# 2018 PROJECT

## Cyber-Attack Detection and Information Security for Industry 4.0

## PROGRESS REPORT

November 2019

ANNIVERSARY 2004-2019

VNU University of Engineering and Technology

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

UTS UNIVERSITY OF TECHNOLOGY, SYDNEY

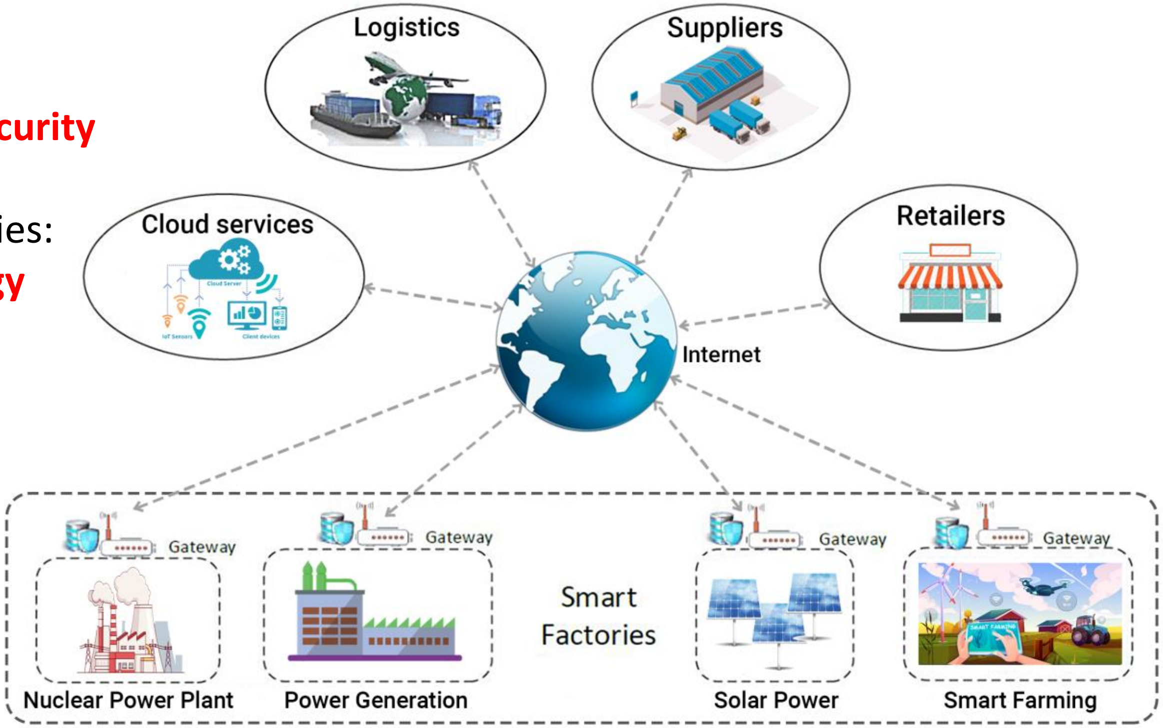
# Project: Cyber-Attack Detection and Information Security for Industry 4.0

## Context - Industry 4.0

- a main driver for the development of smart cities
- a vision of smart factories built with intelligent cyber-physical systems
- breakthrough achievements in many sectors (healthcare, food, and agriculture, …)
- when connected to the cyber world, **cybersecurity risks** become a key concern due to open systems with IP addresses

## Objectives

To provide tools to **enhance cybersecurity** in Industry 4.0 by applying several recently-developed smart technologies: **deep learning**, **blockchain technology** and **physical-layer security**



## Speaker: Nguyen Linh Trung

VNU University of Engineering and Technology, Hanoi, Vietnam

# Project information: Targets

1. A method to detect cyber-security threats in Industry 4.0 through using advanced deep learning algorithms
2. A framework to protect data from cyber-attacks using blockchain technology
3. Solutions to enhance security at the physical interface of information transmission using physical-layer security technology
4. A sustainable research collaboration network in the ASEAN region, in Australia and worldwide, for developing human resource in Vietnam that is able to develop effective cyber-security solutions

# Project information: Members, etc.

- **Project members:**
  1. VNU-UET (Vietnam): Prof. Nguyen Linh Trung (leader)
  2. VNU-UET (Vietnam): Prof. Nguyen Viet Ha
  3. NTU (Singapore): Prof. Dusit Niyato
  4. UTS (Australia): Prof. Eryk Dutkiewicz
  5. UTS (Australia): Dr. Diep Nguyen
  6. UTS (Australia): Dr. Hoang Dinh

