CSET'21

NSR

Probabilistic Attack Sequence Generation and Execution Based on MITRE ATT&CK for ICS Datasets

2021. 8. 9.

Seungoh Choi, Jeong-Han Yun, and Byung-Gil Min

CONTENTS

Security research in industrial control systems (ICSs)

Constraints

Availability

Actual attack are difficult to reproduce at the ICS operating environment.

Dataset

An abnormal dataset that includes attack-related data, should be provided

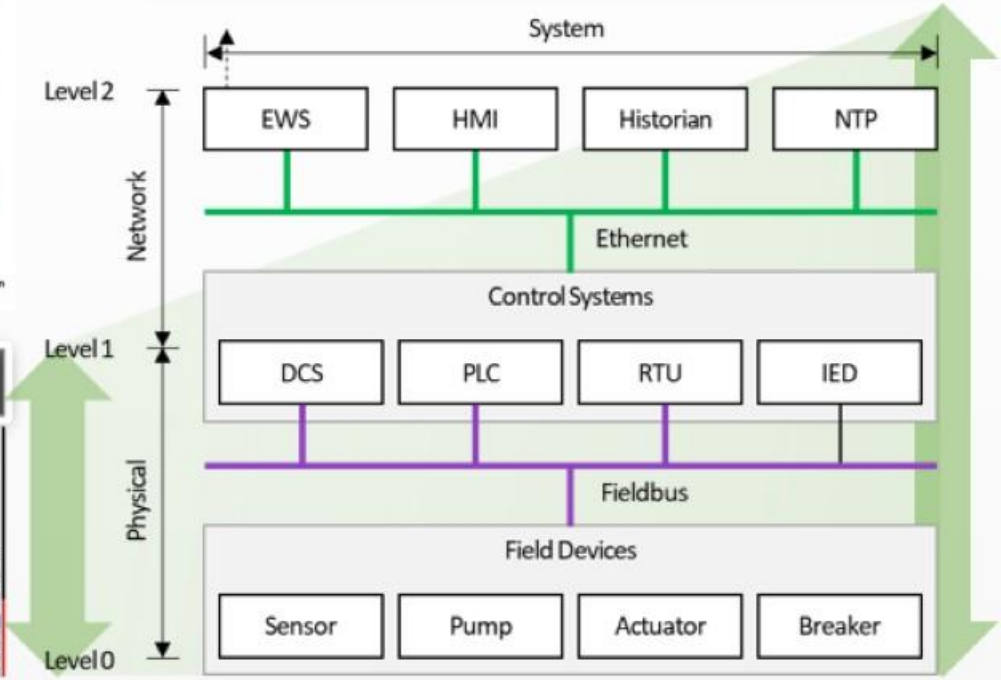
Previous work

HAI Testbed

HAI Dataset

Ongoing work

Developing a Dataset for all ICS levels



Three aspects to develop a abnormal dataset

Reproducibility

An representation that can reproduce abnormal situations

Represented attack sequence based on adversary tactics and techniques

Reality

Adversary tactics and techniques based on real-world observations

Analyzed the existing ICS incident reports to determine the probabilities

Diversity

A model that can reflect more diverse attack sequences

Generated various attack sequences by the probabilities

MITRE ATT&CK + Stochastic Modelling

Generating attack sequence defined as a series of technique with tactic based on MITRE ATT&CK

NSR

MITRE ATT&CK for ICS*

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal o n Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Se rvices	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

