NANYANG TECHNOLOGICAL UNIVERSITY

A Method for Modeling and Evaluation of the Security of Cyber-physical Systems

LI BEIBEI

17th Mar, 2015

OUTLINE

- **Introduction**
- **The Proposed Approach**
  - Cyber attacks
  - System model
  - Factors impacting attacker's decision-making
  - The time of transitions
  - Quantitative parameters
- **Case study**

Introduction

- **Authors**

Orojloo, H., Azgomi, M.A.. Trustworthy Comput. Lab., Iran Univ. of Sci. & Technol., Tehran, Iran

- **Published in**

Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on Sep, 2014.

- **Problem**

Quantitative evaluation of security has always been one of the challenges in the field of computer security.

- **Contribution**

The main contribution is that in the proposed state-based model, the cyber attacks that can lead to physical damages are considered and the factors impacting attacker's decision making in the process of cyber attack to CPS are taken into account.

Cyber Attacks

Cyber attacks against CPSs can be categorized as follows:

- **PA:** Cyber attacks that target the availability of **physical components** through physical damage.
- **CA:** Cyber attacks that target the availability of **cyber components** (e.g., DoS attack).
- **I:** Cyber attacks that target the **integrity of data** that are transmitted to control center from sensors or data that are transmitted to actuator.
- **C:** Cyber attacks that target the **confidentiality of cyber components** (e.g., passive attack through eavesdropping).

