPNET Modeler. Segment IV has appeared on related research works. In area IV as structure procedure for the routing protocol is depicted. In Section V which is contains the regeneration outcomes and examination. At long last area VI gives the end to our examination.

II. OVERVIEW OF DDOS ATTACK

The new assault called a DDoS assault, which is brings about refusal of administration in AMI organize. In this DDoS assault is the assailant initially chooses at least one ordinary hub as injured individual hub. At that point the assailant conveys flooding the information parcels, which contain explicit assault data to these injured individual hubs. At the point when the unfortunate casualty hubs get these assault bundles, they create a high volume of course parcels. The quantity of course bundles will deplete system block and correspondence transmission capacity.

DDoS assaults, for example, rejection of administration or disseminated refusal of administration (DDoS/DoS) will compromise the accessibility of metering information, consequently, undermining the smooth tasks of AMI back-end frameworks answerable for charging and other lattice control activities. In such condition, request side administration will be profoundly blocked and lattice activities like power quality checking would be truly hampered. The keen framework AMI might be focused with DDoS assaults, for example, TCP SYN flooding, UDP flooding assaults or a malignant intension to disorder the system steering table so as to influence the bundle conveyance achievement of the system [1,2,3,4]. What's more, the digital aggressor focusing on the AMI system can soak the accessible system data transfer capacity with volumetric traffic to such an extent that almost no assets will be left to administration demands from genuine system clients.

Yonghe Guo et al [6,8], Distributed Denial of Service attack which is a solitary wellspring of attack and it increment over a few hubs in this way enhancing its destructive impact and making resistance increasingly mind boggling. These assaults can vacation the systems for a few hours, days or weeks by means of digital crooks and these is the fundamental weapon as assault for the digital offenders for focusing to the any associations or organizations. A few times, DDoS assault in which this is maintain a strategic distance from the customary objective web applications, application database of any associations and system guards. DDoS assaults is to do as difficult carry on as it is ordinary web traffic in this manner starting solicitations and hard to identified by customary firewall and other system portal protections to distinguish. The underneath outline is for the calculated model of conveyed refusal of administration attack in AMI system shown in fig.1.

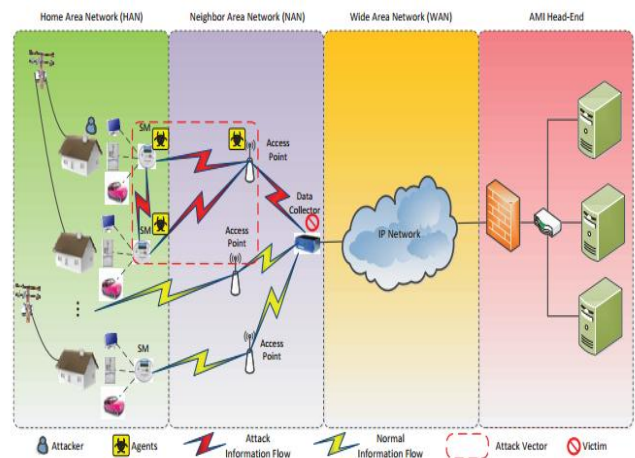


Figure 1: AMI network with Attck and Firewall [8]

A DDoS assault is essentially started by an assault specialist focusing to misuse framework vulnerabilities that will influence the accessibility of system administration and gadgets. According to the model, the attacker's major objective is to incapacitate the exchange speed and planning force of its unprotected abused individuals which can be splendid meters or other edge contraptions related with the AMI compose. The exposure of defenceless contraptions is the essential stage in impelling a DDoS attack in AMI arrange. This stage is then trailed by an attack arrange. In an AMI organize, there are three sorts of assault have been recognized which are assaults focusing on system conventions, assault on system foundations, and assaults on system data transfer capacity.

III. OVERVIEW ABOUT RIVERBED OPNET MODELER FOR AMI NETWORK IN SMART GRID

The reason for OPNET Modeler and IT Guru things, which are getting the spotlight as the best correspondences and frameworks multiplication courses of action, can be pursue back the framework test framework passed on forward as a segment of the endeavour which was mentioned by the Department of Défense to MIT in 1986 and have landed at their present structures in view of relentless undertakings and thinks by the sharing fashioners. OPNET courses of

action have been used and affirmed over 20+ years, and with the developed trust, they are stretching out their degree of utilization to the zones of Network Capacity Planning, Network Engineering, Network Management, etc. OPNET Modeler gives generous stage to structure and separate structures and frameworks.

