

Background :

According to Microsoft Security Intelligence Report 2019, **Malware Encounter Rate in ASEAN region is very high.**

Cyber-Space does not have country borders. It is necessary to eliminate this situation in order to make the cyber-space safe.

Targets:

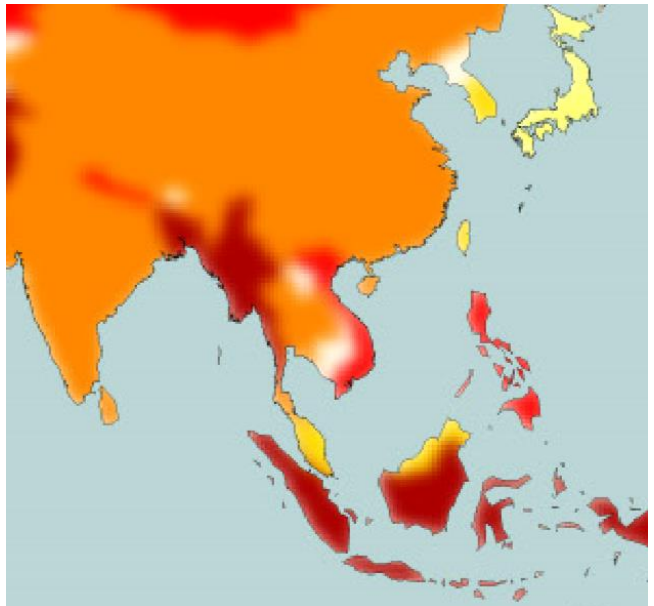
We target the security of the Local Area Networks (LAN)
Enhance the functions of LAN-security monitoring devices and programs, which are currently provided as an open source by **LAN-based Security Monitoring Project.**

Enhancement :

- *Anonymization of captured LAN data*
- *Visualization of data for useful security operation*
- *Statistical analysis of data*
- *Improvement of detection algorithms (with ML)*
(*) such as federated learning (proposed by Google)

Speaker:

Asst.Prof. Norrathep Rattanavipanon(PSU)



Average Monthly Malware Encounter Rate, 2018 (Microsoft, Security Intelligence Report, 2019)



Project Title: ASEAN-Wide Cyber-Security Research Testbed

Project Members :

| Full Name | Institution, Country |
|-------------------------|--|
| Sinchai Kamolphiwong | Prince of Songkla University, Thailand |
| Achmad Basuki | Universitas Brawijaya, Indonesia |
| Mie Mie Su Thwin | University of Computer Studies Yangon, Myanmar |
| Aung Htein Maw | University of Information Technology, Myanmar |
| Hideya Ochiai | The University of Tokyo, Japan |
| Kuljaree Tantayakul | Prince of Songkla University, Thailand |
| Touchai Angchuan | Prince of Songkla University, Thailand |
| Norrathep Rattanavipano | Prince of Songkla University, Thailand |
| Adhitya Bhawiyuga | Universitas Brawijaya, Indonesia |
| Raden Arief Setyawan | Universitas Brawijaya, Indonesia |
| Zhiqing Zhang | The University of Tokyo, Japan |
| Yuwei Sun | The University of Tokyo, Japan |
| Chiruphapa Pawissakan | The University of Tokyo, Japan |

Project Duration :

2 Years: 2020-2022
With one-year extension

Project Budget:

2020-2021: 33,050 USD
2021-2022: 12,345 USD
2022-2023: 5,000 USD

According to survey study, malware encounter rates in ASEAN region are very high. In order to make it a real-world public testbed for cyber-security studies, this project is going to enhance the functions of the monitoring devices provided by LAN-security monitoring project by installing around hundred newly-developed security devices across ASEAN countries. To that end, we are going to develop (i) vulnerability assessment of remote local-area networks, (ii) visualization of data for useful security operation, (iii) improvement of detection algorithms and statistical analysis including the application of federated learning, and (iv) anonymization of captured data for publicizing the data.

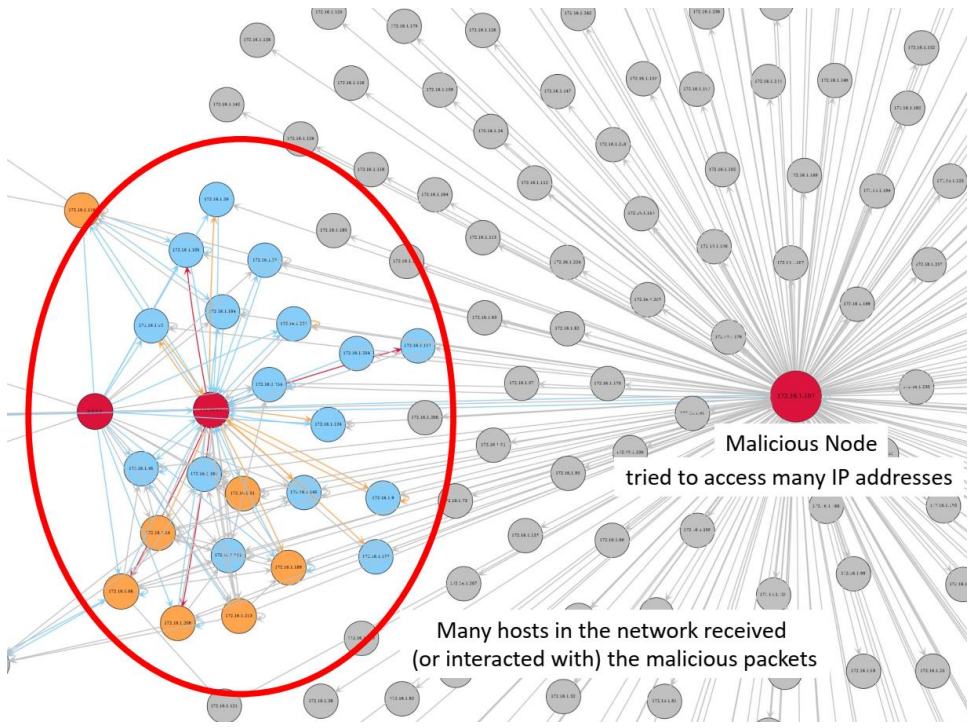
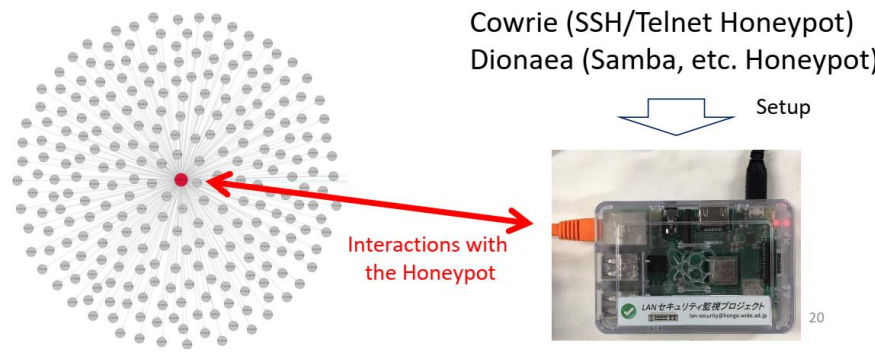