System Model

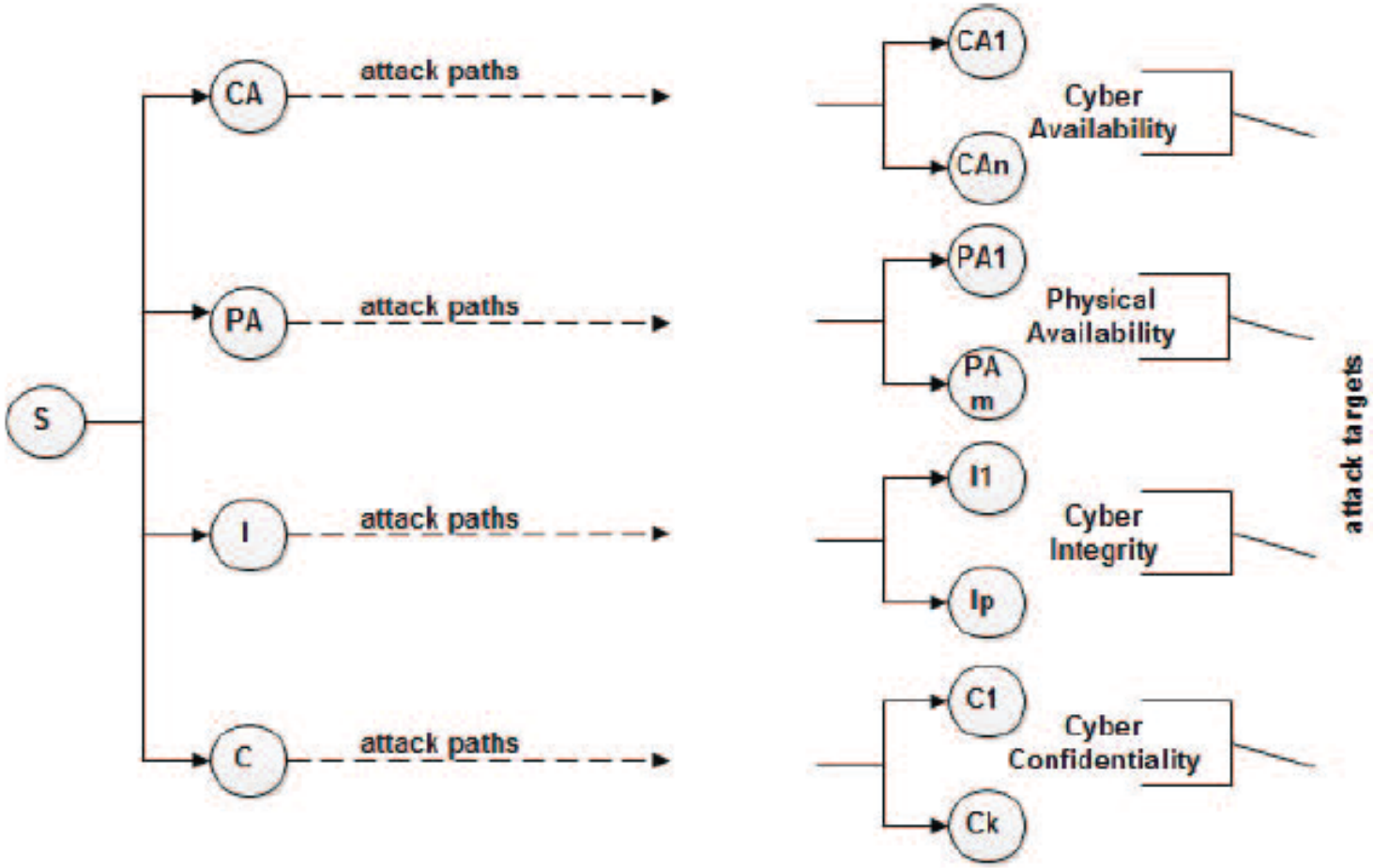

Figure 1. Overall representation of the proposed model

n, m, p, k are the number of components in each category, respectively.