To show a specific section every so often appearing in veritable framework, the portions are to be exhibited using a thing arranged technique. OPNET has been used to show sharp meters and develop a splendid meter orchestrate by passing on wise meters, Ethernet switches, switches, firewalls and servers. To show an adroit meter organize with OPNET, the works were segregated into four areas—model structure, applying bits of knowledge, run modernisation and a while later observe and research the results. In case the results are not tasteful, by then the net-work must be re-shown and subsequently new bits of knowledge applied. The fundamental work stream of OPNET can be found in fig 2. [9, 10,11]

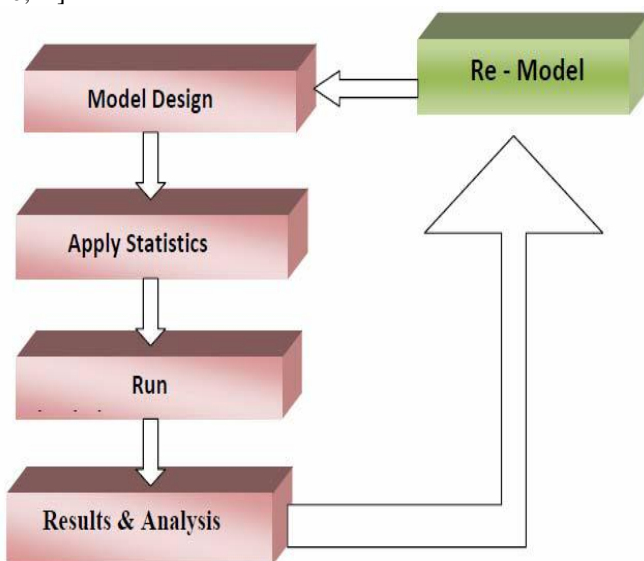


Figure 2. Workflow with OPNET [9]

A smart meter framework is reliable for data access between shrewd meters and the server. The correspondence with meters needs the creation of topology to bond them with the server. To develop a fitting model of a clever meter, compose, three one of a kind models were made inside OPNET condition to separate framework displays. The created models dependent on OPNET have the ability to make immense measures of yield information all through recreations. The renovation models permit quick appraisal of significant presentation estimates, for example, arrange delay, database inquiry reaction time and server use. Recreation sets were characterized by choosing the system model by utilizing required system substances, for example, Application Configuration, Profile Configuration, Virtual Private Network Configuration (VPN), Server, Nodes to be executed and after that determining qualities for info parameters.

Here, nodes are joins as smart meters (two-way communication), Ethernet switches, Ethernet concentration, switches, and other network connecting devices with firewalls are execute over the IP, it shows that help fundamental WLAN affiliation. The estimations for the sagacious meter mastermind which find out the Statistics must be applied for organized models are on a very basic level two sorts—worldwide or circumstance wide experiences and article bits of knowledge. Overall experiences could be

accumulated from the de-checked framework model and the thing estimations could be amassed over centre points [8, 9, 10, 11]

IV. RESEARCH METHODOLOGY

Here, in a Smart meter network arrange structure, the data is transmission subject to the different coordinating show which are picks the best courses between two centre points/devices. In smart meter network organize the Routing conventions are significant components for the courses the information in present day correspondence Networks. There are various sorts of steering conventions are fundamentally applied for the particular system condition for transmission the information. The Routing conventions are essentially founded on steering calculations, which are depend on various measurements as cost, transfer speed, bundle deferral and jump tally to locate the best way to transmit information crosswise over systems. Various kinds of steering convention are as some Routing Protocol The decision of the privilege steering convention relies upon various parameters with utilization of the riverbed OPNET simulation to break down the exhibition of Routing Protocol conventions, which are carried in TCP/IP systems. For every convention, we structured distinctive reproduction situations and get the outcome as in the terms of system with gathered, looked at, and dissected renovation for various parameters as combination, steering traffic, Ethernet delay, video conferencing, bundle start to finish postponement, and voice parcel delay. [12,13]

I. Routing Information Protocol (RIP)

RIP is an institutionalized separation vector dynamic steering convention which is utilized and utilizes for the separation jump consider a directing measurement. RIP is essentially actualized on the UDP as its vehicle convention. It has constraining the quantity of jumps checks between the source and goals who permitted in its ways. RIP is anticipating the steering circles by actualizing a set number of bounces between source to goal who permitted to its ways. RIP has allocated the held port number 520. RIP is permitted the greatest number of allowed bounces as 15, past from that, the course will be considered as inaccessible. RIP has constrained the size of system with effective little system and chooses the ways with littlest bounce includes and furthermore slowest in the system. Be that as it may, RIP might be wasteful in bigger systems with burst traffic. Each RIP switch communicates to different switches the best way dependent on its 2 computation. Every switch refreshes its own directing table by speaking with neighbouring switches. It switches transmits full updates like clockwork RIP has lower control utilization and memory than some other directing conventions. [13, 14, 15,16]

