Monthly Report

Zhang Qi

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

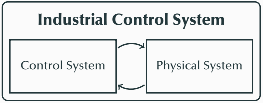
March 28, 2016

Outlines

Architecture of Risk Assessment

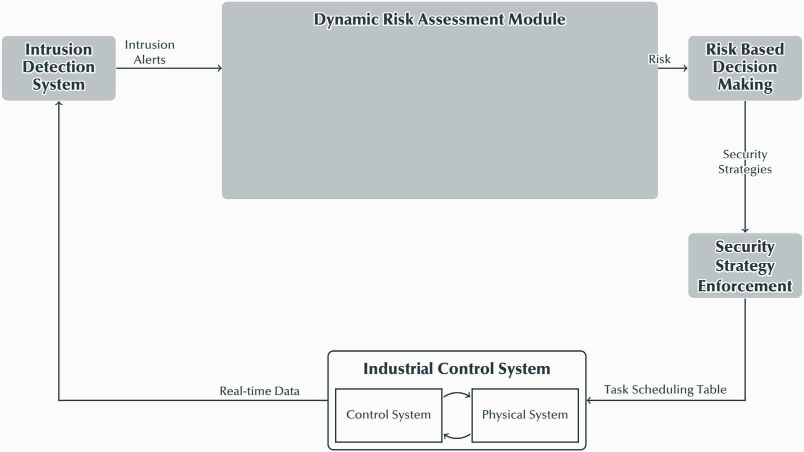
Architecture of Risk Assessment

The architecture of the dynamic risk assessment module is shown as following figure.



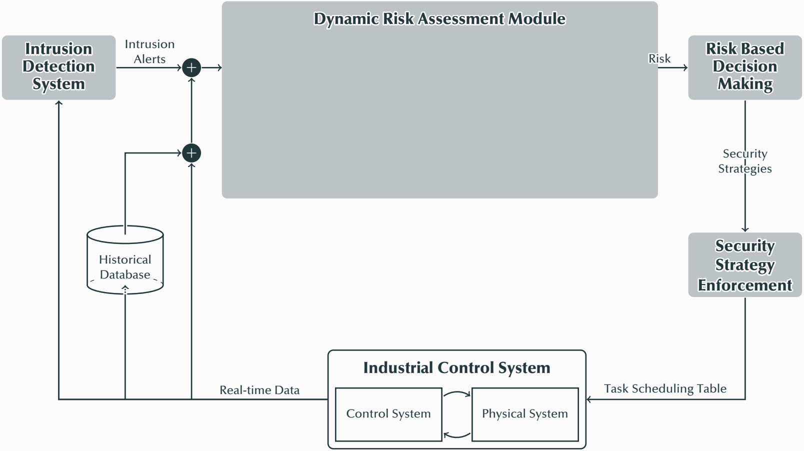
Architecture of Risk Assessment

The architecture of the dynamic risk assessment module is shown as following figure.



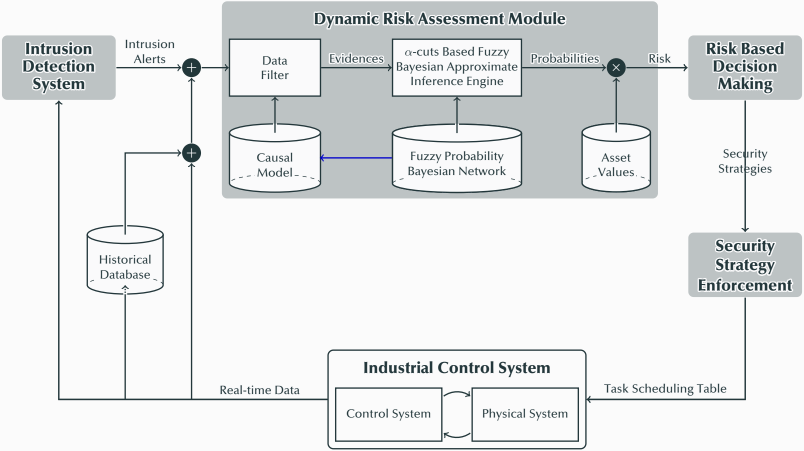
Architecture of Risk Assessment

The architecture of the dynamic risk assessment module is shown as following figure.



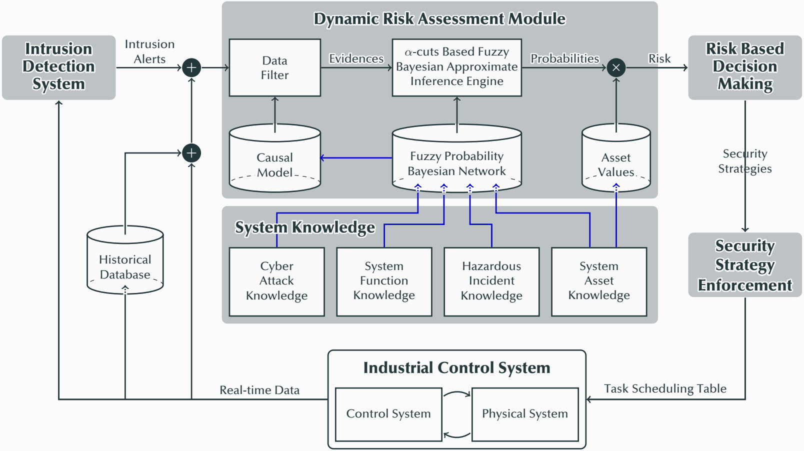
Architecture of Risk Assessment

The architecture of the dynamic risk assessment module is shown as following figure.



Architecture of Risk Assessment

The architecture of the dynamic risk assessment module is shown as following figure.



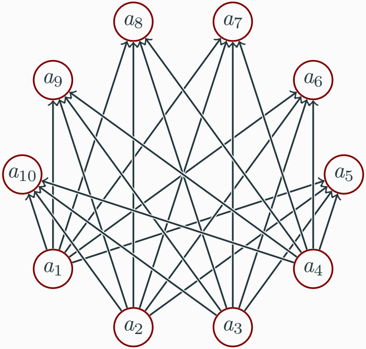
Modelling of Bayesian Network

Simplification of Bayesian Network

In this paper, the resource node is introduced to simplify the Bayesian network, the following figure shows two Bayesian network with/without resource node.

