IPv6 Applicability in SCADA System Network

Ahmed M. Hassaballa [1], Abubakr E. M. ElHussein [2] and Ali A. Agoub [3]

[1] Basic Studies Unit, University of Nyala, Nyala, Sudan, E-mail ahmed_hassaballa2003@yahoo.com

[2] Department of Computer Engineering, Faculty of Engineering, University ofElneelain, Khartoum,Sudan,E-mail abubakr. Elhussein @ neelain.edu.sd

[3] Department of Computer Engineering, Faculty of Engineering and Technology, University of Gezira, Wad-medani, Sudan, Email ali_abdelrahman@yahoo.com

ABSTRACT

The trend today is to build a secure fault tolerant Internet/Intranet connected distributed SCADA system networks using open and standard software/hardware. This paper made use of advances in Ethernet such as Fast/Gigabit Ethernet, micro-segmentation and full-duplex operation using switches, IPv6 enhanced features and TCP/IP to fulfill the real-time requirements for SCADA system network. OPNET Modeler simulator is used for modeling and simulating the network. The various measured delays showed that IPv6 introduction in such network introduces very small (negligible) delay and shows better performance on applying Quality of Service relative to IPv4. Also it is found that delays increase with increased transported packet size.

Keywords: Ethernet, IPv4/IPv6 performance, OPNET, SCADA

1- INTRODUCTION

The Supervisory Control and Data Acquisition (SCADA) system is a category of software application program for process control and management adopted in the industrial environments with the functionality of data acquisition, presentation, communication and control [Berry, 2008]. The SCADA system is composed of elements. The elements include: field instruments, controllers, servers and communication channels [Bailey and Wright, 2003]. Using these elements a centralized or distributed SCADA system network can be

designed based on system design requirement. Traditionally SCADA systems were built with closed vendor's proprietary software/hardware as isolated networks, but the trend is to build Internet/Intranet connected systems with open and standard software/hardware [VAN, 2009]. This trend is challenged with problems such as some software/hardware does not satisfy the real-time guarantees, devices from different vendors do not interoperate and networks subject to security flaws. Researches were conducted addressing these problems with TCP/IP [Reynders and Wright, 2003] on top of Ethernet [IEEE, 1998] technologies ending up with Ethernet industrial automation protocols for real-time guarantees and interoperability. In security area, Internet Protocol security (IPsec) technology, firewalls, intrusion detection/prevention, antivirus software, filtering and Virtual Private Network (VPN) were adopted to secure networks [Stouffer et al, 2006]. The paper based on IPv4 [Postel, 1981] for IPv6 [Deering and Hinden, 1998] study, used a framework of software/hardware for guaranteeing interoperability, real-time, security and fault tolerant requirements. The rest of the paper is organized as follows; section 2 describes the proposed SCADA system network and the network model. Section 3 presents the simulation scenarios, discussion and conclusion.

2.0 SCADA System Network

The proposed network is composed of switched Ethernet 100BaseT Local Area Networks (LANs) Internet/Intranet connected to form Wide Area Network (WAN). The network design requirement include: high data reliability, determinism and security. The data reliability and determinism requirements will be satisfied using TCP/IP on top of Ethernet with Quality of Service (QoS). The security requirement will be satisfied using IPsec [Kent and Seo, 2005] and firewall. The LANs represent sites, control rooms/centers and headquarter. The site could be small, medium or large depending on site design requirement. This paper uses a small site with one controller. The site components are: two routers, two firewalls, two 16 ports Ethernet switches, one server and ten workstations. The server represents the controller and the workstations represent field instruments (six

sensors and four actuators). Refer to figure 1 for a site design. The control rooms/centers and headquarter have similar components, each consist of two routers, two firewalls, three 16 ports Ethernet switches and three servers. The servers represent SCADA application, concentrator and historian. The concentrator concentrates data from all sites belonging to the same control room/center. Refer to figure 2 for control room/center or headquarter network design. The overall network that span a large geographical area in Sudan consist of headquarter, three control rooms/centers and four sites connected to Internet as shown in figure 3. It is assumed that all components are IPv6 enabled.

