SACM Working Group
Internet Draft
Interned status: Standards Track
Expires: August 27, 2017

S. Li
M. Wei
H. Wang
Q. Huang
P. Wang
J.Liao
Chongqing University of
Posts and Telecommunications
February 23, 2017

Anomaly Detection of Industrial Control System based on Modbus/TCP
draft-li-sacm-anomaly-detection-00

Abstract

Aiming at the vulnerability and security threat of Industrial Control System, this document proposed a detection model based on the characteristics of Modbus/TCP protocol.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on August 27, 2017.

Copyright Notice

Table of Contents

1. Introduction

With the development of industrialization and informatization, increasing information technology is applied to the industrial field. Due to the hardware and software, which are widely used in Industrial Control Systems, come from different vendors, and the ICS need to interact the information with the outside net, both of them make Industrial Control Systems more and more open, and face more security threats.

The research of anomaly detection for ICS is introduced as follows. For example, the anomaly detection of communication protocol datagram format has the premise of obtaining a specific proprietary protocol specification, the detection method based on protocol message format is liable to cause lower detection rate, and is not easy to expand. Another anomaly detection mechanism is the configuration of blacklist and whitelist, in order to realize this mechanism, engineers need to run the system, and set the blacklist and whitelist according to the ICS state.

In addition, most research work focus on intrusion detection algorithm, the key to improve the detection rate is to extract efficient features of anomaly detection. Research on intrusion

detection algorithm shows that, the basic principle of neural network method is to use learning algorithm to study the relationship between input and output vectors, and to sum up a new input-output relationship. The neural network algorithm has rather high computational complexity, and very large demand for samples, while it is difficult for Industrial Control System to extract more samples. Genetic algorithm is a natural selection based on the best search algorithm, but it has higher coding complexity, and longer training time.

However, Support Vector Machine algorithm is a kind of data classification method based on statistical learning theory. It has many advantages, such as few samples, good generalization and global optimization. Therefore, the SVM algorithm based on clustering is suitable for the anomaly detection of ICS.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as described in [RFC2119]

1.2. Terms Used

ICS: Industrial Control System.

SVM: Support Vector Machines. SVM is specified in [CoVa1995].

Security: It means the specific security mechanism or security algorithm.

2. Overview of the detection scheme

In this document, the establishment of the system anomaly detection model is based on the periodic characteristics of Industrial Control System and communication protocol message characteristics of Modbus/TCP. The industrial control network equipment involved in the anomaly detection process includes security gateway, programmable logic controller, security management platform and controlled device, wherein the security gateway includes an anomaly detection subsystem and a packet depth analysis system. The packet depth analysis system executes depth analysis and feature extraction for Modbus/TCP packet, the anomaly detection subsystem is used to detect the underlying network data and generate an alarm response to the abnormal data. Depending on the specific technological process, the programmable logic controller issues control commands to the controlled device for orderly production. Security management platform is responsible

for the configuration of security mechanism and the handling of abnormal alarm in the security gateway. Controlled equipment, including level gauge, pressure gauge, temperature sensor and so on, is responsible for the collection of physical quantity in the industrial production process. The detection process is as follows.

(1) Capture the communication data between master and slave devices through the security gateway, and then analyze the data.

(2) According to the packet format of Modbus/TCP protocol, the packet depth analysis system directs at the feature fields that should exist in the packet and the expected values for those fields, analyzes the packets in depth layer-by-layer, and removes the excess attribute characteristics, only leaving the characteristics related to the system behavior patterns.

(3) According to the eigenvectors extracted by the packet depth analysis system, the anomaly detection subsystem constructs the classifier for the purpose of measurement, statistics and abnormal detection, and sends an alarm to the security management platform for abnormal results.

3. A detection model based on Modbus protocol features

Modbus/TCP is an application layer protocol that embeds a Modbus frame into a TCP frame, its message transmission service is to provide communication between client and server, and these devices are connected to an Ethernet TCP/IP network. Modbus/TCP protocol is specified in [RFC793] and [RFC791]. Modbus/TCP packets include two parts, Modbus Application Protocol (MBAP) and Protocol Data Unit (PDU). For the Modbus Application Protocol packet header, it contains the transaction ID, protocol ID, length, and unit ID. The protocol data unit includes the function code and data. The transaction ID represents the packet identification of the Modbus request/response transaction processing. The function code represents the control command, which is sent by the master device to the slave device, each specific function code represents a different operation. According to the source address and the destination address of the packet, the direction of transmission of data packets is generated.

Extract transaction identifier, slave function code, slave communication address, and packet transfer direction eigenvector, port number elements as the eigenvector, and construct a number of different categories of eigenvalues in the eigenvector, which makes the description of the behavior pattern of the system more accurate

and reasonable, and the detection accuracy of detection model is also improved.

An anomaly detection model of SVM based on K-means clustering is constructed by the acquired eigenvectors, and these eigenvectors are based on communication behaviors. This process is shown in Figure 1.

