I.J. Wireless and Microwave Technologies, **2011, 5, 60-66**
Published Online October 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.05.09

Available online at http://www.mecs-press.net/ijwmt

A Trust Evaluation Model for Industrial Control Ethernet Network

ZHOU Sen-xin [a,b], HAN Jiang-hong [a], TANG Hao [a]

[a]*School of Computer and Information, Hefei University of Technology, Hefei Anhui, 230009 ,China*
[b]*Information engineering School of Anhui University of finance & economics, Bengbu Anhui , 233041, China)*

Abstract

Industrial control ethernet networks are more impotant in connecting with equipments each other of enterprise comprehensive automation and integrating information. With the explosive growth of network techniques, the traditional control networks can no longer satisfy the security demands on network connectivity, data storage and information exchanges.New types of networks emerged in recent years in order to provide solutions for the increasing requirements on networked services. We propose a trust evaluation model for industrial control ethernet network . Our study shows the importance and necessity of applying theoretical analyses to understand the complex characteristics of trusted industrial control ethernet networks .

Index Terms: Trusted industrial control ethernet network,Security, Controllability,Survivability, Trust Model

1. Introduction

Recently, the industrial network becomes an indispensable component among automated systems.Especially, as the systems are required to be more intelligent and flexible, the systems should have more sensors, actuators, and controllers, often referred to as field devices. In most cases, these field devices require some type of electrical connection because they are distributed over a certain area. As the number of devices in a system grows and the functions of the system need to be more intelligent,these devices need to exchange the rapidly increasing amount of data among them. Conventionally,these devices are connected with point-to-point or direct connections, where each pair of devices requires at least one electrical cable. This approach is not suitable any more for the system composed of many devices because the number of cables is proportional to the square of the number of devices.As an alternative to the point-to-point connections,many industrial networks have been adopted, which can accommodate various data with shared transmission medium. Because the industrial network has more advantages than the point-to-point connection such as reduction of wiring and ease of maintenance,its application areas have grown to include various applications such as process automation system, automated manufacturing system, and automated material handling system [1,2].

* Corresponding author.
E-mail address: ahcdzsx@126.com

In general, data exchanged on an industrial network can be classified into two groups: real-time and non-real-time data. Non-real-time data do not have stringent time limits on their communication delays experienced during the data exchange. In contrast, real-time data have very strict time limits and the data's value is diminished greatly as the communication delay grows larger. This real-time data can be further divided into periodic and asynchronous data, depending on the periodic nature of the data generation. For example, the data for program download belong to non-real-time data, while digital control command and alarm signal are periodic and asynchronous real-time data, respectively. On many industrial networks, these data types are sharing a single network although they have different requirements on communication.That is, the non-real-time data need assurance of delivery without error and duplication, while the real-time data are concerned mostly on the time taken to reach the destination. Therefore, when building an industrial network, the designer must configure the network to satisfy these requirements.In order to satisfy the real-time requirements, many industrial networks, often referred to as fieldbus, have been developed by various standard organizations since the late 1980s. The IEC 61158 fieldbus standard with eight protocols, including Profibus, Fieldbus Foundation and WorldFIP, was announced as an international standard in the late 1990s [3]. Although the fieldbuses are able to satisfy the real-time requirements of field devices, they suffer from their high hardware and software cost and uncertain interoperability of multiple-vendor systems. These shortfalls are hindering the adoption of fieldbuses in numerous application areas. As an alternative to the fieldbus, Ethernet has attracted some attention because of its simplicity and wide acceptance. However, it has been known that Ethernet is not suitable for industrial networking because the medium access control (MAC) method of Ethernet is the contention-based carrier-sensing multiple access/collision detection (CSMA/CD) that exhibits unstable performance under heavy traffic and unbounded delay distribution [4]. In the last decade,several researchers, including Park and Yoon [4],Christensen [5], and Vitturi [6], have been trying to reduce collisions of Ethernet. Because these approaches require modifications in the data link layer or the TCP/IP layer, these still have limitations for practical applications. Recently, the switched Ethernet shows a very promising prospect for industrial networking because the switching technology can eliminate frame collisions. Because the Ethernet without collisions is no longer unstable under heavy traffic and its delay can be drastically reduced, the adoption of switched Ethernet as an industrial network is seriously considered along with the appearance of inexpensive switches [7–9]. More especially,High-Speed Ethernet (HSE) has been included in IEC 61158 fieldbus mainly as a network backbone at a higher level of automation hierarchy [10].