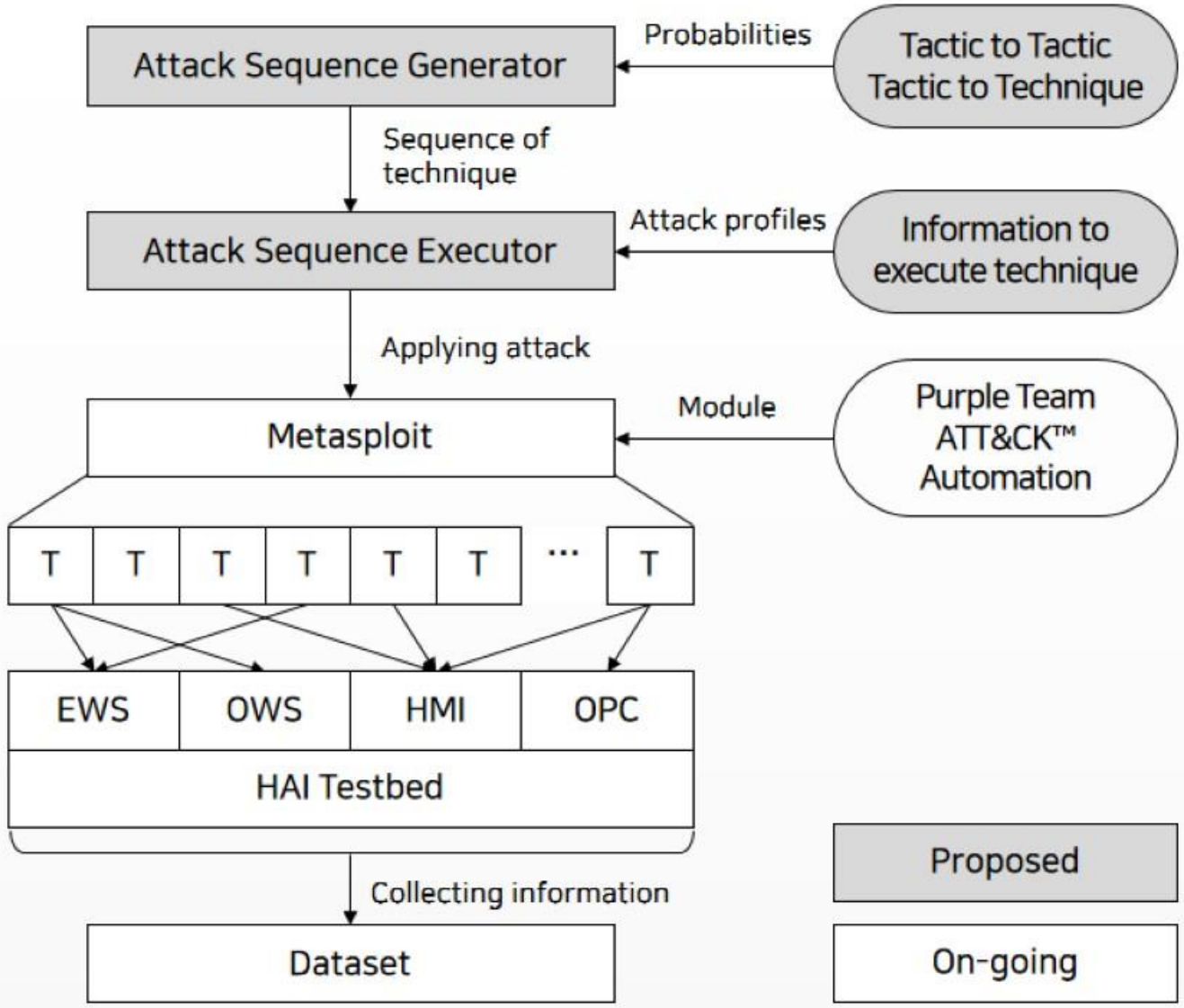
ATT&CK for Enterprise

ATT&CK for ICSs

* We referred to the initial version of ATT&CK for ICSs, which was extensively edited on 29 April 2021 while working on this paper.