Fig 1. Visualized connection graph of a LAN. In this case, it is easier to read the node's IP addresses. However, sometimes it become too complex to read them.



Fig. 2: Monitoring node of LAN-security monitoring project



Project Activities: On-line workshop: Preparation of Monitoring Node Deployment

July 9th, 2020

1. We developed a manual of installing LAN security monitoring device for ASEAN IVO Project.

LAN-Security Monitoring Device

How to Setup for ASEAN IVO Project

Create: 2020-06-24
Update: 2020-07-09

Part I : Preliminary Setup

1. Raspberry Pi OS (Raspbian) Installation

Insert microSD card into your PC.

Download Raspberry Pi Imager from <https://www.raspberrypi.org/downloads/> into your PC, and execute it for installing Raspberry Pi OS into your microSD card.

Choose **Raspberry Pi OS Lite (32-bit)** - A port of Debian with **no desktop environment**



Raspberry Pi OS Lite (32-bit)

A port of Debian with no desktop environment
Released: 2020-05-27
Online - 0.4 GB download

10 pages

2. We setup a data collection server in June.


3. We had an online workshop for installation of monitoring device.



July 9th, 2020

Sensor nodes installation

*** Myanmar-UIT
(20 Nodes)**



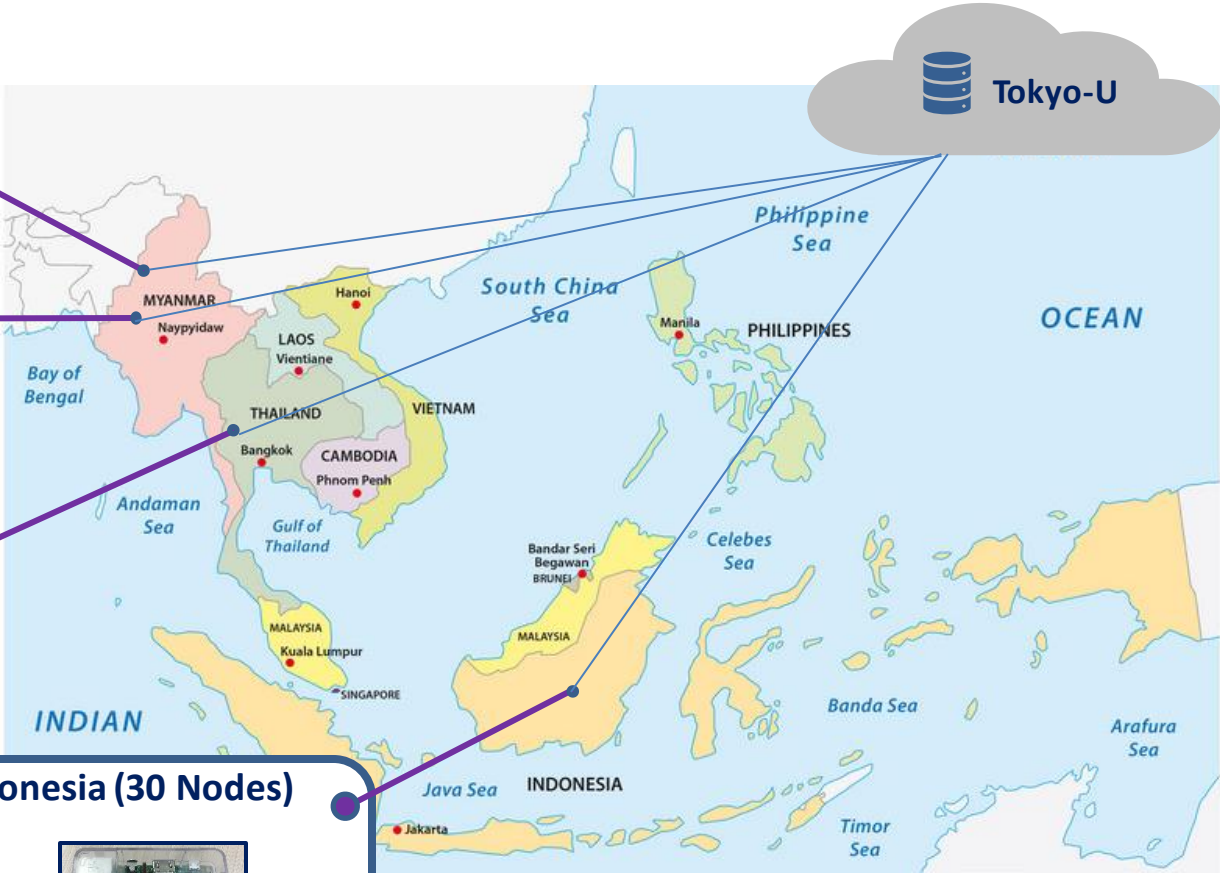
*** Myanmar-UCSY
(30 Nodes)**



**Thailand-PSU
(40 Nodes)**



Indonesia (30 Nodes)



