IoT Real-Time Threat Detection System at Network Edge

Kota Tsuchie　Taketsugu Yao

Solutions that utilize IoT devices have expanded in recent years, and a wide variety of devices have come to be connected to the network edge where IT devices are directly connected. However, unauthorized access into organizations using vulnerable IoT devices as stepping stones has become a problem[1]. For example, there has been a case where an IoT device capable of mobile communication was connected to an office LAN without authorization and allowed an intruder to gain access to the internal network directly from the Internet. This resulted in the leakage of confidential information.

To address this issue, OKI utilized a technology that analyzes the communication characteristics of IoT devices at the network edge to develop the IoT Real-Time Threat Detection System (hereinafter referred to as the System), which will detect unknown devices and unusual communication behavior in a lightweight and real-time manner.

This article introduces the outline and functions of the System, and the verification efforts.

Increasing Security Threats

The complexity of device management stemming from the expanded utilization of IoT devices is behind the increase in threats originating at the network edge. Until now, employee PCs were connected at the network edge and the main security measure was to install agent-type software of asset management systems or endpoint security products in each PC. However, with the introduction of systems that use IoT devices to improve operation and production efficiencies, a wide variety of devices have come to be connected to the network edge. Many of these devices lack computational resources and cannot be equipped with agent-type software. It is also difficult for the administrator to keep track and manage every single device. Therefore, a solution for managing the devices and detecting threats such as unauthorized access is necessary.

NDR and Issues with Existing Configuration

NDR (Network Detection and Response) is a security measure for the network edge. NDR captures mirrored traffic from the network switch to identify the connected devices and detects abnormal traffic patterns from their behaviors. One method of detecting abnormal traffic patterns is machine learning the benign traffic patterns of a device and determining that there is an abnormality such as information leakage or the spread of malware when the traffic pattern deviates. Additionally, NDR is effective as a security measure for IoT devices since it does not require software to be installed in the devices.

One possible NDR system configuration is placing a device that captures network traffic at the network edge and sending the captured results to the cloud server for analysis. However, in such a configuration, the large volume of data transmitted from each network edge to the cloud server may strain the communication bandwidth and affect normal business communication. Furthermore, time will be required to detect and deal with abnormal traffic patterns due to the round-trip propagation delay between data transmission and result notification. Therefore, it is desirable to perform the analysis at the edge, but that would necessitate a high-spec analyzer at each edge raising issues of cost and securing installation space.

Focusing on the issues of the existing NDR mentioned above, OKI has conducted research and development on the IoT Real-Time Threat Detection System that analyzes edge traffic in real-time and detects threats even with edge devices with limited computational resources.

Proposed System and Research Goal

The proposed System captures and analyzes network traffic at the edge device to detect network threats. The edge device of the System uses OKI's "AE2100[2]" AI edge computer that is capable of performing high-speed AI inference processing. **Figure 1** shows the connection configuration of the System. The AE2100 connects to the mirror port of the monitored network switch and captures the traffic flowing through the switch. AE2100 can also be connected to the communication port of the monitored network to inspect monitored devices for vulnerabilities.

The goal of the research is to develop an anomaly detection function that processes traffic and detects threats in real-time using the above configuration.

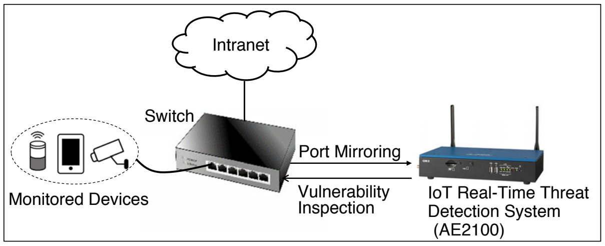


Figure 1. Connection Configuration

Technical Issue and Solution Approach

The technical issue facing the System is how to analyze network traffic in real-time using a device with limited computational resources. Two approaches to resolving this issue is given below.

The first approach is to perform analysis using only the information in the packet headers. Although the conventional methods of analyzing the packet payloads will provide more details about the communicated content, the processing load is heavy and difficult to analyze with an edge device. The information that can be used for analysis is limited using only the packet headers and anomaly detection becomes more challenging. However, the load on the processor will be lighter. In order to achieve such lightweight analysis, OKI has collaborated with a university on a technology to analyze traffic from a small amount of information and applied it to this initiative.

