Multi-Model Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems

Zhang Qi

qiqi@hust.edu.cn

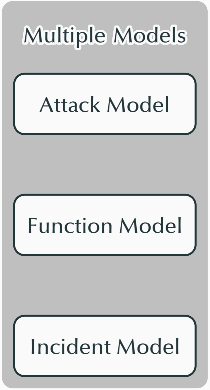
October 12, 2015

Automation School,
Huazhong University of Science and Technology,
Wuhan.

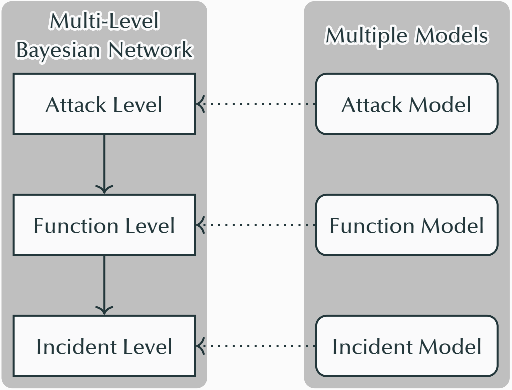
Outlines

Architecture

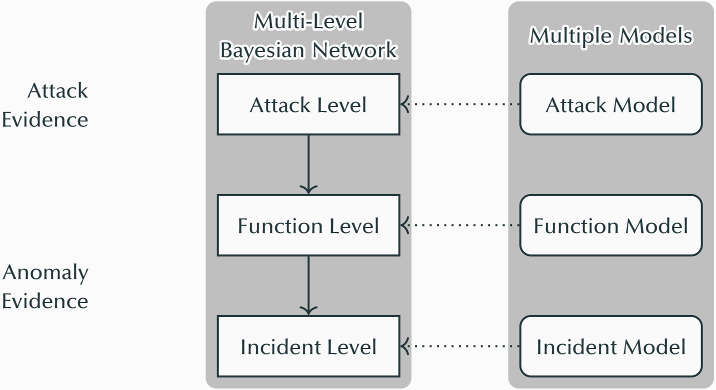
Architecture of Cybersecurity Risk Assessment for ICSs



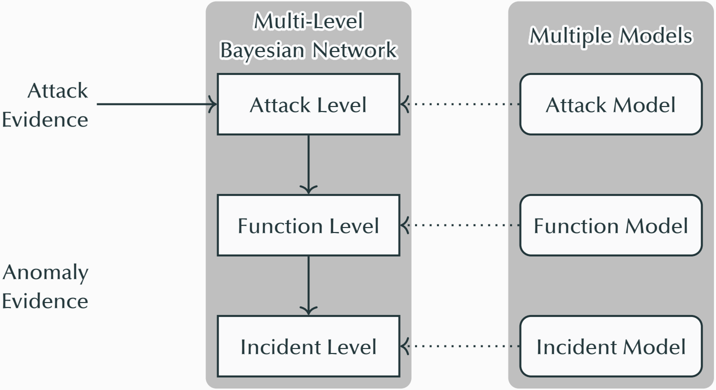
Architecture of Cybersecurity Risk Assessment for ICSs



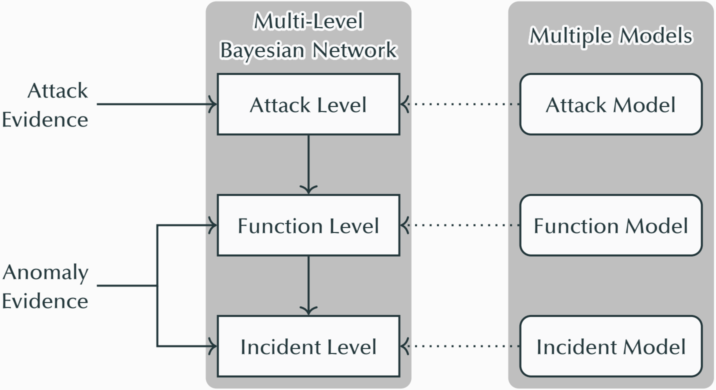
Architecture of Cybersecurity Risk Assessment for ICSs



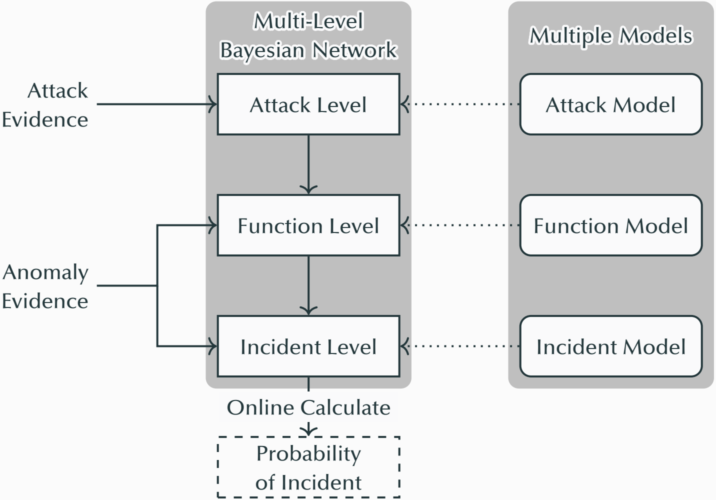
Architecture of Cybersecurity Risk Assessment for ICSs



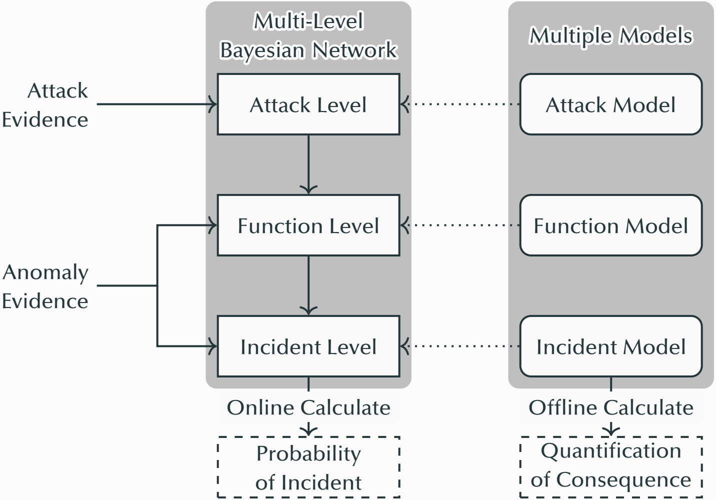
Architecture of Cybersecurity Risk Assessment for ICSs



