A Network Traffic Visualization System for Industrial Control Systems

Kazuya Suzuki [*1] *Kenichi Eso* [*1] *Shunsuke Baba* [*2]

Stable network operation is indispensable for stable operation of industrial control systems. However traditional network management systems and visualization systems do not have enough functions for understanding the condition of their networks. Yokogawa has developed a system for visualizing network traffic that helps operators to quickly understand the current network condition. A network traffic visualization system consisting of two major components, a capturing tool and a traffic viewer, was developed to satisfy the requirements. The capturing tool connected to a network switch or a router captures network packets and sends them to the traffic viewer, which visualizes the state of all packets from sources to destinations. The evaluation with an actual industrial control system proved that this system can detect undesirable events such as suspicious communications that may disturb stable operation of industrial control systems.

INTRODUCTION

The network is essential for modern industrial control systems, and stable network operation is indispensable for stable operation of the entire control system. In this paper, any undesirable event that disturbs stable network operation is called failure. To eliminate such failures, and to quickly detect and respond to the events that may lead to failures, understanding the current network communication conditions is essential. The technologies for understanding the current conditions include network management technology and network visualization technology [(1)-(4)], and tools for visualization are available [(5)-(7)]. However, quick, accurate understanding of the network conditions is not easy with traditional technology. This paper reports on the technology developed by Yokogawa that visualizes the network traffic to intuitively understand the network communication conditions. This visualization technology enables network administrators to quickly understand the communication conditions of the entire network and to promptly take measures regarding the failures and events that may lead to other failures.

ISSUES IN NETWORK MANAGEMENT AND CONVENTIONAL TECHNOLOGIES

For stable operation of control systems, the devices connected to their network must work properly. However, it is difficult for traditional technologies to detect all the failures including illegal malware intrusions and setting errors of devices. For example, it is difficult for an intrusion detection system to detect new-type attacks. In addition, conventional network management systems have difficulty in precisely understanding the network communication conditions. As a result, because it is difficult to automatically confirm if devices are properly working, administrators must confirm the state of devices by themselves.

First, administrators try to understand the communication conditions of the network in which the visualization technology is effective. However, the conventional technologies only display the statistical values of the communication conditions and are not enough for intuitively understanding the communication conditions of the entire network. To solve this problem, Yokogawa has developed a system for visualizing the network traffic that helps administrators intuitively understand the network conditions.

VISUALIZATION SYSTEM

Requirements were defined first, and then a traffic visualization system was developed to satisfy these requirements.

Requirements for a Visualization System

Requirements for a visualization system to help administrators intuitively understand the communication conditions of the entire network are summarized below.

1) No impact on operation

It is essential that the introduction of the system does not disturb the plant operation.

2) Easy to understand

A system usable for engineers other than experts in

[*1] PA Systems Planning Dept.,
Systems Business Division, IA Platform Business Headquarters
[*2] Yokogawa IA Technologies India Private Ltd.

networks or security is required.

3) Flexibility

All packets should be visualized, but it is required that packets that administrators consider unnecessary are filtered out and are not displayed.

4) Real-time visualization

The network conditions need to be visualized in real-time to understand them. In this paper, the word real-time is not necessarily used in its strict sense, but instead, it means promptness to process data as quickly as possible without performing unnecessary buffering.

5) Reproducibility of failures

To identify the cause of a failure, the conditions at the time of the failure occurrence need to be analyzed. For this purpose, the network traffic needs to be saved to reproduce the conditions afterward.

Architecture of Visualization System

Figure 1 shows an example of architecture of the visualization system and target for visualization. The visualization system is composed of the following modules.

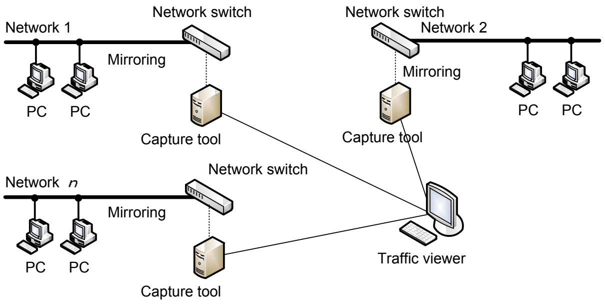

Figure 1 Example of architecture of the visualization system and target for visualization

- Capture tool

This tool captures the network packets, forwards them to the traffic viewer, and at the same time saves them on its hard disc. This tool has a filtering function so that it does not capture unnecessary packets.

- Traffic viewer

This viewer displays the packets captured by the capture tool. This viewer also has a filtering function to not display unnecessary packets.

To use this system, simply enabling the mirroring function of network devices such as network switches and routers is enough. Installing client software on PCs is not required. Therefore, this system hardly affects control systems.

Representing in animated motion

To help administrators understand the network communication conditions quickly and intuitively, this system represents the network traffic in animated motion.