II. OSPF: Open Shortest Path First

It is a directing convention which practices a connection state-run steering calculation that works inside a solitary Autonomous System. OSPF is characterized as variant 2 in RFC 2328 which used to enable switches to progressively



courses to different courses. OSPF is fundamentally courses with promotions containing courses are alluded to as connection state commercials and keep track the track in a smart meter arrange structure, the data is transmission subject to the different coordinating show which are picks the best courses between two centre points/devices. In this protocol switch is supplies the nearby system association state-run with LSA and publicizes to the whole Autonomous System. At the point when another switch is further to the system, it will communicate as hello communications to each neighbour and get the input hi communications from its neighbours. At end of, the switches who set up the associations with the new included switch and furthermore synchronize their steering databases. Each switch communicates connection state update message when system topology changes. Here, every one of the switches might spare a similar data of system topology. Along these lines, each switch in the system who ascertains the best ways to all goals and shows the storage room switch for every transmission. [13, 14, 15,16]

III. Enhanced Interior Gateway Routing Protocol (EIGRP)

The EIGRP or Enhanced IGRP is a Cisco restrictive directing convention which is essentially used for the figure another course calculation called as the DUAL as Diffusing Update Algorithm. It is a half breed convention which has highlights for both of detachment vector and association state shows. It is utilized in TCP/IP and OSI webs. EIGRP are based for Delay, Load, Bandwidth and on unwavering quality and furthermore computing the essential parameters and furthermore gathers information from three tables as the neighbour’s table, topology table and steering table. In this EIGRP, the information about neighbour’s switches that are straightforwardly available through interface that are associated and furthermore the directing tables which are contains the collection of the steering tables that are assembled from every single other neighbour and furthermore the steering table stores the real courses to every one of the goals. EIGRP varies from most separation vector conventions since it doesn’t depend on intermittent course dumps. Subsequently, it is fit for keeping up its topology table. Information that will be guided is potentially exchanged when the new neighbours’ adjacencies is set up. It switches keeps up its own one of a kind coordinating table and tables of its neighbours. It switches imparts to various neighbours if it can’t discover a switch subject to its coordinating database. [13, 14, 15,16]

Here, we utilized the Riverbed OPNET Modeler adaptation for the system reproductions. The OPNET is a thorough system reproduction device with a large number of amazing capacities. It empowers recreation of heterogeneous systems by utilizing the different conventions. In this framework, right off the bat rebuilt system utilizes the OSPF directing and a similar model is then used to mimic EIGRP and the OSPF steering convention. There are various situations with number of AMI system were considered while breaking down the keen meter arrange as brilliant meters as remote associations with passageway which is associated with switch with wired associations where switch is associated with switch and the switch is associated with the server through cloud condition for various directing convention as RIP, OSPF and EIGRP.