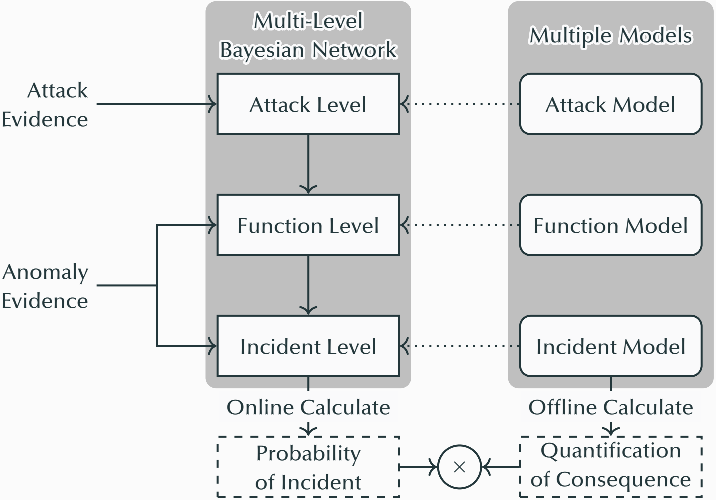
Architecture of Cybersecurity Risk Assessment for ICSs



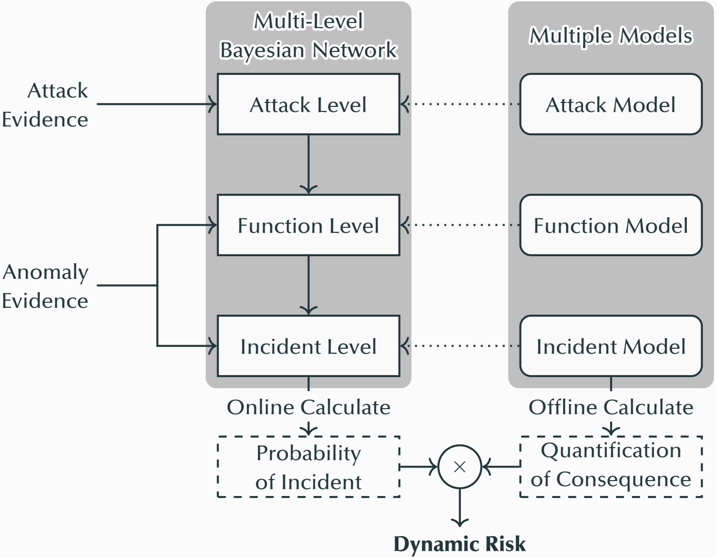
Architecture of Cybersecurity Risk Assessment for ICSs



Architecture of Cybersecurity Risk Assessment for ICSs



Architecture of Cybersecurity Risk Assessment for ICSs



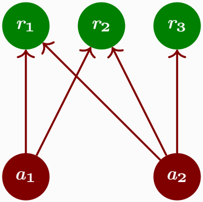
Hazardous Incident Prediction

Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.

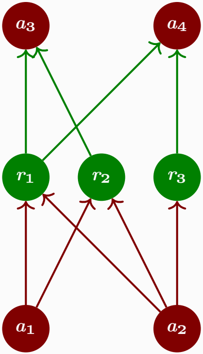
Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



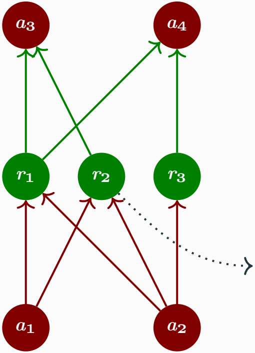
Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



Attack Level

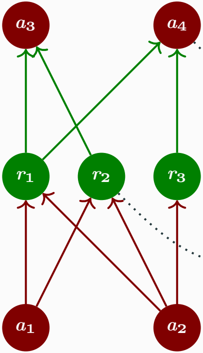
In this paper, the Bayesian network is used to model the relationship between attacks and resources.



$L(a_1)$	T	T	F	F
$L(a_2)$	T	F	T	F
$O(r_2)$	$o_{r_2,1}$	$o_{r_2,2}$	$o_{r_2,3}$	$o_{r_2,4}$
$\overline{O}(r_2)$	$1 - o_{r_2,1}$	$1 - o_{r_2,2}$	$1 - o_{r_2,3}$	$1 - o_{r_2,4}$

Attack Level

In this paper, the Bayesian network is used to model the relationship between attacks and resources.



$O(r_1)$	T	T	F	F
$O(r_3)$	T	F	T	F
$L(a_4)$	$\ell_{a_4,1}$	$\ell_{a_4,2}$	$\ell_{a_4,3}$	$\ell_{a_4,4}$
$\overline{L}(a_4)$	$1-\ell_{a_4,1}$	$1-\ell_{a_4,2}$	$1-\ell_{a_4,3}$	$1-\ell_{a_4,4}$

$L(a_1)$	T	T	F	F
$L(a_2)$	T	F	T	F
$O(r_2)$	$o_{r_2,1}$	$o_{r_2,2}$	$o_{r_2,3}$	$o_{r_2,4}$
$\overline{O}(r_2)$	$1-o_{r_2,1}$	$1-o_{r_2,2}$	$1-o_{r_2,3}$	$1-o_{r_2,4}$

Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

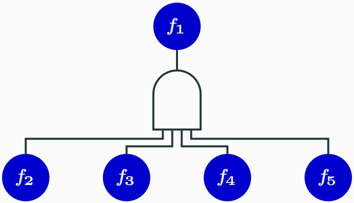
Function Level

Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.

$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

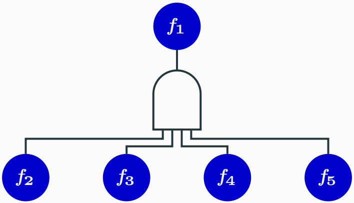
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

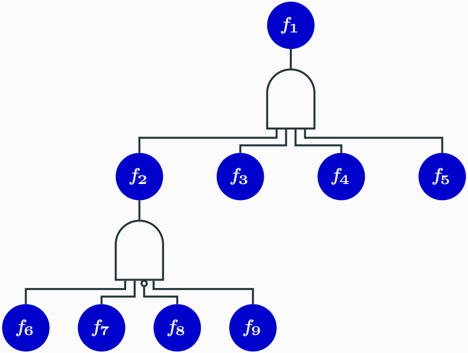
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_2 = F_6 F_7 \overline{F_8} F_9$$

Function Level

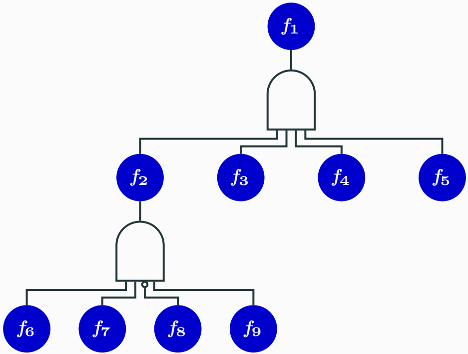
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_2 = F_6 F_7 \overline{F_8} F_9$$

