Packet Analysis of DNP3 Protocol over TCP/IP at an Electrical Substation Grid Modelled in OPNET.

Dion Njova
Department of Electrical and Mining Engineering
University of South Africa
Johannesburg, South Africa
53113934@mylife.unisa.ac.za

Kingsley Ogudo
Department of Electrical & Electronics Engineering, Faculty of Engineering and the Built Environment
University of Johannesburg
Johannesburg, South Africa
kingsley@uj.ac.za

Patrice Umenne
Department of Electrical and Mining Engineering
University of South Africa
Johannesburg, South Africa
umennpo@unisa.ac.za

***Abstract*- In this paper Intelligent Electronic Devices (IED) that use ethernet for communicating with substation devices on the grid where modelled in OPNET. There is a need to test the communication protocol performance over the network. A model for the substation communication network was implemented in OPNET. This was done for ESKOM, which is the electrical power generation and distribution authority in South Africa. The substation communication model consists of 10 ethernet nodes which simulate protection Intelligent Electronic Devices (IEDs), 13 ethernet switches, a server which simulates the substation Remote Terminal Unit (RTU) and the DNP3 Protocol over TCP/IP simulated on the model. DNP3 is a protocol that can be used in a power utility computer network to provide communication service for the grid components. It was selected as the communication protocol because it is widely used in the energy sector in South Africa. The network load and packet delay parameters were sampled when 10%, 50%, 90% and 100% of devices are online. Analysis of the results showed that with an increase in number of nodes there was an increase in packet delay as well as the network load. The load on the network should be taken into consideration when designing a substation communication network that requires a quick response such as a smart gird.**

Keywords—Distributed Network Protocol (DNP3), Intelligent Electronic Devices (IED's), Network load, Packet delay, Substation Network Model.

I. INTRODUCTION

DNP3 is a data acquisition protocol used in the electric utility industry. It is an open [1], interoperable protocol used specifically in the Supervisory Control and Data Acquisition (SCADA) systems [2]. The Distributed Network Protocol (DNP) was originally created by Westronic, Inc. in 1993 for the power industry. It uses three layers of the OSI model: the application layer, data link layer and physical layer. The physical layer can be used with a serial communication channel such as RS-232, as well as fiber. The main aim of this paper is to model a substation communication network, apply the DNP3 protocol and analyze its performance.

DNP3 allows expansion and evolution without compromising reliability and interoperability of the protocol as it follows an object-oriented approach. DNP3 can be modelled by using the ns-2 network simulation tool as was done in [3]. DNP3 uses three layers of the OSI model: the application layer, data link layer and physical layer. The structure of DNP3 is shown in [4]. DNP3 in a network environment involves encapsulation of data frames from the data link layer within the transport layer. In [5] an Automatic Circuit Recloser (ACRs) is used to combine communications via serial ports, one port is used for SCADA DNP3 the other for engineering access connections. The building of a DNP3 message begins at the application layer all the way to the link layer. The DNP3 data link layer frame, which has a size of 292 bytes, is encapsulated unto a TCP segment. The TCP segment is 556 bytes long. The TCP/IP packet has source and destination IP address for inclusion. There are 20 bytes for the IP header and 20 bytes for the TCP. The payload is about 1460 bytes the details of which are given in [6]. The DNP3 protocol is modelled in [6] using ns-2 software, while in this paper we carry out the modelling of DNP3 in a substation grid using OPNET.

A split protocol design can be used to increase the speed response time for DNP3 devices as shown in [7]. The split protocol can be implemented in a utility network with high traffic. In [8] protocols from SCADA systems such as DNP3 are migrated to a smart grid protocol design.

An automatic network protection framework for DNP3 over TCP/IP is presented in [9]. Their system is capable of detecting old and new attacks.

The Constrain Application Protocol (CoAP) which is a web transfer protocol is combined with DNP3 for Machine-to-Machine (M2M) communication to be achieved in a smart grid, this is reported in [10]. CoAP can increase interoperability in a SCADA system.

An evaluation of the DNP3 performance in an IEEE 802.11g wireless ad hoc network, encapsulated in TCP/IP is done in [11]. Results show there that DNP3 is useful for low cost smart grid applications.

In [12] we see a communication system that multiplexes DNP3 traffic. This happens because several Master Terminal Units (MTUs) use the same Remote Terminal Units (RTUs). This is done to ensure that master stations can share access to the same network of remote terminal units prior to commissioning. OPNET [13] can be used to simulate and model DNP3 in a smart grid.