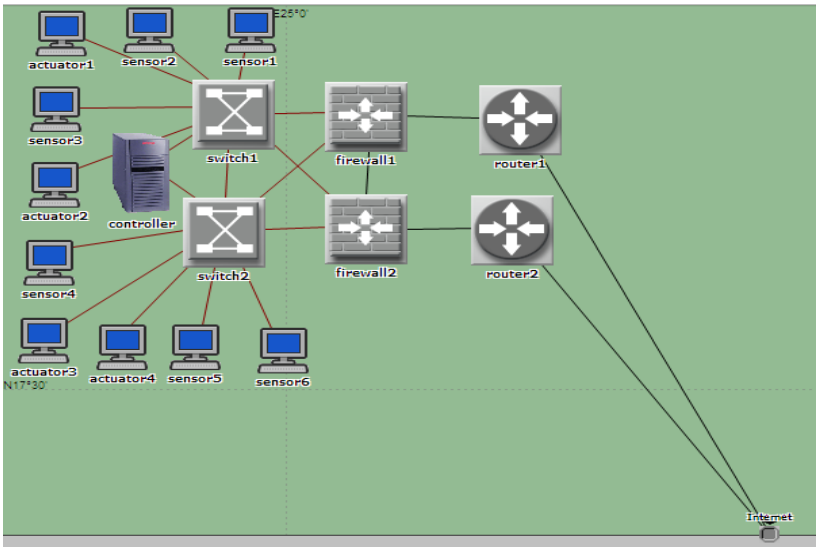

Fig. 1 Site Subnet

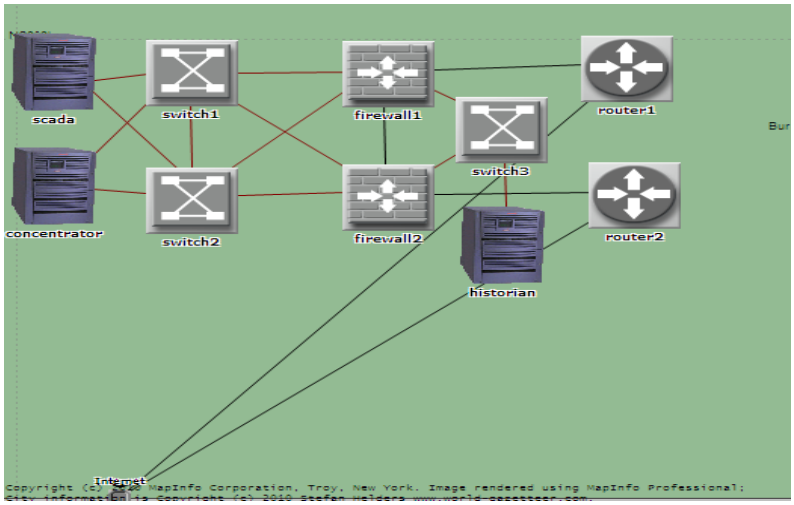

Fig. 2 Control Room/Center

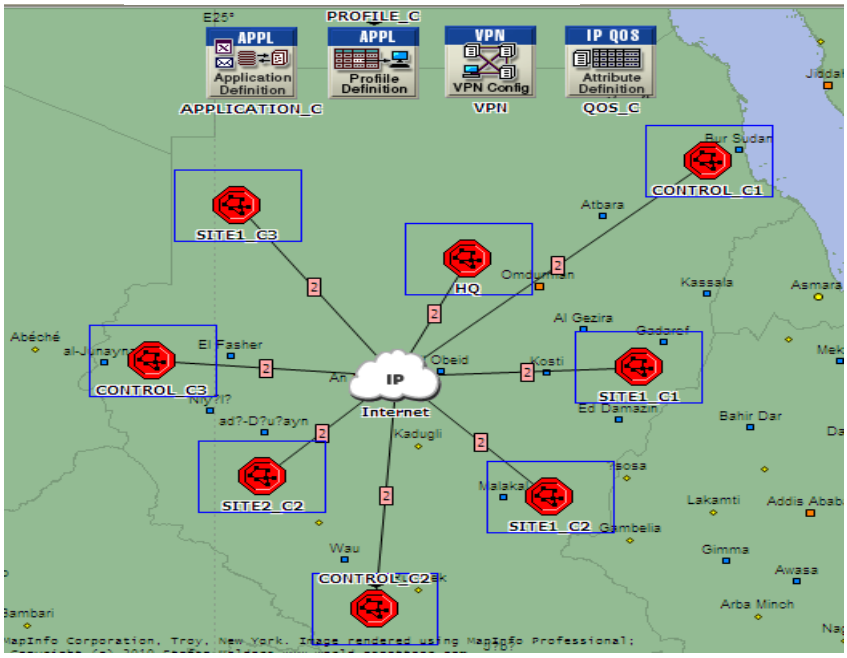

Fig. 3 Overall Network Structure

2.1 Network Model

The work assumes IPv6 enabled smart field instruments and controllers were being used. OPNET Modeler version 14.0 [OPNET, 2009] is used for network modeling and simulation. The smart field instruments were modeled as workstations using the OPNET

Modeler's ethernet_station node model. The workstations attribute are set as shown on table 1.