Function Level

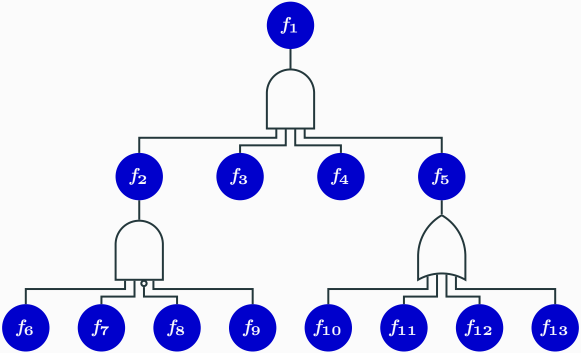
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_5 = F_{10} + F_{11} + F_{12} + F_{13}$$

Function Level

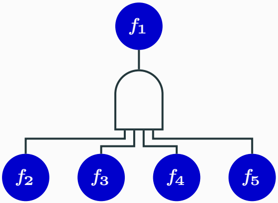
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_5 = F_{10} + F_{11} + F_{12} + F_{13}$$

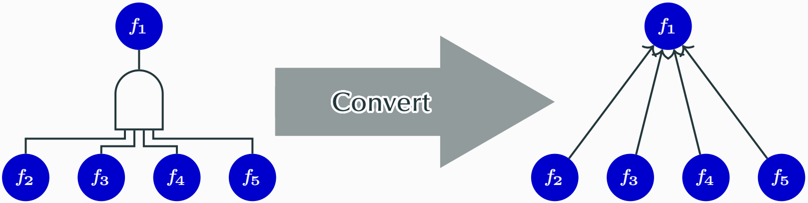
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



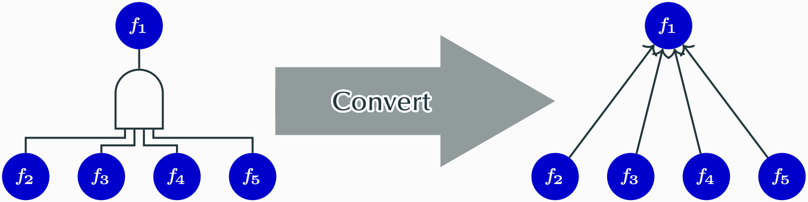
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



Function Level

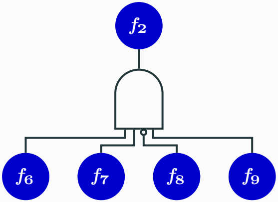
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

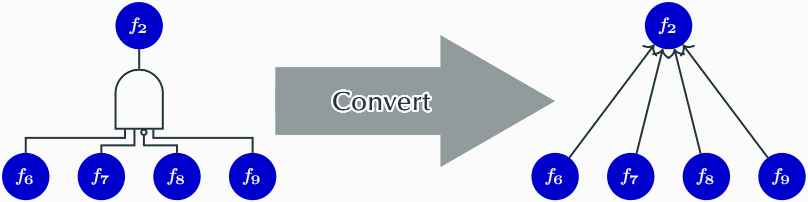
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



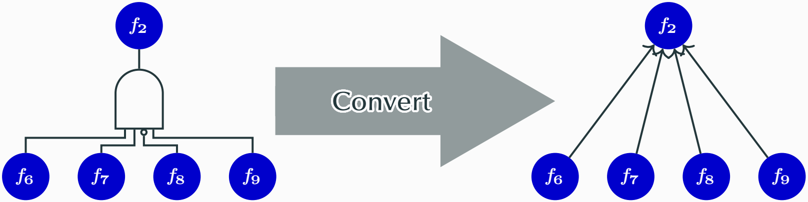
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



Function Level

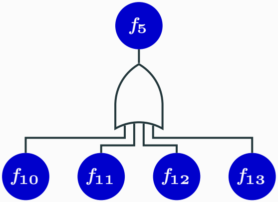
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_6)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_7)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_8)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_9)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_1)$	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1
$\overline{F}(f_1)$	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0

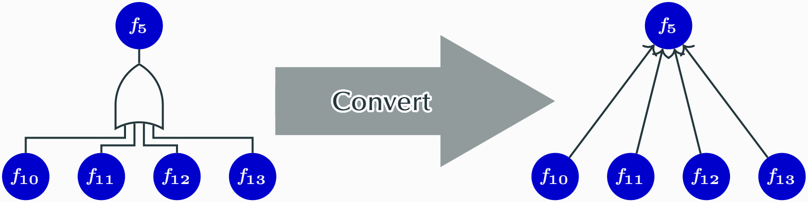
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



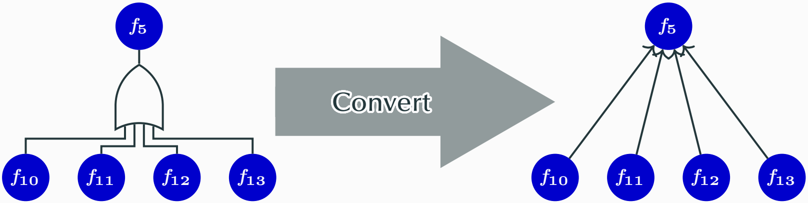
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



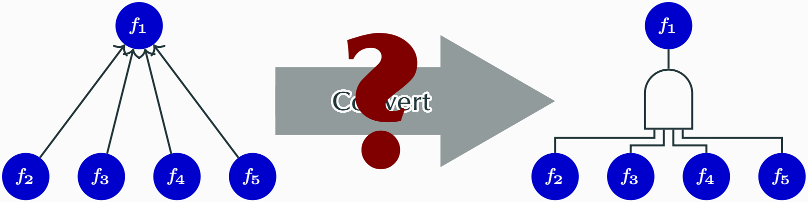
Function Level

To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.

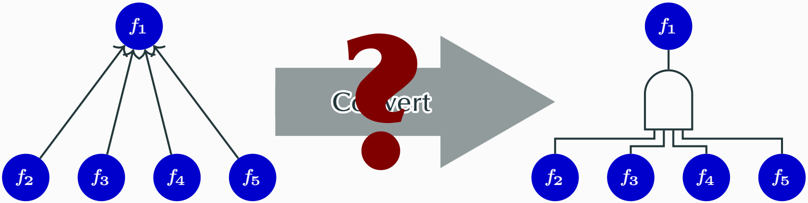


$F(f_{10})$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_{11})$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_{12})$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_{13})$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_5)$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\overline{F}(f_5)$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Function Level

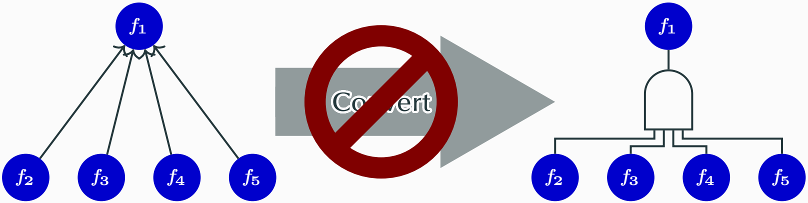


Function Level



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

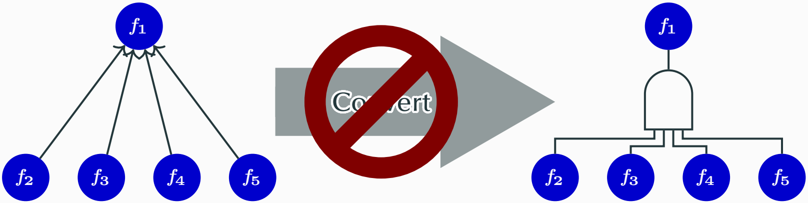
Function Level



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

Function Level

The conditional probability table of the Bayesian network contains more information than the logical gate of the fault tree.