Overview

- Attack sequence generator
  - Generating attack sequence with probabilities
- Attack sequence executor
  - Applying attack sequence with attack profiles
- Attack tool
  - Mestaploit with module from Purple Team ATT&CK Automation
- Attack environment
  - HAI Testbed



Attack sequence generator

- Using **Hidden Markov Model (HMM)** to generate attack sequence based on **MITRE ATT&CK for ICSs**
- Assumption
  - The tactic (x_t) used by the attacker at the current time (t) is only affected by the tactic (x_{t-1}) used by the previous time ($t-1$).(i.e., Markovian property)
  - The technique (y_t) observed at the current time (t) is affected only by the tactic (x_t) at the current time (t).

x_{t-1} → x_t

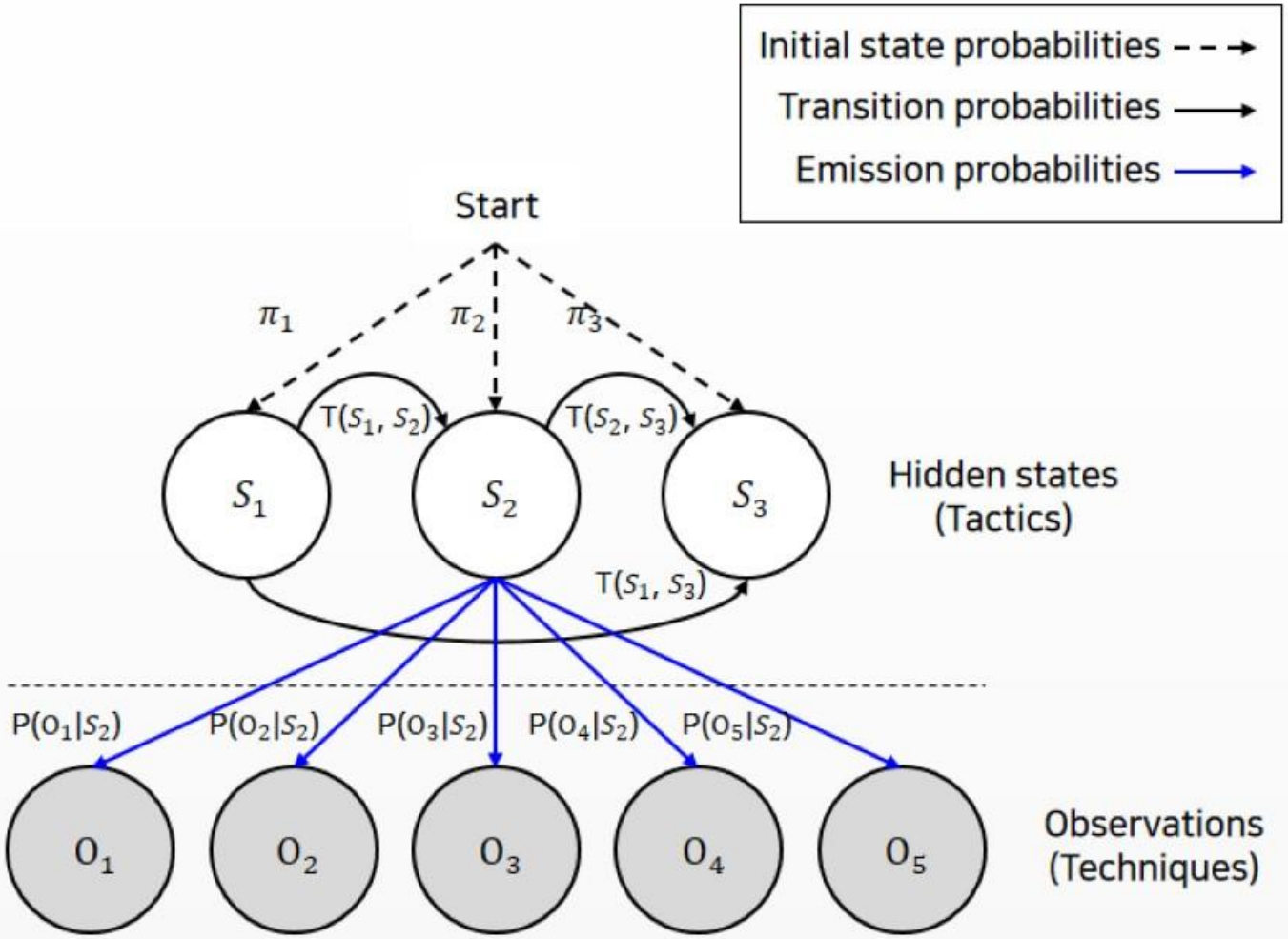
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View

y_t

Attack sequence generator

- HMM configuration
  - ① **Hidden states (S)**
    - → Tactics from MITRE ATT&CK
  - ② **Observations (O)**
    - → Techniques from MITRE ATT&CK