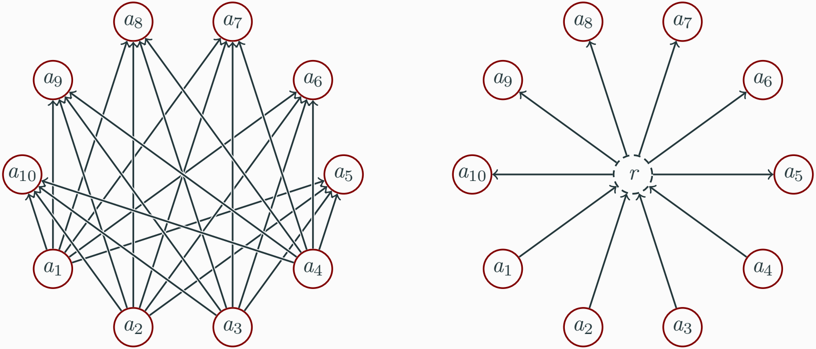
Simplification of Bayesian Network

In this paper, the resource node is introduced to simplify the Bayesian network, the following figure shows two Bayesian network with/without resource node.



Simplification of Bayesian Network

In this paper, the resource node is introduced to simplify the Bayesian network, the following figure shows two Bayesian network with/without resource node.



Estimation of Fuzzy Conditional Probabilities

In this paper, there are only two states of a node in the Bayesian network, which is shown as follows.

$$x = \begin{cases} F, & \text{the corresponding event of node } x \text{ does not happen,} \\ T, & \text{the corresponding event of node } x \text{ does happen.} \end{cases}$$

Estimation of Fuzzy Conditional Probabilities

In this paper, there are only two states of a node in the Bayesian network, which is shown as follows.

$$x = \begin{cases} F, & \text{the corresponding event of node } x \text{ does not happen,} \\ T, & \text{the corresponding event of node } x \text{ does happen.} \end{cases}$$

Assume that a node x has m parent nodes ${}^*x_1, {}^*x_2, \cdots, {}^*x_m$. There exists a conditional probability table of the node x, which is shown as follows.

${}^*x_1$	F	F	$\cdots$	T	T	T
${}^*x_2$	F	F	$\cdots$	T	T	T
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
${}^*x_{m-2}$	F	F	$\cdots$	T	T	T
${}^*x_{m-1}$	F	F	$\cdots$	F	T	T
${}^*x_m$	F	T	$\cdots$	T	F	T
x	p_1	p_2	$\cdots$	p_{2^m-2}	p_{2^m-1}	p_{2^m}

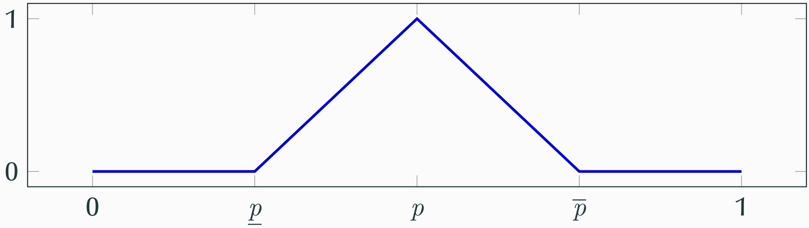
Estimation of Fuzzy Conditional Probabilities

Because the size of historical data of malicious attacks for ICSs is too small, the conditional probabilities from the statistical analysis of historical data is not always accurate. To solve this problem, in this paper, the fuzzy probability is used to replace the crisp probability which is hard to be obtained.

Estimation of Fuzzy Conditional Probabilities

Because the size of historical data of malicious attacks for ICSs is too small, the conditional probabilities from the statistical analysis of historical data is not always accurate. To solve this problem, in this paper, the fuzzy probability is used to replace the crisp probability which is hard to be obtained.

This fuzzy probability is denoted by $\widetilde{p} = (\underline{p}, p, \overline{p})$, where $0 \leq \underline{p} \leq p \leq \overline{p} \leq 1$. The following figure shows the fuzzy number $\widetilde{p}$.



Estimation of Fuzzy Conditional Probabilities

Two strategies to obtain the fuzzy conditional probabilities:

Estimation of Fuzzy Conditional Probabilities

Two strategies to obtain the fuzzy conditional probabilities:

- If the number of fuzzy conditional probabilities is not very large, the experts can estimate the fuzzy conditional probabilities case-by-case.

Estimation of Fuzzy Conditional Probabilities

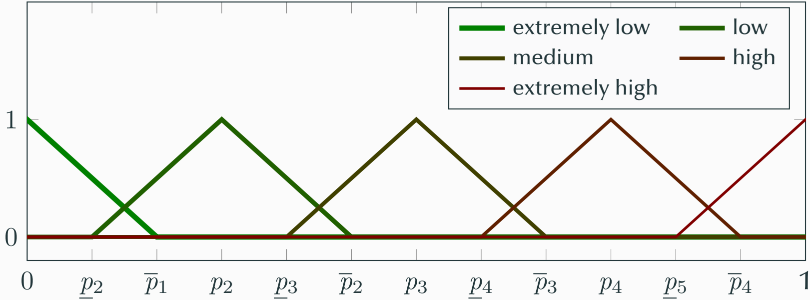
Two strategies to obtain the fuzzy conditional probabilities:

- If the number of fuzzy conditional probabilities is not very large, the experts can estimate the fuzzy conditional probabilities case-by-case.
- If there are a mount of fuzzy conditional probabilities to be estimated, a group of fuzzy probabilities are suggested to be established in advance.

Estimation of Fuzzy Conditional Probabilities

Two strategies to obtain the fuzzy conditional probabilities:

- If the number of fuzzy conditional probabilities is not very large, the experts can estimate the fuzzy conditional probabilities case-by-case.
- If there are a mount of fuzzy conditional probabilities to be estimated, a group of fuzzy probabilities are suggested to be established in advance.