- **New members:**
  1. VNU-UET (Vietnam): Dr. Tran Thi Thuy Quynh (9/2019)
  2. VNU-UET (Vietnam): Dr. Ta Duc Tuyen (9/2019)
  3. VNU-UET (Vietnam): M.Sc. Tran Viet Khoa (PhD student, 9/2019)
  4. VNU-UET (Vietnam): M.Sc. Bui Minh Tuan (PhD student, 9/2019)

- **Project duration**: 7/2018 – 6/2021 (36 months)

# Project Activities: Overall

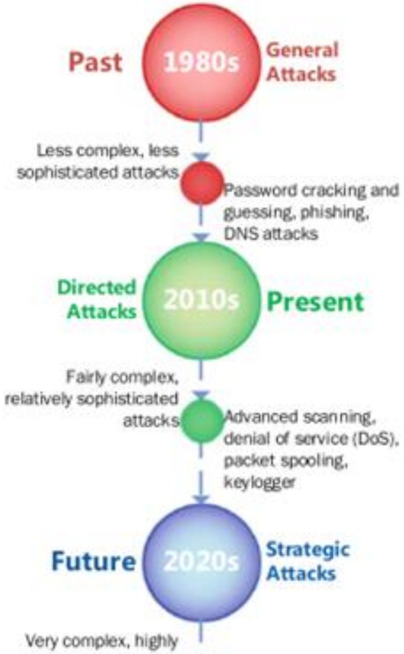
1. **Scientific development**
    - **Task 1**: Analyze and identify potential cyber-security risks in Industry 4.0
    - **Task 2**: Develop an innovative risk assessment model to quantify the risks in Industry 4.0
    - **Task 3**: Implement an online web reference service listing and ranking the risks in Industry 4.0
    - **Task 4**: Develop and implement an innovative method to detect and isolate cyber-security attacks using deep learning
    - **Task 5**: Develop an unprecedented data securing method using blockchain technology
    - **Task 6**: Develop receiver-based friendly jamming and collaborative beamforming methods to safeguard sensors/actuators
2. **Technological Development & Experiments**
    - **Task 7**: Implement and evaluate performance of the proposed blockchain application on a real testbed
3. **Networking**
    - **Task 8**: Annual Workshops and Exhibitions on Cyber-Security

# Project Activities & Results: Scientific - Task 1 (UET)

## Task 1: Analyze and identify potential cyber-security risks in Industry 4.0

❖ Activity

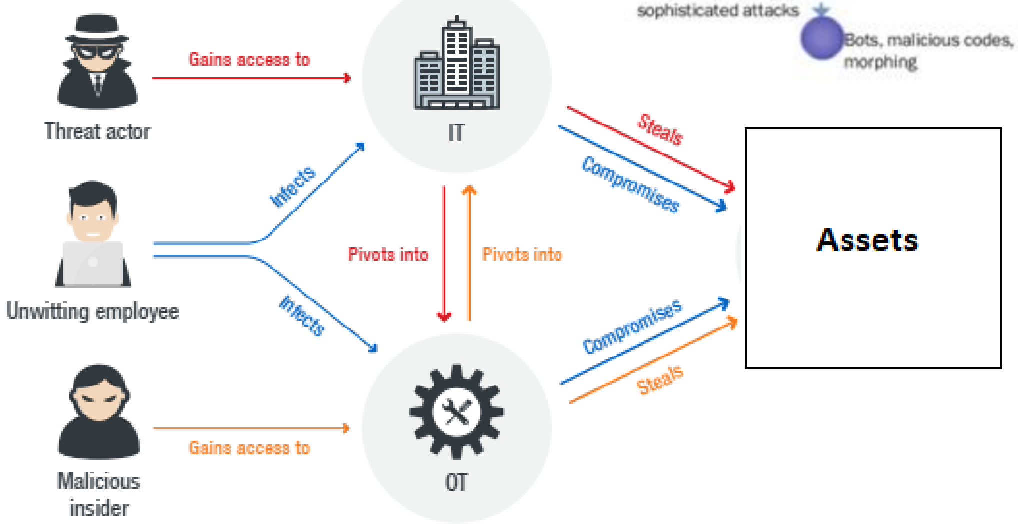
- ✓ Performed a literature study of cyber-security vulnerabilities and potential risks of manufacturing systems in Industry 4.0



Past
1980s
General Attacks
Less complex, less sophisticated attacks
Password cracking and guessing, phishing, DNS attacks
Directed Attacks
2010s
Present
Fairly complex, relatively sophisticated attacks
Advanced scanning, denial of service (DoS), packet spooling, keylogger
Future
2020s
Strategic Attacks
Very complex, highly sophisticated attacks
Bots, malicious codes, morphing