Table 1 Workstation Attribute

Attribute	Value
Ethernet IP address	Auto Assigned
Ethernet Frame bursting	Enabled
Ethernet Operation Mode	Full Duplex
Traffic Generation Start Time (seconds)	Constant(1)
Traffic Generation On State Time (seconds)	Exponential(90.0)
Traffic Generation Off State Time (seconds)	Exponential(0.001)
Packet Generation Interval Time (seconds)	Exponential(0.02)
Packet Generation Packet Size (bytes)	Constant(76)
Packet Generation Segmentation Size (bytes)	No Segmentation

The column on the left side of table 1 represents the attribute fields, while the one on the right represents the values that must be set for the corresponding attributes. To represent a sensor that generates traffic with 72 bytes packet size, the attribute values for the attribute fields are set as shown on table 1. Here Ethernet Operation Mode is set Full Duplex to eliminate collisions, leading to a shorter Ethernet delay time. The Traffic Generation Start Time parameter is set to Constant (1) to make the simulation start up immediately. The Traffic Generation on State Time is set to Exponential (90.0) and Traffic Generation off State Time set to Exponential (0.001) to make the work-station 90% of simulation time generating and sending data, while 10% of the time receiving data. Packet Generation Interval Time is set to Exponential (0.02) to make the time between the generated or received packets 20 milliseconds. The Packet Generation Packet Size is set to Constant

(76) to make the packet size be 76 bytes. The Packet Generation Segmentation Size is set to No Segmentation to avoid packet segmentation. To represent an actuator which is 90% of simulation time receiving commands, the Traffic Generation On State Time (seconds) is set to exponential (10.0) and Traffic Generation Off State Time (seconds) is set to exponential(90.0). All other attribute fields are set as on table 1.

This work uses 72, 520 and 1500 bytes packet size. The smart controllers, scada servers, concentrators and historians were modeled as servers. Table 2 shows the components, the quantity and the node model used in modeling the SCADA system network.

Table 2 SCADA system network components and models

Component	Node model	Qty
Sensor	ethernet_station	24
Actuator	ethernet_station	16
Controller	Compaq_AlphaServer_DS20_500	4
Scada	Compaq_AlphaServer_ES45_100	4
Concentrator	Compaq_AlphaServer_ES45_100	4
Historian	Compaq_AlphaServer_ES45_100	4
Firewall	ethernet2_slip8_firewall	8
Firewall	ethernet4_slip8_firewall	8
16 ports Ethernet switch	ethernet16_switch	20
Router	ethernet4_slip8_gtwy	16
100BaseT link	100BaseT Duplex link	116
PPP DS3 link	PPP_DS3 Duplex link	40
Internet	ip32_cloud	1

The networks traffic consists of Transmission Control Protocol (TCP) [Postel, 1981b] and User Datagram Protocol (UDP) [Postel, 1980] traffics. The traffic is modeled using the OPNET Modeler's default applications, where File Transfer Protocol (FTP) (TCP traffic) is used to model non real-time traffic and Voice over IP application (UDP traffic) is used to model real-time traffic. This traffic model is for applications that use TCP for explicit messages transport and UDP for implicit messages transport. For applications that use only TCP for messages transport, FTP application is used to model the real-time and non-real-time traffics. The Application Config and Profile Config node models were used to characterize the traffic in the network. All modeled networks up to the writing this paper used one control room/center with no QoS, no redundancy and no IPsec implementation. This work used multiple control rooms/centers so as to have a very highly distributed network, in addition to QoS, redundancy and IPsec being implemented.