(1) The k-means clustering algorithm is used to preprocess the protocol feature vector, which randomly selects the k objects as the initialization cluster, and calculates the average of the data in each cluster. The standard criterion function is used to determine whether the cluster center is stable or not.

(2) By using the clustered data as the input data, the SVM classifier is constructed.

(3) There are three main steps involved in SVM algorithm. Firstly, construct the hyperplanes of classification. Secondly, select the appropriate training parameters, which include the penalty factor and the radial basis function. Finally, obtain the decision function in SVM.

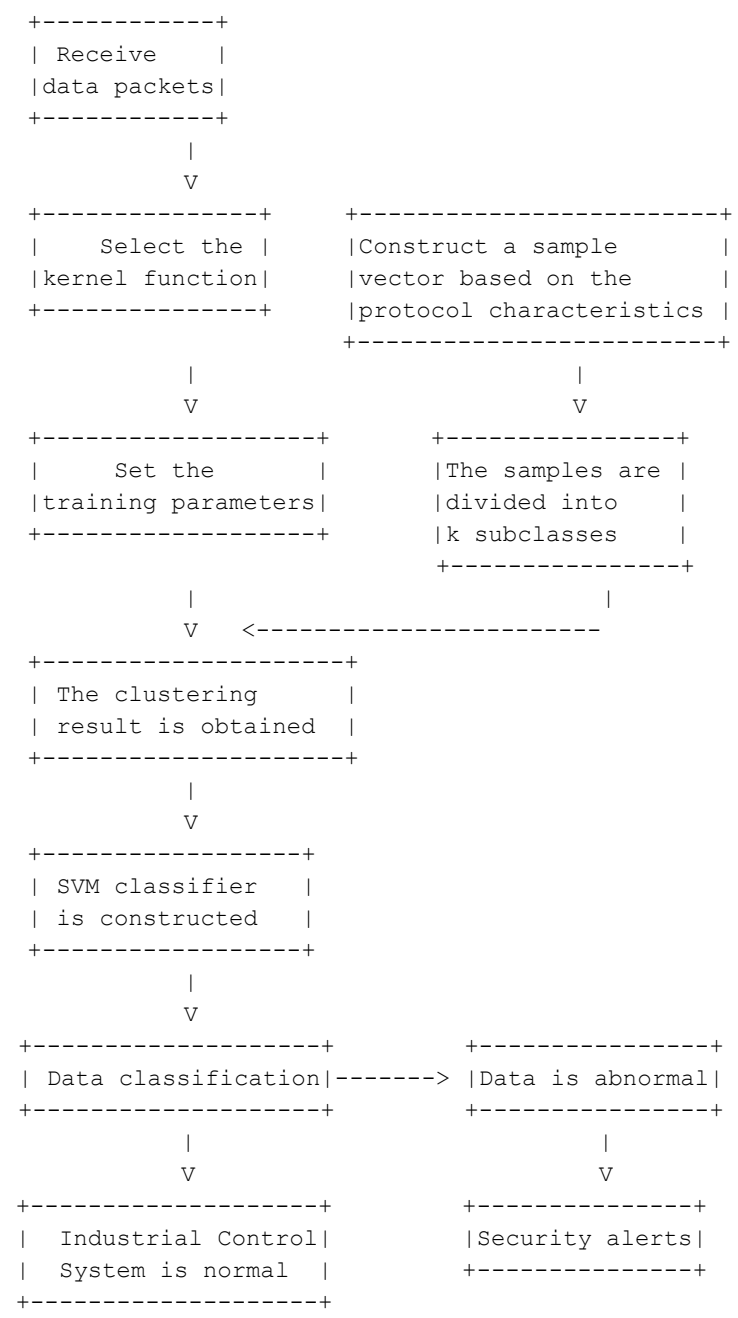

Figure 1 SVM anomaly detection model based on clustering

4. Security Considerations

TBD.

5. IANA Considerations

This memo includes no request to IANA.

6. References

6.1. Normative References

6.2. Informative References

[RFC2119]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC791]
Postel J. RFC 791: Internet protocol[J]. 1981.

[RFC793]
Postel J. RFC 793: Transmission control protocol, September 1981[J]. Status: Standard, 2003, 88.

[CoVa1995]
Cortes C, Vapnik V. Support-vector networks[J]. Machine learning, 1995, 20(3): 273-297.

Authors' Addresses

Shuaiyong Li
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: lishuaiyong@cqupt.edu.cn

Min Wei
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: weimin@cqupt.edu.cn

Hao Wang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: wanghao@cqupt.edu.cn

Qingqing Huang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: huangqq@cqupt.edu.cn

Ping Wang
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road

Chongqing, 400065
China

Phone: (86)-23-6246-1061
Email: wangping@cqupt.edu.cn

Jie Liao
Key Laboratory of Industrial Internet of Things & Networked Control
Ministry of Education
Chongqing University of Posts and Telecommunications
2 Chongwen Road
Chongqing, 400065
China

Email: 928053580@qq.com