- HMM parameters
  - ① **Initial state probability (π)**
    - → Probability of starting at each tactic
  - ② **Transition probability (T)**
    - → Probability of transition between each tactic
  - ③ **Emission probability (E)**
    - → Probability of the occurrence ofthe technique observed in each tactic

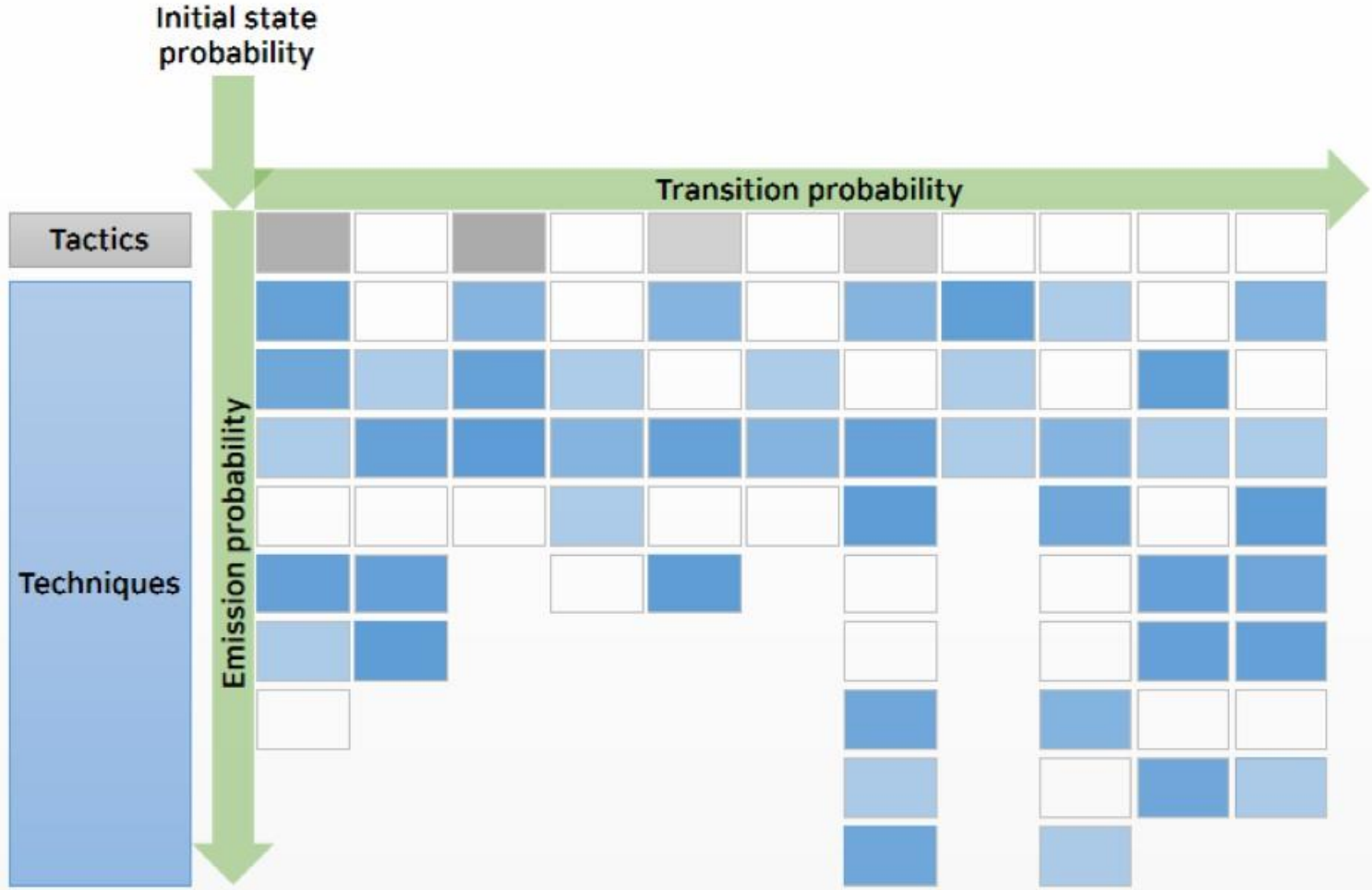


Attack sequence generator

HMM parameters calculation

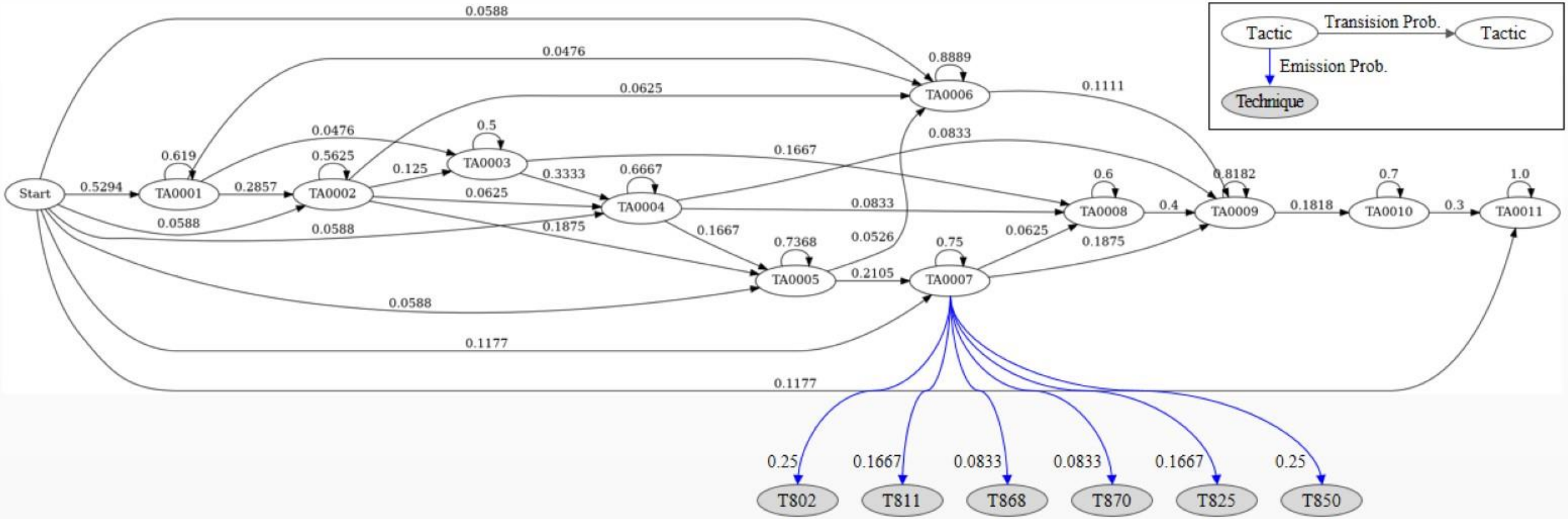
Table 1: Related materials of ICS incidents

