ATLANTIS PRESS

Journal of Robotics, Networking and Artificial Life
Vol. **8**(**3**); December (2021), *pp.* 175–179
DOI: https://doi.org/10.2991/jrnal.k.210922.005; ISSN 2405-9021; eISSN 2352-6386
https://www.atlantis-press.com/journals/jrnal

Research Article

An Emulation Mechanism for PLC Communication Features

I-Hsien Liu[1], Chia-Chun Lai[1], Jung-Shian Li[1], Chi-Che Wu[1], Chu-Fen Li[2], Chuan-Gang Liu[3,*]

[1]*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No. 1, University Rd., East Dist., Tainan City 70101, Taiwan*
[2]*Department of Finance, National Formosa University, No. 64, Wenhua Road, Huwei Town, Yunlin County 63201, Taiwan*
[3]*Department of Applied Informatics and Multimedia, Chia Nan University of Pharmacy & Science, No. 60, Sec. 1, Erren Rd., Rende Dist., Tainan City 71710, Taiwan*

ARTICLE INFO

Article History
Received 09 November 2020
Accepted 29 June 2021

Keywords
Industrial control system
communication
network
device identification
cyber security

ABSTRACT

In recent years, internet has widely used in different fields. To identify a specific device, we usually use the information which attains from network packets such as Internet Protocol (IP) address, Media Access Control (MAC) address and communication port, etc. However, using this kind of information is not enough to identify precisely. Furthermore, most of this kind of information could be imitated easily. Therefore, our research focuses on behavior of communication devices that can identify the devices precisely and create a communication system which is able to imitate the behavior of some specific devices.

1. INTRODUCTION

With the growth of internet technology, there are more and more industrial systems connecting to the internet. This result in devices that can connect to the internet have an explosive increase. As a result, how to specify every device on the internet has become a big problem. Compare to the past, some information such as Internet Protocol (IP) address, Media Access Control (MAC) address, and communication port is commonly used to identify a specific device on the internet. However, using this kind of information is not enough to identify comprehensively because the information can simply be imitated by any other devices. This research focus on the features of communication devices and also provide a mechanism that can analyze these features and generate configuration references which other devices can simply apply. With the customized communication module and the references mentioned above, it can make other devices imitate the behavior of the analyzed device and provide a better effect on device emulation. With the emulation of devices features, it can make the emulation devices close to the specific devices. This communication system might be useful in some special domain such as industrial communication system that need an emulator which can induce hackers to attack the industrial control system.

2. BACKGROUND

This section discusses some research and methods which are commonly applied to perform device identification. This section would involve the general method that mostly used on every internet device in the world and some novel methods that are proposed by other researchers using different kind of emerging technologies.

2.1. Packet Header

When devices communicate with each other, they must use the same protocol. Thus, allow them to understand what the other side transmit. Nowadays, the generally used protocol is the TCP/IP protocol suite. This protocol suite includes a great deal of widely used protocols. Some well-known protocols in the TCP/IP suite are IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), etc., which are performed in different layers. These protocols have their own specific packet header when they are used.

The information in these headers or the combination of different information in different header can be used to identify the source of the internet packet. In the next few paragraphs, this paper will explain the detail of how information in headers is used for device identification.

2.1.1. IP header

IP is the principal protocol in network communication. In the IP header, the major fields are source address and destination address and both exist in IPv4 and IPv6 header. Though the length of the address in IPv4 and IPv6 are different, the main function of these headers is the same. It can identify which device sends out this packet and which device should this packet send to. The two pieces of information could simply identify a specific device, but it is not

[*] *Corresponding author. Email:* chgliu@mail.cnu.edu.tw

enough for precise identification. Some networks may use network address translation and many devices would share a public IP address. In this situation, using an IP address as the only identifier is not enough for device identification.

2.1.2. TCP header

TCP often uses on reliable transmissions such as a webpage, video stream, and file transfer, etc. In the TCP header, there are two fields that can be used for device identification. These two fields are the source port and destination field. However, they cannot be used independently. They need to combine with IP address mentioned in the previous paragraph and carry out a better performance for device identification.

2.1.3. Ethernet frame

Ethernet protocol is a protocol that belongs to the data link layer. Recently, it is the principal protocol in general internet environment. Each Ethernet packet has an Ethernet frame that contains a header. An Ethernet header has four major fields: destination MAC addresses, source MAC addresses, Ethertype and IEEE 802.1Q tag or IEEE 802.1ad tag.

2.2. Traffic Patterns

Various devices will generate different traffic patterns depending on their needs. Some researches use traffic patterns to identify the devices. Research from Hiroki KAWAI has shown that they can analyze traffic patterns and identify devices in different categories [1]. Also, there are some researchers using machine learning to identify IoT devices which can classify all devices that connect to the network into some specific types [2–4].