System Model

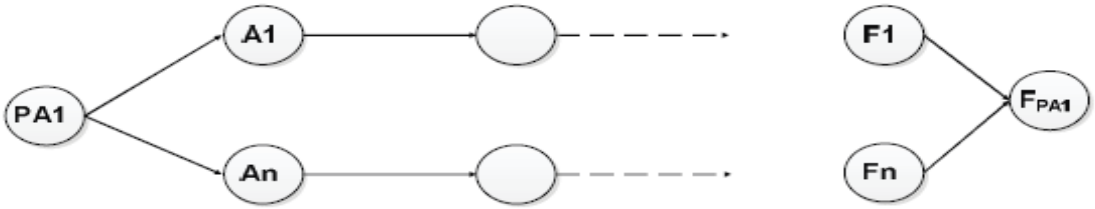

Figure 2. An attack process targeting a physical component

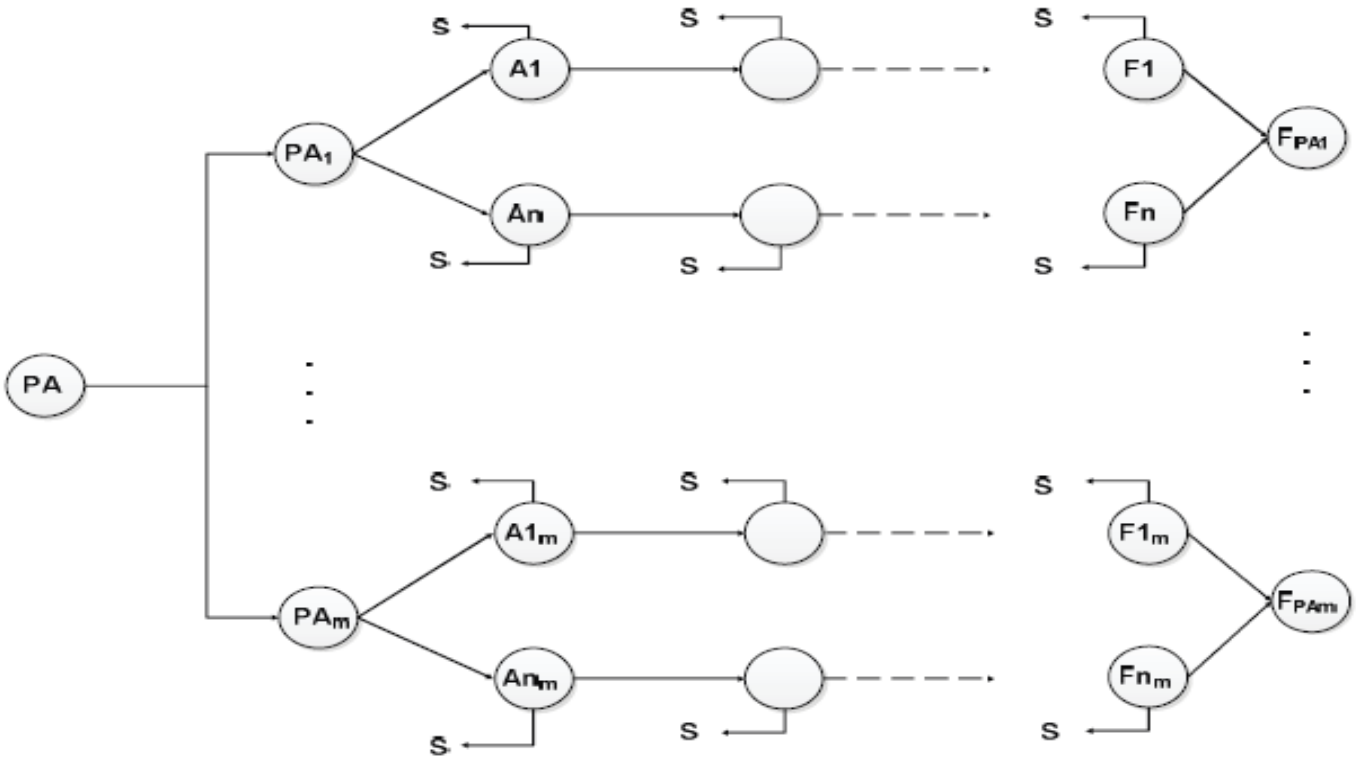

Figure 3. Complete security model for physical components

System Model

The **system security**

$$S = \alpha * PA + \beta * CA + \gamma * I + \theta * C \qquad (1)$$

PA: physical availability
CA: cyber availability
I: integrity
C: confidentiality

$\alpha, \beta, \gamma, \theta$ are coefficients that show the **importance** of the security parameters, and also show the **probability** that an attacker select each of targets.

Factors impacting attacker's decision-making

The factors impacting attacker's decision-makingin cyber attack to physical components in are as follows:

- **Interconnectedness and interdependencies of the component**
- **Kinetic knowledge of the system**
- **Ease of access**
- **Reward**
- **Cost**

System Model

The probability that an attacker choose a physical component *i* as a target in initial state (PA) is derived as follows:

$$P_i = \frac{(\alpha R_i * \beta K_i * \gamma I_i * \theta E_i)/(\lambda * C_i)}{\sum_{j=1}^{m}((\alpha R_j * \beta K_j * \gamma I_j * \theta E_j)/(\lambda * C_j))} \quad (2)$$

R_i: reward for component *i*
K_i: Kinetic knowledge of the attacker to component *i*
I_i: Interconnectedness and interdependencies of the component *i*
C_i: cost of the attack to component *i*
E: ease of access component *i*
$\alpha, \beta, \gamma, \theta, \lambda$ are the coefficients depending on the importance of each factor

In this approach, we only consider the **reward**, **ease of access**, **and cost**.

$$P_i = \frac{(\alpha R_i * \theta E_i)/(\lambda * C_i)}{\sum_{j=1}^{m}((\alpha R_j * \theta E_j)/(\lambda * C_j))} \quad (3)$$

The time of transitions

Let **X** and **Y** be the nonnegative continuous random variables indicating **the attacker's needed time** and **the system's response to an attack**, in current state respectively.

The probability of the successful detection and prevention of the activities of the system: **P(Y >X)**
The success probability of the attacker : **P(X < Y)**

We define the distribution functions of the transitions of the model (i.e., attacker behavior and system response) as a linear combination of uniform distributions. Hence, for the attacker transitions in each state we have:

$$F_X(\mathrm{t}) = \sum_{i=1}^{n} p_i \, \mathrm{F}_{X_i}(\mathrm{t}), \sum_{i=1}^{n} p_i = 1 \qquad (5)$$

The time of transitions

The distribution function of system transitions FY(t) is given by:

$$F_Y(\mathrm{t}) = \sum_{i=1}^{m} q_i \, \mathrm{F}_{Y_i}(\mathrm{t}), \sum_{i=1}^{m} q_i = 1 \qquad (6)$$