The introduction in section 1 discusses literature review and introduces the concept, section 2 contains the methodology, this gives details on the simulation and modelling in OPNET, in section 3 the results are analyzed and discussed and finally section 4 gives the conclusion.

II. METHODOLOGY

A. Substation Communication Network Model

The substation communication network model in Fig. 1 consists of 10 nodes that represent protection IED, 10 ethernet based switches that simulate protection IED switches, two backbone switches, one gateway switch and one substation Remote Terminal Unit (RTU) server . The link between the protection IED and an IED switch is connected with a 100BaseT cable. The link between the IED switch, backbone switch, gateway switch and substation RTU is 1000BaseX. A server simulates the substation RTU.

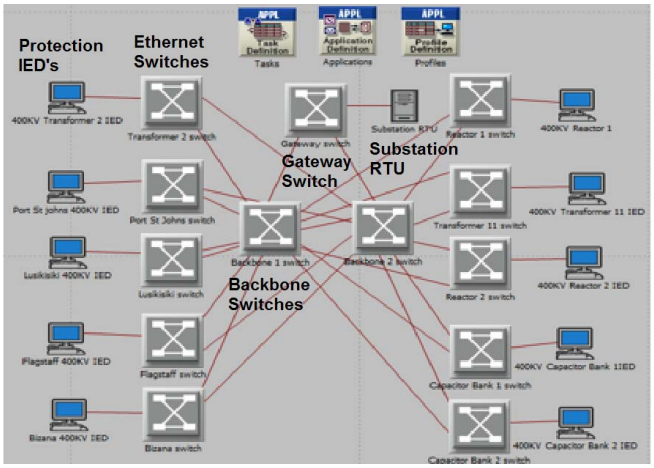

Fig. 1 OPNET Substation Communication Network Model

B. Simulation Configuration

Application definition is the profile in OPNET where the configuration of DNP3 over TCP/IP is done. One row is selected, this allows the definition of one application. The application defined is TCP/IP as can be seen in Fig.2.

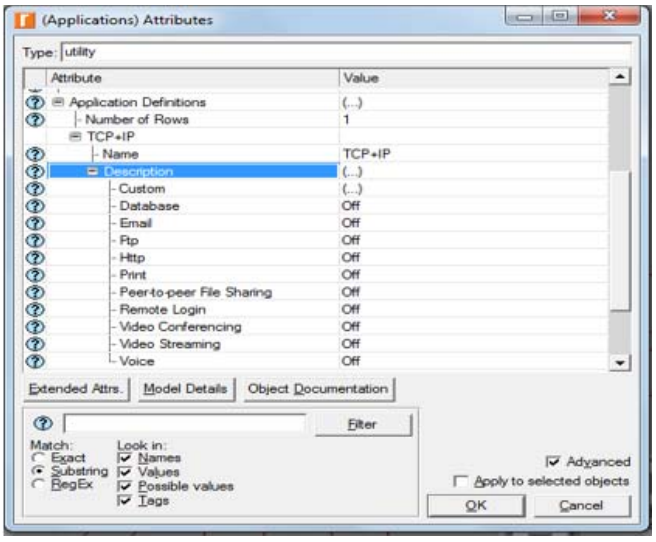

Fig. 2 Application definitions

Fig. 3 shows the manual configuration table for the setting of the DNP3 over IP characteristics. The generation of the traffic between the source and destination is done in this table. The request and response sequence are also configured in this table. The transport protocol is selected from this table.

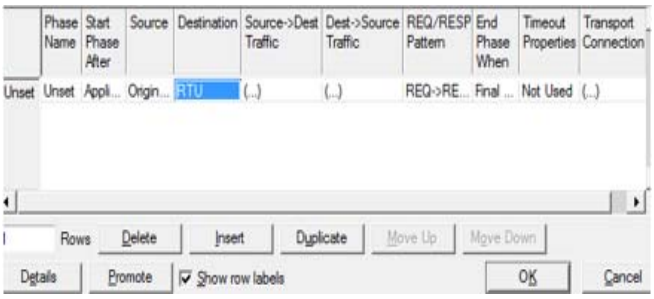

Fig. 3 Manual configuration table for DNP3

IED Traffic characteristics in Fig.4 are configured as follows: initialization time is set to 50 ms, request count is set to 3 seconds, inter-request time is set to 1 second, request packet size is set to 3222 bytes [14], packet per request is set to 3222 bytes and inter-packet time is set to 1 second as can be seen in Fig.4