Fuzzy Risk Assessment

α-cuts Based Fuzzy Bayesian Approximate Inference

Two problems in the inference of Bayesian network:

α-cuts Based Fuzzy Bayesian Approximate Inference

Two problems in the inference of Bayesian network:

- The operation of fuzzy probabilities would come up against a problem, where the result can produce a fuzzy probability not in the interval $[0, 1]$.

α-cuts Based Fuzzy Bayesian Approximate Inference

Two problems in the inference of Bayesian network:

- The operation of fuzzy probabilities would come up against a problem, where the result can produce a fuzzy probability not in the interval $[0, 1]$.
- Many algorithms have been developed for Bayesian inference, such as probability propagation in trees of clusters, variable elimination algorithm, junction tree algorithm. These exact inference algorithms are NP-hard.

α-cuts Based Fuzzy Bayesian Approximate Inference

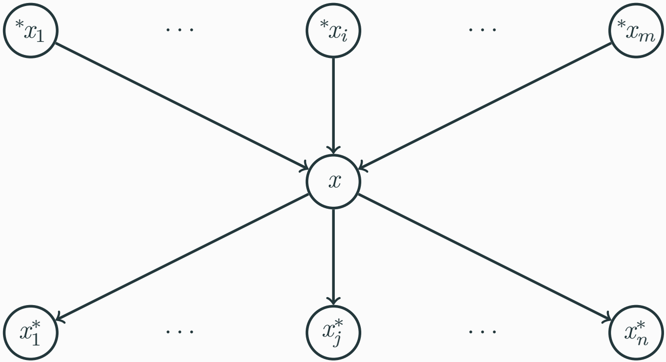
Two problems in the inference of Bayesian network:

- The operation of fuzzy probabilities would come up against a problem, where the result can produce a fuzzy probability not in the interval $[0, 1]$.
- Many algorithms have been developed for Bayesian inference, such as probability propagation in trees of clusters, variable elimination algorithm, junction tree algorithm. These exact inference algorithms are NP-hard.

To solve the aforementioned problems, a novel inference algorithm named **α-cuts Based Fuzzy Bayesian Approximate Inference** is proposed.

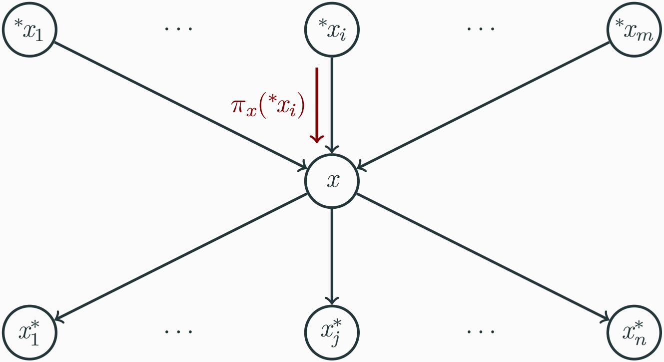
α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



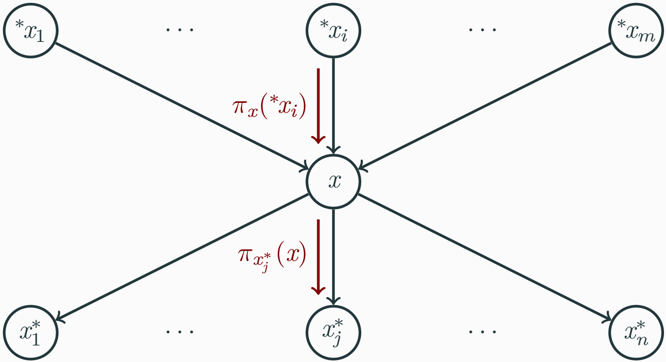
α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



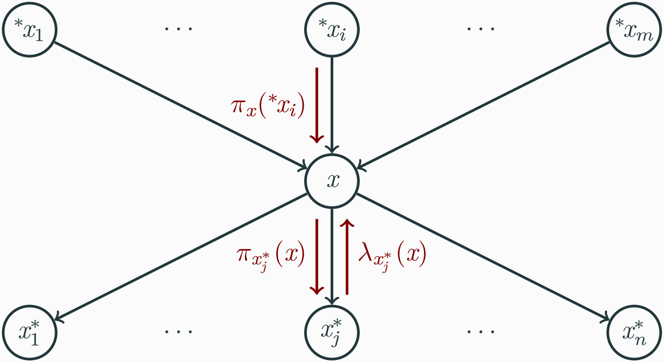
α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



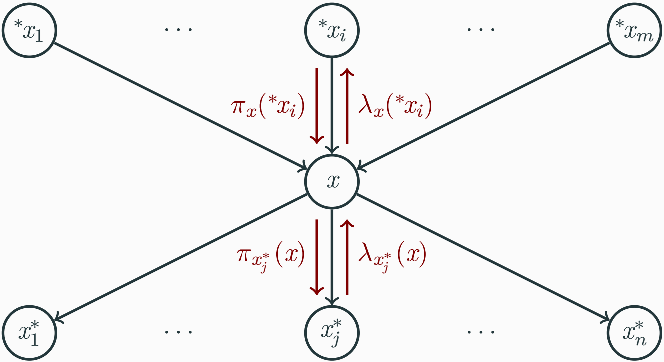
α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



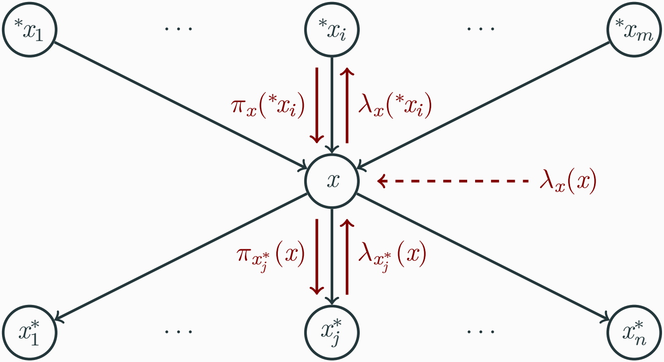
α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. The information spreading process is shown as following figure.