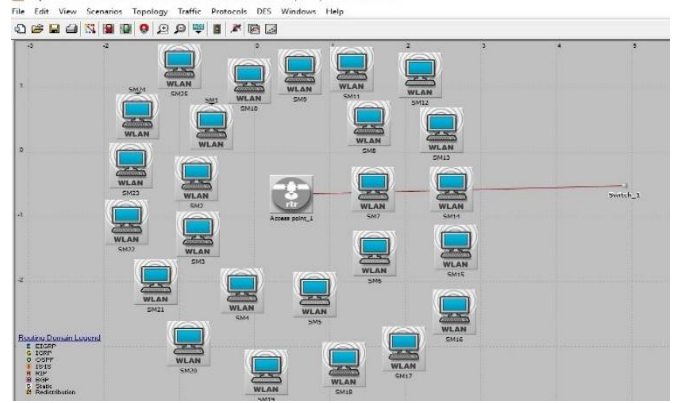


Figure 3. Smart Meter network

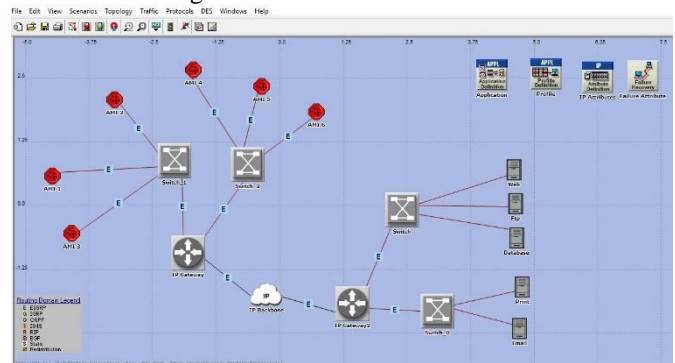


Figure 4. AMI network with EIGRP

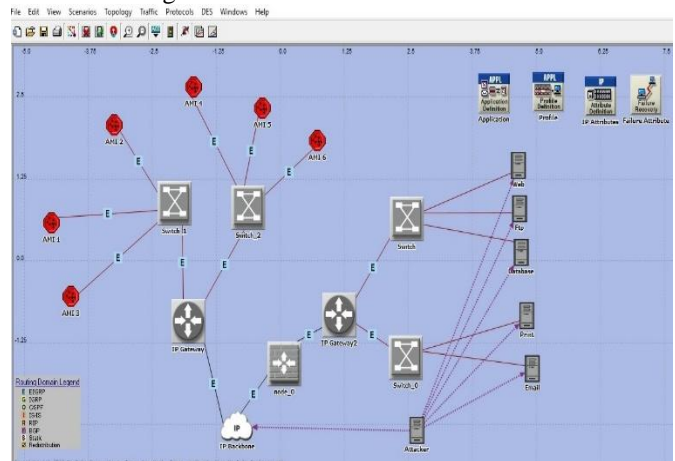


Figure 5. AMI network with EIGRP with Firewall

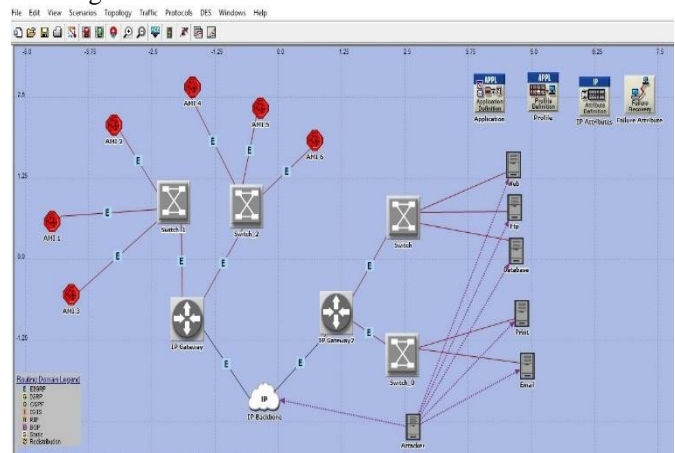


Figure 6. AMI network EIGRP with attacker with Firewall

Here, above Figures as 3 to 6 speaks to as, there are number of shrewd meters which are associated with one of the passageways which is made as AMI system and this passageway is associated with switch with wired association and it is associated with the server through one of the switches in cloud condition. Here in the system, there are number of AMI systems with various directing convention as RIP OSPF and EIGRP with aggressor and with firewall.

V. RESULTS OF SMART METER NETWORK IN RIVERBED OPNET SIMULATOR

We have fragmented down the exhibition of different steering conventions naming RIP, OSPF and EIGRP over an assailant situation and aggressor with firewall situation with comprising of slip8_gateway switches switch, remote hubs, passage in cloud condition on reproducing the system we got the accompanying outcomes for best exertion traffic which are appeared underneath in figures which shows cost of transmission between two switches for various conventions. We likewise have fragmented down overhead on switches and by and large execution as far as Delay, throughput, lining postponement and use and throughput figures 7-18 show the results obtained.