Type	Name (Incident)	Materials
Malware	• Stuxnet (Iran nuclear facilities)	[11, 16]
	• BlackEnergy3, Industroyer (Ukraine power grid)	[3, 15, 18, 29]
	• Triton (Saudi Arabia petrochemical plant)	[5, 18]
	• Duqu	[30]
	• Flame	[25]
	• BlackEnergy (KillDisk)	[12]
	• ACAD/Medre.A	[10]
	• Backdoor.Oldrea (HAVEX)	[18]
	• Conficker	[4]
	• VPNFilter	[17]
	• Bad Rabbit (Ukrainian transportation)	[19]
	• LockerGoga (Norway aluminum company)	[1, 26]
	• NotPetya (Ukrainian organizations)	[32]
	• Ryuk	[13, 26]
	• WannaCry	[14, 26]
PoC	• PLC-Blaster (Worm that runs on Siemens S7 PLC)	[27]
	• SoftPLC	[33]



Attack sequence generator

- HMM parameters setup

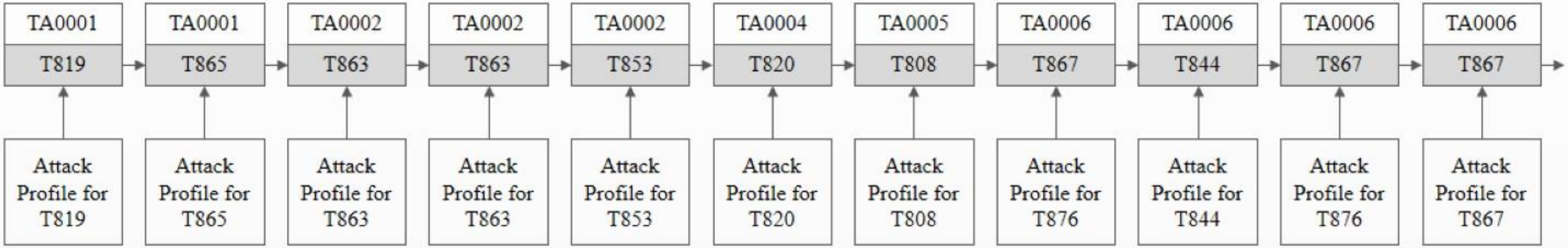


Attack sequence generator

- Transition within attack sequnece
  - Self transition
    - ✓ Multiple techniques can be used within the same tactic.
    - ✓ The same technique can be retried.
  - Terminus transition
    - ✓ When reaching final state "Impact", single attack sequence considered complete.

Attack sequence executor

- (Attack profile) information required to execute each technique constituting the attack sequence
  - Attacker and victim information on executing the attack technique
  - Time information to sequentially perform attack sequence according to the timeline
  - Various options such as commands and file paths to be used

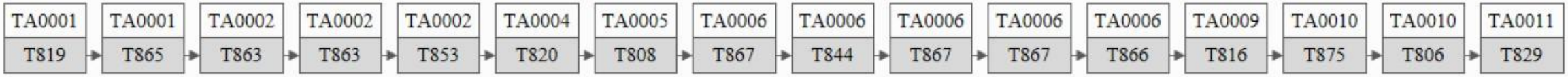


- Execution tool
  - Using Metasploit with post module from the Purple Team ATT&CK Automaiton
  - Currently developing an the automation tool to facilitate attack reproduction

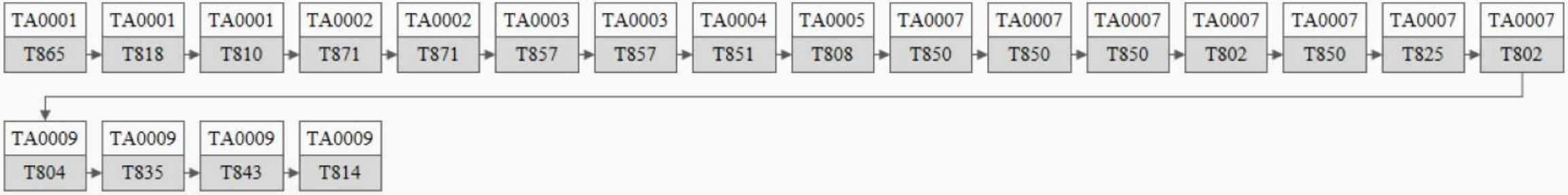
HMM for all ICS incidents

- HMM configuration
  - (Input) State and observation graph with the HMM parameters(π, T, E) for all Incidents attack sequence
  - (output) Attack sequence generated by the HMM for all ICS Incidents
    - ✓ Note that we limited the number of transition as 20 to compare with attack seqeuences.
    - ✓ Examples of generated attack sequence