α-cuts Based Fuzzy Bayesian Approximate Inference

Assuming that node x is a node in Bayesian network $\mathscr{B}$. Its parent node set is ${}^*\boldsymbol{x} = \{{}^*x_1, {}^*x_2, \cdots, {}^*x_m\}$ and child node set is $\boldsymbol{x}^* = \{x_1^*, x_2^*, \cdots, x_n^*\}$. At the $(t+1)$th iteration, the message that x passes to its parent node ${}^*x_i$ is given by following equation.

$$\begin{bmatrix} \lambda_x^{(t+1)}({}^*x_i = F) \\ \lambda_x^{(t+1)}({}^*x_i = T) \end{bmatrix} = \beta \begin{bmatrix} \sum_x \lambda_x(x) \prod_j \lambda_{x_j^*}^{(t)}(x) \sum_{{}^*\boldsymbol{x}_i} p(x|{}^*\boldsymbol{x}_i, {}^*x_i = F) \prod_{k \neq i} \pi_x^{(t)}({}^*x_k) \\ \sum_x \lambda_x(x) \prod_j \lambda_{x_j^*}^{(t)}(x) \sum_{{}^*\boldsymbol{x}_i} p(x|{}^*\boldsymbol{x}_i, {}^*x_i = T) \prod_{k \neq i} \pi_x^{(t)}({}^*x_k) \end{bmatrix},$$

where ${}^*\boldsymbol{x}_i = {}^*\boldsymbol{x} \setminus \{{}^*x_i\}$. And the message that x sends to its child node x_j^* is given by following equation.

$$\begin{bmatrix} \pi_{x_j^*}^{(t+1)}(x = F) \\ \pi_{x_j^*}^{(t+1)}(x = T) \end{bmatrix} = \beta \begin{bmatrix} \lambda_x(x = F) \prod_{k \neq j} \lambda_{x_k^*}^{(t)}(x = F) \sum_{{}^*\boldsymbol{x}} p(x = F|{}^*\boldsymbol{x}) \prod_k \pi_x^{(t)}({}^*x_k) \\ \lambda_x(x = T) \prod_{k \neq j} \lambda_{x_k^*}^{(t)}(x = T) \sum_{{}^*\boldsymbol{x}} p(x = T|{}^*\boldsymbol{x}) \prod_k \pi_x^{(t)}({}^*x_k) \end{bmatrix}.$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The function $\lambda_x(\cdot)$ is the message that the node x sends to itself, which is presented as following equations.

$$\lambda_x(x = F) = \begin{cases} 0, & \text{when } x \in \boldsymbol{E}\text{, and the value of observed } x \text{ is } T\text{,} \\ 1, & \text{otherwise.} \end{cases}$$

$$\lambda_x(x = T) = \begin{cases} 0, & \text{when } x \in \boldsymbol{E}\text{, and the value of observed } x \text{ is } F\text{,} \\ 1, & \text{otherwise.} \end{cases}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

At the end of (t)th iteration, the fuzzy belief of node x is given by following equation.

$$\begin{bmatrix} \mathrm{Bel}^{(t)}(x = F) \\ \mathrm{Bel}^{(t)}(x = T) \end{bmatrix} = \beta \begin{bmatrix} \lambda^{(t)}(x = F) \cdot \pi^{(t)}(x = F) \\ \lambda^{(t)}(x = T) \cdot \pi^{(t)}(x = T) \end{bmatrix},$$

α-cuts Based Fuzzy Bayesian Approximate Inference

At the end of (t)th iteration, the fuzzy belief of node x is given by following equation.

$$\begin{bmatrix} \mathrm{Bel}^{(t)}(x=F) \\ \mathrm{Bel}^{(t)}(x=T) \end{bmatrix} = \beta \begin{bmatrix} \lambda^{(t)}(x=F)\cdot\pi^{(t)}(x=F) \\ \lambda^{(t)}(x=T)\cdot\pi^{(t)}(x=T) \end{bmatrix},$$

where

$$\begin{bmatrix} \lambda^{(t)}(x=F) \\ \lambda^{(t)}(x=T) \end{bmatrix} = \begin{bmatrix} \lambda_x(x=F)\prod_j \lambda^{(t)}_{x_j^*}(x=F) \\ \lambda_x(x=T)\prod_j \lambda^{(t)}_{x_j^*}(x=T) \end{bmatrix},$$

and

$$\begin{bmatrix} \pi^{(t)}(x=F) \\ \pi^{(t)}(x=T) \end{bmatrix} = \begin{bmatrix} \sum_{^*\boldsymbol{x}} P(x=F|^*\boldsymbol{x})\prod_k \pi^{(t)}_x(^*x_k) \\ \sum_{^*\boldsymbol{x}} P(x=T|^*\boldsymbol{x})\prod_k \pi^{(t)}_x(^*x_k) \end{bmatrix}.$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The iteration will be terminated when at least one of the conditions which are shown in following inequations are satisfied.

$$t \geq t_{\max},$$
$$\forall x \in \mathscr{B}, \;\; D\Big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\Big) \leq D_{\min},$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The iteration will be terminated when at least one of the conditions which are shown in following inequations are satisfied.

$$t \geq t_{\max},$$
$$\forall x \in \mathscr{B}, \quad D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big) \leq D_{\min},$$

where $D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big)$ represents the Hamming distance between two fuzzy numbers $\mathrm{Bel}^{(t)}(x = T)$ and $\mathrm{Bel}^{(t-1)}(x = T)$. The Hamming distance is defined as following equation.

$$D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big) = \int_0^1 \left|\mu^{(t)}(\rho) - \mu^{(t-1)}(\rho)\right| \mathrm{d}\rho.$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The iteration will be terminated when at least one of the conditions which are shown in following inequations are satisfied.

$$t \geq t_{\max},$$
$$\forall x \in \mathscr{B}, \quad D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big) \leq D_{\min},$$

where $D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big)$ represents the Hamming distance between two fuzzy numbers $\mathrm{Bel}^{(t)}(x = T)$ and $\mathrm{Bel}^{(t-1)}(x = T)$. The Hamming distance is defined as following equation.

$$D\big(\mathrm{Bel}^{(t)}(x = T), \mathrm{Bel}^{(t-1)}(x = T)\big) = \int_0^1 \left|\mu^{(t)}(\rho) - \mu^{(t-1)}(\rho)\right| \mathrm{d}\rho.$$

When the iteration is terminated, the $\mathrm{Bel}^{(t)}(x)$ is considered to be the approximate posterior fuzzy probability of node x under the evidence set $\boldsymbol{E}$.

$$\widetilde{p}(x = T|\boldsymbol{E}) \approx \mathrm{Bel}^{(t)}(x = T).$$

α-cuts Based Fuzzy Bayesian Approximate Inference

It is note that, there are only two kinds of operations of fuzzy probability in the inference of the fuzzy Bayesian network: addition and multiplication.