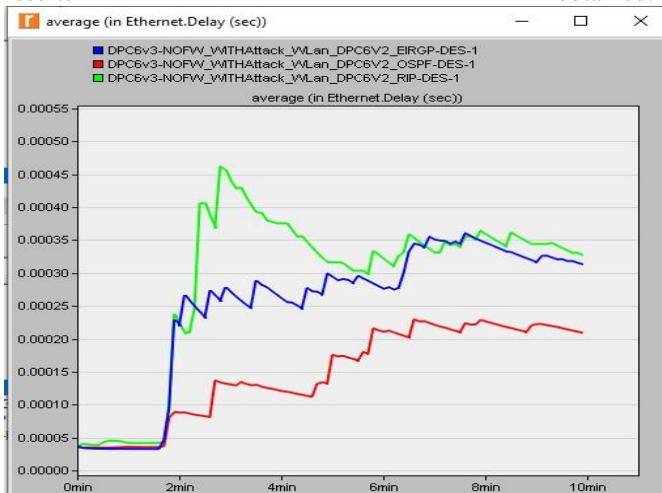


Figure 7. Delay without firewall with Attack

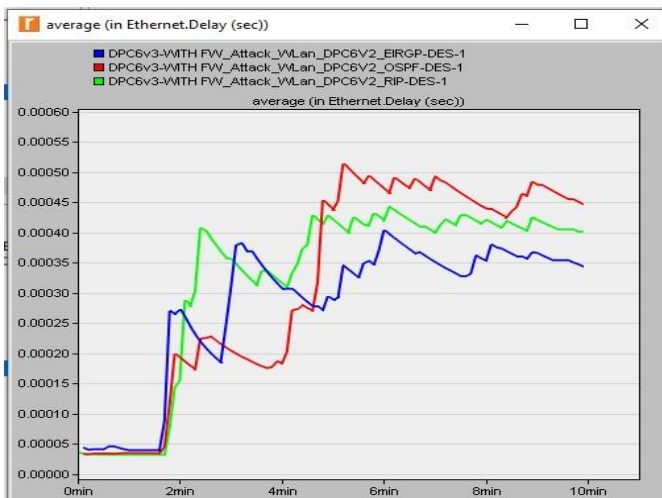


Figure 8. Delay with firewall with Attack

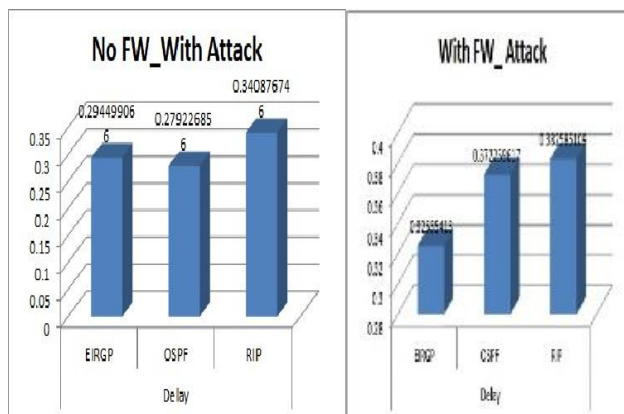


Figure 9. Delay without firewall with attack and with firewall with attack

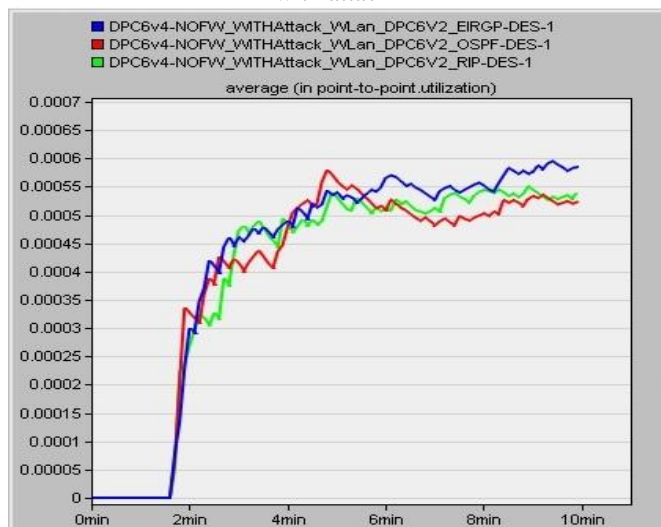


Figure 10. Utilization without firewall with attack

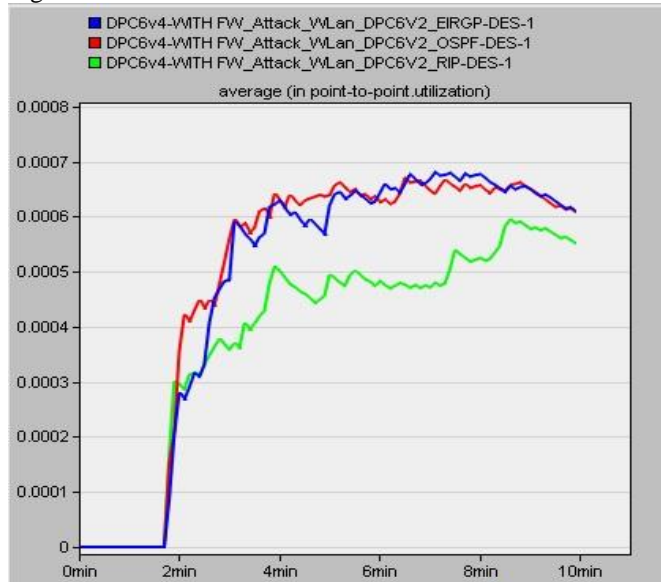


Figure 11. Utilization with firewall with attack

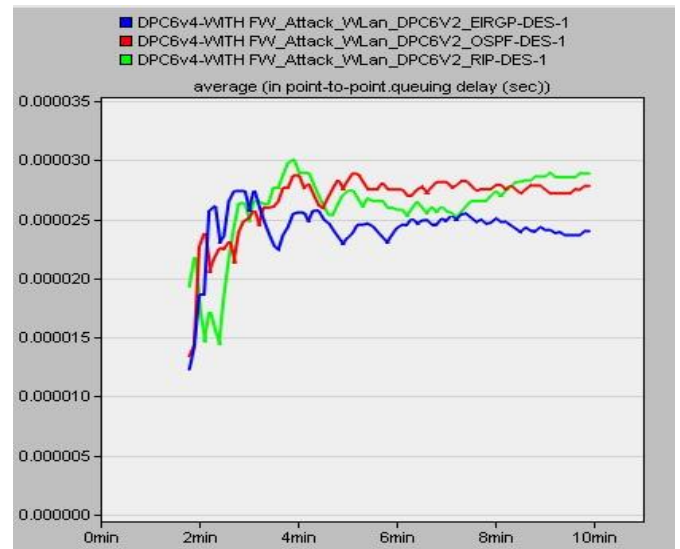
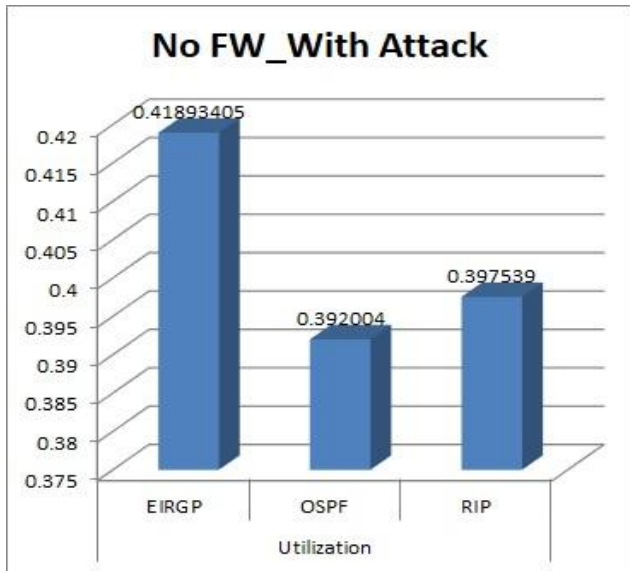