2.1.1 Data Flow

A controller receives data from smart field devices, processes the data locally for local control and sends it to a concentrator at the control room/center. The concentrator on receiving the data from all controllers belonging to the same control room/center, it sends the data to a scada application and historian servers on the same control room/center, also it sends the same concentrated data to the HQ's scada application and historian servers. Controllers on sites receive commands from their respective scada application servers on control rooms/centers. Scada application servers in control rooms/centers receive commands from HQ's scada application server. Historian servers are accessed by control rooms/centers and HQ. The mentioned data flow is set using the server's node application destination preferences attribute parameter.

2.1.2 Firewall

The firewall node is configured to bypass only FTP and Voice over IP traffic using the proxy server information parameter. The allowed passing traffic represents the industrial automation traffic.

2.1.3 Virtual Private Network

The virtual private network (VPN) provides a secure communication over non secure communication environment such as the Internet. Thus to secure communications between sites, control rooms/centers and the HQ over the Internet, VPN solutions are needed. For IPv4 environment, the IP VPN Config node is used to configure the VPN tunnels specifying tunnel sources and destinations, in addition to clients list in compulsory operation mode using the VPN configuration parameter. For IPv6 bidirectional tunnels with specifying clients list are configured using the router's node IPv6 parameters, in addition to configuration using IP VPN Config node. IPsec is implemented using router's node security attribute, where IPsec parameters such as IPsec Information and tunnel interfaces are configured. The authentication and encryption algorithms used on this work, for both protocols (IPv4 and IPv6) are SHA-1[NIST, 2001] and 3DES [NIST, 1999] respectively.

2.1.4 Quality of Service

Quality of Service (QoS) is configured for IPv4 and IPv6 environments on nodes (servers, firewalls and routers) using the node's IP attribute sub field named IP QoS Parameters, in addition to QoS Attribute Config node. This work uses the following QoS configuration, in addition to OPNET Modeler default values:

- Interface information: The interface information is configured as shown on table 3.

Table 3 Interface information configuration

Parameter	Value

QoS scheme	FIFO
Buffer size	1 Mbytes
Reserved bandwidth type	Relative
Maximum reserved bandwidth	75%

- Traffic policies: Two traffic classes (tr1 and tr2) are defined and the Differentiated Services Code Point (DSCP) property value for each traffic class is set to Expedited Forwarding (EF).
- Weighted Fair Queuing (WFQ) / Dynamic Weighted Fair Queuing (DWFQ) profiles: Two classes are defined and configured with relative bandwidth type, enabled priority and queue 64 packets limit.

3.0 Simulation scenarios and Discussion

Simulation scenarios were conducted with VPN (IPsec) for IPv4 and IPv6 environments with 50% of background traffic utilizations and with 72, 520 and 1500 bytes packet size to determine the network performance and to provide baseline scenarios for performance enhancements using QoS. The simulation scenarios collected results include global summary, node and link point-to-point statistics with the maximum value for the intended statistics being reported. The global statistics summary collected results are shown on table 4. Figure 4 compares the global IPv4/IPv6 Ethernet delay for 72, 520 and 1500 bytes transported packet size.

Table 4 Global statistics summary for 50% background traffic utilization

Statistics	Packet size (bytes)	IPv4 (millisecond)	IPv6 (millisecond)
Ethernet delay	72	0.84969	0.86850
	520	0.91234	0.92252
	1500	1.07920	1.08210
TCP download response time	72	232.83	240.23
	520	235.33	240.71
	1500	233.40	237.07
TCP upload response time	72	228.23	2350.8
	520	234.77	245.49
	1500	221.55	242.58
UDP end-to-end delay	72	66.227	65.283
	520	65.592	66.200
	1500	64.886	65.343
UDP delay variation	72	0.0000234	0.0001346
	520	0.0000064	0.0001346
	1500	0.0000051	0.0000499