Project Activities: Online workshop:

"LAN Security Monitoring Device"

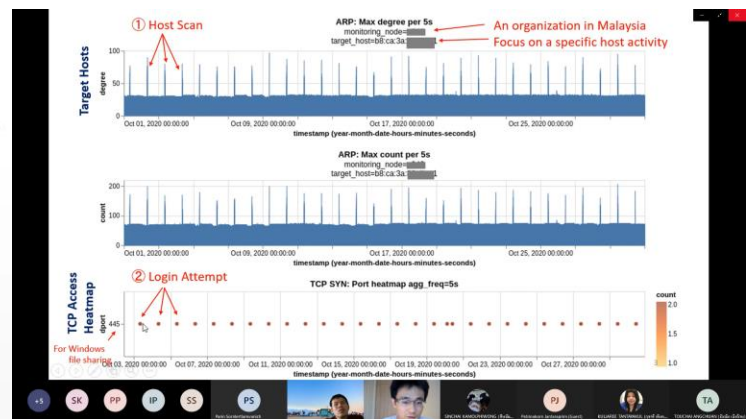
October 1st, 2021

We organized an **online hand-on workshop** for distribution and installation of the LAN security monitoring nodes.

The screenshot shows a PowerPoint slide with the following content:

- Title:** LAN-Security Monitoring Project
- Background:** Cyber Security Research
- Objective:** Research on LAN Security
- Project Lead:** Associate Prof. Ph.D., Hideya Ochiai (UTokyo, Japan) Prince of Songkla University & The University of Tokyo
- Project Location:** ASEAN-WIDE Cyber Security Research Testbed (NICT)
- Date:** October 1st, 2021

The slide features a network diagram with nodes and connections. The presentation interface includes a sidebar with navigation options and a bottom toolbar with icons for notes, comments, and other functions.



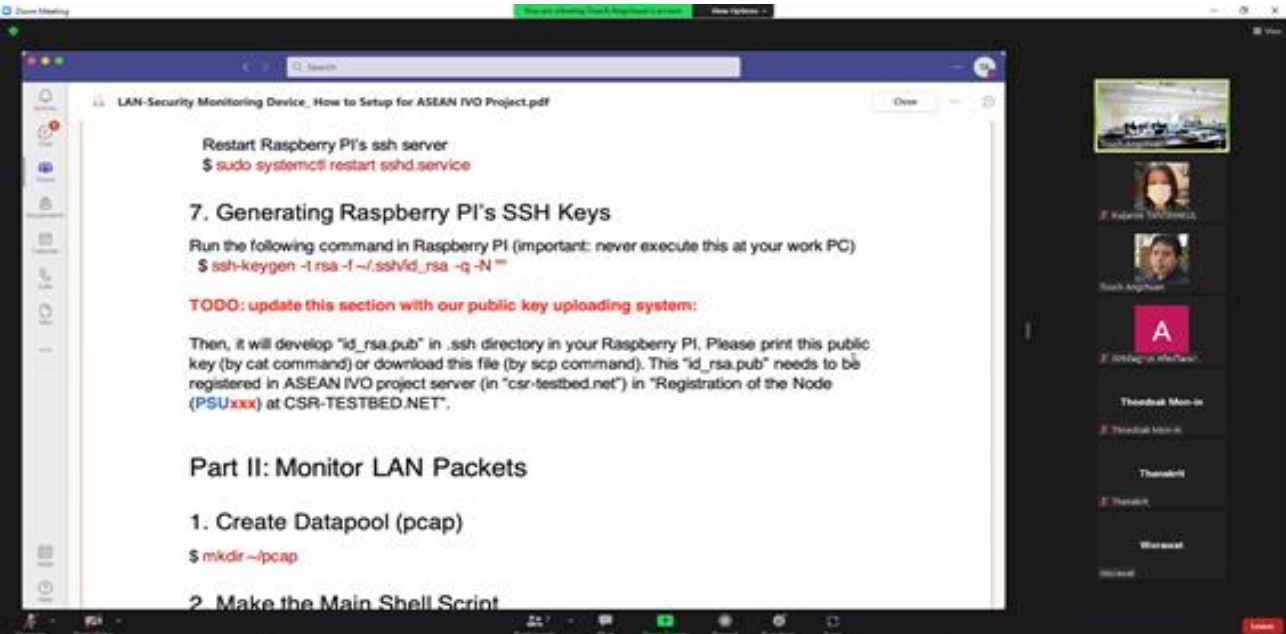
The screenshot shows a Zoom meeting interface with a grid of participants. The participants' names and avatars are visible, including:

- SINCHAI KAMOLPHIWONG
- PJ
- PS
- TA
- 落
- Y Phonsakorn
- KULIAREE TANTARAKUL (Guest)
- poonak Wongjareaid
- Yanchai Pongtong (Guest)
- Patimakorn Jantaramach
- TOUCHAI ANGSIRAN (Guest)
- Sakornchai Khaitrakul
- NORRATHEP RATTANAVIRAN
- Patimakorn Jantaramach (Guest)
- SINCHAI KAMOLPHIWONG
- RONNADORN SANTEE (Guest)

"LAN Security Monitoring Device"

February 17th, 2022

We organized a hybrid workshop for distribution and installation of the LAN security monitoring nodes.