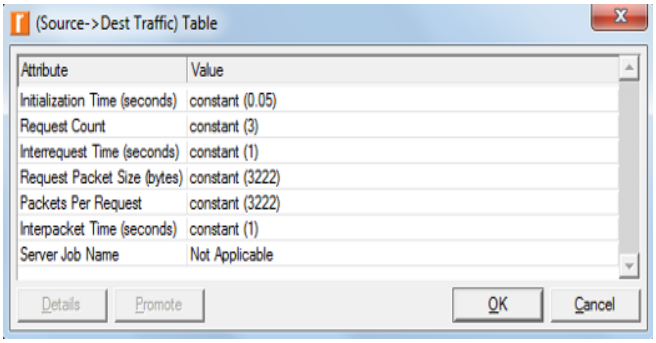

Fig. 4 IED Traffic characteristics

Substation RTU traffic characteristics in Fig. 5 are set as follows: request processing time is set to 50 ms, response packet size is 1024 [13], packet per response is 1024 and inter-packet time is set at 1 second.

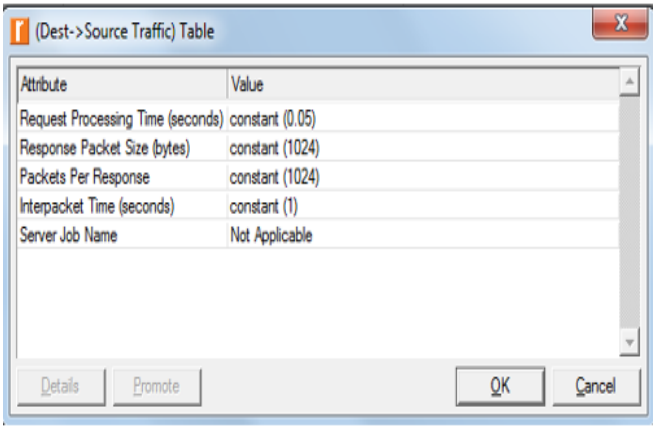

Fig. 5 Substation RTU Traffic characteristics

III. RESULTS AND DISCUSSION

The substation model has ten devices on the network and the parameters were taken at different loading of the network. The first measurement was taken when 10 percent of the devices were online. The second measurement was taken when 50 percent of the devices were online. The third when 90 percent of the devices were in service and the fourth when all the devices were in service. It can be seen in Fig.6 that as the number of devices online increases the number of load packets increases.

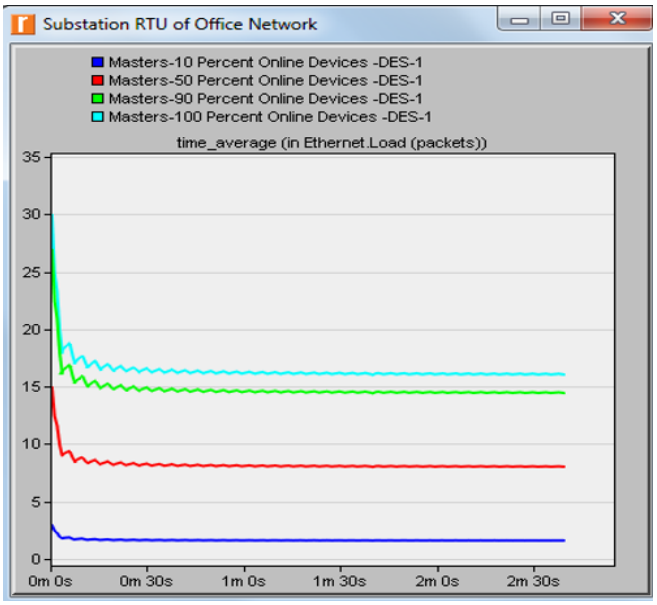

Fig. 6 Ethernet load packets

Fig. 7 shows the ethernet load packets per second distribution with different percentage of IED devices online. The load on the network at 10% of the IED devices online is 3 packets/sec, at 50% is 10 packets/sec, at 90% is 18 packets/sec and at 100% is 20 packets/sec.

