Estimating link availability and timing delays in Ethernet-based Networks

Jeyasingam Nivethan¹, Mauricio Papa¹, Peter J. Hawrylak²
Tandy School of Computer Science¹, Department of Electrical Engineering²
The University of Tulsa, Tulsa, OK, USA

Email: { nivethan, mauricio-papa, peter-hawrylak }@utulsa.edu

Abstract

Availability is an important requirement in networks used to control physical processes such as those present in the U.S. Critical Infrastructure, also known as Process Control Systems (PCS) or Supervisory Control and Data Acquisition (SCADA) systems. For instance, the IEC 61850 family of standards defines the network protocol for electric substations and the interface the substation presents to the Internet in the Smart Grid. Most of these networks currently use IEEE 802.3 Ethernet as opposed to legacy deployments using direct point-to-point connections that required a total of $n*(n-1)/2$ connections, also known as the n^2 problem. IEC 61850 (and other industrial protocols) operate in an environment where messages must arrive in time to be processed and action taken by control equipment. Thus, this delicate network becomes a target for attackers that may attempt to delay message delivery to negatively affect availability and cause problems, possibly leading to a blackout or unsafe state of the system. Components and processes must be designed to handle delayed messages. This paper presents a theoretic model that can be used to estimate the round-trip-time of a message over Ethernet under different link loads. A discrete event simulator called OMNeT++ was used to build a simulation and validate the proposed model. Simulation results indicate that the model is accurate.

Relevance

- SCADA protocols used in critical infrastructure protection often have strict response time constraints.
- Proposed model helps to evaluate end-to-end messaging delays which may be critical in various domains such as the Smart Grid and emergency response systems.
- Modular model can be used to evaluate additional delays caused by added security measures such as encryption and integrity checking.
- The model has been validated using the OMNeT++ platform. The modular nature of the platform makes the proposed model highly modular and easy to expand.

Modeling Network Delays

- A probabilistic algorithm models the entrance of packets to the channel based on the current load so that the remaining capacity of the channel is utilized by the sender.
- A channel operating under a 75% load can only be used by the sender 25% of the time.
- A uniform random number generator is used to produce numbers between 0 and 1 and these numbers are compared with the given load of the channel.
- The basic pseudo code is described in Algorithm 1 below.

Algorithm 1 pseudocode

$l \equiv$ channel load (in percentage)
 $r \equiv$ random number, generated from uniform distribution($0 < r < 1$)
repeat
 $r = \text{uniform}(0, 1)$; //random number between 0-1
 if ($r \leq l$) **then**
 wait for a constant time
 else
 send message
 end if
until n number of packets sent

$l \equiv$ channel load (in percentage)
 $r \equiv$ uniform random number ($0 < r < 1$)
 $P(r > l) = l$ (1)
 $P(r \leq l) = 1 - l$ (2)
 $m \equiv$ number of messages sent in n number of cycles through the loop
 $n \equiv$ number of cycles through the loop required to send m number of messages
Therefore, the probability for a message being sent per iteration is $\frac{m}{n}$:

$$P(r > l) = \frac{m}{n} \quad (3)$$

From equation (2) and (3)

$$1 - l = \frac{m}{n} \quad (4)$$

Rearranging Equation (4) yields

$$n = \frac{m}{1-l} \quad (5)$$

$T \equiv$ The transmission time for a message (Figure 1)

$wTotal \equiv$ Total waiting time added through n cycles.

Waiting time is added whenever a message is not sent.

Therefore, during n cycles of the algorithm, waiting time was added (n - m) times, and the total wait time, wTotal is

$$wTotal = T * (n - m); \quad (6)$$

Substituting n from Equation (5) yields

$$wTotal = T \left(\frac{m}{1-l} - m \right) \quad (7)$$

Rearranging Equation (7) yields

$$wTotal = m * T \left(\frac{l}{1-l} \right) \quad (8)$$

Therefore, the per message waiting time w is

$$w = T \left(\frac{l}{1-l} \right) \quad (9)$$

c is the total transmission time for a message (with one switch)

Therefore, the end to end delay (t) is

$$t = c + w \quad (10)$$

Substituting w from equation (9) yields

$$t = c + T \left(\frac{l}{1-l} \right) \quad (11)$$

Equation (11) shows how the end-to-end delay and roundtrip times change according to the channel load.

This equation can then be used to estimate the round trip time of messages transmitted over a switched network.

Figure 1: Waiting Time (w) and Message Time (T)

OMNeT++ Simulation

Figure 2: Network Setup with one switch

- HostA sends Ethernet control frames to HostB and HostB sends reply messages to HostA.
- Admission of packets into the network is controlled using the proposed probabilistic model shown in Algorithm 1.
- The simulation has been repeated twenty times with different random number seeds
- One million simulation packets have been sent and received during each simulation.
- This experiment has been done over a 10Mbps channel and a 100Mbps channel.
- Values of l range from 0 to 1 in 0.1 increments and T=0.2064ms for 10Mbps and T=0.02064ms for 100Mbps (T is the transmission time for the actual 258byte message that OMNeT++ uses)

Results

The theoretical (TH) and experimental (EX) results and their difference (DIF) are shown below. All values are in milliseconds.

	10Mbps			100Mbps		
l	TH	EX	DIF	TH	EX	DIF
0.0	0.8256	0.8256	0	0.0826	0.0826	0
0.1	0.8715	0.8715	-3.7e-6	0.0872	0.0871	-3.7e-7
0.2	0.9288	0.9288	-4.1e-5	0.0929	0.0929	-4.1e-6
0.3	1.0025	1.0026	-5.5e-5	0.1003	0.1002	-5.5e-6
0.4	1.1008	1.1008	-4.2e-6	0.1101	0.1101	-4.2e-7
0.5	1.2384	1.2384	-8.0e-6	0.1238	0.1238	-8.0e-7
0.6	1.4448	1.4447	1.2e-4	0.1445	0.1445	1.2e-5
0.7	1.7888	1.7889	-7.5e-5	0.1789	0.1789	-7.5e-6
0.8	2.4768	2.4767	1.7e-4	0.2477	0.2477	1.7e-5
0.9	4.5408	4.5401	6.4e-4	0.4541	0.4540	6.4e-5
1.0	∞	∞	-	∞	∞	-

Table 1: Theoretical and Experimental results and the Difference

Round trip time increases with the channel load in an exponential manner and it reaches infinity when the channel is full of load. The difference between the theoretical and experimental results is very small as can be seen in the Table 1. The theoretical model has been verified by simulation.

Figure 3: RTT vs. Load Theoretical & Experimental on same plot

Future Work

- Development of a closed form expression to estimate the round-trip-time of messages in the electric substations, specifically IEC 61850 networks, for different substation configurations.
- Expanding this approach to incorporate more complex network topologies as well as various other industrial protocols.
- Queuing delays will be incorporated.
- Introducing security vectors such as encryption, additional layers, etc. and analyzing the performance overhead and the end to end delays.
- Framework to support regulatory compliance testing and next generation substation network design.

Acknowledgement

This material is based on research sponsored by DARPA under agreement number FA8750-09-1-0208. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.

Using the following admission control algorithm the network load has been modeled and the theoretical model has been derived