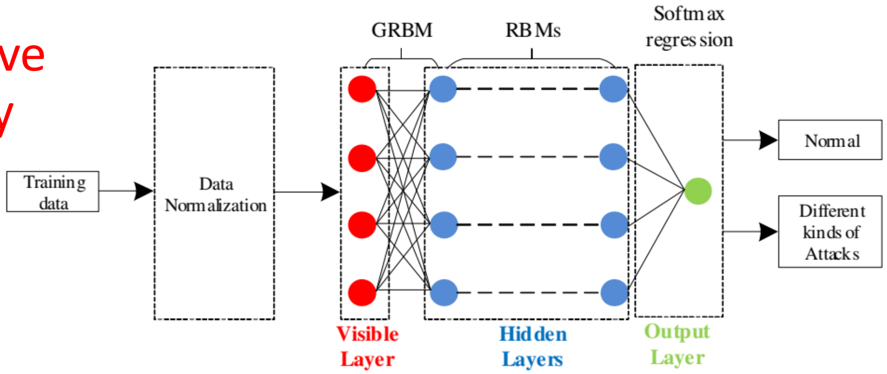
❖ Result

- ✓ Look at the interaction between Operation Technology (**OT**) and Information Technology (**IT**): IoT, CPS, Clouds, ...
- ✓ List of main vulnerabilities and risks in manufacturing in I4
- ✓ Typical case-studies



# Project Activities & Results: Scientific - Task 4 (UET, UTS)

## Task 4: Develop and implement an innovative method to detect and isolate cyber-security attacks using deep learning

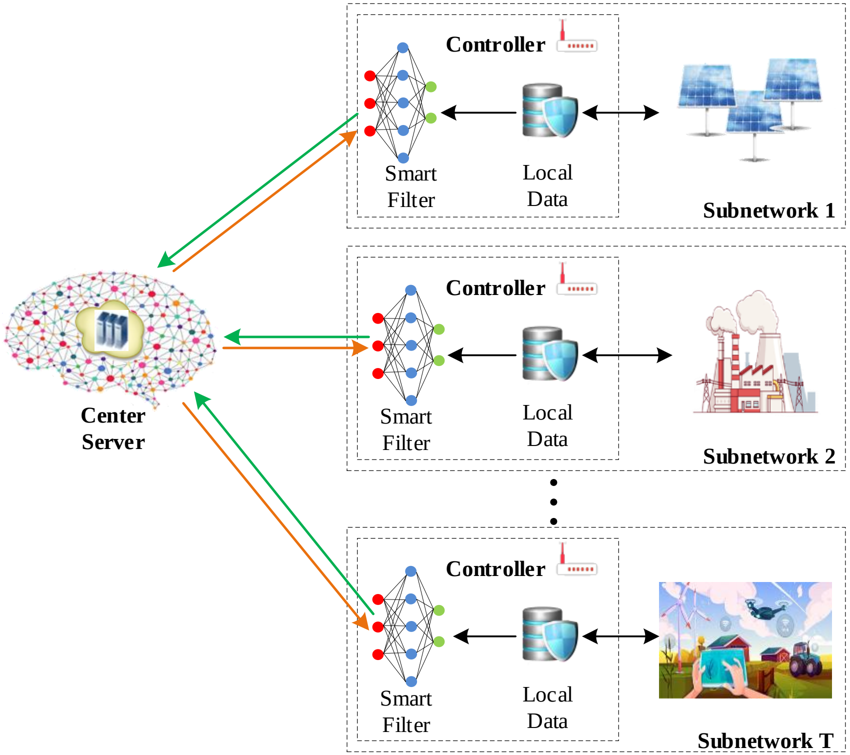


❖ Activity

- ✓ Studied how to apply different deep learning algorithms for cyber-security attack detection in I4
- ✓ Used public data for experiments

❖ Result

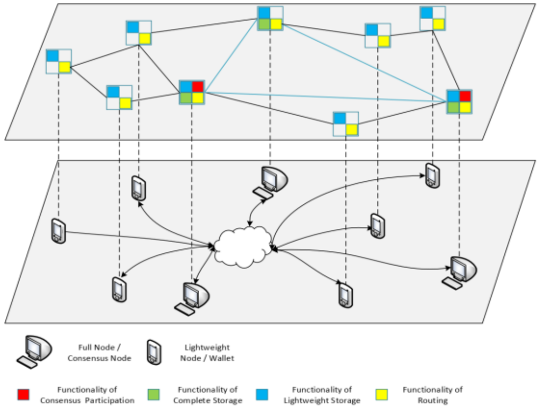
- ✓ Developed "smart filters" at the IoT gateways to promptly detect and prevent cyberattacks using collaborative learning
- ✓ Each filter uses data in its network to train its cyberattack detection model based on deep learning
- ✓ Trained model shared with other IoT gateways
- ✓ Detection accuracy improved
- ✓ Information disclosure reduced