α-cuts Based Fuzzy Bayesian Approximate Inference

It is note that, there are only two kinds of operations of fuzzy probability in the inference of the fuzzy Bayesian network: addition and multiplication.

The fuzzy numbers are expressed by α-cutsfor calculation. For example, the triangular fuzzy probability $\widetilde{p} = (\underline{p}, p, \overline{p})$ is defined as following equation.

$$\mu(\rho) = \begin{cases} \dfrac{\rho - \underline{p}}{p - \underline{p}}, & \text{when } \underline{p} \leq \rho \leq p, \\ -\dfrac{\rho - \overline{p}}{\overline{p} - p}, & \text{when } p < \rho \leq \overline{p}, \\ 0, & \text{otherwise.} \end{cases}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

There are two expression of fuzzy probability:

$$\widetilde{p} = (\underline{p}, p, \overline{p}),$$

$$\widetilde{p} = \big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in [0, 1],$$

where

$$\ell(\alpha) = \alpha(p - \underline{p}) + \underline{p},$$

$$u(\alpha) = \overline{p} - \alpha(\overline{p} - p).$$

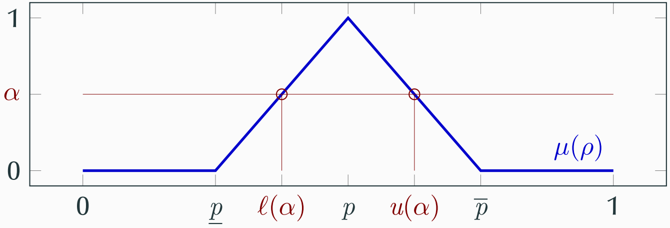
α-cuts Based Fuzzy Bayesian Approximate Inference

There are two expression of fuzzy probability:

$$\widetilde{p} = (\underline{p}, p, \overline{p}),$$
$$\widetilde{p} = \big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in [0, 1],$$

where
$$\ell(\alpha) = \alpha(p - \underline{p}) + \underline{p},$$
$$u(\alpha) = \overline{p} - \alpha(\overline{p} - p).$$

The relationship between two kinds of expressions are shown in the following figure.



α-cuts Based Fuzzy Bayesian Approximate Inference

The basic operations of addition and multiplication between fuzzy numbers used in LBP algorithm are given as following equations.

$$\begin{aligned}\widetilde{n}_1 + \widetilde{n}_2 &= \big[\ell_1(\alpha), u_1(\alpha)\big] + \big[\ell_2(\alpha), u_2(\alpha)\big] \\ &= \big[\ell_1(\alpha) + \ell_2(\alpha), u_1(\alpha) + u_2(\alpha)\big], \forall \alpha \in [0, 1],\end{aligned}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The basic operations of addition and multiplication between fuzzy numbers used in LBP algorithm are given as following equations.

$$\begin{aligned}
\widetilde{n}_1 + \widetilde{n}_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] + \left[\ell_2(\alpha), u_2(\alpha)\right] \\
&= \left[\ell_1(\alpha) + \ell_2(\alpha), u_1(\alpha) + u_2(\alpha)\right], \forall \alpha \in [0,1], \\
\widetilde{n}_1 \times \widetilde{n}_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] \times \left[\ell_2(\alpha), u_2(\alpha)\right] \\
&= \left[\ell_1(\alpha) \times \ell_2(\alpha), u_1(\alpha) \times u_2(\alpha)\right], \forall \alpha \in [0,1].
\end{aligned}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The basic operations of addition and multiplication between fuzzy numbers used in LBP algorithm are given as following equations.

$$\begin{aligned}
\widetilde{n}_1 + \widetilde{n}_2 &= \big[\ell_1(\alpha), u_1(\alpha)\big] + \big[\ell_2(\alpha), u_2(\alpha)\big] \\
&= \big[\ell_1(\alpha) + \ell_2(\alpha), u_1(\alpha) + u_2(\alpha)\big], \forall \alpha \in [0, 1], \\
\widetilde{n}_1 \times \widetilde{n}_2 &= \big[\ell_1(\alpha), u_1(\alpha)\big] \times \big[\ell_2(\alpha), u_2(\alpha)\big] \\
&= \big[\ell_1(\alpha) \times \ell_2(\alpha), u_1(\alpha) \times u_2(\alpha)\big], \forall \alpha \in [0, 1].
\end{aligned}$$

It is noted that, a crisp number can be regarded as a special fuzzy number whose membership function is a unit-impulse function. Therefore, the operations between fuzzy number and crisp number are shown as following equations.

$$\begin{aligned}
\widetilde{n}_1 + n_2 &= \big[\ell_1(\alpha), u_1(\alpha)\big] + n_2 \\
&= \big[\ell_1(\alpha) + n_2, u_1(\alpha) + n_2\big], \forall \alpha \in [0, 1],
\end{aligned}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

The basic operations of addition and multiplication between fuzzy numbers used in LBP algorithm are given as following equations.

$$\begin{aligned}
\widetilde{n}_1 + \widetilde{n}_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] + \left[\ell_2(\alpha), u_2(\alpha)\right] \\
&= \left[\ell_1(\alpha) + \ell_2(\alpha), u_1(\alpha) + u_2(\alpha)\right], \forall \alpha \in [0, 1], \\
\widetilde{n}_1 \times \widetilde{n}_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] \times \left[\ell_2(\alpha), u_2(\alpha)\right] \\
&= \left[\ell_1(\alpha) \times \ell_2(\alpha), u_1(\alpha) \times u_2(\alpha)\right], \forall \alpha \in [0, 1].
\end{aligned}$$