Then, the success probability of the attacker's action in each state is given by:

$$P(\mathrm{X} < \mathrm{Y}) = \int_{-\infty}^{\infty} P(\mathrm{X} < \mathrm{Y} \mid \mathrm{Y} = t) f_y(\mathrm{t})\,\mathrm{dt} \qquad (7)$$

where, $f_Y(t)$ is the density function of the random variable Y . Since X and Y are continuous random variables, we can rewrite the above integral as follows:

$$P(\mathrm{X} < \mathrm{Y}) = \int_{-\infty}^{\infty} P(\mathrm{X} < t) f_y(\mathrm{t})\,\mathrm{dt} = \int_{-\infty}^{\infty} F_X(t) f_y(\mathrm{t})\,\mathrm{dt} \qquad (8)$$

The time of transitions

With the replacement of (5), (6) in this integral, we will have:

$$P(\mathrm{X} < \mathrm{Y}) = \int_{-\infty}^{\infty} \left(\sum_{i=1}^{n} p_i \, \mathrm{F}_{X_i}(\mathrm{t}) \right) \left(\sum_{j=1}^{m} q_j \, \mathrm{F}_{Y_j}(\mathrm{t}) \right) dt$$

$$= \sum_{i=1}^{n} \sum_{j=1}^{m} p_i q_i \int_{0}^{b} \mathrm{F}_{X_i}(\mathrm{t}) f_{Y_j}(\mathrm{t}) \, \mathrm{dt} \qquad (9)$$

Finally, the transition probability matrix of the deterministic-time Markov chain (DTMC) is achieved by using the (1), (2), (3), (4) and (9).

Quantitative parameters

- ***The average visit rate.*** The average number of times the state is visited before the DTMC reaches one of the absorbing states. This visit rate for a state Vi can be obtained by solving the following equation:

$$V_i = q_i + \sum_j V_j q_{ji}, \;\; i, j \in X_s \qquad (10)$$

where, q_i is the probability that DTMC start in state i, X_s is the set of states and is the average visit rate of the state i.

- ***Mean sojourn time.*** The time the system stays in a state i in a model. Let Z_i be the continuous random variable for outgoing transition i from state s . The mean sojourn time for the state s is given by:

Quantitative parameters

$$h_s = \int_0^b \left(\prod_{i=1}^{k} (1 - F_{Z_i}(t)) \right) dt \qquad (11)$$

where, $F_{zi}(t)$ is the distribution function of random variable Z_i, and h_s is the mean sojourn time for the state s.

We assume that the uniform random variable X_i is distributed over interval [a_i , b_i]. Therefore, the mean sojourn time for a security failure state (S_F) for steady state analysis purpose is given by:

$$S_F = E(X) = \sum_{i=1}^{m} p_i \left(\frac{a_i + b_i}{2} \right) \qquad (12)$$

where, X is a linear combination of uniform distributions X_1, … X_m .

Quantitative parameters

- ***Mean time to security failure (MTTSF)***

$$MTTSF = \sum_{i \in X_t} V_i h_i \qquad (13)$$

where, V_i is the average visit rate of state i and h_i represent the mean sojourn time for state i.

- ***Steady state security***

$$V = V \cdot P, \sum v_i = 1 \qquad (14)$$

The DTMC steady-state probabilities v_i can be computed as follows:

$$\pi_i = \frac{v_i h_i}{\sum_j v_j h_j}, \; i, j \in X_s \qquad (15)$$

where, V is the steady-state probability vector of DTMC and P is the transition probability matrix.

Quantitative parameters

After computing the steady-state probabilities of SMP states, the steady state security of CPS may be written as follows:

$$S_{steady} = 1 - (\sum_{i=1}^{n} F_{CA_i} + \sum_{i=1}^{m} F_{PA_i} + \sum_{i=1}^{p} F_{I_i} + \sum_{i=1}^{k} F_{C_i}) \quad (16)$$

where, F_{CAi} , F_{PAi} , F_{Ii} , F_{Ci} , are the steady-state probabilities (π_i) of SMP.

- ***Steady state physical availability***

$$A = 1 - (\sum_{i=1}^{m} F_{PA_i}) \qquad (17)$$

where, F_{PAi} are the physical availability failure states.