This paper presents the trust evaluation model of the switched Ethernet as communication network for interconnecting various components of real-time control systems. It looks at the factors affecting network performance, starting from basic statistical tools, such as queuing theory. It considers what techniques are available for assessing whether a network is capable of meeting the desired service levels, which are likely to be expressed in terms of throughput, delay and packet loss. We consider what techniques are available for assessing whether a network is capable of meeting the desired service levels, likely to be expressed in terms of throughput, delay and packet loss. Traditional queuing-based methods of dimensioning and the challenges offered by new insights into data arrival patterns are examined. We also demonstrate how modern QoS management techniques can control, but also complicate, prediction, and will finally illustrate how semi-empirical statistical techniques offer some resolution.

This paper is organized into six sections including this introduction. Section 2 gives Real-time performance analysis for industrial Ethernet network, and Section 3 presents the analysis for Self-similar behaviour of the switched Ethernet. A trust evaluation model for industrial control Ethernet network is implemented and evaluated in Section 4, and a set of Ethernet control network system model for trust evolution in opnet 14.5 simulation environment is implemented and its trust value is evaluated in Section 5. Finally, summary and conclusions are presented in Section 6.

2. Real-time performance analysis for Industrial Ethernet Network

The networks, systems, software applications, and data of many enterprises and organizations form a critical foundation and essential structure for industrial network. Without a reliable and functional network, the network control system is not secure. There are three key components of control networks analysis are network architecture, network protocols, and network performance analysis. The goal of a control network is to provide a

guaranteed quality of service such as deterministic time delays and maximum throughput for real-time control applications. These networks target various types of industrial automation and processing applications and are distinguished through static parameters such as data rate, message size, medium length, supported topology, number of nodes, and dynamic parameters such as MAC mechanism, message connection type,interoperability, and interchangeability. The modeling and control of NCSs are based on the analysis framework in time-delay systems which have been studied for several decades. In general, delays occur in the transmission of signals or materials between different subsystems.

In general, there are four major contributions to the delay in passing a single packet across a communications line. These are:the serialisation delay, which is given by the time it takes to transmit a single packet across a telecommunications link;the propagation delay, which is dependent on the length of the circuit and is calculated by dividing the length of the medium by the speed of light in that medium ; the queuing delay, i.e. the time the packet spends in the transmitting device output buffer awaiting serialisation/transmission, which is dependent on link utilisation and service time ; the time taken for the router to process packets.

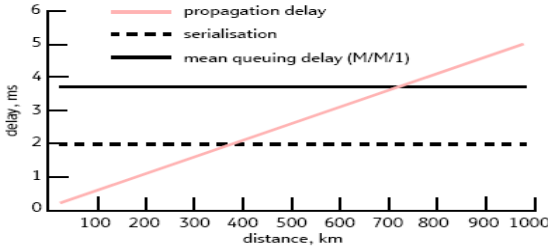

Figure 1. proportional impact of propagation delay

Figure 1 shows how these contribute to the delay for a 2048 kbit/s link, running at a utilisation of 65% carrying 512-byte packets. It can be seen that at distances below 350 km, the propagation delay is insignificant, becoming the dominant contributor to packet propagation when the circuit length exceeds 700 km.The queuing component is normally evaluated using one of two models: M/M/1 where the packet size is variable, and M/D/1 where the packet size is constant. (here the symbol M indicates Markovian behaviour and D indicates Deterministic behaviour). The queuing mechanism is held to comprise three main components — an arrivals process, the queue server and the service process. Following through the statistical analysis of this traffic gives a final prediction of the mean queuing delay (based on the average packet size and serial delay) as:

mean queuing delay = serialisation delay $\times$ ρ /(1- ρ)

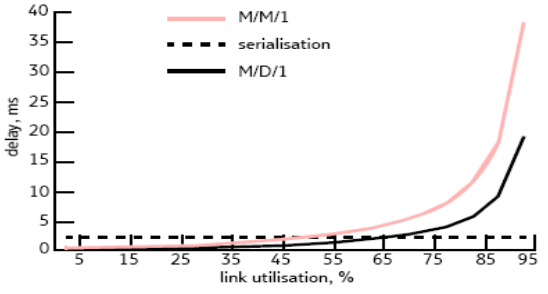

Figure 2. Queuing delay as function of link utilisation

It can easily be seen from Fig 2 that the queuing delay is almost negligible at link utilisations of less than 35%, but that it becomes progressively more important,increasing dramatically as link utilisation exceeds 70%. The

analysis so far has worked exclusively with mean values of delay; however, network providers are increasingly been asked for service level guarantees of network performance. [12]

3. Self-similar behaviour

Recent studies have demonstrated self-similarity in LAN and WAN traffic; Kim and Min [14] used a G/M/1 queuing model1 to model a network with self-similar traffic. They compared the analytic average queuing delay of self-similar traffic to the delay of a simulated model, to obtain a useful method for delay prediction. The simulation was done using OPNET, adjusting a single parameter of the truncated power-tail (TPT) distribution, thus allowing the analytic curve to follow the simulated results. They were able to predict the delay by computing the TPT, based on the measured Hurst parameter of the input traffic, the data arrival rate and the utilisation of the router.They were able to generate a model using selfsimilar arrival times and exponentially distributed service times and packet sizes. When H=0.5 the behaviour of G/M/1 tends to be close to M/M/1 but the average queuing delay of a router modelled by G/M/1 was shown to be greater than that from M/M/1, with the gap increasing with the magnitude of the Hurst parameter[15]. This comparison is shown in Fig 3.