Figure 14. Queuing Delay with firewall with attack

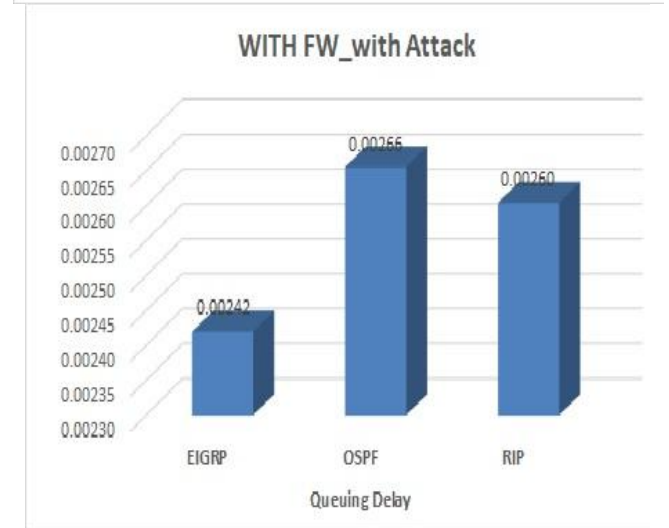
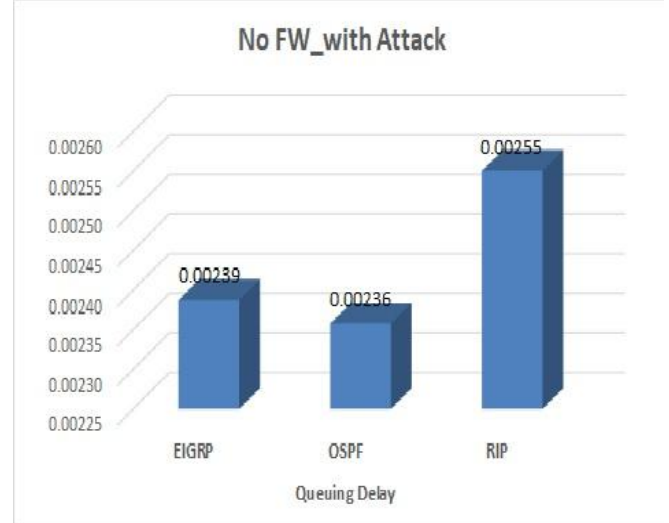
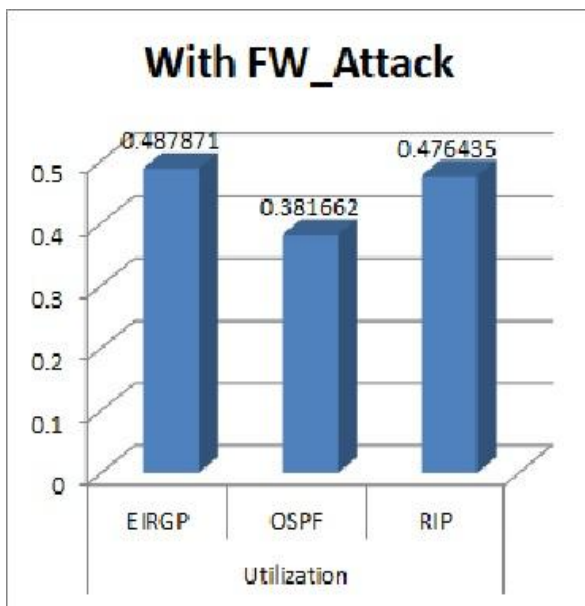


Figure 15. Queuing Delay with without firewall with attack and with firewall with attack