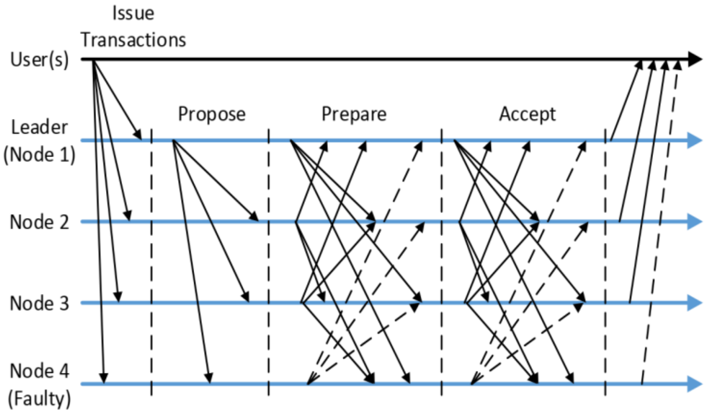
# Project Activities & Results: Scientific - Task 5 (NTU, UTS)

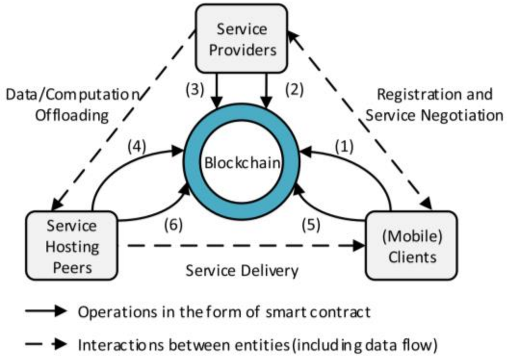
## Task 5: Develop an unprecedented data securing method using blockchain technology

- Activity
  - ✓ Surveyed development of decentralized consensus mechanisms and mining strategy management in blockchain networks
- Result
  - ✓ Design perspectives: distributed consensus system and incentive mechanism
  - ✓ Strategy adoption for self-organization by the individual nodes in the blockchain backbone networks
  - ✓ Emerging blockchain applications in telecom and impacts of consensus mechanisms
  - ✓ Open issues in protocol design for blockchain consensus and related potential research directions



Full Node / Consensus Node
Lightweight Node / Wallet
🟥 Functionality of Consensus Participation
🟩 Functionality of Complete Storage
🟦 Functionality of Lightweight Storage
🟨 Functionality of Routing

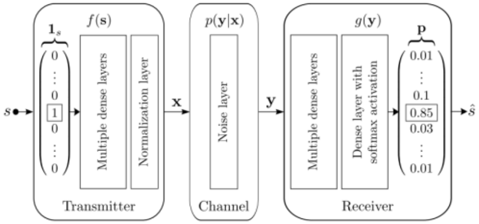


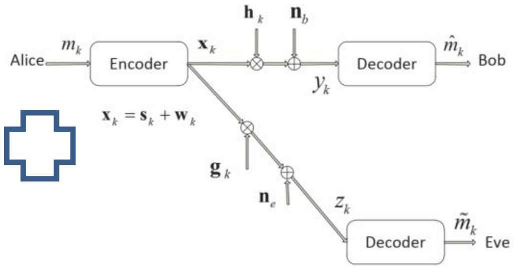


Service Providers
Data/Computation Offloading
Registration and Service Negotiation
(3)
(2)
(4)
(1)
Blockchain
Service Hosting Peers
(6)
(5)
(Mobile) Clients
Service Delivery
Operations in the form of smart contract
Interactions between entities (including data flow)

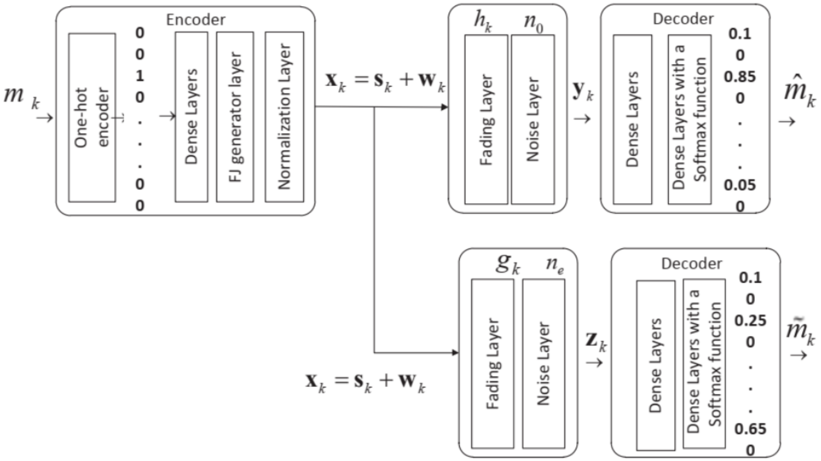
# Project Activities & Results: Scientific - Task 6 (UET, UTS)

Task 6: Develop receiver-based friendly jamming and collaborative beamforming methods to safeguard sensors/actuators