$F(f_2)$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	**F**
$F(f_3)$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	**F**
$F(f_4)$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	**F**
$F(f_5)$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	**F**
$F(f_1)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**0.5**
$\overline{F}(f_1)$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0.5**

Incident Level

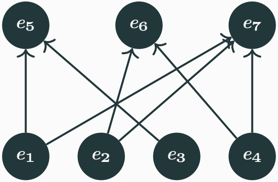
The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.

Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

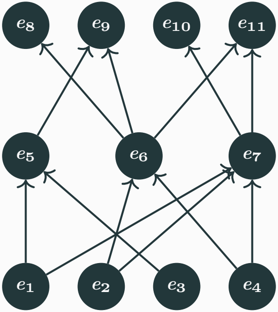
A typical Bayesian network of incident is shown in following figure.



Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

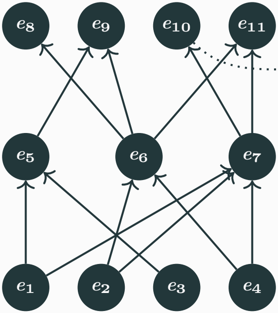
A typical Bayesian network of incident is shown in following figure.



Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.

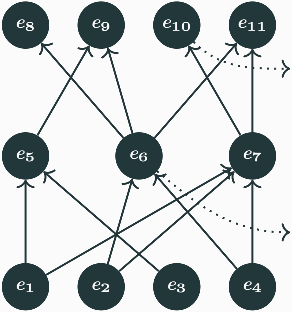


$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

Incident Level

The occurrence of one incident may cause another incidents, in this paper, the Bayesian network is also used to model the causal relationship amongst the potential incidents.

A typical Bayesian network of incident is shown in following figure.



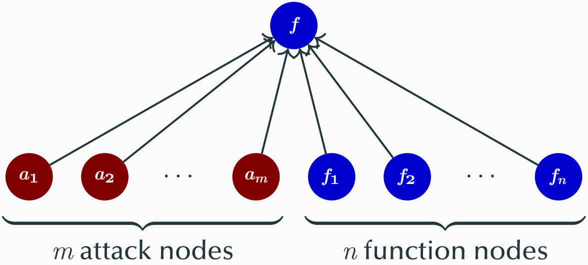
$H(e_7)$	T	F
$H(e_{10})$	$h_{e_{10},1}$	$h_{e_{10},2}$
$\overline{H}(e_{10})$	$1-h_{e_{10},1}$	$1-h_{e_{10},2}$

$H(e_2)$	T	T	F	F
$H(e_4)$	T	F	T	F
$H(e_6)$	$h_{e_6,1}$	$h_{e_6,2}$	$h_{e_6,3}$	$h_{e_6,4}$
$\overline{H}(e_6)$	$1-h_{e_6,1}$	$1-h_{e_6,2}$	$1-h_{e_6,3}$	$1-h_{e_6,4}$

Information Transfer between Levels

The cyber attacks can lead to system function failures, and the function failures may cause the industrial incidents. To analyze the risk propagation, an information transfer is necessary between the three aforementioned layers.

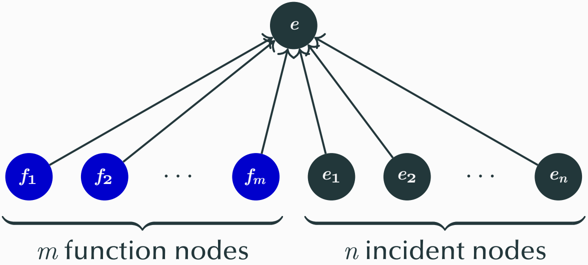
The following figures show two kind of information transfer.



Information Transfer between Levels

The cyber attacks can lead to system function failures, and the function failures may cause the industrial incidents. To analyze the risk propagation, an information transfer is necessary between the three aforementioned layers.

The following figures show two kind of information transfer.



Collection of Evidence

There are two kind of evidence need to be collected:

- **Attack Evidence**, contains the attack information, such as attack time, attack type, attack object, etc.
- **Anomaly Evidence**, contains the information about the anomaly, such as function failure, function restoration, incident occurrence, etc.

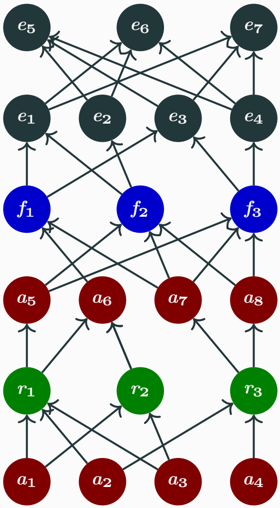
Collection of Evidence

There are two kind of evidence need to be collected:

- **Attack Evidence**, contains the attack information, such as attack time, attack type, attack object, etc.
- **Anomaly Evidence**, contains the information about the anomaly, such as function failure, function restoration, incident occurrence, etc.

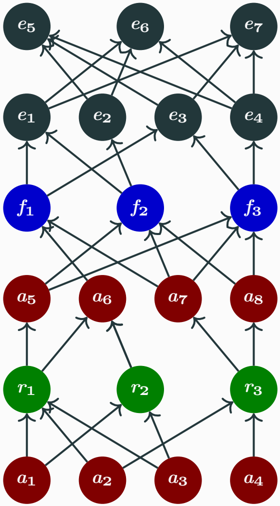
For each evidence, there exists a corresponding node in the multi-level Bayesian network. When the intrusion detection system or the monitoring system finds an evidence, the corresponding node will be marked in the multi-level Bayesian network.

Calculation of Incident Probability



The left figure shows a typical multi-level Bayesian network.

Calculation of Incident Probability

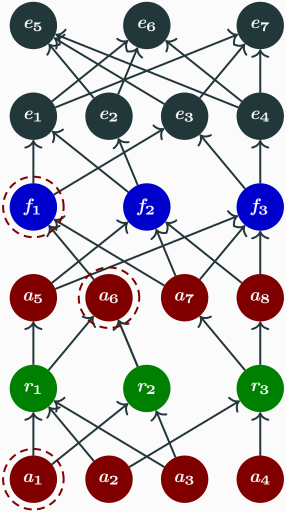


The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Calculation of Incident Probability



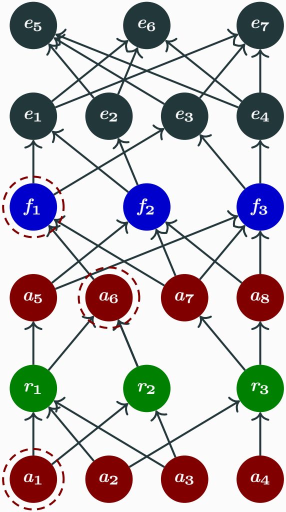
The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Then the nodes a_1, a_6, and f_1 are marked with **red** dashed circles.