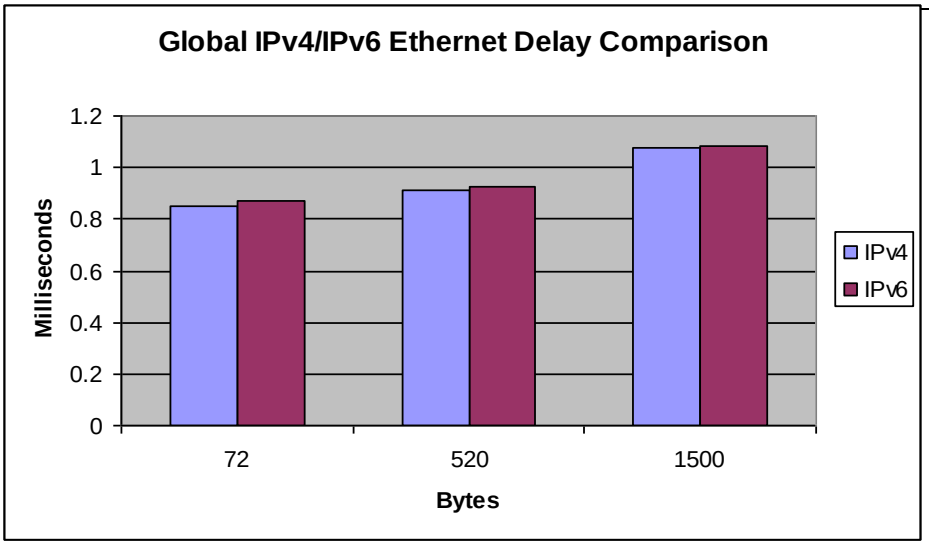

Fig. 4 Global IPv4/IPv6 Ethernet Delay Comparison

On investigating the global statistics for IPv4 and IPv6 networks with 50% background traffics utilization in table 4, it is found that introduction of IPv6 introduces a very small increase in delays. For Ethernet delay, it is found that IPv6 introduces 0.01881, 0.00118 and 0.00290 milliseconds increase in Ethernet delay for packet sizes 72, 520 and 1500 bytes respectively relative to IPv4. The minimum delay difference is obtained using 520 bytes packet size, which concludes that the improvement in Ethernet delay could be obtained using moderate packet size. This is the reason that industrial automation uses moderate packets size (e.g. 128 bytes). For IPv6, the lowest Ethernet delay is 0.86850 milliseconds obtained using 72 bytes packet size and the highest Ethernet delay is 1.08210 milliseconds obtained using 1500 bytes packet size. Thus global Ethernet delay increases with increased packet sizes.

In the area of TCP download response time, IPv6 introduces 9.40, 5.37 and 3.67 milliseconds increase for 72, 520 and 1500 bytes packet size respectively relative to IPv4. TCP download response time increases with packet size increase for IPv4, but for IPv6, it increases for 520 bytes and decreases for 1500 bytes packet size. For TCP upload response time IPv6 introduces 6.85, 10.72 and 21.03 milliseconds increase in response time relative

to IPv4 for 72, 520 and 1500 bytes packet size respectively. On comparing UDP end to end delay, IPv6 showed an increase of 0.608 and 0.457 milliseconds for 520 and 1500 bytes packet size respectively relative to IPv4 with a decrease of 0.944 milliseconds for 72 bytes packet size.

On comparing UDP delay variation, it is found that IPv6 showed higher values relative to IPv4. IPv6 showed an increase of 0.1112, 0.1282 and 0.0448 microseconds for 72, 520 and 1500 bytes packet size respectively relative to IPv4.

On investigating the node IP end to end delay and node IP end to end delay variation, it is found that the node IP end to end delay is within 8 milliseconds and the node IP end to end delay variation is within 0.5 milliseconds for both protocols.

In the area of link statistics, it is found that IPv6 has a better link performance relative to IPv4. The lowest IPv6 throughput (5,063.5) is exercised by CONTROL_C2 to Internet and the highest throughput (5,428.9) is reported by Internet to CONTROL_C1 for 1500 bytes packet size traffic. The lowest IPv6 utilization (50.581%) is obtained by CONTROL_C1 to Internet for 72 bytes packet size, while the highest utilization (55.712%) is obtained by CONTROL_C3 to Internet for 1500 bytes packet size.

On comparing IPv4 and IPv6 performance, based on results in table 4, node IP end to end delay, node IP end to end delay variation and link point-to-point statistics, it is clear that introducing IPv6 protocol has relatively negligible effect on network performance relative to IPv4. Comparing the collected delay statistics with the real time delay requirements for SCADA WAN communication, it is found that the delay statistics values (0.86850 milliseconds for 72 bytes, 0.92252 milliseconds for 520 bytes and 1.08210 milliseconds for 1500 bytes packet size) are more than adequate for electric grid that requires Ethernet delay not exceeding 12 milliseconds and manufacturing WAN

communication network that requires Ethernet delay not exceeding 100 milliseconds (VAN, 2006, IEEE, 2004).