November 16, 2023 at Vientiane

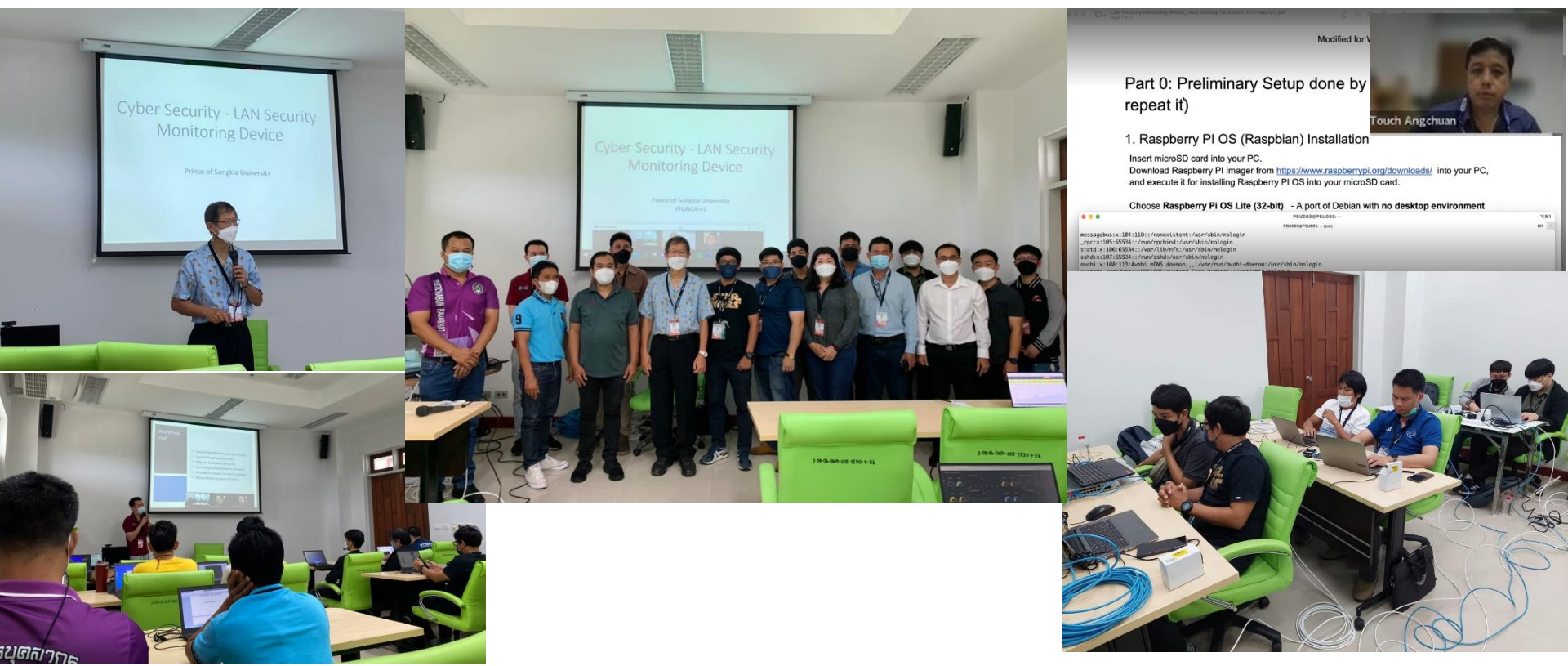
ASEAN IVO Project Review 2023

Project Activities: Hybrid Workshop on WUNCA 41st

"LAN Security Monitoring Device"

August 5th, 2022

We organized a hybrid workshop for distribution and installation of the LAN security monitoring nodes.



Project Activities: On-site Workshop on WUNCA 42nd

February 8th, 2023

We gave an academic talk, titled "Wireless Ad Hoc Federated Learning: A Fully Distributed Cooperative Machine Learning", to disseminate the results from this project.