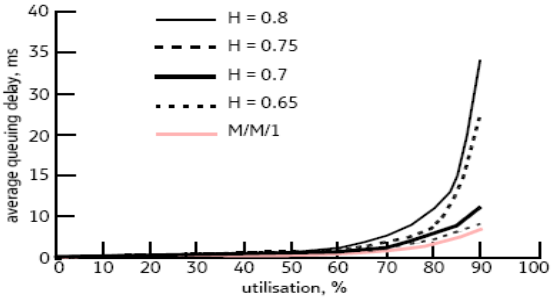

Figure 3. comparison between m/m/1 and G/M/1(self-similar) delay and utilization plots

4. A Trust Evaluation Model for Industrial Control Ethernet Network

Trust is important and critical for network security.It integrates with several components of network management,such as risk management, access control and authentication.Trust management is to collect, analyze and present trustrelated evidence and to make assessments and decisions regarding trust relationships between entities in a network.In this paper, we will focus on the evaluation of entity trust based on trust information provided by computing the TPT, based on the measured Hurst parameter of the input traffic, the data arrival rate and the utilization of the router at control networks layer.We also study The source node makes a decision on trusting the target node based on the portfile it receives from the target node at networked devices layer.Other layer trust information will be computed based on their trustrelated evidence.

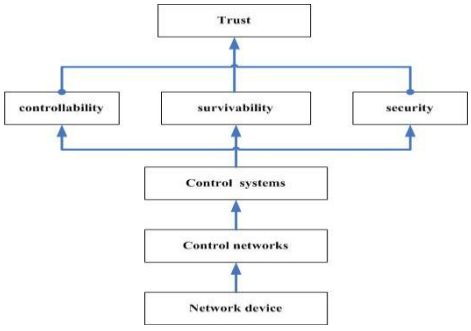

Figure 4. Trust Evaluation Model

A. Networked devices layer

Networked devices include smart sensors, smart actuators and networked controllers.Smart sensors and actuators have three major features: data acquisition, intelligence and communication ability. Each node (sensors, actuators and controllers) maintains a table of the history for their availabilities. The performance of a particular node in the network is stored in the local environment . Devices that operate in an control network are energy constrained.When a request is sent by a source node for recommendations about a particular node, a node may be selfish and not reply so as to conserve its energy. Due to lack of recommendations, the source node is unable to determine a reliable trust level on a particular target node in the network even though the node may be a trustworthy node.Therefore, to deal with such a situation, an exchange of portfile takes place. At the end or break of any communication between two nodes, they exchange a credential letter based on their experience with each other. When a node n has finished communication with a node x, the following exchange takes place:node n to node x:(n trusts x, context c1; time t1; n trusts x, context c2; time t2 ……n trusts x, context cn; time tn,K) This means that node n trusts node x in the context ci at a time stamp ts. Context here can be quality of service (QoS) or Availability (A)..[13]

B. Control networks layer

There are three key components of control networks analysis are network architecture,network protocols, and network performance analysis. Network architecture allows devices such as sensors, actuators, and controllers to be interconnected together, using less wiring, and requiring less maintenance than a point-to-point architecture. It also makes it possible to distribute processing functions and computing loads into several small units. The performance metrics of network systems that impact control system requirements include access delay, transmission time, response time, message delay,message collisions, message throughput, packet size, network utilization, and determinism boundaries. The goal of a control network is to provide a guaranteed quality of service such as deterministic time delays and maximum throughput for real-time control applications.There are now a large number of networks available for applications at the information level as well as at the device level. These networks target various types of industrial automation and processing applications are distinguished through static parameters such as data rate, message size, medium length, supported topology, number of nodes,and dynamic parameters such as MAC mechanism, message connection type,interoperability, and interchangeability.The trust for this layer is decided by utilisation and Hurst parameter of the input traffic. As is shown fig3 when utilisation is more 80% for h = 0.8 the average queuing delay will be more 10ms.Here the layer will be not trustworthy.[11]

C. Control systems layer

The goal of NCS design is to guarantee the stability and the performance of applied control systems, i.e., meets the control system specifications. These specifications include phase margin, gain margin, overshoot, steady state error, and tracking error.Simply speaking, the limited network bandwidth introduces unavoidable time delays in a control system. These time delays could potentially degrade a system's performance and possibly cause system instability. The trust for this layer is decided by system control model and trust value of above layer.