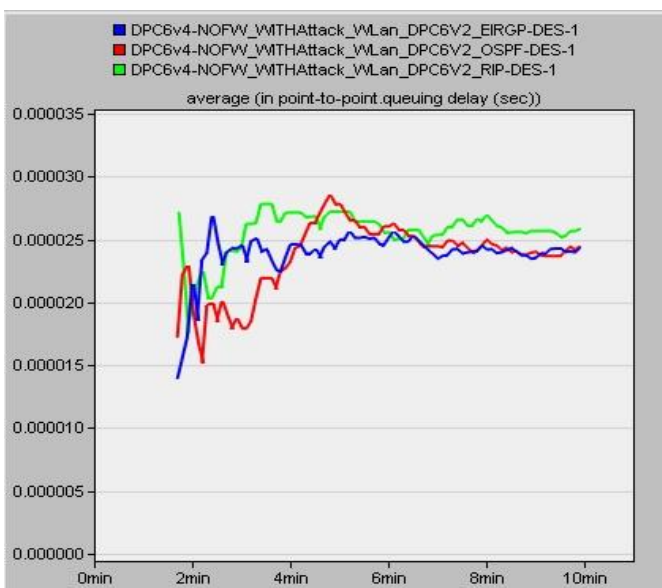


Figure 13. Queuing Delay without firewall with attack

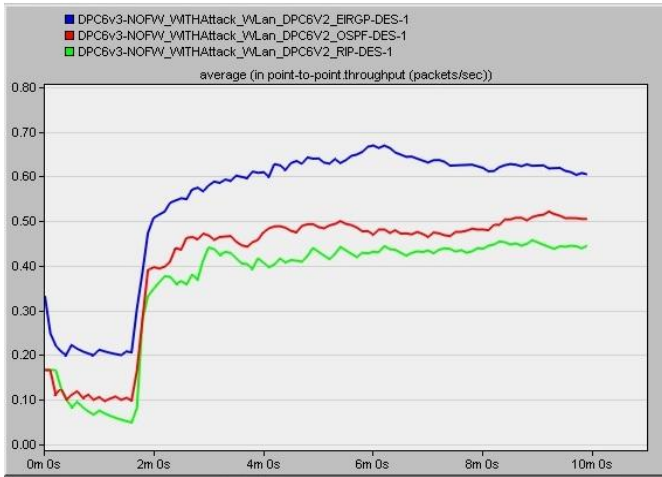


Figure 16. Throughput without firewall with attack

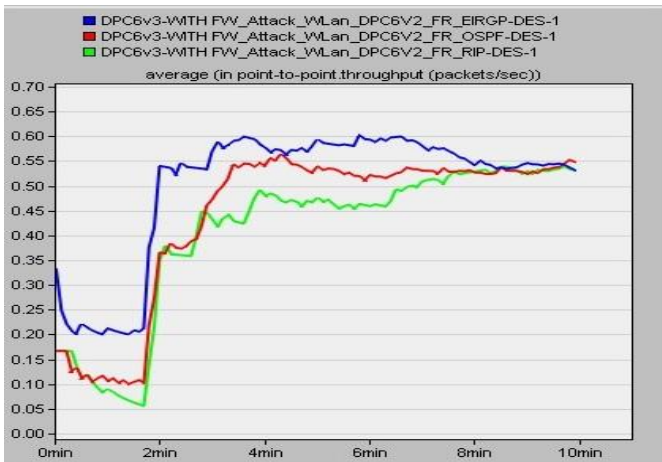


Figure 17. Throughput with firewall with attack

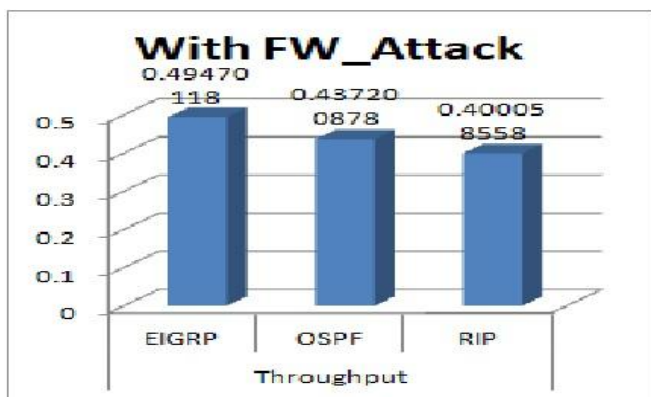
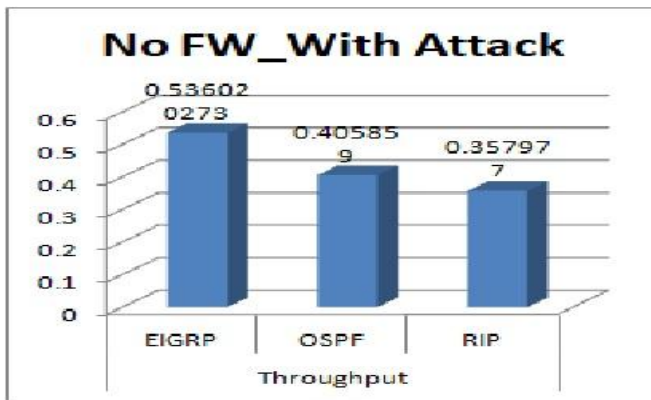


Figure 18. Throughput with without firewall with attack and with firewall with attack