The second approach is to utilize a VPU (Vision Processing Unit), which can execute AI analysis on hardware. In AI analysis, advanced analysis can often be performed using deep learning. However, deep learning places a heavy load on the processor, and therefore it required the use of a high-spec device to analyze flowing traffic in real-time. VPU is hardware specialized for deep learning inference processing, and enables even the edge device to execute high speed processing. The System realizes real-time analysis at the edge by using the VPU installed in the AE2100.

The anomaly detection functions developed under the solution approach presented above are described in the next section.

Anomaly Detection Functions

The System has two types of anomaly detection function. One is for when connecting devices to the network and the other is for when devices are in operation.

(1) Connection Anomaly Detection

The connection anomaly detection function executes in isolation when a device is connected to the network. Specifically, it consists of an unauthorized device detection function that detects connection of an unintended device and a vulnerability detection function that detects vulnerabilities in the connected device. The device identification technology that serves as the fundamental technology to enable these functions was developed in collaboration with a university[3]. The device identification technology will be described first followed by the descriptions of each anomaly detection function.

The feature of the device identification technology lies in its ability to identify a multitude of device types using only the header information from the first 200 packets of a traffic flow. The identification of the device type is illustrated in **Figure 2**. The figure shows the traffic patterns of a network camera and a smart power plug. The horizontal axis represents the time of the generated communication packets while the vertical axis represents the packet size. As for the traffic pattern of the network camera, control packets are initially generated when connecting to the camera from a terminal such as a PC. This is followed by a video data stream from the camera. In case of the smart power plug, after the initial control packets at the time the plug is connected, packets for switching the power on/off flow irregularly. The device identification technology learns such traffic patterns specific to a device type. Utilization of the technology enables the unauthorized device detection function described later to be realized, and the inspection time of the vulnerability detection function can be shortened.

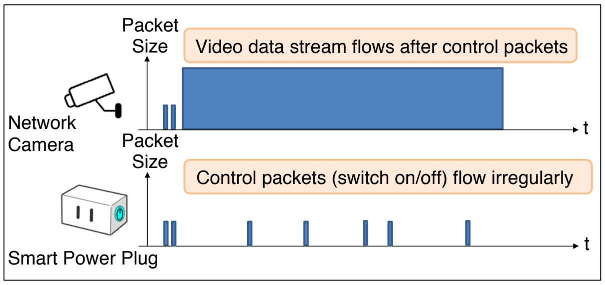

Packet Size
Video data stream flows after control packets
Network Camera
t
Packet Size
Control packets (switch on/off) flow irregularly
Smart Power Plug
t

Figure 2. Device Identification Technology

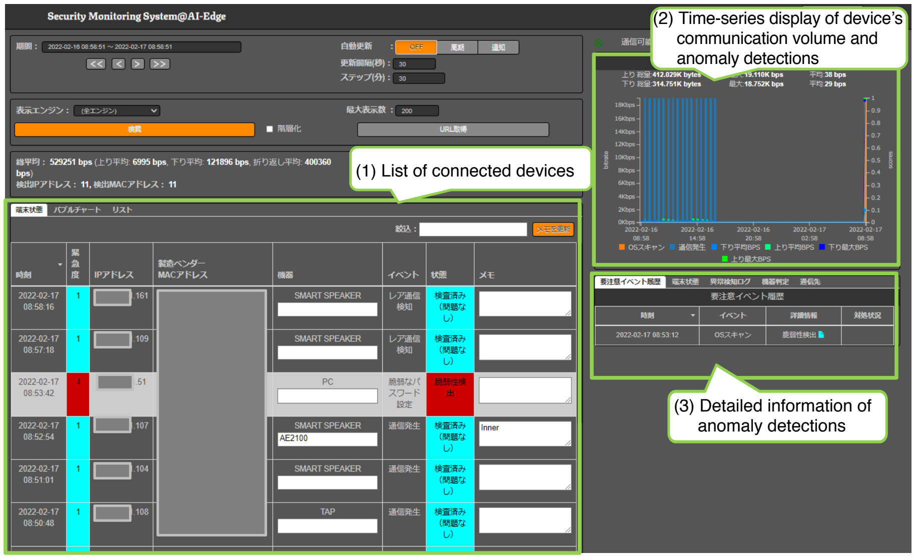
Unauthorized device detection function identifies a device as unknown when the traffic pattern does not resemble the characteristics of any known device type using the device identification technology. If the device is identified as an unknown type, it is determined that an unauthorized device has been connected.