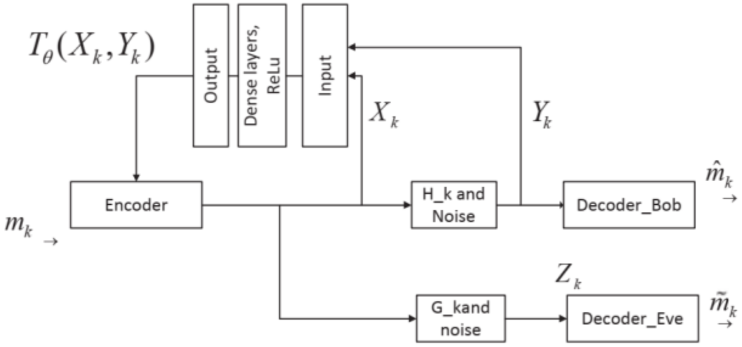




- ❖ Activity
  - ✓ Studied deep learning applications for Physical Layer Security (PLS)
  - ✓ Studied using Auto-encoder based friendly jamming (AE-FJ) for PLS
  - ✓ Studied using mutual information neural estimation (MINE) based friendly jamming for PLS



- ❖ Result
  - ✓ Developed AE-FJ as a lightweight solution to secure IoT communications at physical layer: low complexity at receiver side
  - ✓ Developed MINE-based friendly jamming

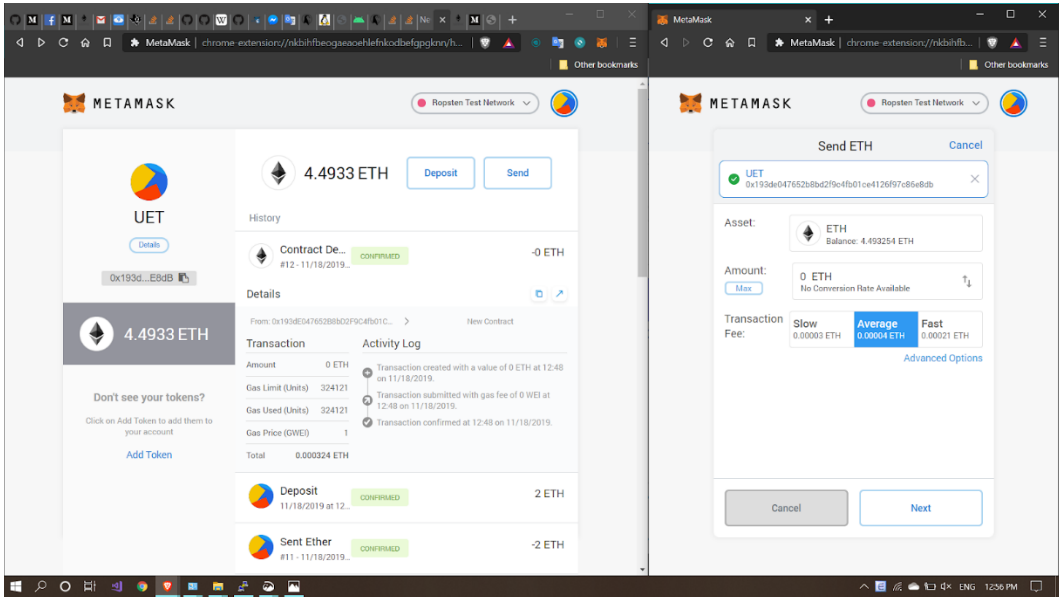


# Project Activities & Results: Technological - Task 7 (UET, NTU, UTS)

Task 7: Implement and evaluate performance of the proposed blockchain application on a real testbed

- Activity
  - ✓ Studied design of a blockchain testbed for smart grid (NTU)
  - ✓ Look for a industrial partner to apply security solutions for Industry 4.0

- Result
  - ✓ Constructed a private Ethereum network to study blockchain for smart grid
  - ✓ Agreed to jointly develop a platform at a smart factory of Viettel, with two security solutions: Deep learning for cyberattack detection and blockchain for data integrity


MetaMask | chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/h...

Other bookmarks

METAMASK

Ropsten Test Network

UET

Details

0x193d...E8dB

4.4933 ETH

Don't see your tokens?

Click on Add Token to add them to your account

Add Token

4.4933 ETH

Deposit Send

History

Contract De... #12 - 11/18/2019... CONFIRMED -0 ETH

Details

From: 0x193dE047652B8bD2F9C4fb01C... > New Contract

Transaction

| | |
|---|---|
| Amount | 0 ETH |
| Gas Limit (Units) | 324121 |
| Gas Used (Units) | 324121 |
| Gas Price (GWEI) | 1 |
| Total | 0.000324 ETH |

Activity Log

Transaction created with a value of 0 ETH at 12:48 on 11/18/2019.

