Laying Foundation for SCADA System Protocol Performance Modelling

Alade Akinwumi
Department of Computer Science, Babcock University, Nigeria

Ajayi Olutayo
Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria

Okolie Samuel
Department of Computer Science, Babcock University, Nigeria

Alao Olujimi
Department of Computer Science, Babcock University, Nigeria

Abstract – Supervisory Control and Data Acquisition (SCADA) System which is a member of the set of Industrial Control System (ICS) is notable for control and monitoring of national critical infrastructure such as electricity supply network, oil/gas system, railways system and all those critical infrastructure that are geographically spread. This necessitates the need for a rem control centre where information from other locations are dispatched to, after initial processing at the fields (remote locations).

The focus of the paper is to examine the peculiarity of SCADA System protocols and the requirements for its performance model. It has been observed that while hundreds of papers have been written on SCADA System security, very few studies have delved into issues of its peculiar protocols talk less of their performance. A general introduction to protocol performance is made followed by review of existing performance models for the TCP/IP Protocols suite used for the internet. Some protocol performance evaluation and metrics are then considered.

The difference between the demands of data flow in TCP/IP protocols suite and that of the SCADA System protocol reference model are clearly depicted in figures 4 and 5. With the obvious variation in data flow demands of the two, we are able to highlight the vital elements required of SCADA System Protocol performance model.

Index Terms – Critical, Metrics, Model, Performance, Protocols, SCADA, TCP/IP.

1. INTRODUCTION

The motivation for this research is the identified gap in area of SCADA System protocols performance evaluation. While hundreds of papers have been written on the security of SCADA System, there is scarcity of papers emanating from researches on performance of SCADA System protocols. Attention is concentrated on SCADA System security research as threats to SCADA System would have tremendous impacts on the functioning of the critical infrastructure such as electricity network, oil and gas pipe lines and water supply system which it is expected to monitor.

Some of the papers written on SCADA Systems security are: i) "Vulnerability Assessment of Cyber security for SCADA Systems" by Chee-Wooi, Liu and Manimaran [1] in which the impact of cyber attack on SCADA Systems and compliance requirements of the North American Electric Reliability Corporation (NERC) to meet the standard of security necessary to face the ever growing cyber security challenges on SCADA Systems were discussed; ii) Fernandez and Larrondo-Petrie [2] paper titled "Designing Secure SCADA Systems Using Security Patterns" in which they proposed methods that can be used to build SCADA System security by using security patterns as a designing tool; iii) In Anjos, Brito and Motta-Pires [3]'s paper – "A Model for Security Management of SCADA Systems" – SCADA System management using "Ponder" framework to formally specify the rule validation, application policies check of conformity of the SCADA System to the prevailing standards on security of critical systems information and iv) SysAdmin, Audit, Network and Security (SANS) Institute conducted security survey on SCADA control process in 2013. Luallen and Filkins[4] in the report titled "SANS SCADA and Process Control Security Survey" 70 % of the system operators among the 700 interviewed saw the risks to their SCADA Systems as very severe while 33 % concluded that they had had incidents in the past; v) Ahmed et al [5] in their paper titled "A SCADA System Testbed for Cyber security and Forensic Research and Pedagogy" presented a newly built test bed for studying the cyber security of SCADA System of a models consisting of the following industrial processes – waste water system, power transmission and distribution system.

In his paper titled, "Theory of Performance", Elger [6] explained that there is performance when results that are valuable are produced by an individual, group of people. This can be extended to a system, machine or components such as SCADA Communication protocols that are expected to produce tangible, measurable and valuable results. The performance of SCADA Communication protocols are discussed in the subsequent subsections.

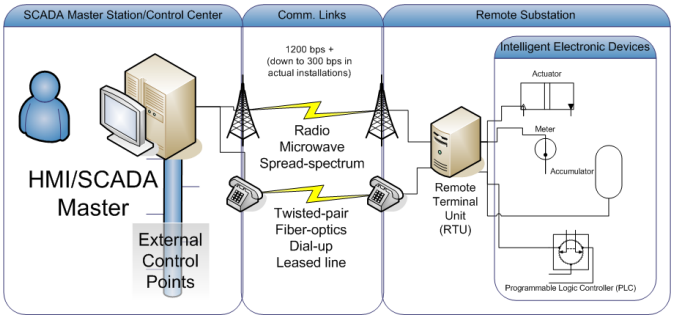

Figure 1: SCADA System

Source:Electrical Technology - https://www .electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html

2. RELATED WORK

Some of the existing analytical (mathematical) models for protocols performance are examined below:

Shahabudeen and Motani [7] in their paper titled "Short Paper: Performance Analysis of a MACA based Protocol for Ad hoc Underwater" derived an analytical model that supports the analysis of the effect of some parameters on expected throughput and service time of a MACA (Multiple Access with Collision Avoidance) based underwater MAC protocol. The parameters considered are: the number of network nodes (N), Propagation delay (D), packet length (L), batch size (B), k (detection and decoding probability), RTS back-off window size (W) and tA (ACK time). Representing the six states in the MACA underwater based MAC protocol by a Markov Chain model, metrics such as the throughput was derived.