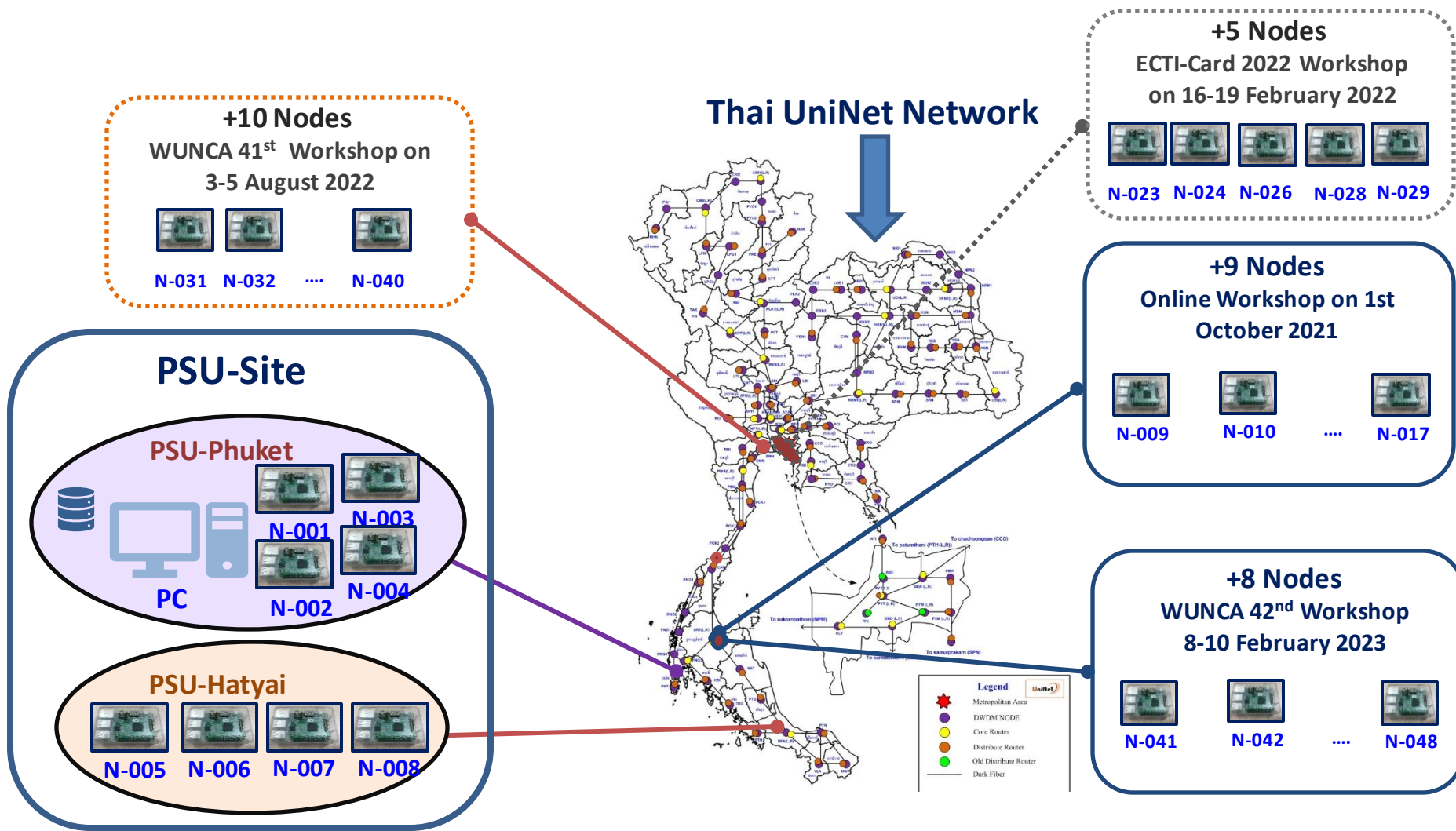


February 9th, 2023

We organized an onsite workshop, titled "LAN Security Monitoring Device", for distribution and installation of the LAN security monitoring nodes.



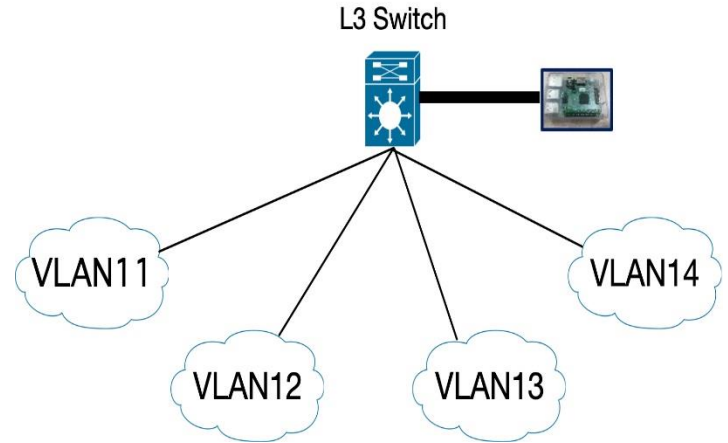
70 people trained from 40 institutes, 43 nodes installed



Sensor nodes installation in Campus Network (multiple VLAN)

In order to deploy one LAN security monitoring node per one network in VLAN environment. This work propose a solution that use only one node connected to L3 switch through VLAN trunk.

Network configuration file (/etc/network/iface.d/eth0 in AIVO-node can be shown as:



```

auto lo inet loopback
iface lo inet loopback

#management vlan
auto eth0
iface eth0 inet static
    address 172.30.80.8
    netmask 255.255.255.0
    gateway 172.30.80.1
auto eth0.11
iface eth0.11 inet manual
    vlan-raw-device eth0
    address 172.30.11.8
    netmask 255.255.255.0
    
```

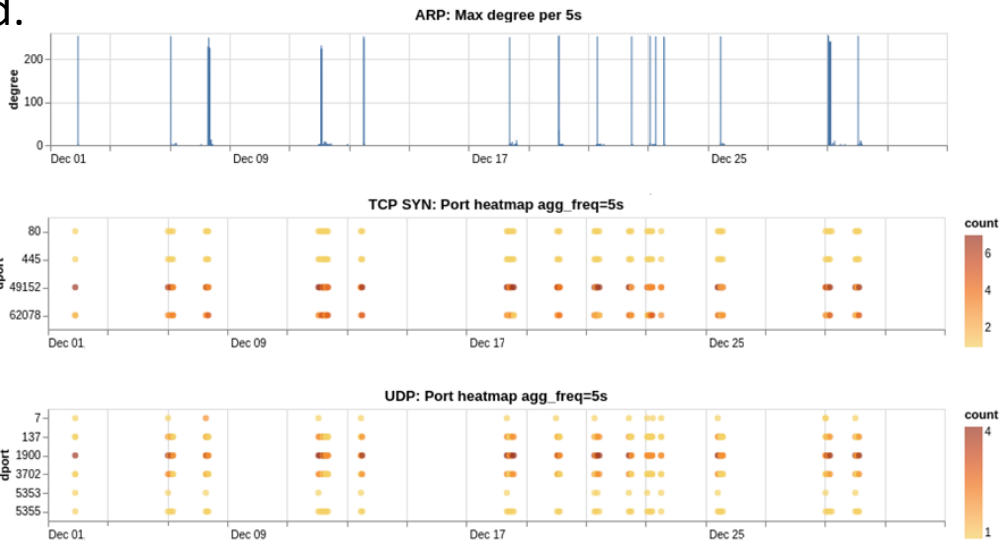
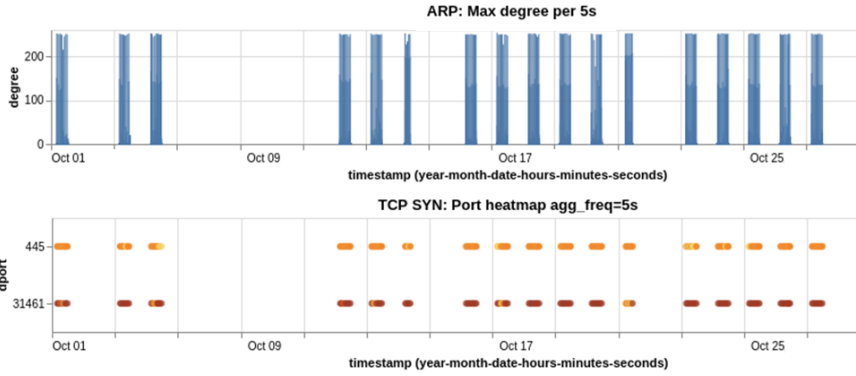
```

auto eth0.12
iface eth0.12 inet manual
    vlan-raw-device eth0
    address 172.30.12.8
    netmask 255.255.255.0
auto eth0.13
iface eth0.13 inet manual
    vlan-raw-device eth0
    address 172.30.13.8
    netmask 255.255.255.0
auto eth0.14
iface eth0.14 inet manual
    vlan-raw-device eth0
    address 172.30.14.8
    netmask 255.255.255.0
    
```