① Attack sequence where reached final state



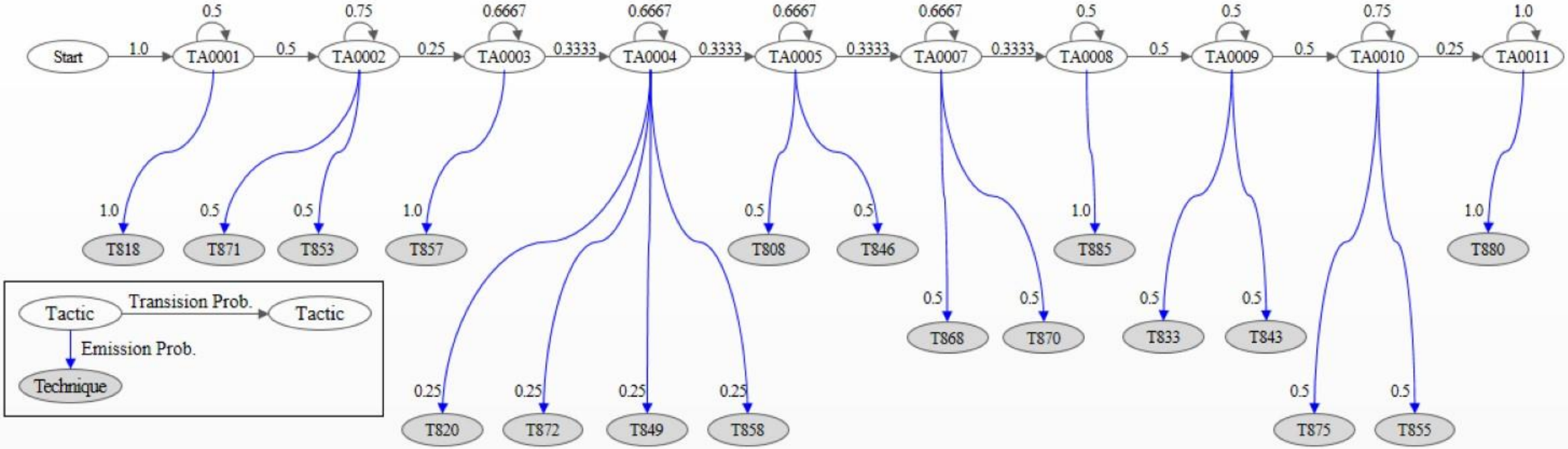
② Attack sequence where not reached final state



HMM for specific ICS incident

HMM configuration

(Input) State and observation graph with the HMM parameters for TRITON malware attack sequence



(Output) Triton-like attack sequence

TA0001	TA0002	TA0002	TA0002	TA0003	TA0003	TA0004	TA0004	TA0005	TA0007	TA0007	TA0008	TA0009	TA0010	TA0011
T818	T871	T871	T853	T857	T857	T872	T872	T808	T870	T868	T885	T833	T855	T880

MITRE ATT&CK + Hidden Markov Model (HMM)

Attack Sequence Generation and Execution

Discussion

Attack sequence generation

- **Probability issues**
  - The propabilities are likely not a representative for all adversaries.
  - The propabilities cannot be automatically obtained to evolve for attack patterns.

Attack sequence execution

- **Target of attack execution**
  - We did not aim to attack the same devices that were subjected to every real ICS attack.
  - It was limited to the HAI testbed.

Development of a dataset of which all levels of the HAI testbed are covered with:

1) Using the proposed method to generate attack sequence for an abnormal data

2) then implement and test to execute at the HAI testbed


NSR
National Security Research Institute
Q & A