- Drawing communication packet paths

The packets of the network traffic among devices are represented by using animation. In the basic mode, all the packets are drawn on a two-dimensional network chart as an arrow. The behavior of the packets from sources to destinations is drawn using animation. In the three-dimensional mode, the height of the arrow for each packet represents a destination port number.

- Coloring

The color of an arrow for each packet can be changed according to types of the protocol or networks transmitted to.

- Detailed information

Detailed information on each packet cannot be seen while the network traffic is being drawn in real-time. To solve this problem, the drawing can be temporarily suspended to display the detailed information of packets.

SYSTEM INSTALLATION AND EVALUATION

System Installation

This system can be applied to various networks. Figure 2 shows a typical example of a control system network to which the system is applied.

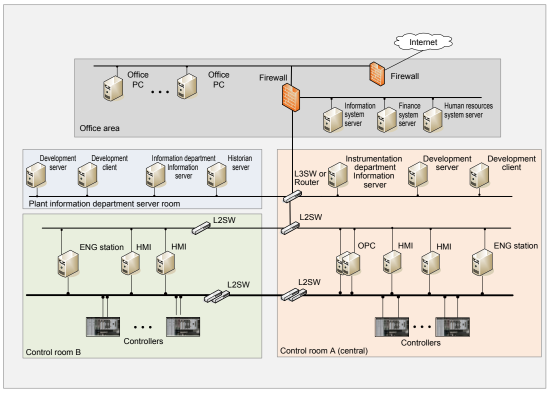

Figure 2 An example network to which the visualization system is applied

- Installing capture tools at multiple locations

In this system, packets captured by the capture tool are displayed. In other words, packets cannot be displayed unless they reach the capture tool. To avoid such situation, this system is designed so that multiple capture tools can be installed in the network. The capture tools installed at multiple locations capture mirrored packets and send them to the traffic viewer, which displays these packets collectively.

- Effective installation location

Ideally, capture tools should be installed at all network switches in the network. However, if the installation at all network switches is difficult, capture tools are installed at selected ones. To monitor inside the network, installing a capture tool at the layer-2 switch located at the center of the communication is recommended. To monitor the communication with external networks, installing a capture tool at default gateways and the like is recommended.

Examples of the System Operation

This system was applied to a control system for an operation experiment. Some drawing examples are shown below.

- Under normal conditions

Figure 3 shows a visualized network traffic under normal conditions with no problems in the network. Arrows between hosts indicate that these pairs of hosts are communicating at that moment.

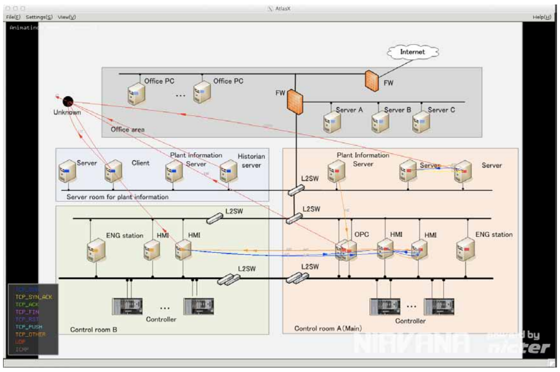

Figure 3 Under normal conditions

- Port scans caused by malware infection (two-dimensional display)

Figure 4 shows a situation in which a certain host is generating a large amount of communication packets. This indicates that this host is infected with malware and is performing a port scan looking for possible targets to intrude. This system has a function to draw an arrow between hosts for each packet. Thus, when a large number of packets are transmitted between specific hosts, a large number of arrows are drawn, which look like a thick line.

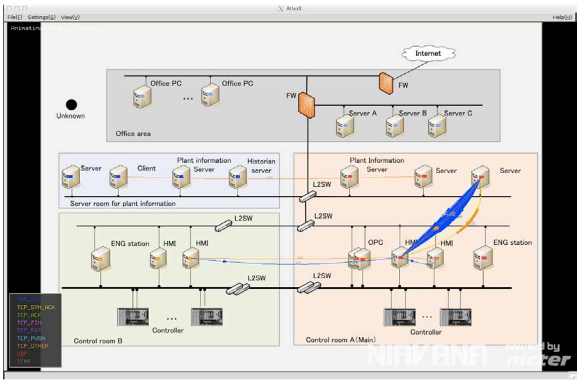

Figure 4 A drawing example indicating port scans (two-dimensional display)

- Port scans to a specific host (three-dimensional display)

Figure 5 shows a three-dimensional display of communication packets to a certain host. This example indicates port scans to a specific host. This is a three-dimensional representation while the above is two-dimensional.