3. FEATURES OF DEVICES

Each device has its special features when they are communicating. This research focus on the behavior of devices when they transmit packets. In our previous research, we find that the latency of the response packet between each device is unique. This discrepancy can be caused by various factors in different layers.

3.1. Physical Layer

The devices produced by the same factory with different models will have their unique features due to the variation of assembly lines. Regardless of the same model, they still exist unique features because of the standard error which is allowed by its supplier. Even more, the manufacturing tolerance that set by the manufacturer will also increase the diversity of features in devices.

3.2. Transport Layer

When devices transmit on the internet, they need to determine the protocol that is used in transport layer. Different protocols will result in respective behavior and generate a distinctive feature of devices. For instance, when set up an OpenVPN environment, using UDP protocol might provide lower latency than using TCP protocol [5]. This shows that which protocol is used will impact the features of devices.

3.3. Application Layer

Every device has an operating system. Both the executive application and operating system on the device would affect the behavior. Moreover, the same function programmed in a different language would lead to various features. Different version of firmware may also increase the diversity of features. In conclusion, the application layer has many factors that will affect the behavior of the device.

4. EXPERIMENT AND RESULT

This research proposes a communication system that contain a mechanism of feature analysis which can generate data to perform devices emulation. The experiment uses a Schneider Programmable Logic Controller (PLC) to be an emulate device, using a Windows 10 PC responsible for analyzing other devices. Owing to the experiment device, the experiment will use a specific protocol which is commonly used in industrial control system called Modbus. Also, our communication system is programmed in C++ and run on Linux which can perform a better latency control of communication. Figure 1 is the overview of the system. This system can be separated into two parts. In Figures 2 and 3, it shows that the system has two major chains. The first chain is responsible for device analyzation and the second chain is responsible for emulation of the device.

4.1. Analysis Side

On the analysis side, it uses a computer to send the request of response, then send to the device being analyzed. When the

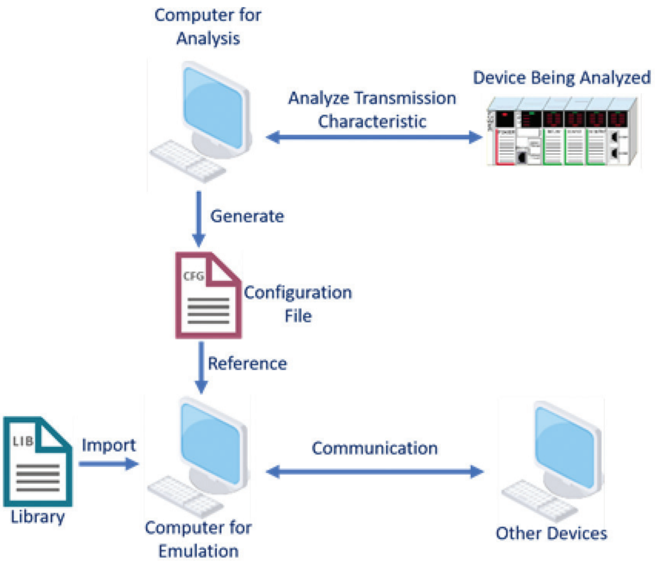

Figure 1 | Overview of our specific communication system.

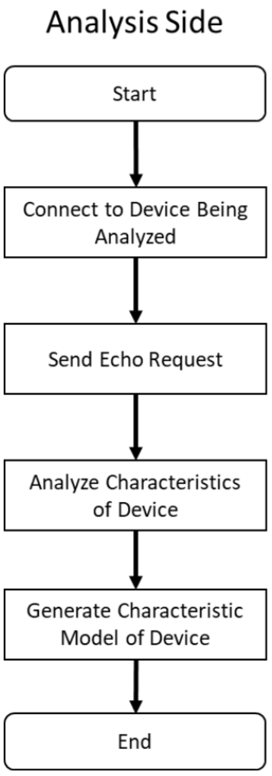
Analysis Side
Start
Connect to Device Being Analyzed
Send Echo Request
Analyze Characteristics of Device
Generate Characteristic Model of Device
End

Figure 2 | Flow chart of the analysis side of specific communication system.

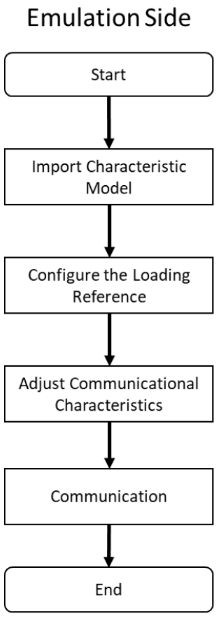
Emulation Side
Start
Import Characteristic Model
Configure the Loading Reference
Adjust Communicational Characteristics
Communication
End

Figure 3 | Flow chart of the emulation side our specific communication system.

device being analyzed response to our computer, the computer then record its round-trip time. After the analyzation, the analysis side sorts out these data into a feature model and arranges the data to a configuration file that can be used for the emulation side.