(1) Visualization of Suspicious Behavior of a Local Area Network

As the LAN's traffic is complex for normal network system operators and IoT system operators, suspicious behavior is usually invisible. We have designed a dashboard that visualizes host activities, especially suspicious cases based on the packet capture at the monitoring node. It shows how it made ARP scan, and how it accessed the monitoring node with TCP/UDPs by heat map. Through this user-interface, the system operators can check suspicious behavior and make security actions such as isolation of the node from the network if necessary. The network researchers can make further categorization using the signatures created on the dashboard.

Suspicious Access Patterns with ARP scan and TCP port access.



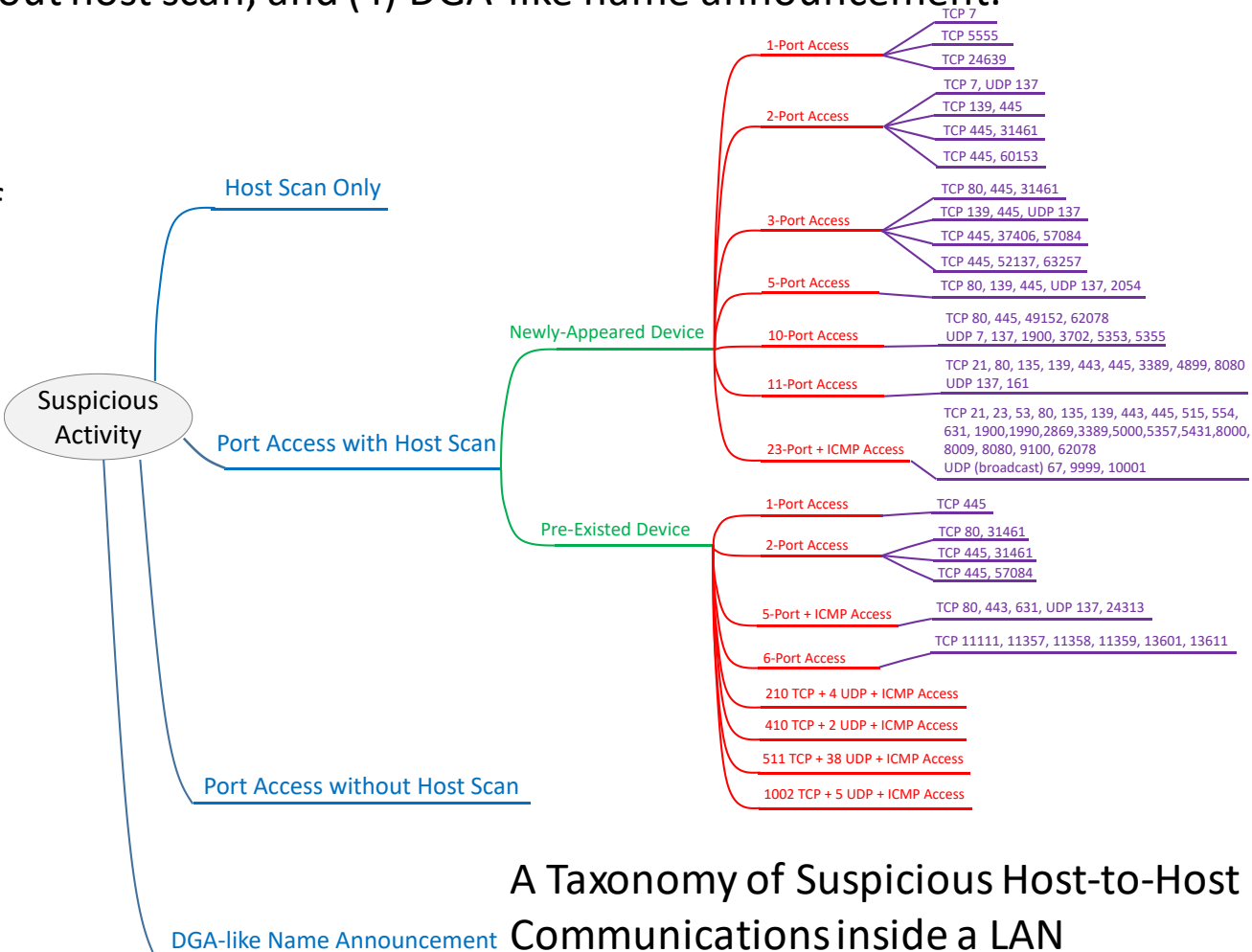
Suspicious Access Patterns with ARP scan and TCP/UDP port access.

(2) A Taxonomy of Suspicious Host-to-Host Communications

From the observations of port access patterns and ARP features, we drafted a taxonomy of suspicious host-to-host communications inside a local area network. We discovered that the suspicious behavior can be categorized as (1) Host Scan Only, (2) Port access with host scan, (3) Port access without host scan, and (4) DGA-like name announcement.

These suspicious behaviors can be further divided into sub categories. The edge of the categories can identify the pattern of combination accesses, which may come from the same malware.

While developing this taxonomy, we also found same suspicious activities are appeared in many local area networks.