The vulnerability detection function inspects devices for vulnerabilities. Specifically, it conducts a port inspection on the devices to check if unnecessary TCP/UDP ports are open. It also checks whether the opened ports can be connected with a simple ID/PASS (password) by running a crosscheck against a list of commonly used passwords. Generally, it is desirable to perform vulnerability inspection with a wide range of inspection items to ensure there are no omissions, but that will be time consuming. This function uses the results of the device identification technology to optimize the inspection items for each device and speed up inspection time. Therefore, during port inspection, only the ports that require attention depending on the device type are inspected. In case of network cameras and other similar IoT devices, inspection is limited to ports that are susceptible to attacks such as the remote connection ports for telnet and file transfer ports for ftp. In password inspection, a list of ID/PASS is prepared for each device type to reduce the number of inspection items. For instance, a PC's PASS is crosschecked against a list of PASS that users tend choose frequently, whereas an IoT device is crosschecked against a list of often used default ID/PASS to reduce inspection items.

(2) Operation Anomaly Detection

Operation anomaly detection function runs during device operation to analyze the network traffic of the connected device and detects abnormal traffic patterns such as malware activity and information leakage. In order to detect such events, unsupervised machine learning is used to learn the regular traffic patterns of devices and detection of irregularities in the patterns are considered cyberattacks. Conventionally, an AI approach required high-spec equipment to analyze network traffic in real-time, thus difficult to implement on an edge device. However, in recent years, VPUs have been developed as hardware that exclusively executes inference processing for deep learning, and have come to be installed in edge devices. Operation anomaly detection utilizes the VPU installed in the AE2100 to analyze network edge traffic in real-time and detect cyberattacks. The function is in the research and development stage, and currently, a method based on existing research[4] is implemented in the AE2100. It is undergoing evaluation in an experimental network environment, and also its operation is being verified in a demonstration experiment described later.

To verify the efforts thus far, an evaluation was conducted in an experimental network environment to determine the viable communication rate for the implemented method's real-time processing. As a result of the evaluation, it was confirmed that traffic with a communication rate of up to 9Mbps can be processed in real-time when operated with a VPU[5]. Currently, the function is undergoing operation at a demonstration site to verify whether the current method can withstand actual operation. In a move to develop a cyberattack detection method, evaluation of this method's detection accuracy is planned for the future. Additionally, there is a plan to enhance the method to improve the



期間： 2022-02-16 08:58:51 ～ 2022-02-17 08:58:51

更新間隔(秒)： 30
ステップ(分)： 30
最大表示数： 200

総平均： 529251 bps (上り平均: 6995 bps, 下り平均: 121896 bps, 折り返し平均: 400360 bps)
検出IPアドレス： 11, 検出MACアドレス： 11

時刻	緊急度	IPアドレス	製造ベンダー MACアドレス	機器	イベント	状態	メモ
2022-02-17 08:58:16	1	[redacted].161	[redacted]	SMART SPEAKER	レア通信検知	検査済み（問題なし）	
2022-02-17 08:57:18	1	[redacted].109	[redacted]	SMART SPEAKER	レア通信検知	検査済み（問題なし）	
2022-02-17 08:53:42	4	[redacted].51	[redacted]	PC	脆弱なパスワード設定	脆弱性検出	
2022-02-17 08:52:54	1	[redacted].107	[redacted]	SMART SPEAKER AE2100	通信発生	検査済み（問題なし）	Inner
2022-02-17 08:51:01	1	[redacted].104	[redacted]	SMART SPEAKER	通信発生	検査済み（問題なし）	
2022-02-17 08:50:48	1	[redacted].108	[redacted]	TAP	通信発生	検査済み（問題なし）	

(1) List of connected devices

(2) Time-series display of device's communication volume and anomaly detections

上り 総量:412.029K bytes　19.110K bps　平均:38 bps
下り 総量:314.751K bytes　最大:18.752K bps　平均:29 bps

要注意イベント履歴

時刻	イベント	詳細情報	対処状況
2022-02-17 08:53:12	OSスキャン	脆弱性検出	

(3) Detailed information of anomaly detections

Figure 3. Dashboard Screen

throughput that can be processed in real-time so that it can be applied to environments with high communication loads.

Visualization and Notification Functions

The System has functions to visualize the anomaly detection results through dashboard and report output, and it can be accessed from a Web browser. It also has a notification function that enables the occurrence of threats to be notified via email.

The dashboard screen is shown in **Figure 3**. A list of connected devices is shown on the left side of the screen (1), and information such as IP/MAC address, manufacturer, device type determined by the device identification technology, and device status is provided. The status of the device is color-coded according to the attention level that the device requires, thus devices with high urgency can be seen at a glance. Detailed information for each device can be checked on the right side of the screen. Information includes the time-series transition of communication volume and number of anomaly detections (2), and details of the anomaly detections and communication destinations (3).