Case study

We assume a simple CPS with m=2 physical components, and n=1 cyber component. And we assign $\alpha = 0.4, \beta = 0.3, \gamma = 0.2, \theta = 0.1$.

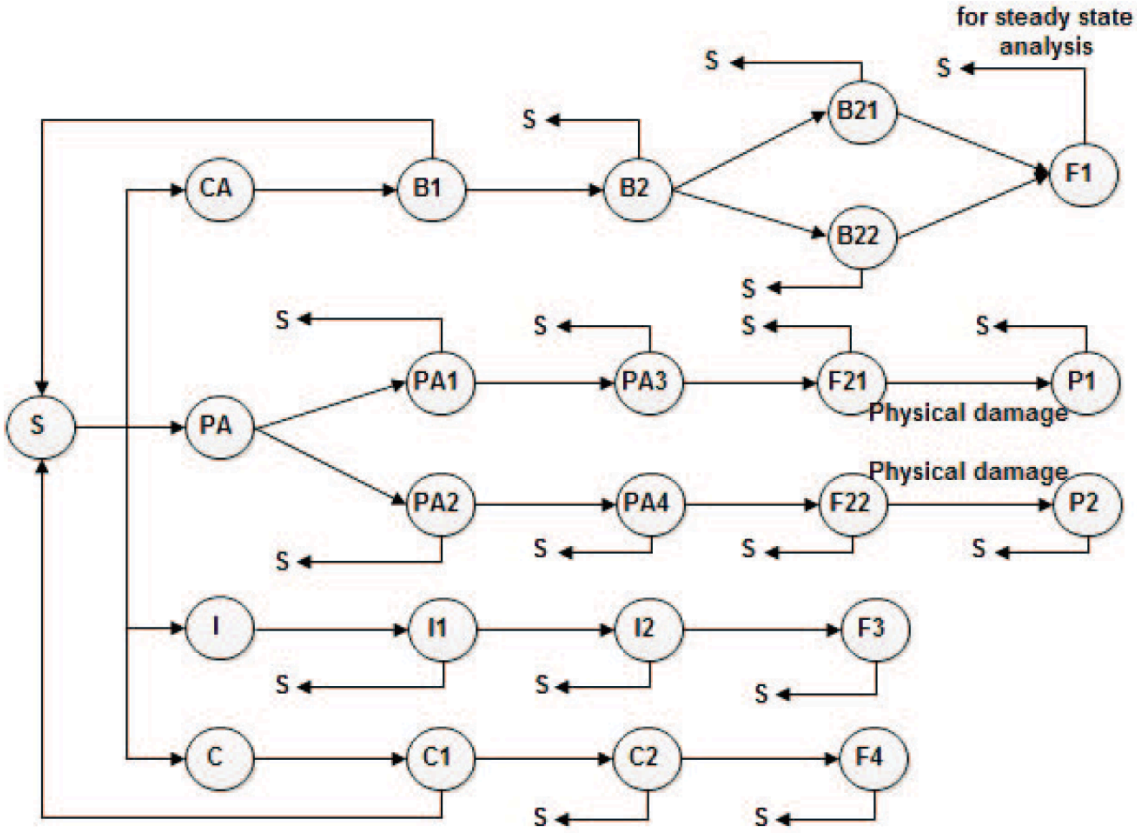

Figure 4. The model of the illustrative example

Case study

To each transition is assigned two time intervals with equal probabilities. For example, for *PA->PA1* we have: [0, 20] with the probability 0.5 and [20, 40] with the probability 0.5. The transition probability matrix of the DTMC is achieved by using the (1), (2), (3), (4) and (9). By using the equation (10), the average visit rate of each state is obtained. Since the system is initially in the state S , p_s in this equation is equal to 1 and p_i for other states is zero. In next step, by using (11) and (12), the mean sojourn time of all states are calculated. Then, the steady-state probabilities of the SMC are calculated by using the equation (15). Finally, by using (13), (16) and (17), we will have:

- MTTSF=665h
- Steady- state security = 0.9936
- Steady-state physical availability = 0.9962 .

NANYANG
TECHNOLOGICAL
UNIVERSITY

Thanks