Table 1 | The statistical table of experiment device

Device	Sample size	Average	Standard deviation
Schneider PLC	10,000	5.9258	0.378033
Emulator	10,000	5.9304	0.391371

Table 2 | The Kolmogorov–Smirnov test result

Most extreme differences	Absolute	0.006
	Positive	0.001
	Negative	−0.006
Kolmogorov–Smirnov Z		0.403
Asymp. Sig. (two-tailed)		0.997

4.2. Emulation Side

On the emulation side, a device can either run our specific communication program or import our customize library. Both of them can load the feature model generated by the analysis side. Furthermore, the system adds a specific parameter called the loading parameter. Using the loading parameter, it can imitate the features of the device. Meanwhile, the device is at the working status.

4.3. Analysis Result

To analyze the result of our emulation, our result focuses on the latency of response messages. The result of analysis chooses Kolmogorov–Smirnov test for analyzation. Table 1 is the statistical table of our experiment. The analysis computer sends 10,000 read register Modbus packet to both Schneider PLC and our emulator.

To explain how to evaluate the result, this paper will briefly explain the Kolmogorov–Smirnov test in the next paragraph. In Kolmogorov–Smirnov test, we assume that two samples come from the same distribution. In the result of the test, there is a field called asymptotic significance. In general, if asymptotic significance is greater than 0.05 or 0.1, it means that two samples come from the same distribution.

Table 2 is the Kolmogorov–Smirnov test of our experiment. The asymptotic significance is 0.997 which is greater than 0.01. In other words, the emulation device can respond in the same features as the true Schneider PLC.

5. CONCLUSION

This paper proposes a mechanism to improve the emulation of device that focused on the difference of behavior on devices. This paper analyzes the response latency of device, then create a features model which can be applied to our specific commutation system. Our specific communication system can load the model file and provide a load parameter that can imitate the loading of device which is the behavior of device in working status. Also, according to the statistical table, this paper show that the system proposed can let normal computer imitate the same behavior as the working PLC.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

ACKNOWLEDGMENTS

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 109-2218-E-006-014-, MOST 109-2218-E-006-510- and MOST 109-2221-E-041-001-.

REFERENCES

[1] H. Kawai, S. Ata, N. Nakamura, I. Oka, Identification of communication devices from analysis of traffic patterns, 2017 13th International Conference on Network and Service Management (CNSM), IEEE, Tokyo, Japan, 2017, pp. 1–5.

[2] O. Salman, I.H. Elhajj, A. Chehab, A. Kayssi, A machine learning based framework for IoT device identification and abnormal traffic detection, Trans. Emerging Tel. Technol. (2019), e3743.

[3] A.J. Pinheiro, J. de M. Bezerra, C.A.P. Burgardt, D.R. Campelo, Identifying IoT devices and events based on packet length from encrypted traffic, Comput. Commun. 144 (2019), 8–17.

[4] Y. Meidan, M. Bohadana, A. Shabtai, J.D. Guarnizo, M. Ochoa, N.O. Tippenhauer, et al., ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis, Proceedings of the Symposium on Applied Computing, Association for Computing Machinery, NY, USA, 2017, pp. 506–509.

[5] I. Coonjah, P.C. Catherine, K.M.S. Soyjaudah, Experimental performance comparison between TCP vs UDP tunnel using OpenVPN, 2015 International Conference on Computing, Communication and Security (ICCCS), IEEE, Pointe aux Piments, Mauritius, 2015, pp. 1–5.

AUTHORS INTRODUCTION

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Mr. Chia-Chun Lai

He was born in Taichung, Taiwan in 1997. He received his B.S. degree from the Department of Electrical and Computer Engineering, National Chiao Tung University, Taiwan in 2019. He is acquiring the master's degree in Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

Prof. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.

Dr. Chi-Che Wu

He is a research assistant in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU). He obtained his PhD in Electronic Engineering of College of Electrical Engineering and Computer Science from National Kaohsiung University of Science and Technology in 2020. His research interests relate to the mobile computing, cloud computing, information security, internet communication, industrial control system and Object-Oriented programming.

Prof. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in Information Management, Finance and Banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.

Prof. Chuan-Gang Liu

He is an Associate Professor in the Department of Applied Informatics and Multimedia, Chia Nan University of Pharmacy and Science. He received the B.Sc. degree from the Department of Electrical Engineering, Tam Kang University, in 2000. Then he graduated from the National Cheng Kung University with M.S. and PhD degrees in Electrical Engineering. His research interests are in the areas of optical networks control, wireless networks, EPON, VANET, network security, cloud computing and TCP performance analysis.