According to the underneath table and contrast and others conventions and dissecting the consequence of the exhibition of different steering conventions naming RIP, OSPF, and EIGRP over a situation for the Delay, Utilization, throughput and lining Delay with no firewall with assault and with firewall and assault cost of transmission, switch overhead, throughput, connect usage and lining postpone we can say that EIGRP has best execution generally speaking as it has minimal expense of transmission(as Delay), lower switch overhead than RIP and OSPF and most extreme throughput among all directing convention and lining deferral of it is least than OSPF and RIP and it likewise has most noteworthy connection use than OSPF and RIP. Thus, at long last EIGRP is performs great as it has cost of transmission and has ideal switch overhead and by and large execution as far as throughput, Queuing deferral and connection usage over the OSPF RIP. Thus, for best exertion administration that is transmission of information parcels EIGRP performs superior to different conventions for throughput, lining deferral, usage and overhead.

VI. RESULT ANALYSIS

Network Parameters	Protocols	No FW_With Attack	With FW_Attack
Delay	EIRGP	0.294	0.325
	OSPF	0.279	0.372
	RIP	0.341	0.383
Throughput	EIGRP	0.495	0.536
	OSPF	0.437	0.406
	RIP	0.400	0.358
Utilization	EIRGP	0.419	0.382
	OSPF	0.392	0.488
	RIP	0.398	0.476
Network Convergence	EIRGP	0.489	0.575
	OSPF	10.949	11.638
	RIP	1.287	1.614
Queuing Delay	EIRGP	0.00239	0.00242
	OSPF	0.00236	0.00266
	RIP	0.00255	0.00260

EIGRP>OSPF>RIP



VII. CONCLUSION

Here, researched the introduction of three critical sorts of coordinating shows: RIP, OSPF and EIGRP using OPNET. Three novel topologies had been developed and the modernisation of each directing show in all of the three topologies had been performed. Here, it shows that EIGRP differentiated and OSPF and RIP show and it find as EIGRP show is better than OSPF and RIP with respect to Delay, throughput, Network Utilization, Network mix range and coating delay EIGRP using cross breed in the introduction, associate state requires to guide out the whole framework close to the beginning In which, EIGRP has the features of both association state and partition vector show thus gives improved memory and CPU use. It doesn't require a different levelled framework arrangement to work adequately and has progressively significant control on timing issues. EIGRP is logically unfaltering and unsurprising in both little and for the most part colossal frameworks.

REFERENCES

1. Ping Yi, Ting Zhu, Qingquan Zhan, Yue Wu, Jianhua Li "A Denial of Service Attack in Advanced Metering Infrastructure Network" IEEE ICC 2014 pg. No. 1029-1034
2. 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
3. Md. Mahmud Hasan, Hussein T. Mouftah "Cloud-Centric Collaborative Security Service Placement for Advanced Metering Infrastructures" IEEE TRANSACTIONS ON SMART GRID 2017
4. Beibei Li, Rongxing Lu, and Gaoxi Xiao "HMM-Based Fast Detection of False Data Injections in Advanced Metering Infrastructure" 2017 IEEE
5. Tejaskumar Bhatt, Dr. Chetan Kotwal, Dr. Nirbhaykumar Chaubey "Survey on Smart Grid: Threats, Vulnerabilities and Security" IJECS ISSN 2348-117X Volume 6, Issue 9 September 2017
6. 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
7. 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.
8. Yonghe Guo, Chee-Wooi Ten, Shiyuan 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.
9. M. Rahman, Amanullah Mto "Investigation of Bandwidth Requirement of Smart Meter Network Using OPNET Modeler" Smart Grid and Renewable Energy, 2013, 4, 378-390
10. Opnet Modeler, OPNET Technologies Inc. <http://www.opnet.com>
11. 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
12. Tejaskumar Bhatt, Dr. Chetan Kotwal, Dr. Nirbhaykumar Chaubey "Implementing AMI network using Riverbed OPNET Modeler for DDoS attack" International Journal Computer Science and Engineering volume-7 Issue 2 February 2019
13. Don Xu and Ljiljana Trajković "Performance Analysis of RIP, EIGRP, and OSPF using OPNET"
14. Syed Yasir Jalali, Sufyan Wani and Majid Derwesh "Qualitative Analysis and Performance Evaluation of RIP, IGRP, OSPF and EGRP Using OPNET" Advance in Electronic and Electric Engineering ISSN 2231-1297, Volume 4, Number 4 (2014), pp. 389-396
15. Anjali gupta Aditi Sharma Prabhjot kaur Pankaj Rakheja "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network" International Journal of Computer Applications (0975 – 888) Volume 48– No.18, June 2012
16. Shah.A, Waqas J. Rana "Performance Analysis of RIP and OSPF in Network Using OPNET" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013
17. K. Brown and L. Christianson, "OPNET Lab Manual to Accompany Business Data and Communications," 2005
18. D. Bian, Y. Wu, "Real-time Co-simulation Platform using OPAL-RT and OPNET for Analyzing Smart Grid Performance" 2015 IEEE
19. 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.