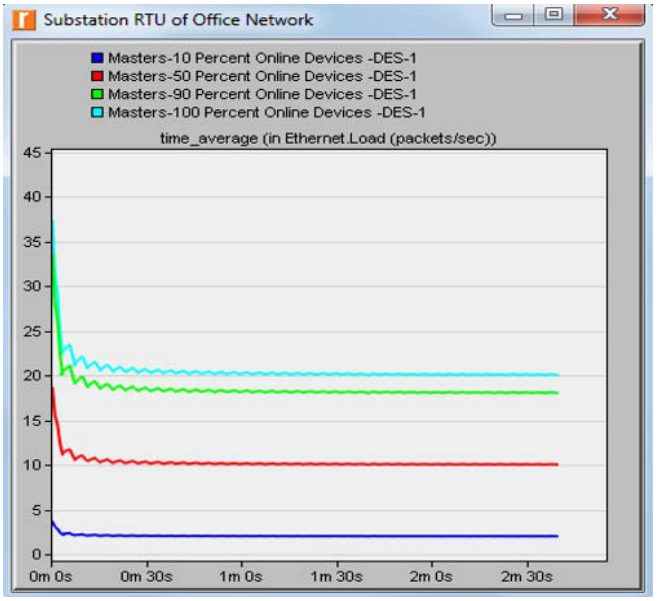

Fig. 7 Ethernet load packets/sec

Fig. 8 shows the received ethernet packets at the substation RTU end. In the figure it can be seen that with an increase in the number of devices online there is also an increase in traffic received.

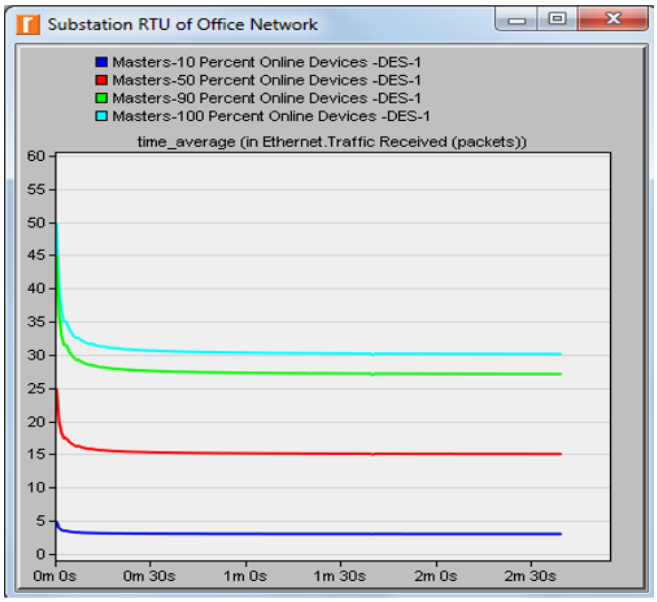

Fig. 8 Ethernet traffic received packets

Fig. 9 shows the IP traffic sent from the 400 KV transformer IED. Fig.10 shows the IP traffic received at the substation RTU end as seen in the model in Fig. 1. These figures show that with an increase in the number of devices online there is an increase in the traffic on the network. The figures also show that the sent traffic is less than the received traffic. It is because the substation RTU in the model is receiving data from multiple devices at the same time as they come online.