It is noted that, a crisp number can be regarded as a special fuzzy number whose membership function is a unit-impulse function. Therefore, the operations between fuzzy number and crisp number are shown as following equations.

$$\begin{aligned}
\widetilde{n}_1 + n_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] + n_2 \\
&= \left[\ell_1(\alpha) + n_2, u_1(\alpha) + n_2\right], \forall \alpha \in [0, 1], \\
\widetilde{n}_1 \times n_2 &= \left[\ell_1(\alpha), u_1(\alpha)\right] \times n_2 \\
&= \left[\ell_1(\alpha) \times n_2, u_1(\alpha) \times n_2\right], \forall \alpha \in [0, 1].
\end{aligned}$$

α-cuts Based Fuzzy Bayesian Approximate Inference

In this paper, the normalization algorithm developed by Dubois and Prade[1] are employed to normalize the fuzzy numbers. Assuming $\widetilde{n}_1$ and $\widetilde{n}_2$ are two fuzzy numbers, the normalization algorithm is shown as the following equation.

$$\beta \begin{bmatrix} \widetilde{n}_1 \\ \widetilde{n}_2 \end{bmatrix} = \begin{bmatrix} \left[\frac{\ell_1(\alpha)}{\ell_1(\alpha) + u_2(\alpha)}, \frac{u_1(\alpha)}{u_1(\alpha) + \ell_2(\alpha)} \right], \forall \alpha \in [0, 1] \\ \left[\frac{\ell_2(\alpha)}{\ell_2(\alpha) + u_1(\alpha)}, \frac{u_2(\alpha)}{u_2(\alpha) + \ell_1(\alpha)} \right], \forall \alpha \in [0, 1] \end{bmatrix}.$$

[1] Didier Dubois and Henri Prade. The use of fuzzy numbers in decision analysis. *Fuzzy information and decision processes*, pages 309–321, 1982.

α-cuts Based Fuzzy Bayesian Approximate Inference

In the process of Bayesian inference, it is hard to calculate the analytical expression of the iterating results.

α-cuts Based Fuzzy Bayesian Approximate Inference

In the process of Bayesian inference, it is hard to calculate the analytical expression of the iterating results.

To solve this problem that is hard to obtain the analytical expression, a compromised computation strategy is proposed. This computation strategy adopts finite interval values to represent a fuzzy number approximately.

α-cuts Based Fuzzy Bayesian Approximate Inference

In the process of Bayesian inference, it is hard to calculate the analytical expression of the iterating results.

To solve this problem that is hard to obtain the analytical expression, a compromised computation strategy is proposed. This computation strategy adopts finite interval values to represent a fuzzy number approximately.

There is a set of $\alpha \in [0, 1]$ which is denoted by $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, $\forall i, j = 1, 2, \cdots, n$, if $i \neq j$, then $\alpha_i \neq \alpha_j$.

α-cuts Based Fuzzy Bayesian Approximate Inference

In the process of Bayesian inference, it is hard to calculate the analytical expression of the iterating results.

To solve this problem that is hard to obtain the analytical expression, a compromised computation strategy is proposed. This computation strategy adopts finite interval values to represent a fuzzy number approximately.

There is a set of $\alpha \in [0,1]$ which is denoted by $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, $\forall i, j = 1, 2, \cdots, n$, if $i \neq j$, then $\alpha_i \neq \alpha_j$. In this paper, for a fuzzy number $\big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in [0,1]$, the proposed computation strategy is to calculate the finite interval values $\big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in \boldsymbol{\alpha}$.

α-cuts Based Fuzzy Bayesian Approximate Inference

In the process of Bayesian inference, it is hard to calculate the analytical expression of the iterating results.

To solve this problem that is hard to obtain the analytical expression, a compromised computation strategy is proposed. This computation strategy adopts finite interval values to represent a fuzzy number approximately.

There is a set of $\alpha \in [0,1]$ which is denoted by $\boldsymbol{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, $\forall i, j = 1, 2, \cdots, n$, if $i \neq j$, then $\alpha_i \neq \alpha_j$. In this paper, for a fuzzy number $\big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in [0,1]$, the proposed computation strategy is to calculate the finite interval values $\big[\ell(\alpha), u(\alpha)\big], \forall \alpha \in \boldsymbol{\alpha}$. In this paper, the set of α which is shown in the following equation is suggested.

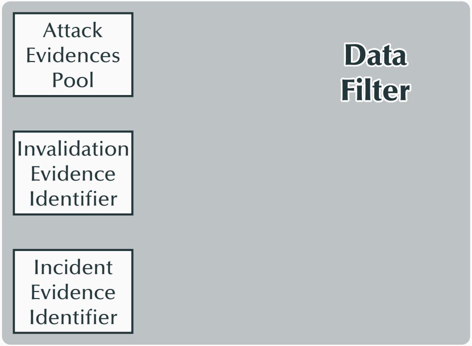
$$\boldsymbol{\alpha} = \left\{ \alpha_i \middle| \alpha_i = \frac{i-1}{n-1}, i = 1, 2, \cdots, n \right\}.$$

Data Filter

The architecture of the data filter is shown in the following figure.

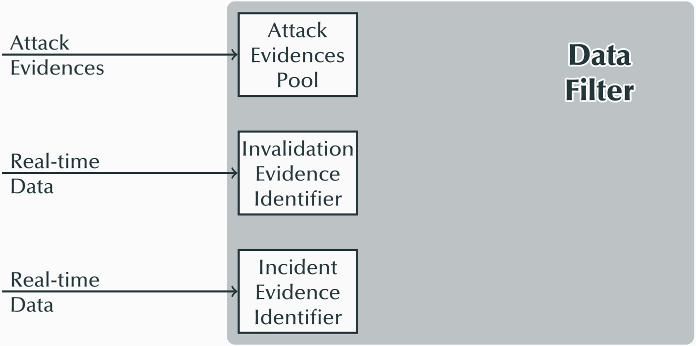
Data Filter

The architecture of the data filter is shown in the following figure.