Transaction submitted with gas fee of 0 WEI at 12:48 on 11/18/2019.

Transaction confirmed at 12:48 on 11/18/2019.

Deposit 11/18/2019 at 12... CONFIRMED 2 ETH

Sent Ether #11 - 11/18/2019... CONFIRMED -2 ETH

MetaMask | chrome-extension://nkbihfb...

Other bookmarks

METAMASK

Ropsten Test Network

Send ETH Cancel

UET 0x193de047652b8bd2f9c4fb01ce4126f97c86e8db

Asset: ETH Balance: 4.493254 ETH

Amount: Max 0 ETH No Conversion Rate Available

Transaction Fee: Slow 0.00003 ETH | Average 0.00004 ETH | Fast 0.00021 ETH

Advanced Options

Cancel Next

ENG 12:56 PM

Say it your way

# Project Activities & Results: Networking - Task 8 (UET, UTS, NTU)

Task 8: Annual workshops and exhibitions on cyber-security

- Activity
  - ✓ Kick-off meeting (Dec 2018)
  - ✓ 1st IVO Workshop (Mar 2019)
  - ✓ Special session @ ISCIT (Sep 2019)
- Result
  - ✓ PTIT (Hanoi), NICT-Tokyo, NICT-Bangkok
  - ✓ U. Tokyo, LQDTU (Hanoi), HUST (Hanoi)

FIRST ASEAN IVO WORKSHOP
Cybersecurity and Information Security in Industry 4.0
March 26 & 27 at VNU-UET in Hanoi, March 28 at Novotel in Ha Long
UTS
NICT
IEEE ComSoc

# Publications

- Journal Papers:

| No: | Paper title | Author | Affiliation | Journal | Publisher | Volume,Number, Pages |
|---|---|---|---|---|---|---|
| 1 | A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks [Tasks 5, 7] | W Wang,<br>DT Hoang,<br>P Hu,<br>Z Xiong,<br>D Niyato,<br>P Wang,<br>Y Wen,<br>D Kim | NTU, UTS | IEEE Access | IEEE | vol. 7, pp. 22328-22370, 2019 |

# Publications

❖ Conference Papers:

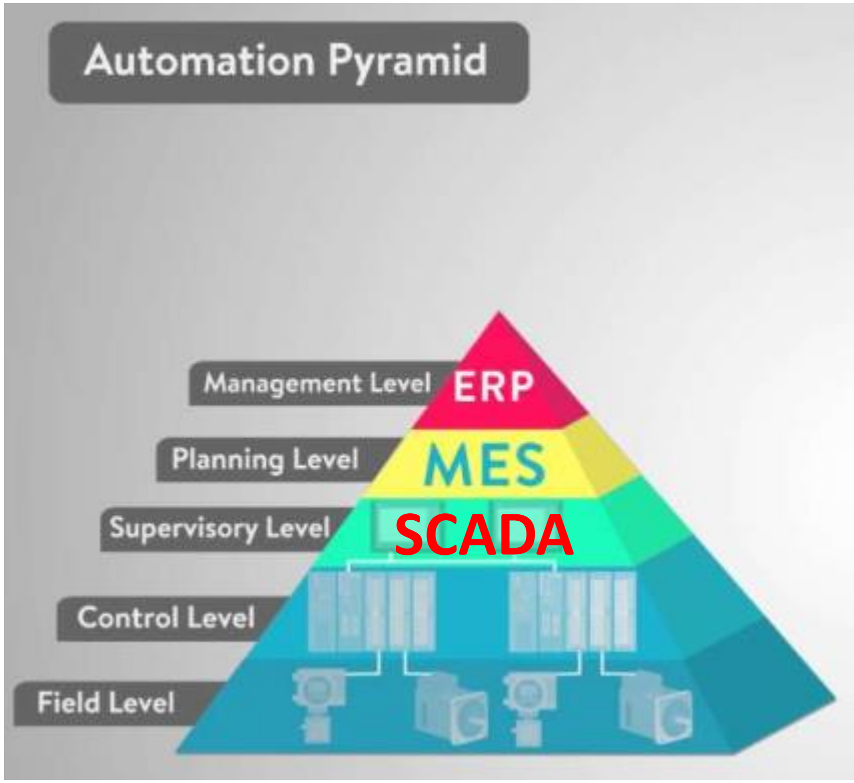
| No: | Paper title: | Author names | Affiliation | Conference name | date | venue |
|---|---|---|---|---|---|---|
| 1 | Network Coding with Multimedia Transmission: A Software-Defined-Radio based Implementation [Task 6] | TTT Quynh,<br>TV Khoa,<br>LV Nguyen,<br>NL Trung | VNU-UET | International Conference on Recent Advances in Signal Processing, Telecommunications and Computing | March 2019 | Hanoi, Vietnam |
| 2 | Collaborative Learning Model for Cyberattack Detection Systems in IoT Industry 4.0 [Task 4] | TV Khoa,<br>YM Saputra,<br>DT Hoang,<br>NL Trung,<br>DN Nguyen,<br>NV Ha,<br>E Dutkiewicz | VNU-UET, UTS | IEEE Wireless Communications and Networking Conference | 6-9 April 2020 | Seoul, South Korea |
| 3 | Autoencoder based Friendly Jamming [Task 6] | BM Tuan,<br>TD Tuyen,<br>NL Trung,<br>NV Ha | VNU-UET | IEEE Wireless Communications and Networking Conference | 6-9 April 2020 | Seoul, South Korea |