"Performance modeling of the O-MACA" was described in the work of Zhang, Naït-Abdesselam and Bensaou [8] with emphasis on the wireless sensor networks having constraints of energy supplies, limited memory and processing capacities. As the sensors' energy is generally not rechargeable, an energy saving protocol that would prolong the lifetime of nodes is required. Unfortunately, the effective and simple IEEE 802.11 which is the most popular MAC protocol is not energy efficient. Other protocols such as S-MAC and O-MAC are developed to address those constraints. O-MAC's ability to save energy derives from the fact that it turns off third party nodes to save energy. The previous researchers had confirmed the competitive advantage of O-MAC over IEEE 802.11 through simulation but not theoretically. The focus of this research is to prove theoretically the known performance advantages of O-MAC over the popular IEEE 802.11. Among the metrics derived are end-to-end throughput, energy consumption per node and the link error probability.

The models developed by Bruno, Conti and Gregory [9] in the paper titled, "Performance Modelling and Measurements of TCP Transfer Throughput in 802.11-based WLANs" is only concerned with characterization of the TCP evolution, so as to evaluate TCP throughputs of data transferred even when there are congestion and loss events resulting from noisy channels and bottled networks. The ultimate goal is to model the network backlog and throughput analytically. The model computes the average number of backlogged node after successful transmission and the throughput.

Medina and Bohacek [10] studied the "performance of neighbor discovery in proactive routing protocols" evaluating the average number of neighbours that a node has, the probability of type I and type II errors and the impact of neighbor discovery on connectivity are derived. The authors explained that a Type I error occurs when a node believes that it has a neighbor when actually it cannot communicate with this node. In Type II error, a node is unaware that it is able to communicate with a node. The models developed allow the evaluation of the average number of neighbours that a node believes it has, the probability of Type I and Type II errors and the impact of neighbor discovery on connectivity.

In these models, TCP/IP Protocols suite based networks are considered with peer to peer data transmission. There are still gaps to be filled in area of performance models of protocols used in Industrial Control System (ICS) such as SCADA System. The foundation to modelling SCADA System protocols is, hence, laid in the following sections.

3. FOUNDATION FOR SCADA SYSTEM PROTOCOLS PERFORMANCE MODEL

3.1. Typical Protocol Performance Metrics

Among the several existing definition of System Performance, one that covers the hardware, software and the end users is that "the performance of a system is how its software is using its hardware when they are serving the workload created by the users" [11]. As the definition varies so also are the metrics used for system performance.

Lee, Kim, Hong and Gil-Haeng [12] identified four essential network performance metrics (NPM): Availability, Loss, Delay and Utilization. Each of these is split further into either 2 or 3 components (Figure 2). Availability is summarized as combination of functionality and connectivity in the network layer; Loss is the percentage of packets that is lost along the way from sender to receiver with a know interval of time. It consists of two metrics viz. round-trip and one-way loss. Delay

is the time it takes a packet to traverse the channel from the sending end to the receiving end in a one-way trip or time to make an average round-trip. In figure 2, three factors are considered: one-way delay, round trip delay and the variance of the delay. Utilization is the same as the link throughput expressed as a percentage of the access rate.

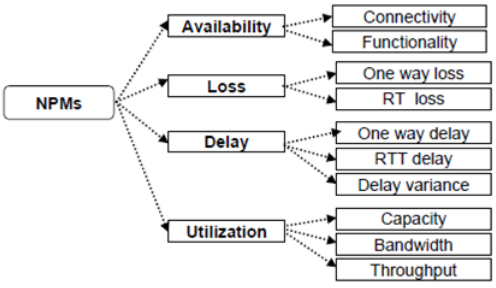

Figure 2: Network Performance Metrics

Source: Lee, Kim, Homg and Gil-Haeng (2004)

Hanemann, Liakopoulos, Molina and Swany [13] in their paper titled "A Study on Network Performance Metrics and their Composition" were of the opinion that of all the metrics that can be used to measure network performance, the most relevant to assessing network performance can be grouped into four:

- availability
- loss & error
- delay
- bandwidth

Availability is the measure of the network's robustness – the percentage time of uninterrupted services to the users. For the node or link, it refers to it is the percentage of time of smooth running.