D. Trust layer

This layer is to provide a dynamic trust evolution that is multi-dimensional, that is,the trust evolves depending on controllability,survivability and security.The trust evolution may be quality of work done by control system for specific demands.It is a function of controllability,survivability and security defined by the user.

5. Experiments

We devised a set of Ethernet control network system model for trust evolution in opnet 14.5 simulation environment . Some experimental data and trust evaluation computing at a time are as follows:

TABLE I. TABLE OF TRUST EVALUATION COMPUTING AT A TIME

layer	parameters	Computing formula	Trust value
Networked devices	(a0.75y,QoS,80) (a0.75y,A,90)	If A>70 then trust = QoS	Trust value for Node a to y is 80%
control networks	H=0.8, utilization=70% delay time=9ms	For real time control signal=(delay time)/10* (*:real time control delay time requests lower then 10ms)	Trust value for this layer is 90%
Control systems	System stability=100%, sytem performance =98%	If System stability>=90% then trust = sytem performance	Trust value for this layer is 98%
Trust layer	Controllability=80%, survivability=72% , security=98%	Trust =(-clog2c+-s1log2s1+-s2log2s2)/T (c: Controllability,s1: Controllability,s2: Controllability,T=c+s1+s2)	Trust value for this layer is abou 0.83

6. Conclusions

Our work is just the first step on the exploration of understanding industrial control Ethernet networks trust management. We proposed a evaluation rule based on the global estimation result. This general rule can help to design rules that are feasible for different situations. Evaluation rules based on controllability,survivability and security of industrial control Ethernet networks makes the evaluation adaptive to trust dynamics. Trust dynamics is one of the main issues in autonomous networks. So it is necessary to integrate more trust contents into the evaluation rule.Future work will investigate adding more parameters to availability and quality of service for the derivation of trust. An optimization model for trust evaluation rule of industrial control Ethernet networks is needed. Other areas for future work include a more precise definition of controllability,survivability and security.

Acknowledgment

This paper is supported by National Nature Science Foundation of china under Project Number: 60473042 and 2009 Major Science Foundation Subject for the Education Department of Anhui Province under Project Number ZD200905.

References

[1] A. Willig, A. Wolisz, Ring stability of the PROFIBUS tokenpassing protocol over error-prone links, IEEE Trans. Ind. Electron. 48 (2001) 1025– 1033.
[2] S. Lee, K.C. Lee, M.C. Han, J.S. Yoon, On-line fuzzy performance management of Profibus networks, Comput. Ind. 46 (2001) 123– 137.
[3] IEC 61158-4, Digital data communications for measurement and control—Fieldbus for use in industrial control systems—Part 4: Data link protocol specification (IEC, 1999).
[4] J.H. Park, Y.C. Yoon, An extended TCP/IP protocol for real-time local area network, Control Eng. Pract. 6 (1998) 111 – 118.
[5] K.J. Christensen, A simulation study of enhanced arbitration methods for improving Ethernet performance, Comput. Commun.21 (1998) 24– 36.
[6] S. Vitturi, On the use of Ethernet at low level of factory communication systems, Comput. Stand. Interfaces 23 (2001)267– 277.
[7] G. Ye, H. Deng, L. Chen, L. Liu, X. Wang, A prototype switched Ethernet data acquisition system, Fusion Eng. Des. 43 (1999) 413– 416.
[8] B.Y. Choi, S. Song, N. Birch, J. Huang, Probabilistic approach to switched Ethernet for real-time control applications, Proceedings of Seventh International Conference on Real-Time Computing Systems and Applications, 2000, pp. 384– 388.

[9] E. Vonnahme, S. Ruping, U. Ruckert, Measurements in switched Ethernet networks used for automation systems, Proceedings of 2000 IEEE International Workshop on Factory Communication Systems, 2000, pp. 231– 238.
[10] D.A. Glanzer, Plantwide data integration using FOUNDATION fieldbus, Hydrocarbon Process. 80 (2001) F20– F22.
[11] M.Y. Chow, Y. Tipsuwan, Network-based control systems: a tutorial, 27th Annual Conference of the IEEE Industrial Electronics Society, Denver, 2001, pp. 1593– 1602.
[12] G.C. Walsh, Y. Hong, Scheduling of networked control systems,IEEE Control Syst. Mag. 21 (2001) 57– 65.
[13] Gokhale and Trivedi, "Analytical Models for Architecture-Based Software Reliability Prediction: A Unification Framework", IEEE Transactions Volume 55, Issue 4, 2006, pp. 578–590. International Journal of Grid and Distributed Computing Vol.3, No.1, March, 2010