# Societal Impact

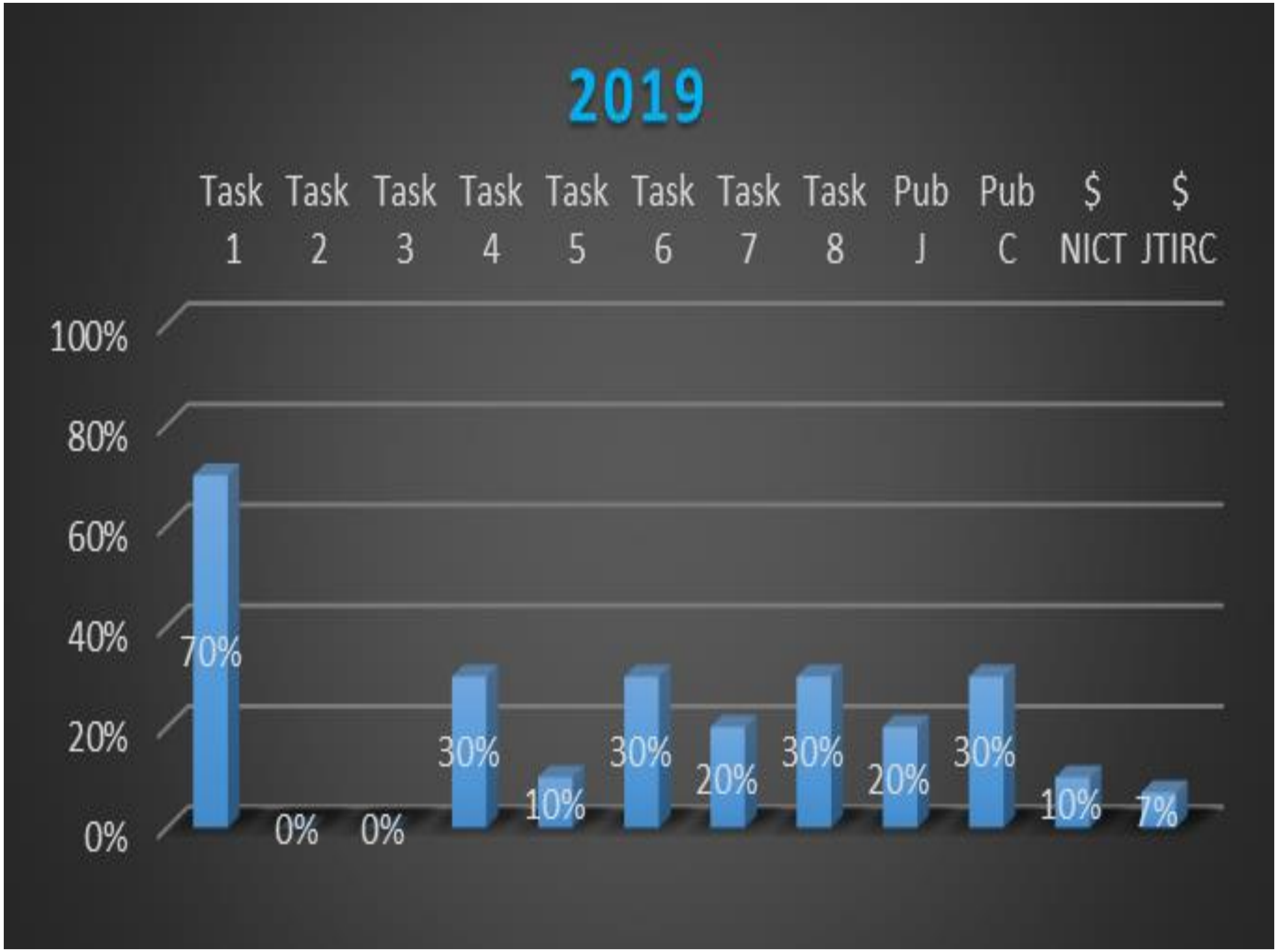
- ❖ Application: Smart factory @ Viettel
- ❖ SCADA – Supervisory Control and Data Acquisition
- ❖ Enhanced security via:
  - ✓ Cyber-attack detection w DL
  - ✓ Data integrity w blockchain
- ❖ State-level research proposal:
  - ✓ submit 11/2019
  - ✓ start in 01/2021 (if successful)