The metrics for loss and error concern assessment of either transmission errors, fault on equipment or congestion on the network.

Bandwidth metrics determines data quantity that can be transferred per unit time on the network.

Cooper and Piumarta [14] defined latency (delay) as the elapsing time between data that is being sent and its final delivery. They also identified four components of network delay (Figure 3) as:

Transmission delay: the time for placing the bits onto the physical medium. It is the time that it will take the router to push out the packet; it is a function of the link's transmission rate and packet's length.

Propagation delay: the time taking by a packet to travel over a medium from sender to receiver or it is the time that it takes it takes a bit to traverse one router to the next; it depends on the physical distance between the routers.

Queuing delay: the time that a packet spends while waiting in a queue to be processed by sender or receiver.

Processing delay: the time needed to examine the packet's header and determines its destination [14], [15]. Types of delay are illustrated in figure 3.

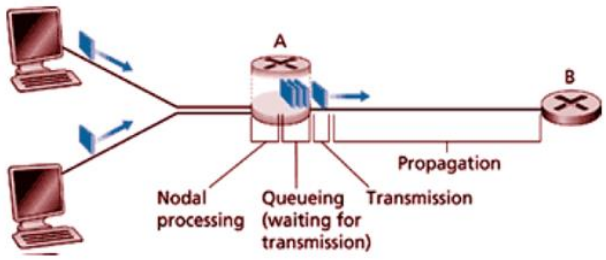

Figure 3: Types of Delay

Source: Kleinrock [15]

3.2. Comparison of Data Flow in TCP/IP protocols suite with SCADA EPA

Figure 4 depicts the data flow from the source through bridge and router down to the destination in a TCP/IP protocols suite model while figure 5 shows data flow from the source (Master e.g. Master Terminal Unit - MTU) to the destination (Slave e.g. Remote Terminal Unit - RTU) in SCADA System with Enhanced Protocol Architecture (EPA) reference. There is neither bridge nor router along the path from the source to the destination in the SCADA System as we have in the TCP/IP protocols suite model. Obviously, the delay that occurs in the router would not apply to SCADA System. Also clear from these figures is that there is higher overhead for data transfer along the five layers of the TCP/IP protocols suite model in figure 4 than that incurred to traverse the 3 layers of the EPA in figure 5.

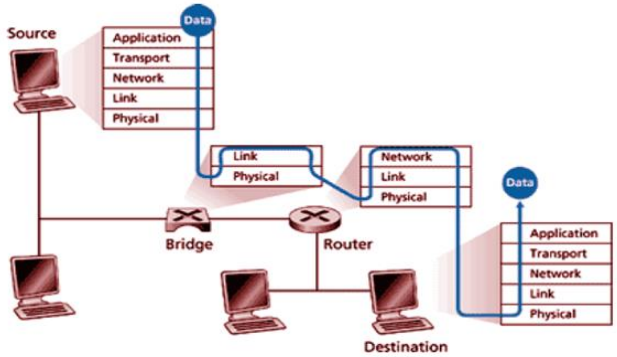

Figure 4: Data Flow on TCP/IP Protocol Model
Source: Kleinrock [15]

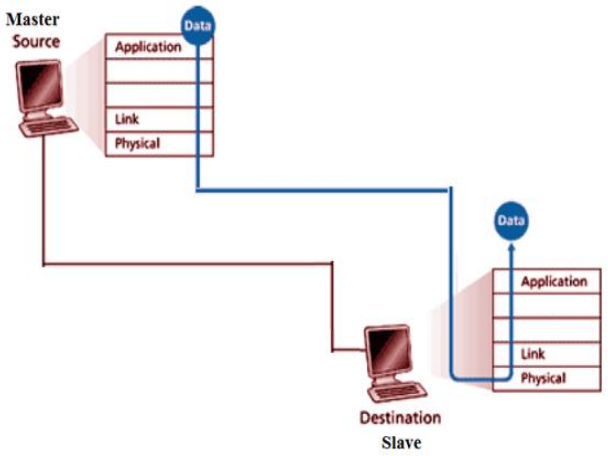

Figure 5: Data Flow on SCADA System EPA Model

Source: Adapted from figure 4

4. DISCUSSIONS

It is evident from Figures 4 and 5 that apart from the variation in number of layers in the TCP/IP Protocols suite and the SCADA System EPA reference, the presence of the bridge and router on the path of the former complicates dataflow more in TCP/IP suite than in the EPA system. These differences between the TCP/IP Protocols suite and the EPA model used in SCADA system buttress the need for a quite unique performance model for the SCADA system.

