http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (22): 6827-6831, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.6827.6831

Trust Evaluation Method for Industrial Control Ethernet Network

Sen xin Zhou, Decheng Wu and Chao Li
Management Science And Engineering School of Anhui University Of Finance and Economics,
233030, Bengbu Anhui, 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 .

Keywords: Trusted industrial control ethernet network, security, controllability,survivability, trust model

INTRODUCTION

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 in the last decade, the traditional centralized server-based management can no longer satisfy the requirements of next generation networks. So people started to propose new concepts of network infrastructure and management.In the meanwhile,the fast proliferation of networked devices and applications,such as sensor networks and pervasive computing, integrates information technology into our environments. These dramatic changes create unique challenges for network management and control. innovative solutions are required for managing network security and dynamics, astronomical number of data and enormous information exchanges(Lee *et al*., 2001).

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 (Walsh and Ye, 2001). 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(Willig and Wolisz, 2001; Lee *et al*., 2001).

This study 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

Corresponding Author: Sen xin Zhou, Management Science And Engineering School of Anhui University Of Finance and Economics, 233030, Bengbu Anhui, China

QoS management techniques can control but also complicate, prediction and will finally illustrate how semi-empirical statistical techniques offer some resolution(Vitturi, 2001).

This study is organized into six sections including this introduction. Section 2 gives Real-time performance analysis for industrial Ethernet network, A trust evaluation model for industrial control Ethernet network is implemented and evaluated in Section 3 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 4. Finally, summary and conclusions are presented in Section 5.

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 (Ye *et al*., 1999). 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(Choi *et al*., 2000).

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.

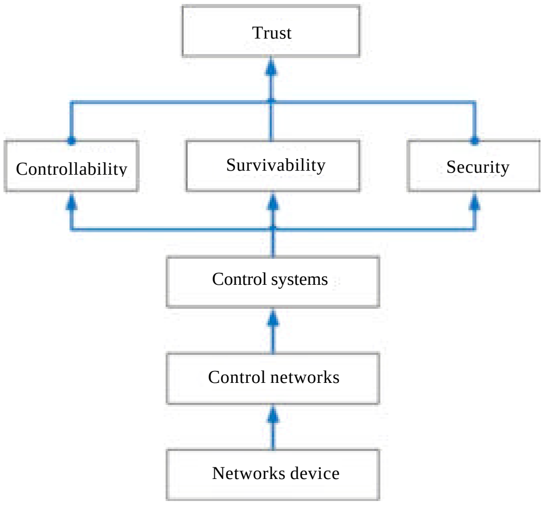

Fig. 1: Proportional impact of propagation delay

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. In the case of the M/M/1 queue, both the arrivals and service processes are governed by a Poisson distribution, whereas with the M/D/1 queue, the arrivals process has the Poisson form and the service process is deterministic (Chinni *et al*., 2008).

The impact of link utilisation on queuing delay is shown in Fig. 2. 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%.It can also be seen that the queuing impact is more pronounced for an M/M/1 type queue.At relatively long service times, if for example lowspeed links are used, the queuing delays become rather less than user acceptable.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. A large number of transactions will experience delays that are either shorter or longer than

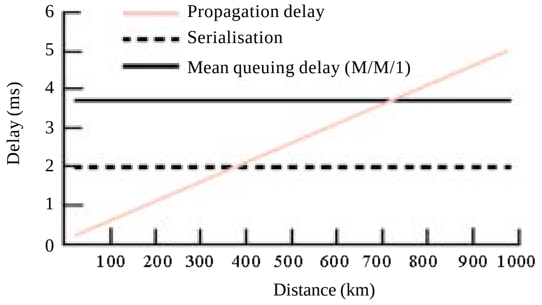

Fig. 2: Queuing delay as a function of link utilisation

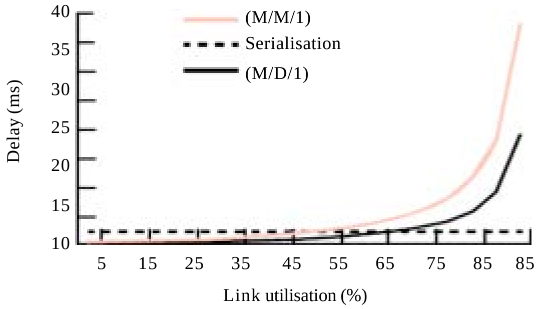

Fig. 3: Trust Evaluation Model

the mean; consequently it is dangerous to base service guarantees on mean delay figures. Further statistical analysis, for the above example, shows that if the mean delay for a telecommunications system is given as 2 ms, then 90% of packets will experience a delay of 8.92 ms or less; 95% will experience a delay of 12.4 ms or less and 99% will experience a delay of 14.8 ms or less(Smith, 2006).