The networks performance can further be enhanced by implementing QoS. The QoS parameters were configured and implemented as shown on section 2.1.4 for IPv6 network. Simulation scenarios were conducted and the global statistics summary is reported as shown in table 5. Figure 5 compares global IPv6 Ethernet delay with and without QoS implementation.

Table 5 Global statistics summary for 50% background traffics for IPv6 with QoS

Statistics	Packet size (bytes)	IPv6 (milliseconds)
Ethernet delay	72	0.85596
	520	0.90755
	1500	1.09290
TCP download response time	72	225.80
	520	237.95
	1500	227.53
TCP upload response time	72	222.61
	520	219.45
	1500	225.31
UDP end-to-end delay	72	66.885
	520	66.184
	1500	67.056
UDP delay variation	72	0.4326
	520	0.0627
	1500	0.0097

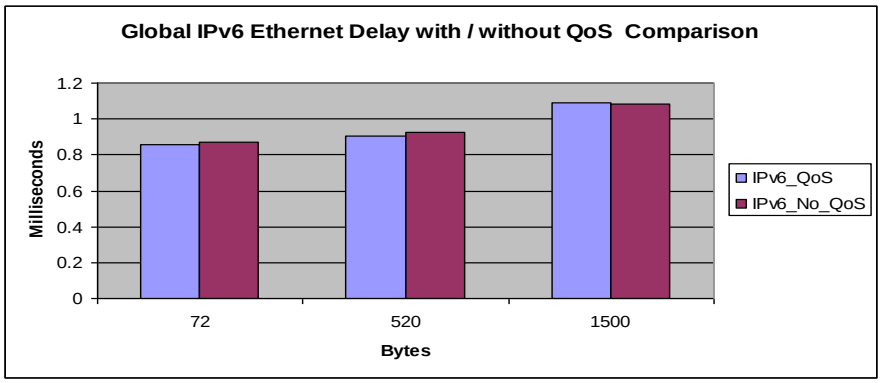

Fig. 5 Global IPv6 Ethernet delay with / without QoS Comparison

On comparing Ethernet delay for IPv6 without QoS (table 4) and IPv6 with QoS (table 5), it is found that applying QoS decreased Ethernet delay for 72 and 520 bytes packet size and increased it for 1500 bytes packet size. The decreases are 0.00905 and 0.00497 milliseconds for 72 and 520 bytes packet size respectively, while the increase is 0.0108 seconds for 1500 bytes packet size. In the area of TCP down load and upload response times, it is found that the response time deceases as the packet size increases. Table 6 shows TCP download/upload response time differences. In UDP end to end delay there is an increase in delay for 72 and 1500 bytes packet size, and a decrease in 520 bytes packet size. The decrease is 0.016 milliseconds for 520 bytes packet size. The increase is 1.602 milliseconds for 72 bytes and 1.713 milliseconds for 1500 bytes packet size. In UDP end to end delay variation there is a decrease in 520 bytes and 1500 bytes packet size, and an increase in 72 bytes packet size. The decrease is 0.00719 microseconds for 520 bytes and 0.00402 microseconds for 1500 bytes packet size. The increase is 0.298 for 72 bytes packet size. Generally based on collected results, the application of QoS on IPv6 network showed an IPv6 performance enhancement especially for moderate packet size.

Table 6 TCP download/upload response times difference

Statistics	Packet size (bytes)	IPv6 with and without QoS difference (milliseconds)
TCP download response time	72	0.01443
	520	0.00276
	1500	0.00954
TCP upload response time	72	0.01247
	520	0.02684
	1500	0.01727

3.1 CONCLUSION

The results showed that IPv6 can be applied in SCADA system network. The paper's work also realizes that Ethernet with TCP/IP can go real, and be used in SCADA systems for industrial automation for IPv6 protocol if the proper network components are selected and carefully implemented/configured with real time requirement in mind. The work major findings are that IPv6 introduces a very small (negligible) delay relative to IPv4, delays increase with increasing transported packet size and IPv6 has better performance when QoS being used on WAN.