Calculation of Incident Probability



The left figure shows a typical multi-level Bayesian network.

Assuming that the evidence list is

$$a_1, a_6, f_1$$

Then the nodes a_1, a_6, and f_1 are marked with **red** dashed circles.

Finally, the algorithm named Probability Propagation in Trees of Clusters (PPTC) can calculate the probabilities of all the hazardous incidents.

Dynamic Risk Assessment

Decouple of Incident Consequences – Step 1

for each incident e_i, analyze its consequence and generate a consequence set

$$\boldsymbol{c}_i = (c_1, c_2, \cdots, c_n).$$

The meaning of $\boldsymbol{c}_i$ is that the occurring of the incident e_i will threaten the elements in consequence set $\boldsymbol{c}_i$.

For example, the incident e_i is an explosion of a reactor, which may cause worker casualties, air pollution, facilities damages, and products loss. The consequence set of e_i is

$$\boldsymbol{c}_i = (\text{workers}, \text{air}, \text{facilities}, \text{products}).$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$.

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

For each incident e_k of the incident set $\boldsymbol{e}_j$, the corresponding consequence set $\boldsymbol{c}_k$ satisfies the following condition:

$$\boldsymbol{c}'_j \subseteq \boldsymbol{c}_k.$$

Decouple of Incident Consequences – Step 3

For each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, generate a corresponding auxiliary node x_j. According to the **traceability** of $\boldsymbol{C}'$

$$\forall \boldsymbol{c}' \in \boldsymbol{C}', \exists \boldsymbol{c} \in \boldsymbol{C}, \boldsymbol{c}' \subseteq \boldsymbol{c},$$

there must be a consequence set $\boldsymbol{c}_i \in \boldsymbol{C}$, where $\boldsymbol{c}'_j \subseteq \boldsymbol{c}_i$. So, for each $\boldsymbol{c}'_j \in \boldsymbol{C}'$, we can find the incident set

$$\boldsymbol{e}_j = (e_{i_1}, e_{i_2}, \cdots, e_{i_n}).$$

For each incident e_k of the incident set $\boldsymbol{e}_j$, the corresponding consequence set $\boldsymbol{c}_k$ satisfies the following condition:

$$\boldsymbol{c}'_j \subseteq \boldsymbol{c}_k.$$

Therefore, the parent nodes of the auxiliary node x_j are incident nodes $e_{i_1}, e_{i_2}, \cdots, e_{i_n}$.

Decouple of Incident Consequences – Step 4

For each auxiliary node x_j, generate a conditional probability table. A typical conditional probability table of auxiliary node x_j is shown as following table.

$H(e_{i_1})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_2})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_3})$	T	T	T	$\cdots$	F	F	F
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$H(e_{i_{n-2}})$	T	T	T	$\cdots$	F	F	F
$H(e_{i_{n-1}})$	T	T	F	$\cdots$	T	F	F
$H(e_{i_n})$	T	F	F	$\cdots$	F	T	F
$H(x_j)$	1	1	1	$\cdots$	1	1	0
$\overline{H}(x_j)$	0	0	0	$\cdots$	0	0	1

Classification of Incident Consequences

In this paper, there are three main kinds of incident consequences to be considered:

- **Harm to Humans:**
  - temporary harm,
  - permanent disability,
  - fatality.
- **Environmental Pollution:**
  - air pollution,
  - soil contamination,
  - water pollution.
- **Property Loss:**
  - damage of materials,
  - damage of products,
  - damage of equipment.

Quantification of Incident Consequences

- **Harm to Humans Q_H:**
  If the decision-maker would like to increase the cost of an investment by Δc to reduce the probability of a fatality by Δp,

$$Q_H = \Delta c / \Delta p.$$

- **Environmental Pollution Q_E:**
  The monetary loss of environmental pollution is defined as

$$Q_E = Penalty + Compensation + HarnessCost.$$

- **Property Loss Q_P:**
  The cost of replacement is used to quantify the loss of property Q_P, such as the loss of materials, products, and equipment.

Calculation of Dynamic Risk

Due to the following two reasons:

- there is no overlapping between the consequences of any two auxiliary nodes x_i and x_j, $i \neq j$,
- the auxiliary nodes contain all the consequences of incidents,

the dynamic cybersecurity risk can be defined as

$$\mathscr{R} = \sum_{i=1}^{m'} p(x_i)\, q(x_i),$$

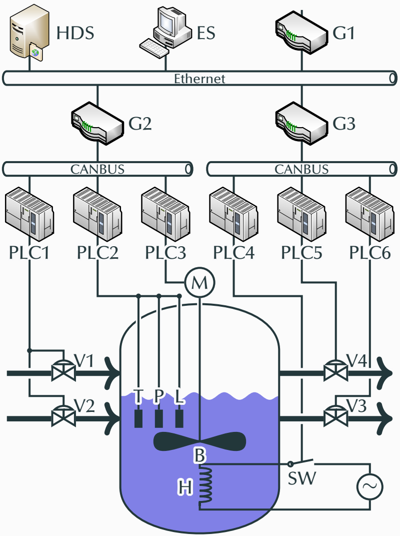
where

- $p(x_i)$ is the occurrence probability of the auxiliary node x_i,
- $q(x_i)$ is the monetary loss of the auxiliary node x_i.

Simulation

Simulation Platform

The simulation object is a chemical reactor whose control structure is shown as the following figure.

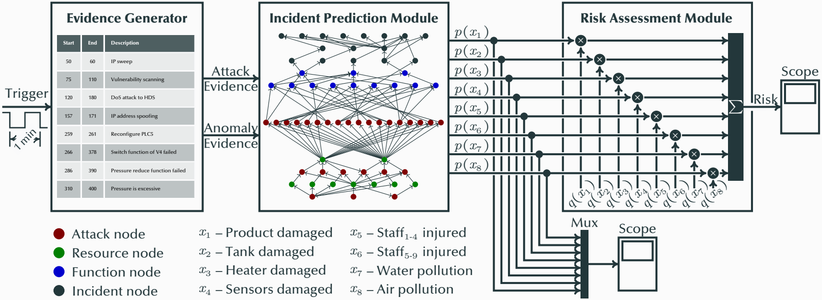


Legend

HDS	Historical data server
ES	Engineer station
G1	Gateway of Ethernet
G2	Gateway of CANBUS
G3	Gateway of CANBUS
PLC1	Controller of V1 and V2
PLC2	Data collection of P, T and L
PLC3	Controller of M
PLC4	Controller of SW
PLC5	Controller of V4
PLC6	Controller of V3
V1	Valve of material
V2	Valve of another material
V3	Valve of product
V4	Valve of pressure reducing
M	Motor of B
SW	Switch of H
P	Pressure sensor
T	Temperature sensor
L	Liquid level sensor
B	Blender
H	Heater