VIETTEL

Say it your way

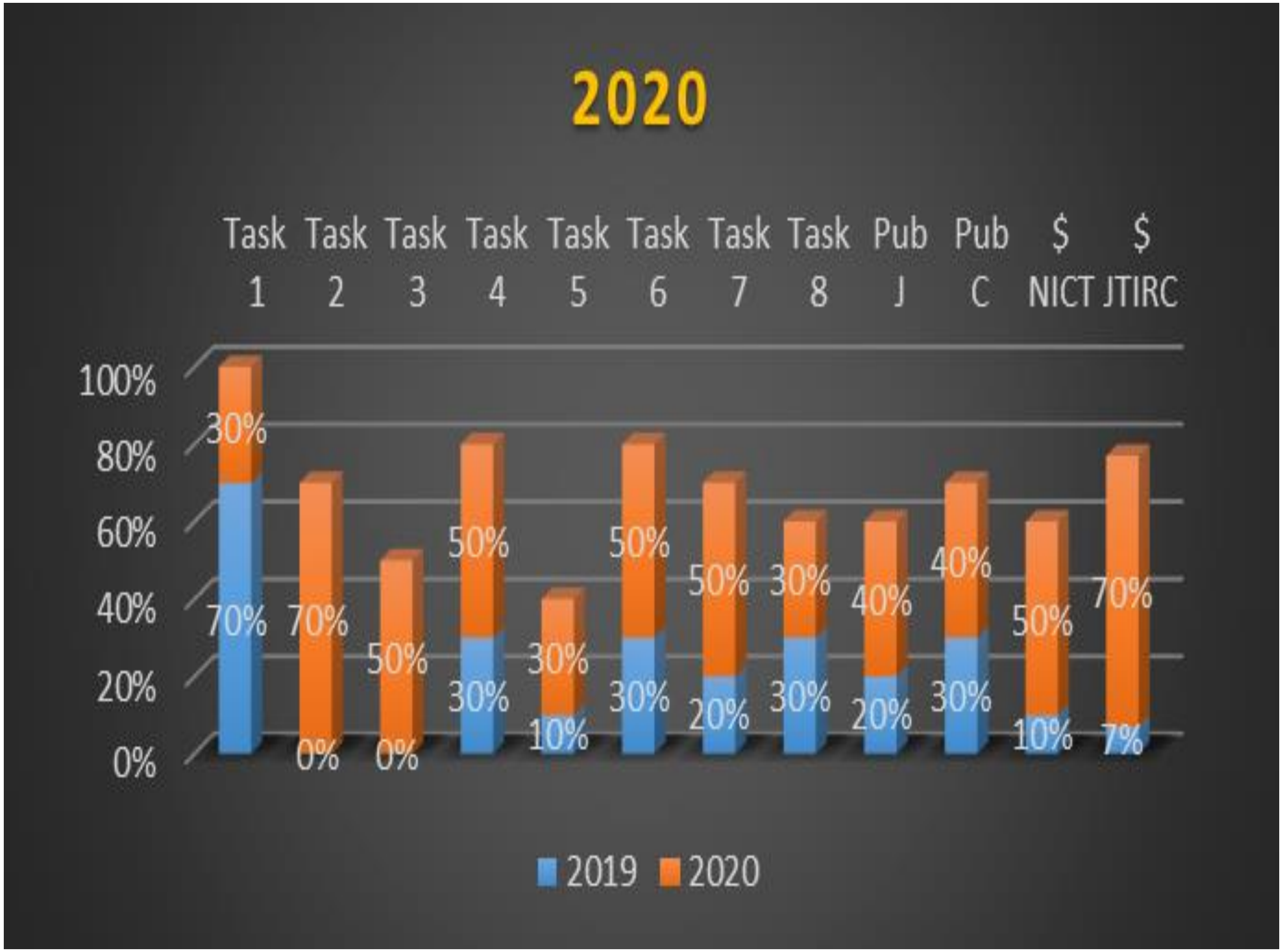


# Conclusion: 2019



- ❖ Slow start due to recruiting 2 PhD students, OK since 7/2019
- ❖ Scientific: preliminary results
- ❖ Technological: exploring phase
- ❖ Networking: OK
- ❖ Publication: OK
- ❖ Budget: slow spending

# Future: 2020



- Scientific: security solutions to be detailed
- Technological: basic design to complete
- Networking:
  - 2nd workshop
  - Annual meeting
- Publication: focused
- Budget:
  - Equipment
  - Visit NICT
  - Journal/Conf
  - 2nd workshop
  - Meeting