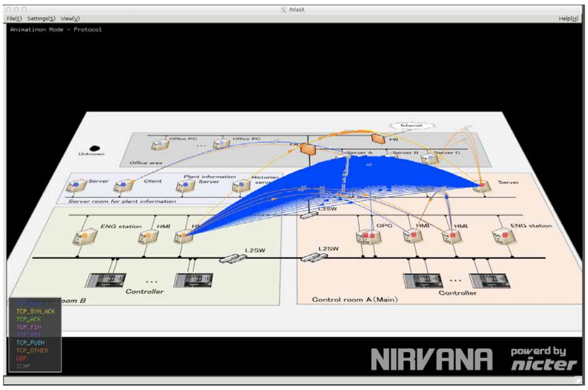

Figure 5 A drawing example indicating port scans (three-dimensional display)

- Massive communication packets from a host

Figure 6 shows a situation in which a certain host is infected with malware and is sending a large amount of packets to multiple hosts.

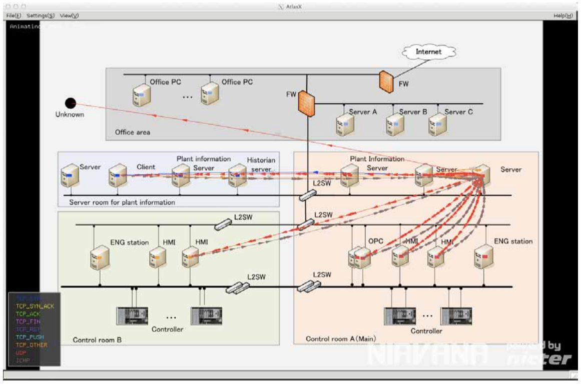

Figure 6 A drawing example of massive communication packets

System Evaluation

The system developed on the basis of the requirements was evaluated qualitatively.

1) No impact on operation

The only preparation for using this system is to set up mirroring of the network devices. No client software is required to be installed in PCs. Therefore, the impact of this system on the control systems is negligible.

2) Easy to understand

This system has achieved the visualization for which even engineers other than network experts can understand the occurrence of an unusual communication situation visually and intuitively. This system has a filtering function to display only the packets that the administrator considers necessary, allowing easy understanding. In addition, the capability of changing colors of the arrows depending on the types of the protocol or networks transmitted to is effective for easier understanding.

3) Flexibility

The filtering functions of both the capture tool and traffic viewer allow selection of the packets for display. This enables flexible drawing, and also helps easy understanding as described above.

4) Real-time visualization

This system draws network traffic without data buffering to ensure a real-time property.

5) Reproducibility of failures

The capture tool has a function to save the packets. An administrator can reproduce the past failures by specifying the start time.

Effectiveness of this System

The effectiveness of this system is summarized below.

● Detecting unusual communication

This technology help operators to recognize unexpected communications from their control systems to external networks, which means that unidentified devices are connected to the control systems or unidentified communication occurred from identified devices. This requires operators to handle this issue immediately.

● Detecting absence of necessary communication

In control systems, all communication transactions must be recognized and controlled. This system can detect the absence of necessary communication caused by setting errors or the like, and enables administrators to respond to such inconsistency.

CONCLUSION

We developed a traffic visualization system to support plant or network operators to understand their network conditions. We first summarized requirements for the system, implemented the system, and evaluated the system.

Tools for automatic detection of unauthorized communication or absence of normal communication still remain for future development. Although full automatic analysis is difficult, Yokogawa hopes to develop a tool that analyzes network traffic according to the conditions defined by administrators, and implement such functions in it that automatically filter out unnecessary packets as much as possible.

This development was carried out jointly with the National Institute of Information and Communication Technology. The authors wish to express their sincere gratitude to persons concerned.

REFERENCES

(1) R. Kawahara, K. Ishibashi, et al., "Detection accuracy of network anomalies using sampled flow statistics," IEEE Global Communications Conference, Washington, DC, USA, 26-30 November 2007, pp. 1959-1964

(2) T. Karagiannis, K. Papagiannaki, et al., "BLINC: Multilevel traffic classification in the dark," ACM SIGCOMM Computer Communication Review, Vol. 35, No. 4, 2005, pp. 229-240

(3) K. Ohno, H. Koike, et al., "IP Matrix: An effective visualization framework for cyber threat monitoring," Proceedings of the 9th International Conference on Information Visualisation (IV05), IEEE, 2005, pp. 678-685

(4) Y. Hideshima, H. Koike, "STARMINE: A visualization system for cyber attacks," Asia Pacific Symposium on Information Visualisation (APVIS), 2006, pp. 131-138

(5) OETIKER+PARTNER, RRDtool, http://oss.oetiker.ch/rrdtool/

(6) OETIKER+PARTNER, MRTG, http://oss.oetiker.ch/mrtg/

(7) Cacti Group, Inc., cacti, http://cacti.net/

* All product names or names mentioned in this paper are either trademarks or registered trademarks of their respective holders.