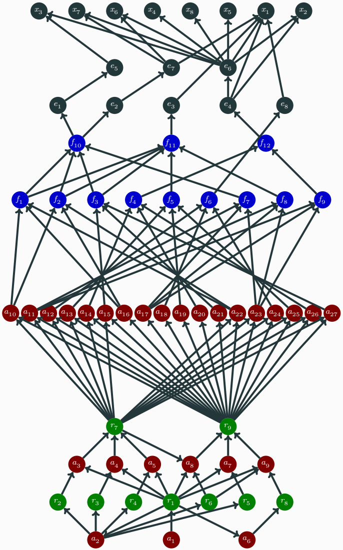
Simulation Platform

The simulation platform is implemented in Matlab, which consists of three modules: an evidence generator, an incident prediction module, and a risk assessment module.



Simulation Platform

The multi-level Bayesian network of the chemical reactor is shown as following figure.



a_1 – Network Scanning
a_2 – Vulnerability scanning
a_3 – Buffer overflow attack on HDS
a_4 – FTP attack on HDS
a_5 – Brute force attack on HDS
a_6 – DoS attack on HDS
a_7 – Buffer overflow attack on ES
a_8 – Privilege escalation attack on ES
a_9 – Spoofing attack on ES
a_{10} – DoS attack on PLC1
a_{11} – DoS attack on PLC2
a_{12} – DoS attack on PLC3
a_{13} – DoS attack on PLC4
a_{14} – DoS attack on PLC5
a_{15} – DoS attack on PLC6
a_{16} – Reconfigure PLC1
a_{17} – Reconfigure PLC2
a_{18} – Reconfigure PLC3
a_{19} – Reconfigure PLC4
a_{20} – Reconfigure PLC5
a_{21} – Reconfigure PLC6
a_{22} – Man-in-the-middle attack on PLC1
a_{23} – Man-in-the-middle attack on PLC2
a_{24} – Man-in-the-middle attack on PLC3
a_{25} – Man-in-the-middle attack on PLC4
a_{26} – Man-in-the-middle attack on PLC5
a_{27} – Man-in-the-middle attack on PLC6
r_1 – IP addresses of HDS and ES
r_2 – Buffer overflow vulnerability
r_3 – FTP server vulnerability
r_4 – Login vulnerability
r_5 – Buffer overflow vulnerability
r_6 – Authentication vulnerability
r_7 – Administrator authority of HDS
r_8 – Crash of HDS
r_9 – Administrator authority of ES
f_1 – Traffic control of V1
f_2 – Traffic control of V2
f_3 – Traffic control of V3
f_4 – Pressure reducing
f_5 – Heating function
f_6 – Mixing function
f_7 – Liquid level sensation
f_8 – Temperature sensation
f_9 – Pressure sensation
f_{10} – Liquid level control
f_{11} – Temperature control
f_{12} – Pressure control
e_1 – Excessive liquid level
e_2 – Low liquid level
e_3 – Temperature anomaly
e_4 – Excessive pressure
e_5 – Heater dry fired
e_6 – Reactor explosion
e_7 – Liquid overflow
e_8 – Blender stop
x_1 – Production damaged
x_2 – Tank damaged
x_3 – Heater damaged
x_4 – Sensors damaged
x_5 – Staff$_{1\text{-}4}$ injured
x_6 – Staff$_{5\text{-}9}$ injured
x_7 – Water pollution
x_8 – Air pollution

Simulation Platform

The list of evidences is shown as following table.

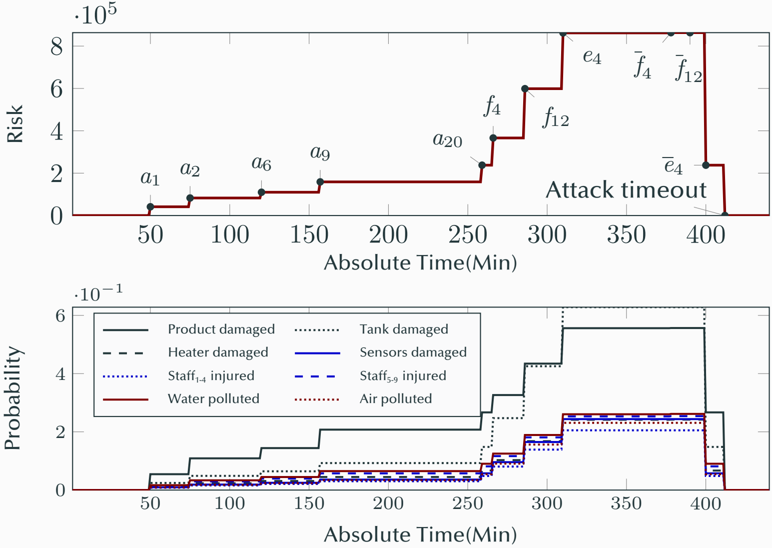
Start	End	Description	Symbol
50	60	IP sweep	$L(a_1)$
75	110	Vulnerability scanning	$L(a_2)$
120	180	DoS attack to HDS	$L(a_6)$
157	171	IP address spoofing	$L(a_9)$
259	261	Reconfigure PLC5	$L(a_{20})$
266	378	Switch function of V4 failed	$F(f_4)$
286	390	Pressure reduce function failed	$F(f_{12})$
310	400	Pressure is excessive	$H(e_4)$

Simulation Platform

The quantification of consequences is shown as following table.

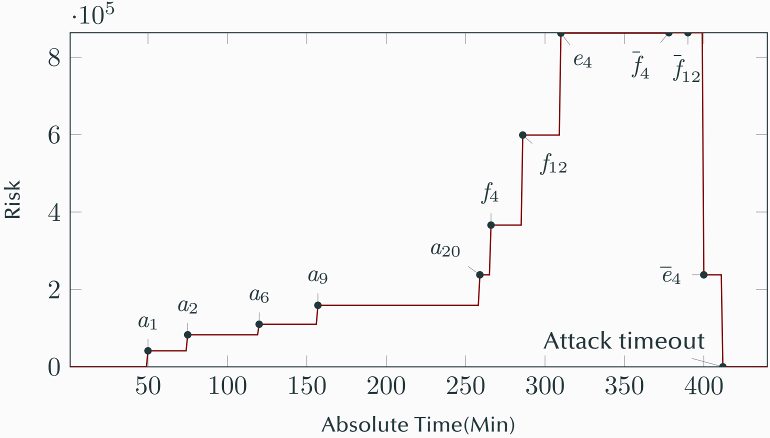
Incident Symbol	Description of Incident	Quantification of Consequence($)
x_1	Product damaged	50,000
x_2	Tank damaged	500,000
x_3	Heater damaged	10,000
x_4	Sensors damaged	10,000
x_5	$\text{Staff}_{1\text{-}4}$ injured	800,000
x_6	$\text{Staff}_{5\text{-}9}$ injured	1,000,000
x_7	Water pollution	200,000
x_8	Air pollution	200,000