Demonstration Efforts

As an application example of the System, two demonstration efforts that OKI is currently conducting will be introduced.

(1) Internal Network Monitoring

Organizations require countermeasures against cyberattacks not only at the Internet access points, but also within onsite networks to deal with attacks caused by both external intruders and internal fraudsters. OKI's customer, the central government ministries and agencies, is one of those organizations. OKI's System has been installed in the government's internal network, and the anomaly detection function is currently undergoing performance evaluation. **Figure 4** shows the condition of the demonstration. The purpose of the demonstration is mainly to evaluate the effectiveness of the anomaly detection function during device operation. Abnormal download traffic from the file server during non-business hours and traffic that simulates the spread of malware infection are purposely generated to verify whether these events can be detected.

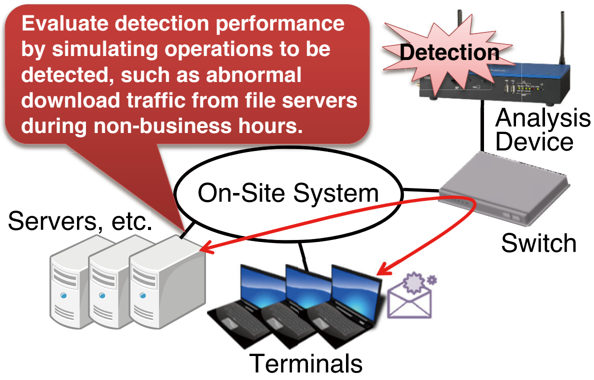

Evaluate detection performance by simulating operations to be detected, such as abnormal download traffic from file servers during non-business hours.
Detection
Analysis Device
On-Site System
Servers, etc.
Switch
Terminals

Figure 4. Central Government Ministries and Agencies' Internal Network Monitoring Demonstration

(2) Factory Network Monitoring

Lately, targets of cyberattacks have expanded to factory equipment. There have been cases where malware from an infected in-house PC made its way into the network to which factory equipment is connected causing temporary suspension of operations. Therefore, OKI has installed the System in its factory, and evaluation is being conducted to determine whether it is possible to visualize assets and vulnerabilities in the factory using the connection anomaly detection function, thereby stopping threats such as malware infection before they occur. Through actual installation of the System, the traffic patterns of the network equipment in the factory became clear such as the unexpected communication of network equipment and unexpected the settings of connected devices. The purpose of the demonstration is mainly to identify issues in an actual operation of factory network monitoring. The demonstration is planned to be expanded outside the company, and operational issues that are brought to light will be fed back to system development.

Conclusion

This article introduced the IoT Real-Time Threat Detection System, which detects security threats at the network edge. Using lightweight traffic analysis of packet headers and VPU-based AI processing, the System realizes highly real-time security monitoring on edge devices with limited computational resources.

Based on knowledge obtained from demonstrations, OKI will further enhance the current detection functions, develop new functions, and improve the System to solve operational problems in the field.

Acknowledgment

Parts of the system-installed functions described in this article were developed in collaboration with Professor Shingo Ata of Osaka City University, and OKI expresses its deepest gratitude. ◆◆

References

1) BBC News, Raspberry Pi used to steal data from Nasa lab, 24 June 2019
https://www.bbc.com/news/technology-48743043

2) Takamitsu Shimada: Realizing High-Speed Deep Learning Inference with AI Edge Computer “AE2100”, OKI Technical Review, Issue 234, Vol.86 No.2, December 2019
https://www.oki.com/en/otr/2019/n234/pdf/otr-234-R05.pdf

3) H. KAWAI et al.: Identification of Communication Devices from Analysis of Traffic Patterns, Proc. 13th International Conference on Network and Service Management (CNSM 2017), Japan, 2017

4) T. D. Nguyen et al.: “D ÏoT: A Federated Self-learning Anomaly Detection System for IoT”, Proc. 39th IEEE International Conference on Distributed Computing Systems (ICDCS2019), July 2019

5) Kota Tsuchie et al: Implementation and Evaluation of Real-Time Threat Detection System at the Network Edge, IEICE technical report, vol.121, No.434, IN2021-31, pp.1-6, March 2022

Authors

Kota Tsuchie, Network Technologies R&D Department, Innovation Promotion Center

Taketsugu Yao, Network Technologies R&D Department, Innovation Promotion Center