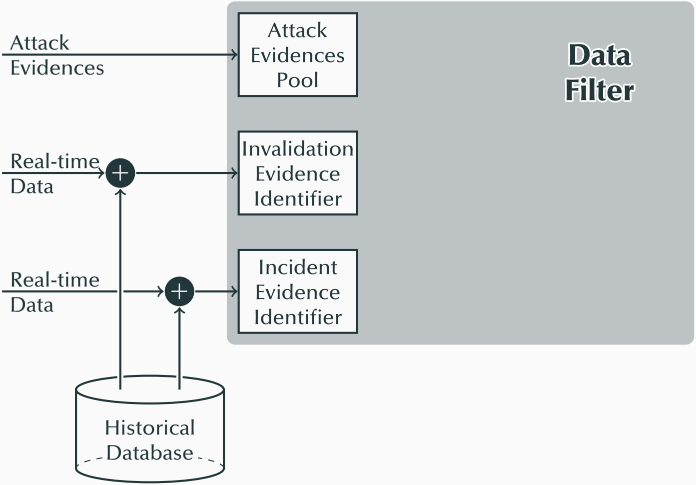
Data Filter

The architecture of the data filter is shown in the following figure.



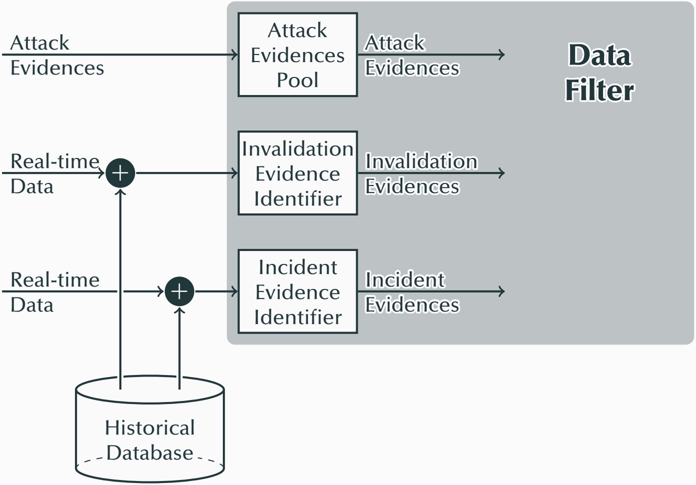
Data Filter

The architecture of the data filter is shown in the following figure.



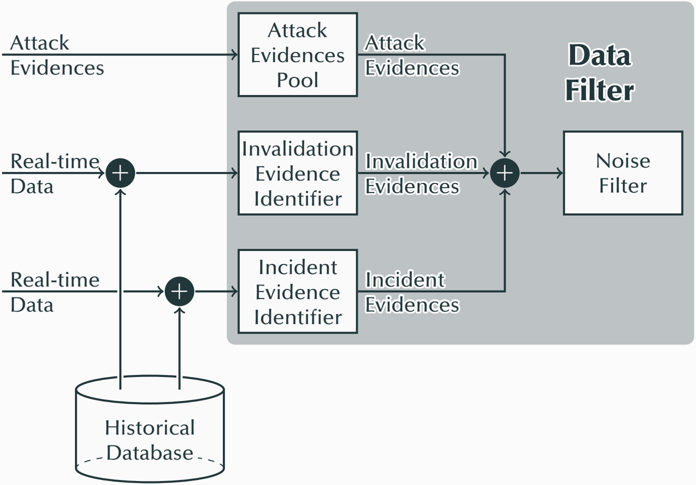
Data Filter

The architecture of the data filter is shown in the following figure.



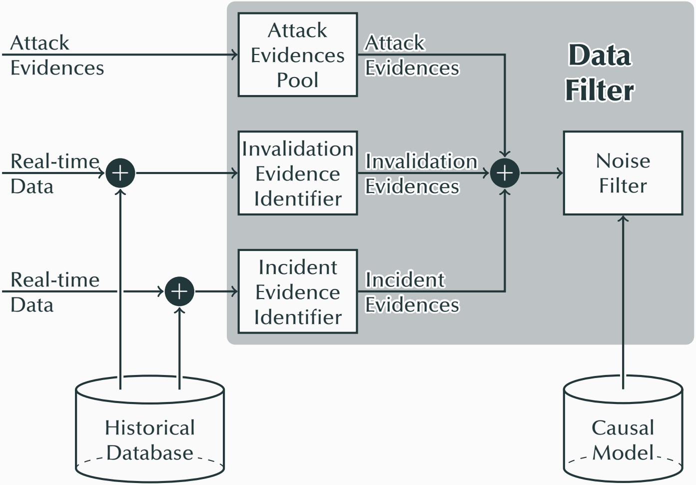
Data Filter

The architecture of the data filter is shown in the following figure.



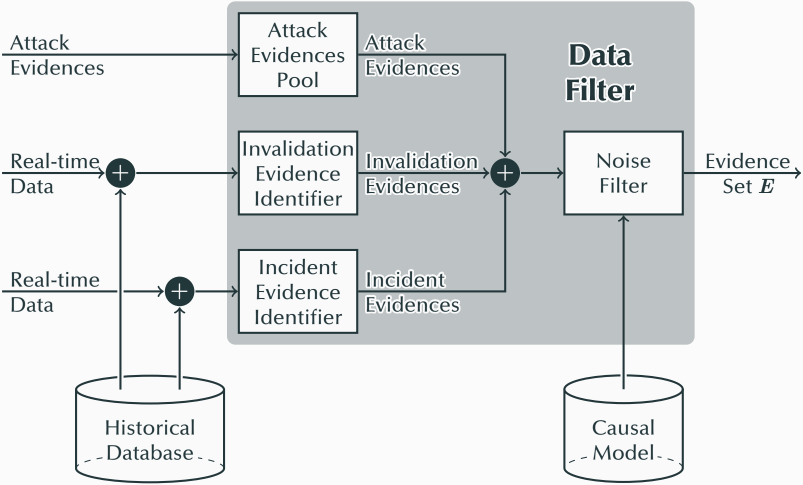
Data Filter

The architecture of the data filter is shown in the following figure.