Simulation and Result Analysis

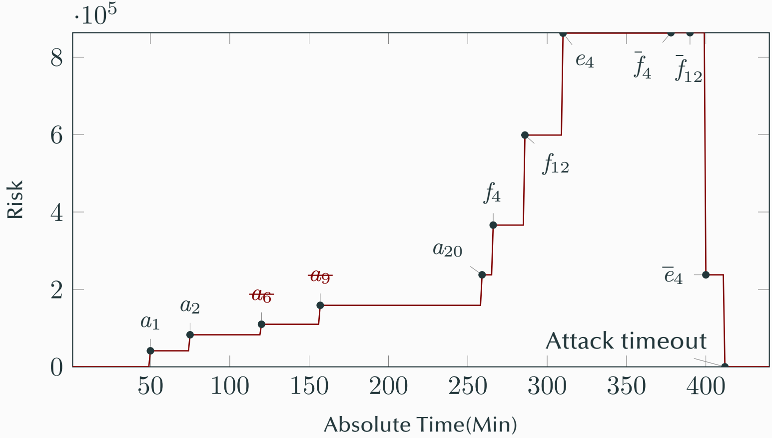


Simulation and Result Analysis

In the previous simulation, the curve of the cybersecurity risk is shown as the **red** line in the following figure.

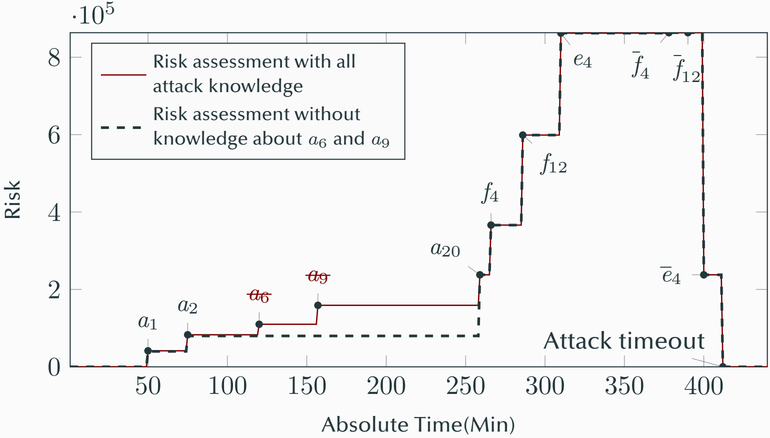


To validate the ability to deal with the unknown attacks, the attack knowledge about attack $\cancel{a_6}$ and attack $\cancel{a_9}$ is removed from the multi-level Bayesian network.



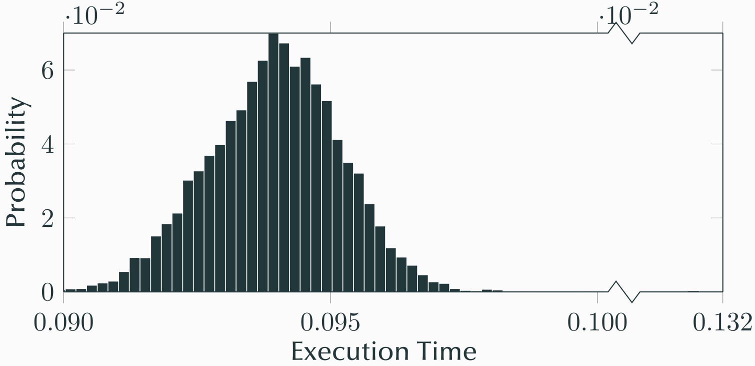
Simulation and Result Analysis

Then an identical multi-step attack on the system is launched to the system. The new cybersecurity risk curve is shown the dashed line in the following figure.



Simulation and Result Analysis

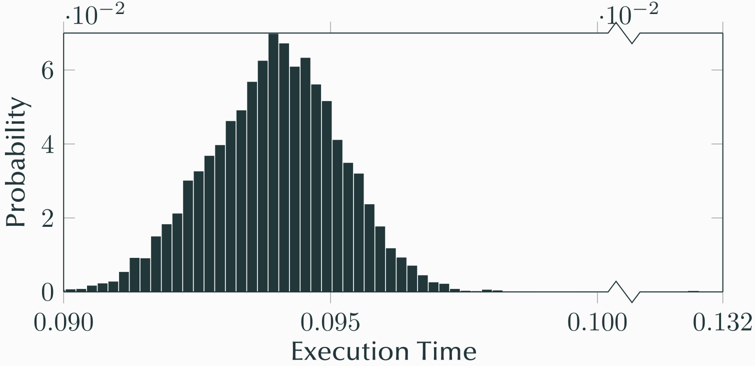
We repeat the first simulation 5,000 times, and the execution time of 5,000 calculations is recorded. This simulation is run on a machine with Intel Pentium processor G3220 (3M Cache, 3.00GHz) and 4GB DDR3 memory. The following figure shows the distribution of the 5,000 execution times.



Simulation and Result Analysis

Some parameters of the following figure:

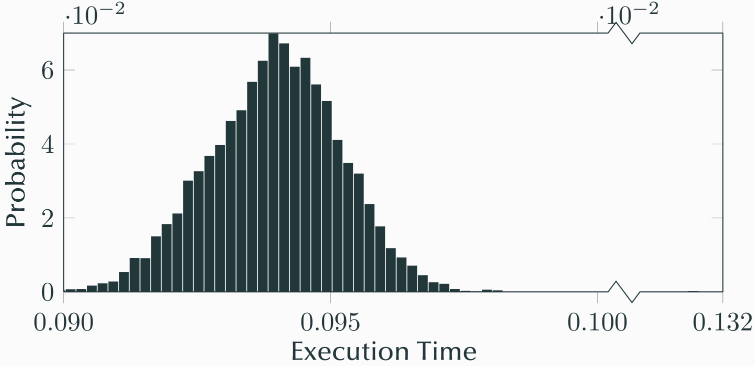
- The average execution time of a risk assessment is 94.1ms.



Simulation and Result Analysis

Some parameters of the following figure:

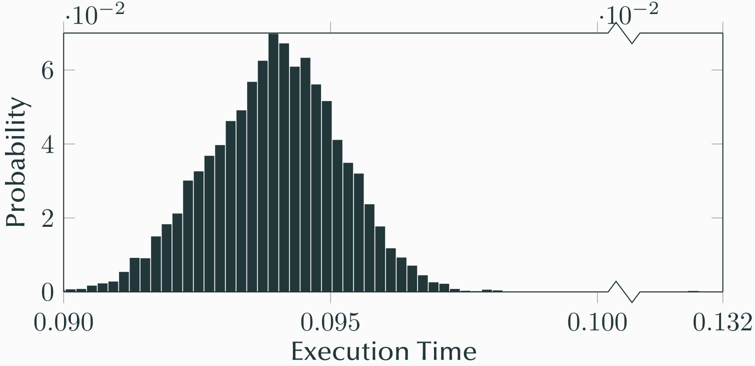
- The average execution time of a risk assessment is 94.1ms.
- The minimum execution time of a risk assessment is 89.9ms.