TRUST EVALUATION METHOD 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 study, 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 (Park and Yoon, 1998).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.

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(Vonnahme *et al*., 2000). The performance of a particular node in the network is stored in the local environment . When a request is sent by a source node for trust recommendations about a particular node, 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.

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 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 Fig. 3 when utilisation is more 80% for h = 0.8 the average queuing delay will be more 10 ms.Here the layer will be not trustworthy (Smith, 2006).

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.

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.

EXPERIMENTS

We devised a set of Ethernet control network system model for trust evolution in opnet 14.5 simulation environment . As required for the Truncated Binary Exponential Back-Off algorithm, the wait periods after a collision in each Ethernet station are strictly bound between lower and upper limits. To simulate realistic network conditions, our specification model includes bursty traffic generators. Bursty traffic is an infinite sequence of frames with sub-sequences of closely spaced (in time) frames interspersed with sub-sequences of widely spaced (in time) frames, i.e., a plot of frames over time shows peaks and plateaus. Bursty traffic has a long tailed (power law) probability distribution and is typically modeled using a Poisson Pareto Burst (Christensen, 1998).Processes with heuristics to enable a close fit to observed data. To circumvent the issue of having to choose correct heuristics, a simple power law distribution is used in our setup(Chow and Tipsuwan, 2001).

When the average queue size is below a preset minimum bound, no packet is marked. When the average queue size exceeds the minimum queue length, the marking probability increases linearly until the average queue size attains the preset maximum queue length. As probability is normally not set to 100%, the queue size might rise above the maximum preset size. Hence, a limit parameter is provided to set a hard maximum for the size of the queue. RED uses a number of predefined and computed parameters. The predefined parameters are maximum dropping or marking probability, minimum and maximum queue lengths and queue weight. The parameters computed per iteration are count, average queue length, queue length and dropping or marking probability. Count is the number of frames since the last marked frame. For our simulation, we used the same values for the predefined parameters. In addition, the algorithm uses a linear function of time to determine the time interval since the queue was empty. In our case, we use simple difference in measured times to achieve this effect. Trust evolution of other layer was computed with data which we had collected.

CONCLUSION

The management of industrial control Ethernet networks has gained increasing attention because of their wide applications and control difficulties. Without the global management and control on the network, a small change in local domain may result in dramatic behavior changes on the whole network. Therefore, it is essential to understand the behavior of indutrial control networks before conducting any network management and control. In this work, we study the characteristics of Ethernet networks under the context of distributed trust management. Even though the trust evaluation rule we used is very simple, our analyses show extraordinary complexity in terms of the system performance. The analytic results enable us to design the evaluation rule that achieves desired performance.

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 study 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.

REFERENCE

Chinni, S., J. Thomas, G. Ghinea and Z. Shen, 2008. Trust model for certificate revocation in ad hoc networks. Ad Hoc Networks, 6: 441-457.

Choi, B.Y., S. Song, N. Birch and J. Huang, 2000. Probabilistic approach to switched Ethernet for real-time control applications. Proceedings of 7th International Conference on Real-Time Computing Systems and Applications, December 12-14, 2000, Cheju Island, South Korea, pp: 384-388.

Chow, M.Y. and Y. Tipsuwan, 2001. Network-based control systems: A tutorial. Proceedings of the 27th Annual Conference of the IEEE Industrial Electronics Society, November 29-December 2, 2001, Denver, pp: 1593-1602.

Christensen, K.J., 1998. A simulation study of enhanced arbitration methods for improving Ethernet performance. Comput. Commun., 21: 24-36.

Lee, S., K.C. Lee, M.C. Han and J.S. Yoon, 2001. On-line fuzzy performance management of Profibus networks. Comput. Ind., 46: 123-137.

Park, J. and Y. Yoon, 1998. An extended TCP/IP protocol for real-time local area networks. Control Eng. Pract., 6: 111-118.

Smith, E.A., 2006. Understanding performance issues in IP networks. BT Technol. J., 24: 172-178.

Vitturi, S., 2001. On the use of Ethernet at low level of factory communication systems. Comput. Stand. Interfaces, 23: 267-277.

Vonnahme, E., S. Ruping and U. Ruckert, 2000. Measurements in switched Ethernet networks used for automation systems. Proceedings of the IEEE International Workshop on Factory Communication Systems, September 6-8, 2000, Porto, pp: 231-238.

Walsh, G.C. and H. Ye, 2001. Scheduling of networked control systems. IEEE Control Syst., 21: 57-65.

Willig, A. and A. Wolisz, 2001. Ring stability of the PROFIBUS token-passing protocol over error-prone links. IEEE Trans. Ind. Electron., 48: 1025-1033.

Ye, G., H. Deng, L. Chen, L. Liu and X. Wang, 1999. A prototype switched Ethernet data acquisition system. Fusion Eng. Des., 43: 413-416.