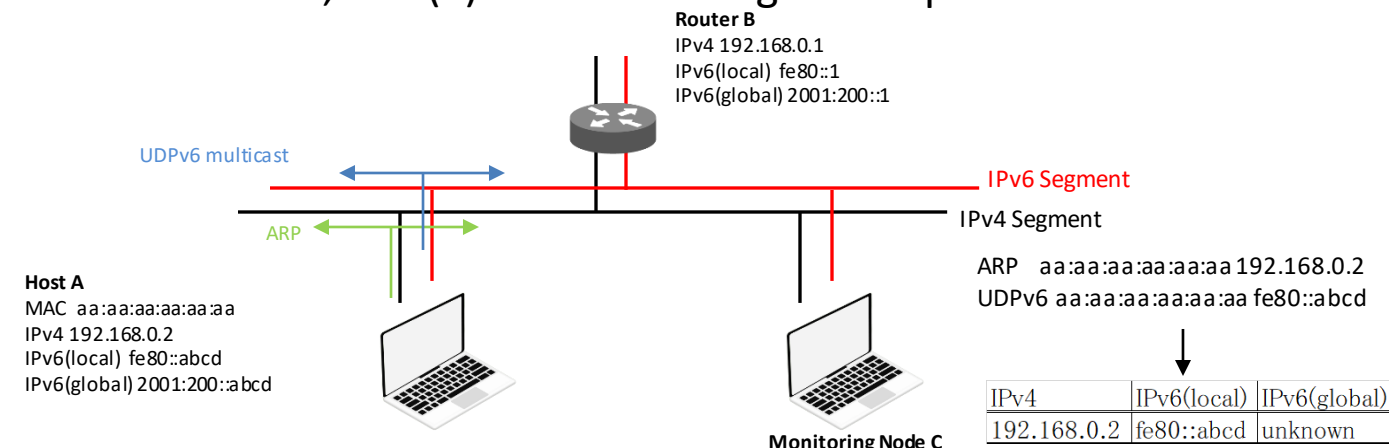


A Taxonomy of Suspicious Host-to-Host Communications inside a LAN

(3) Traffic Redirection of IPv6 Segment for Further Analysis

In a Local Area Network, even without IPv6 network configurations, hosts joined in a LAN automatically have IPv6 link-local addresses and can make interactions between them as a peer-to-peer manner. As IPv6 channel can be a security hole (even in IPv4 only network), we have developed a traffic redirection method (1) for identifying suspicious hosts in IPv6 address domain, and (2) for monitoring the suspicious traffic.

With this method, we could find 103 IPv4-IPv6 address pairs for 155 hosts.



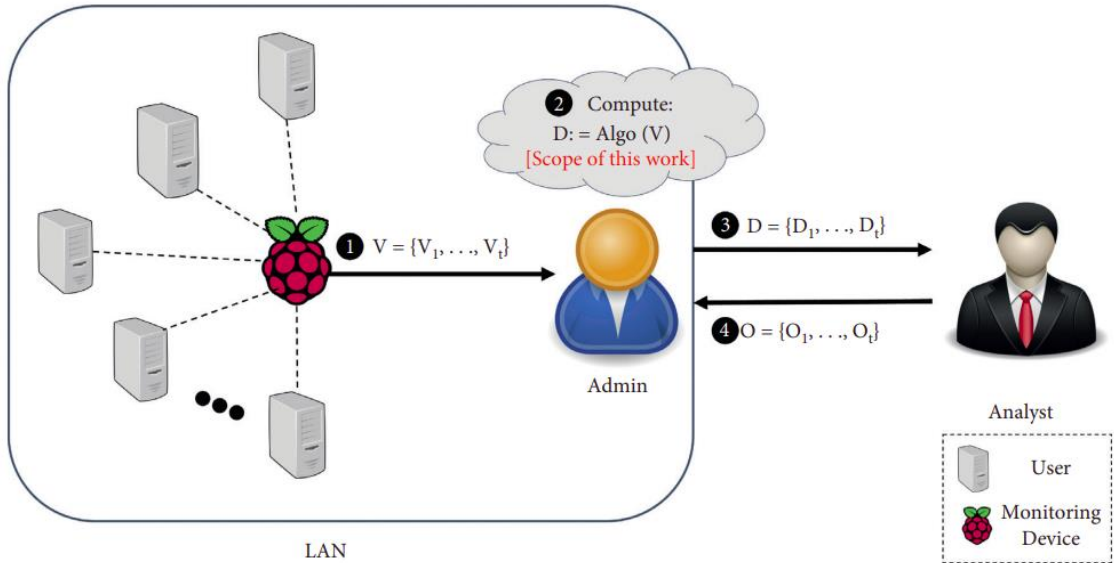
Mechanism for IPv6 Address Matching

| MAC address | Assigned IPv4, IPv6 Addresses |
|-------------|--------------------------------|
| a8:0c | ['192.168.230', 'fe80::a203'] |
| a8:67 | ['192.168.142', 'fe80::ab15'] |
| 50:07 | ['192.168.48'] |
| 00:89 | ['192.168.157'] |
| 98:cb | ['192.168.203'] |
| a0:25 | ['192.168.37'] |
| b4:df | ['192.168.166', 'fe80:::71c6'] |
| 00:82 | ['192.168.167', 'fe80:::d650'] |
| 84:d9 | ['fe80:::66d9'] |

} IPv4-IPv6 address pairs found
 } IPv4-only hosts found
 ← An IPv6-only host found

Discovered IPv4-IPv6 Pairs

(4) Anonymization of captured data via Differential Privacy



We anonymize captured ARP data by applying differential mechanisms on ARP-degree data. We consider two mechanisms:

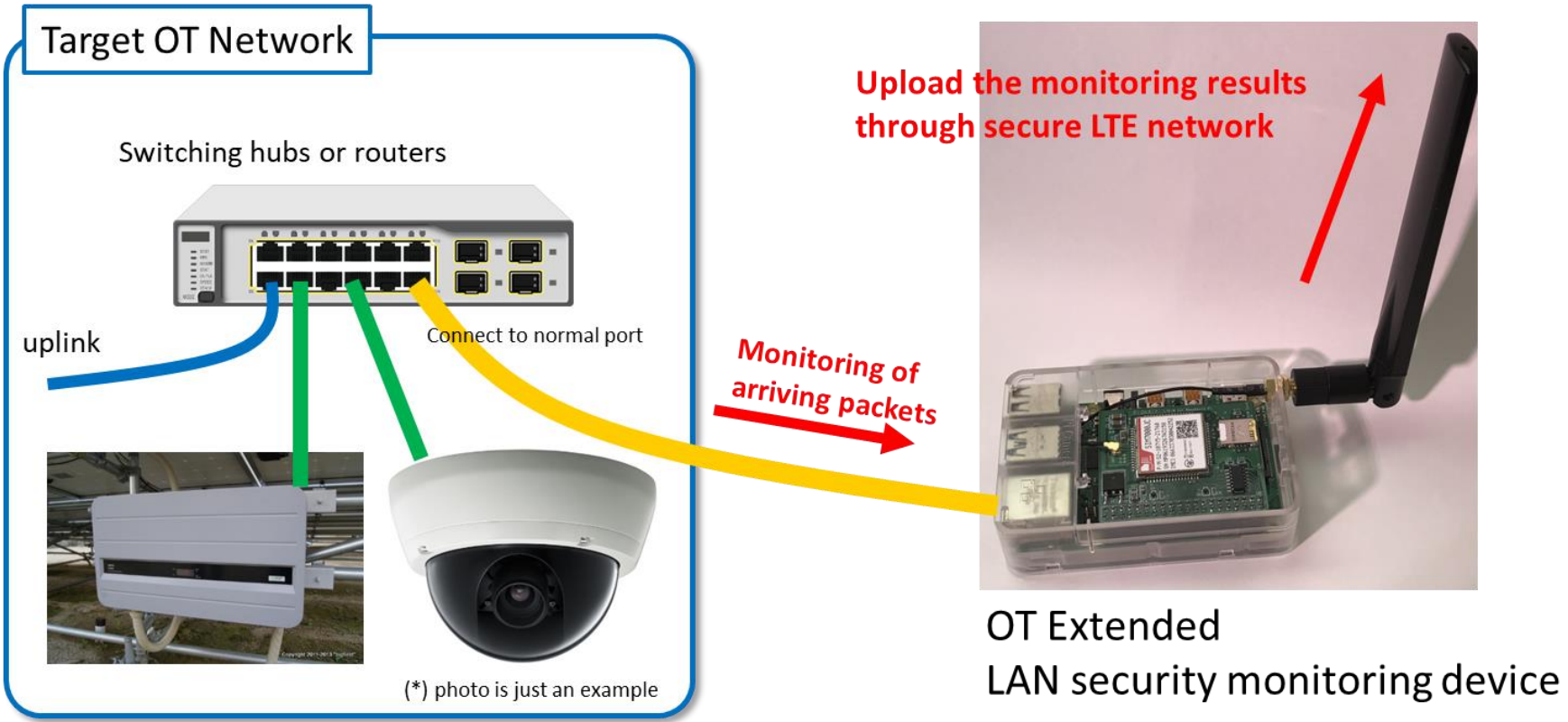
- Naïve approach – perturbing ARP-degree data directly
- Histogram-based approach – transforming ARP-degree data into histogram and perturbing histogram

Our finding: these mechanisms provide the following privacy guarantee:

- Naïve approach – hide user relationship
- Histogram-based approach – hide presence of individual users

(5) LTE-Support for OT-extended Monitoring

- LAN is also used in many OT (Operational technology) network, which is sometimes isolated from the Internet but malware can be intruded.
- We have developed LTE-support for LAN-monitoring system.



Presentations at International Conferences:

| No: | Paper title: | Author names | Affiliation | Conference name: | The date of the conference | The venue of the conference |
|-----|---|---|--|--|----------------------------|-----------------------------|
| 1 | Releasing ARP Data with Differential Privacy Guarantees For LAN Anomaly Detection | N. Rattanavipanon, D. Ponnoprat, H. Ochiai, K. Tantayakul, T. Angchuan, S. Kamolphiwong | Prince of Songkla University, Chiang Mai University, The University of Tokyo | International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON) | 19/05/2021 | Virtual |
| 2 | Poster: Detecting Anomalous LAN Activities under Differential Privacy | N. Rattanavipanon, D. Ponnoprat, H. Ochiai, K. Tantayakul, T. Angchuan, S. Kamolphiwong | Prince of Songkla University, Chiang Mai University, The University of Tokyo | The Network and Distributed System Security Symposium (NDSS) | 27/02/2023 | San Diego |

Published Journal Papers:

| No: | Paper title: | Author names | Affiliation | Journal name: | The publisher of the Journal | The volume number and Pages |
|-----|---|---|--|-------------------------------------|------------------------------|-----------------------------|
| 1 | Detecting Anomalous LAN Activities under Differential Privacy | N. Rattanavipanon, D. Ponnoprat, H. Ochiai, K. Tantayakul, T. Angchuan, S. Kamolphiwong | Prince of Songkla University, Chiang Mai University, The University of Tokyo | Security and Communication Networks | Hindawi | 2022 |

How does our project create the social impacts:

- 1) We have done hands-on workshops to train and share our knowledge to 70 people. We hope that our network will be expanded.
- 2) We have also given an academic talk about our project to hundreds of audience.
- 2) Contribution for anonymization of captured data for publicizing the data.

The findings of our project are:

- (i) Vulnerability assessment of *remote local-area networks*,
- (ii) Visualization of data for useful security operation,
- (iii) *Improvement of detection algorithms and statistical analysis*
including the application of federated learning, and
- (iv) Anonymization of captured data for publicizing the data

1. Scientific and Technological:

(i) some publications and knowledge sharing what we have found:

(i) vulnerability assessment of remote local-area networks,

(ii) improvement of detection algorithms and statistical analysis including the application of federated learning,

2. Application development:

to extend visualization of data for useful security operation to application development

Thank you for your kind attention

Q&A