Simulation and Result Analysis

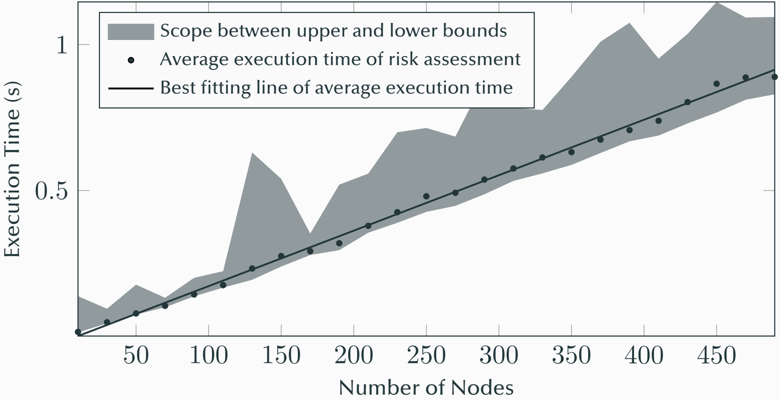
Some parameters of the following figure:

- The average execution time of a risk assessment is 94.1ms.
- The minimum execution time of a risk assessment is 89.9ms.
- The maximum execution time of a risk assessment is 131.6ms.



Simulation and Result Analysis

Finally, 25 multi-level Bayesian networks with different node sizes are adopted to show the possible upper/lower bounds and the scalability of our approach.

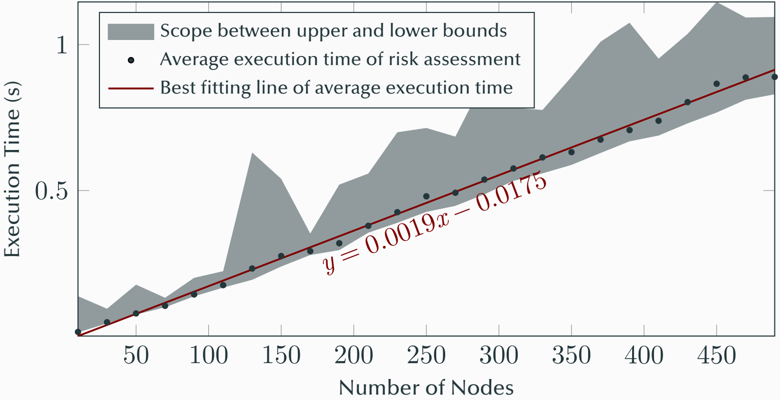


Simulation and Result Analysis

In the following figure, the fitting line

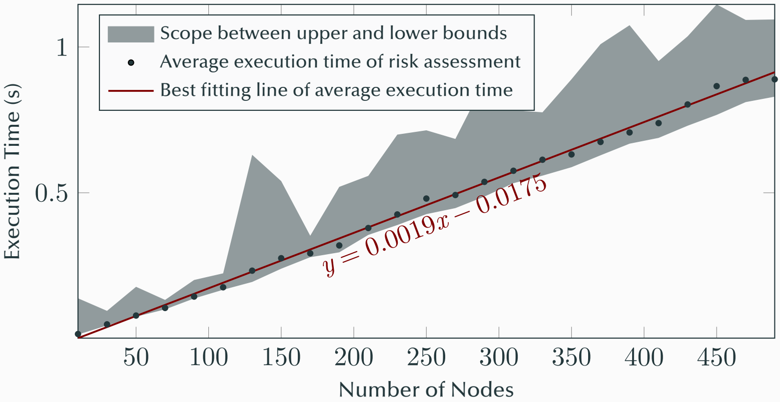
$$y = 0.0019x - 0.0175$$

matches well with the correlation coefficient $r = 0.9987$.



Simulation and Result Analysis

This means that the execution time of the risk assessment scales linearly with the increase of the node size of the multi-level Bayesian network.



Conclusion and Prospect

Conclusion

- By considering the characteristics of ICSs, a novel multi-level Bayesian network was proposed, which integrated a knowledge of attack, system function, and hazardous incident.

Conclusion

- By considering the characteristics of ICSs, a novel multi-level Bayesian network was proposed, which integrated a knowledge of attack, system function, and hazardous incident.
- The attack knowledge and system knowledge were combined to analyze the potential impact of attacks, so the proposed approach had the ability of assessing the risk caused by unknown attacks.

Conclusion

- By considering the characteristics of ICSs, a novel multi-level Bayesian network was proposed, which integrated a knowledge of attack, system function, and hazardous incident.
- The attack knowledge and system knowledge were combined to analyze the potential impact of attacks, so the proposed approach had the ability of assessing the risk caused by unknown attacks.
- A unified quantification approach for a variety of consequences of industrial accidents was introduced. Furthermore, the proposed approach could eliminate the error of risk caused by the overlapping amongst hazardous incidents.

Conclusion

- By considering the characteristics of ICSs, a novel multi-level Bayesian network was proposed, which integrated a knowledge of attack, system function, and hazardous incident.
- The attack knowledge and system knowledge were combined to analyze the potential impact of attacks, so the proposed approach had the ability of assessing the risk caused by unknown attacks.
- A unified quantification approach for a variety of consequences of industrial accidents was introduced. Furthermore, the proposed approach could eliminate the error of risk caused by the overlapping amongst hazardous incidents.
- By using a simplified chemical reactor control system in Matlab environment, the designed dynamic risk assessment approach was verified.

Prospect

There are some shortcomings of the proposed risk assessment approach need to be improved.

- **Current research work has no ability for self-learning.**

Prospect

There are some shortcomings of the proposed risk assessment approach need to be improved.

- **Current research work has no ability for self-learning.**
- **The sub-second computation time cannot meet some hard real-time systems requirements.**

Prospect

There are some shortcomings of the proposed risk assessment approach need to be improved.

- **Current research work has no ability for self-learning.**
- **The sub-second computation time cannot meet some hard real-time systems requirements.**

In the future, a dynamic cybersecurity risk assessment, which can automatically adjust the conditional probability and structure of the multi-level Bayesian network by analyzing the real-time data, will be researched, and several approximate inference methods will be attempted in the risk assessment.

Thank You!

Thank You!

You can obtain this slide from my Github:

zqmillet@github.com:Presentation.for.Loughborough.University

Thank You!

You can obtain this slide from my Github:

`zqmillet@github.com:Presentation.for.Loughborough.University`

And I have pushed the code of the simulation to my Github, too.

`zqmillet@github.com:Multi-level.Bayesian.Network`

Any Questions?