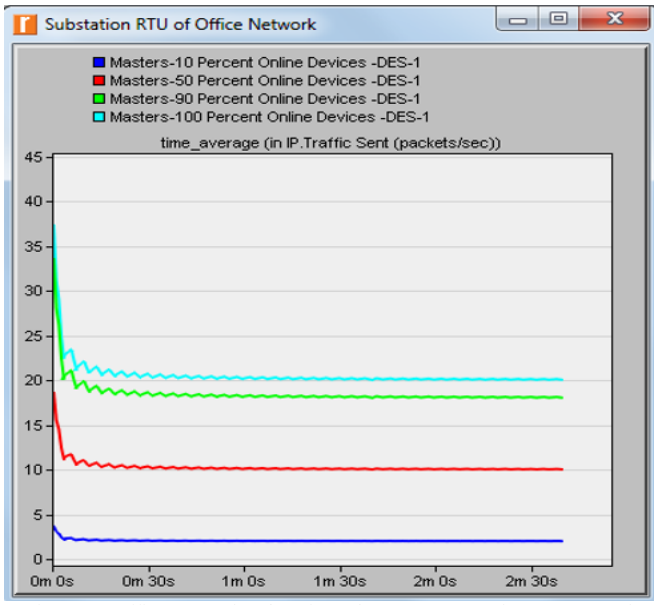

Fig. 9 IP traffic sent packets/sec from the 400 KV transformer IED end

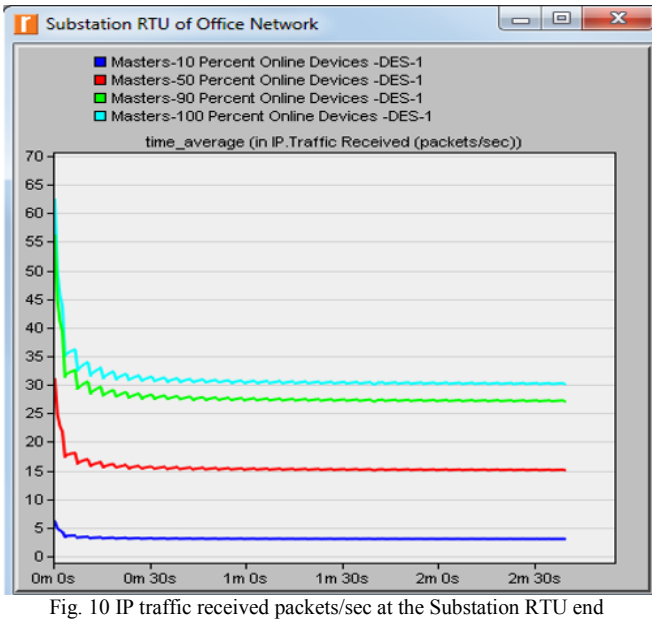

Fig. 10 IP traffic received packets/sec at the Substation RTU end

Fig. 11 shows the sent and received traffic between the 400 KV transformer protection IED and the IED switch. From the figure it can be seen that the sent traffic is more than the received traffic. The reason for this is that on the same link there is data losses along the line therefore the received data should be less than the sent data.

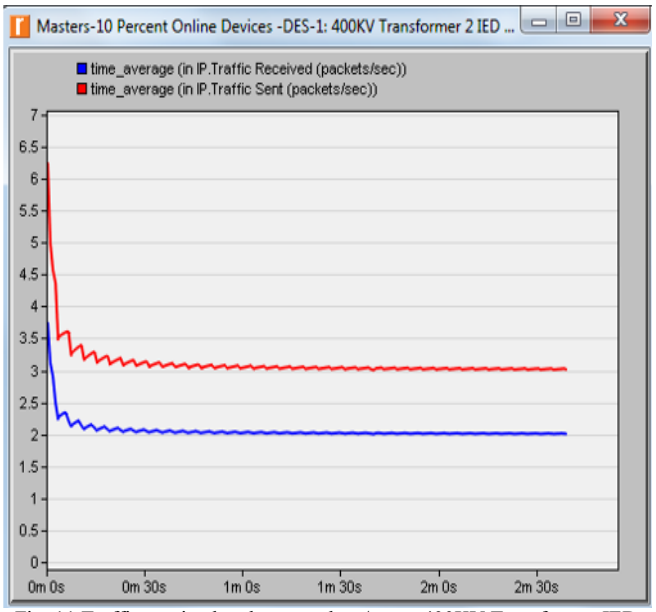

Fig. 11 Traffic received and sent packets/sec at 400KV Transformer IED end.

Fig. 12 shows ethernet delay for the model and that with an increase in devices online, there is also an increase in time delay. Fig. 12 shows that the time delay ranges between (0.160 – 0.2) ms.