In view of the distinct characteristics of SCADA communication protocols that set them apart from Protocols that fully comply with the 7-layers of OSI or 5-Layers TCP/IP Protocols Suite, some of the earlier metrics might not apply to the SCADA Systems. As discussed earlier, SCADA System protocols are built upon Enhanced Protocol Architecture (EPA) reference Model that has only three layers: Application, Data Link and Physical. Secondly, SCADA System protocol communication is Master/Slave type unlike the TCP/IP protocols suite-based networks discussed in the related works just considered which have Peer-to-Peer protocol communication. The absence of bridges and routers on the data flow path of SCADA System between the master station and any of the slaves implies that the delays associated with these devices are eliminated (Figure 5).

5. CONCLUSION

In this paper we highlight the peculiarity of the SCADA System protocols that necessitates the need to develop specific model for its performance evaluation and reveal the reason why the several available models of protocols performance evaluation might not be suitable. Developing such model for SCADA System protocols is a gap requiring further research.

REFERENCES

[1] T. Chee-Wooi, C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems", IEEE TRANSACTIONS ON POWER SYSTEMS, vol. 23, No. 4, 2008.

[2] E.B. Fernandez and M.M. Larrondo-Petrie, "Designing secure SCADA systems using security patterns", Proceedings of the 43rd Hawaii International Conference on System Sciences, pp. 1 – 8, 2010.

[3] I.M. Anjos, A.M. Brito and P.S. Motta, "A model for security management of SCADA systems", IEEE Computer and Automation Engineering, pp. 448 – 451, 2008.

[4] M.E. Luallen and B. Filkins, "SANS SCADA and process control security survey", SANS Institute InfoSec. Available at https://ics.sans.org/media/sans-scada-survey-2013.pdf, 2003.

[5] I. Ahmed, V. Roussev, W. Johnson, S. Senthivel and S. Sudhakaran, "A SCADA system testbed for cyber security and forensic research and pedagogy", Proceedings of the ICSS. Conference, Los Angeles, CA, USA. doi : 10.1145/3018981 .3018994, 2016.

[6] D. Elger, "Theory of performance", Available at https://www.webpages.uidaho.edu/ele/scholars/Results/Workshops/Facilitators_Institute/Theory%20of%20Performance.pdf, 2016.

[7] S. Shahabudeen and M. Motani, "Short paper: Performance analysis of a MACA based protocol for adhoc underwater networks", Proceedings of Association for Computing Machinery WUWNet'09 Conference, Berkeley, CA, USA. ACM. 978-1-60558-821-6, 2009.

[8] J. Zhang, F. Naït-Abdesselam and B. Bensaou, "Performance modelling of the O-MAC protocol", Proceedings of Association for Computing Machinery PM2HW2N'07 Conference, Chania, Crete Island, Greece, 2007.

[9] R. Bruno, M. Conti and E. Gregori, "Performance Modelling and Measurements of TCP Transfer Throughput in 802.11-based WLANs", ACM 1-59593-477-4/06/0010, 2006.

[10] A. Medina and S. Bohacek, "A Performance model of neighbour discovery in proactive routing protocols", Proceedings of Association for Computing Machinery on PE-WASUN'10, October 17–18, 2010, Bodrum, Turkey. ACM 978-1-4503-0276-0/10/10, 2010.

[11] R. Puigjaner, "Performance Modelling of Computer Networks", Proceeding of IFIP/ACM Latin America Networking Conference, La Paz, Bolivia, 2003.

[12] H. Lee, M. Kim, J.W. Hong and G. Lee, "QoS parameters to network performance metrics mapping for slave monitoring", Proceedings of APNOMS, Sydney, Australia, 2004.

[13] A. Hanemann, A. Liakopoulos, M. Molina, D.M. Swany, "A Study on network performance metrics and their composition", Available at http://www.emeraldinsight.com/doi/abs/10.1108/10650740610704135, 2013.

[14] E. W. Cooper and I.K. Piumarta, "Computer networks", Available at http://www.ritsumei.ac.jp/~piumarta/networks/notes/NetWeek01_Notes.pdf, 2014.

[15] L. Kleinrock, "Lesson 1 - Computer Networks and Internet – Overview", Computer Networking and Management. Available at http://www.lk.cs.ucla.edu/LK/Inet/birth.html, 2015.