REFERENCES

Bailey, D. and Wright, E. (2003). *Practical SCADA for Industry* (1). Newnes, Oxford. : pp: 4-6

Berry, B. (2008). SCADA Tutorial: A Fast Introduction to SCADA Fundamentals and Implementation. White paper, available at: http://www.dpstele.com/pdfs/white_papers/scada.pdf

Deering, S. and Hinden, R. (1998). Internet Protocol, Version 6 (IPv6) Specification. Std. Track, RFC 2460. Available at: http:// www. ietf.org/rfc/rfc2460.txt

IEEE 1646. (2004). Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation

IEEE, (1998). IEEE/ANSI Std 802.3-1998 Carrier Sense with Collision Detection (CSMA/CD) Access Method an Physical Layer Specification (including 100BaseT, Full Duplex, Gigabit Ethernet)

Kent, S. and Seo, K. (2005). Security Architecture for the Internet Protocol. Std. Track. RFC 4301.Available at: http://tools.ietf. org/html/rfc4301

NIST, (1999). FIPS PUB 46-3: DATA ENCRYPTION STANDARD (DES). (Includes3DES). Publication, available at: http://csrc.nist. gov /publications/fips/fips46-3/fips46-3.pdf

NIST, (2001). FIPS PUB 180-2: Specification for Secure Hash Algorithm. Publication. Available at: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2 withchangenotice.pdf

OPNET. (2009). Optimized Network Engineering Tool. Available at: http://www.opnet.com

Postel, J. (1980). User Datagram Protocol. RFC 768. Available at: http://www.ietf.org/rfc/rfc768.txt

Postel, J. (1981). Internet Protocol Specification. Std. 5, RFC 791. Available at: http://www.ietf.org/rfc/rfc791.txt

Postel, J. (1981b). Transmission Control Protocol Specification. RFC 793. Available at: http://www.ietf.org/rfc/rfc0793.txt

Reynders, D. and Wright, E. (2003). *Practical TCP/IP and Ethernet Networking* (1). Newnes, Oxford. : pp: 74-77

Stouffer, K., Falco, J. and Kent, K. (2006). Guide to Supervisory Control And Data Acquisition (SCADA) andIndustrialControl System Security. Document, available at: http://cs- www.ncsl.nist.gov/groups/SMA/fisma/ics/documents/Draft-SP800-82.pdf

VAN, Deliverable D04.1-1. (2006). Real Time for Embedded Automation Systems. Available at: http://www.vaneu.eu/sites/van/pages/files/D04.11_FinalV1_2_060702.pdf

VAN, Deliverable D-1.3-1-V5. (2009). Trend Screening and Self evaluation Final Evaluation and Conclusions. Version 5, report, available at: http://www.van-eu.eu/sites/van/pages/files/D-1.3-1-V5-version-1.01. pdf

تطبيق مرسوم الانترنت الاصدارة السادسة (**IPv6**)
فى شبكة نظام سكادا

احمد محمد حسب الله[1]، أبوبكر الصديق ميرغنى الحسين[2] وعلى محمد عبد الرحمن عجوب[3]

[1] وحدة الدراسات الاساسية ، جامعة نيالا ، نيالا ، السودان ، بريد الكترونى
ahmed_hassaballa2003@yahoo.com
[2] قسم هندسة الحاسوب ، كلية الهندسة ، جامعة النيلين ، الخرطوم ، السودان ، بريد الكترونى
abubakr.elhussein@neelain.edu.sd
[3] قسم هندسة الحاسوب ، كلية الهندسة و التكنولوجيا ، جامعة الجزيرة ، ود مدنى ، السودان ، بريد الكترونى
ali_abdelrahman@yahoo.com

الملخص

الاتجاه السـائد اليوم هو بناء شـبكات سـكادا مأمونة موثوقة عديمة الخطأ على شـبكة الانترنت / الانترانت باستخدام معيار مفتوح و قياسى البرمجيات / العتاد المادى . هذه الورقة استفادت من التقدم التكنولوجى فى الايثرنت مثل الايثرنت السريعة / جيجابت ايثرنت ، التجزئة المايكروية و تراسل البيانات مزدوج الاتجاه مع استخدام المفاتيح ، ميزات ال IPv6 المحسـنة و ال TCP/IP لتلبية الاحتياجات فى الوقت الحقيقى لشـبكة نظام سـكادا الواسـعة . تم استخدام ال OPNET Modeler لنمذجة و محاكاة الشبكة . أظهرت مختلف التأخيرات المقاسة أن استخدام IPv6 فى شبكة كهذه يضيف تأخير صغير جدا (ضئيل) و أداء افضل عند تطبيق جودة الخدمة مقارنة بال IPv4 . ايضا وجد أن التأخيرات تزداد بازدياد حجم الرزمة المرسلة.