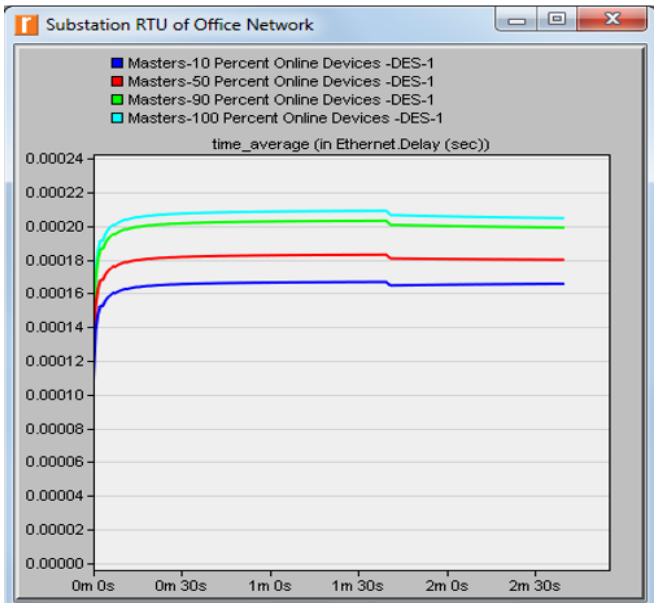

Fig. 12 Ethernet delay/sec

Fig. 13 shows the sent throughput from the transformer IED, while the consecutive figure shows the received throughput at the substation RTU unit end. Both figures show that with an increase in the number of devices online, there is a corresponding increase in data throughput. The figures also show that the throughput is stable therefore the network model is operating correctly. In the figures it can be seen that the DNP3 protocol carries data in the range of kbps. These figures show that the received throughput exceeds the sent throughput because the substation RTU receives data from several devices coming online.

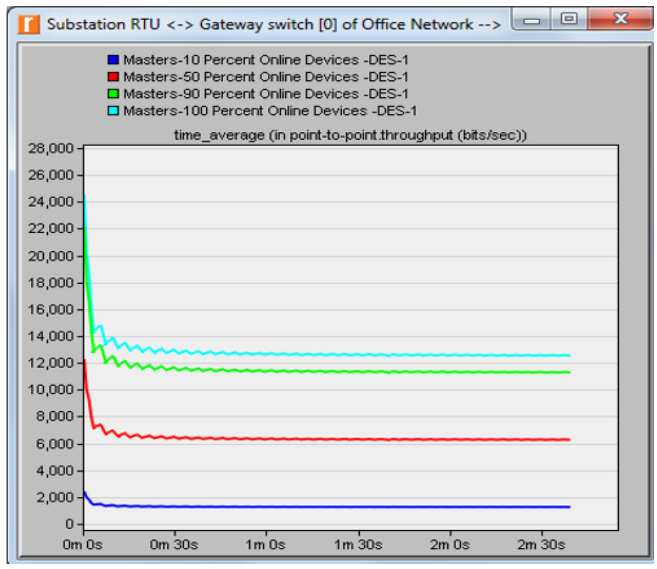

Fig. 13 Sent throughput (bps)

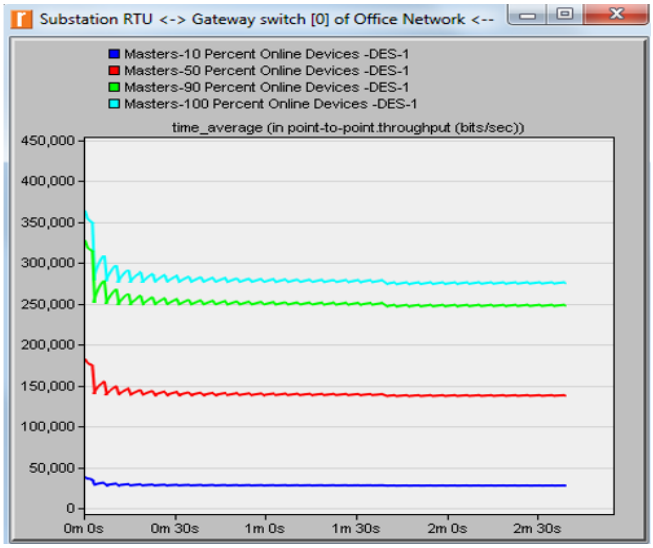

Fig. 14 Received throughput (bps)

Table I below summarizes the ethernet delay and load on the network. This is determined at 10%, 50%, 90% and 100% of the devices online. The table indicates that the ethernet delay tends to saturate to some extent as you increase the number of devices online. The delay is in the region of 200 μs for these networks.

TABLE I PERFORMANCE WHEN 10%, 50%, 90% AND 100% OF DEVICES ARE ONLINE

10% Online	Minimum	Average	Maximum
Ethernet Delay	14.001µs	165.65µs	167.33µs
Load packets	1	1.6050	3
50% Online	Minimum	Average	Maximum
Ethernet Delay	18.771µs	179.89µs	184.68µs
Load packets	5	8.0250	15
90% Online	Minimum	Average	Maximum
Ethernet Delay	29.327µs	198.98µs	203.66µs
Load packets	9	14.445	27
100% Online	Minimum	Average	Maximum
Ethernet Delay	32.327µs	204.55µs	209.6µs
Load packets	10	16.050	30

IV. CONCLUSION

This paper shows the design of a substation communication network model using DNP3 protocol applied over the model with ethernet in OPNET. The modeling shows that DNP3 has a data rate in kbps and a delay in the range of 0.2 ms. In addition, it has been observed in the simulation that with an increase in the number of IED devices in the substation network there is an increase in the ethernet delay and the packet load on the network. It can be concluded that when designing a substation communication network, the packet load on the network must be taken into consideration if a quick response is required as in a smart grid system.

ACKNOWLEDGMENT

We would like to acknowledge the University of South Africa and the University of Johannesburg in assisting to provide the resources to fund this work.

REFERENCES

[1] Prakash J.V., "Advantages of the DNP3 Communication Protocol in Water and Wastewater Telemetry Systems", https://www.automation.com/pdf_articles/1261002_DNP3WaterWastewaterWP.pdf, 2012.

[2] Bailey D. and Wright E., "Practical SCADA for Industry", *Perth: IDC Technologies*, pp. 1-18, 2003.

[3] Neeraja T.P., Sivraj P. and Sasi K.K., "Sensor Based Communication Network for WACS with DNP3", *Procedia Technology,* vol 21, pp. 76-81, 2015, https://doi.org/10.1016/j.protcy.2015.10.012.

[4] Cheng L., "Study and Application of DNP3.0 In Scada System", *International Conference on Electronic and Mechanical Engineering and Information Technology*, Harbin, China, pp. 4563-4566, 2011. doi: 10.1109/EMEIT.2011.6024045.

[5] Hung H, "Automatic Circuit Recloser (ACR) communications using P25 RMU (Radio Modem Unit)", *Dissertation submitted to the University of Southern Queensland*, 2016.

[6] Ortega A., Shinoda A.A. and Schweitzer C. M., "Performance Analysis of Smart Grid Communication Protocol DNP3 over TCP/IP in a Heterogeneous Traffic Environment", *IEEE Colombian Conf. Communications and Computing, Medellin Colombia,* May 22-24, 2013, DOI:10.1109/ColComCon.2013.6564828.

[7] Richard A. and Kubi P.A., "Design and performance of a split protocol architecture on Distributed Network Protocol 3", *IEEE International Conference on Electro Information technology*, Lincoln, USA, May 14-17, 2017, DOI:10.1109/EIT.2017.8053364.

[8] Lu X. et al, "On Network Performance Evaluation toward the Smart Grid: A case Study of DNP3 over TCP/IP", *IEEE Global Telecommunications Conference,* Houston, USA, Dec. 5-9, 2011, DOI:10.1109/GLOCOM.2011.6134406.

[9] Bai J., Hariri S. and Nashif Y.A., "A Network Protection Framework for DNP3 over TCP/IP Protocol", *IEEE/ACS 11th International Conference on Computer Systems and Applications*, Doha, Qatar, pp. 9-15, 2014, DOI: 10.1109/AICCSA.2014.7073172.

[10] Shin I.J., Eom D.S. and Song B.K., "The CoAP-based M2M Gateway for Distribution Automation System using DNP3.0 in Smart Grid Environment", *IEEE International Conference on Smart Grid Communications*, Miami, USA, 2015, pp. 713-718, DOI:10.1109/SmartGridComm.2015.7436385.

[11] Ortega A. et al, "Simulation of the DNP3 Protocol Over TCP/IP on a Network IEEE 802.11g Ad-hoc with smart meter", *IEEE, Conference ANDESCON*, Arequipa Peru, Oct. 19-21, 2016, doi: 10.1109/ANDESCON.2016.7836213.

[12] Zecena J.C.C. and Molina V.L.O., "Hydra-A DNP3 multiplexing platform for SCADA system switchover", *IEEE 24th International Conference on Electronics, Electrical Engineering and Computing*, Cusco, Peru, Aug. 15-18, 2017, DOI: 10.1109/INTERCON.2017.8079649.

[13] Sethi A.S. and Hnatyshin V.Y., "The Practical OPNET User Guide for Computer Network Simulation", *New York, Taylor and Francis Group, LLC*, 2019, pp. 1-528. ISBN 9780367380953.

[14] G. Clarke, D. Reynders and E. Wright, "Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems", *IDC Technologies*, England, 2004. PP.166-168.