Data Filter

The architecture of the data filter is shown in the following figure.



Data Filter

In this paper, for the invalidation evidences and the incident evidences, an index $C(x = T)$ is proposed to measure the confidence level of an evidence $x = T$, which is shown as the following equation.

$$C(x = T) = \max_{\boldsymbol{p} \in \boldsymbol{P}} \left\{ \sum_{i=m}^{n} \binom{i}{n} \eta^i (1-\eta)^{n-i} \right\},$$

Data Filter

In this paper, for the invalidation evidences and the incident evidences, an index $C(x = T)$ is proposed to measure the confidence level of an evidence $x = T$, which is shown as the following equation.

$$C(x = T) = \max_{\boldsymbol{p} \in \boldsymbol{P}} \left\{ \sum_{i=m}^{n} \binom{i}{n} \eta^i (1 - \eta)^{n-i} \right\},$$

where $\boldsymbol{P}$ is the path set of node x, n is the number of elements in path $\boldsymbol{p}$, m is the number of elements in the set $\boldsymbol{p} \setminus \boldsymbol{E}$, η is the false negatives rate of IDS.

Data Filter

In this paper, for the invalidation evidences and the incident evidences, an index $C(x = T)$ is proposed to measure the confidence level of an evidence $x = T$, which is shown as the following equation.

$$C(x = T) = \max_{\boldsymbol{p} \in \boldsymbol{P}} \left\{ \sum_{i=m}^{n} \binom{i}{n} \eta^i (1 - \eta)^{n-i} \right\},$$

where $\boldsymbol{P}$ is the path set of node x, n is the number of elements in path $\boldsymbol{p}$, m is the number of elements in the set $\boldsymbol{p} \setminus \boldsymbol{E}$, η is the false negatives rate of IDS. If the condition which is shown in the following equation is satisfied, the evidence $x = T$ is regarded as noise evidence caused by system faults.

$$C(x = T) < C_{\min},$$

Data Filter

In this paper, for the invalidation evidences and the incident evidences, an index $C(x = T)$ is proposed to measure the confidence level of an evidence $x = T$, which is shown as the following equation.

$$C(x = T) = \max_{\boldsymbol{p} \in \boldsymbol{P}} \left\{ \sum_{i=m}^{n} \binom{i}{n} \eta^i (1-\eta)^{n-i} \right\},$$

where $\boldsymbol{P}$ is the path set of node x, n is the number of elements in path $\boldsymbol{p}$, m is the number of elements in the set $\boldsymbol{p} \setminus \boldsymbol{E}$, η is the false negatives rate of IDS. If the condition which is shown in the following equation is satisfied, the evidence $x = T$ is regarded as noise evidence caused by system faults.

$$C(x = T) < C_{\min},$$

where $C_{\min}$ is the minimum value of evidence confidence level, and $C_{\min}$ can be equal to 2.5%, 5%, etc.

Data Filter

If a function node f has only one path $\boldsymbol{p} = \{a_1, a_2, \cdots, a_{10}\}$. Now, there are only a_1, a_2, and a_3 are detected by IDS, and the invalidation of this function is detected by invalidation evidence identifier. The false negatives rate of IDS $\eta = 2.5\%$ and the minimum evidence confidence level $C_{\min} = 1\%$.

Data Filter

If a function node f has only one path $\boldsymbol{p} = \{a_1, a_2, \cdots, a_{10}\}$. Now, there are only a_1, a_2, and a_3 are detected by IDS, and the invalidation of this function is detected by invalidation evidence identifier. The false negatives rate of IDS $\eta = 2.5\%$ and the minimum evidence confidence level $C_{\min} = 1\%$. So, the false negatives number m obeys the binomial distribution $B(10, 0.025)$.

Data Filter

If a function node f has only one path $\boldsymbol{p} = \{a_1, a_2, \cdots, a_{10}\}$. Now, there are only a_1, a_2, and a_3 are detected by IDS, and the invalidation of this function is detected by invalidation evidence identifier. The false negatives rate of IDS $\eta = 2.5\%$ and the minimum evidence confidence level $C_{\min} = 1\%$. So, the false negatives number m obeys the binomial distribution $B(10, 0.025)$. The confidence level of evidence $f = T$ is shown as the following equation.

$$
\begin{aligned}
C(f = T) &= \sum_{i=7}^{10} \binom{i}{10} 0.025^i (1 - 0.025)^{10-i} \\
&= 6.8542 \cdot 10^{-10}.
\end{aligned}
$$

Data Filter

If a function node f has only one path $\boldsymbol{p} = \{a_1, a_2, \cdots, a_{10}\}$. Now, there are only a_1, a_2, and a_3 are detected by IDS, and the invalidation of this function is detected by invalidation evidence identifier. The false negatives rate of IDS $\eta = 2.5\%$ and the minimum evidence confidence level $C_{\min} = 1\%$. So, the false negatives number m obeys the binomial distribution $B(10, 0.025)$. The confidence level of evidence $f = T$ is shown as the following equation.

$$\begin{aligned} C(f = T) &= \sum_{i=7}^{10} \binom{i}{10} 0.025^i (1 - 0.025)^{10-i} \\ &= 6.8542 \cdot 10^{-10}. \end{aligned}$$

Because $C(f = T) = 6.8542 \cdot 10^{-10} < C_{\min}$, the evidence $f = T$ is a noise evidence.

Risk Assessment

The evidences generated by attack evidence pool, invalidation evidence identifier, and incident evidence identifier, are sent to the noise filter.

Risk Assessment

The evidences generated by attack evidence pool, invalidation evidence identifier, and incident evidence identifier, are sent to the noise filter. The α-cuts based fuzzy Bayesian approximate inference engine receives the evidences without noise caused by system faults, then calculates the fuzzy probabilities of all asset nodes $\widetilde{p}(z)$.

Risk Assessment

The evidences generated by attack evidence pool, invalidation evidence identifier, and incident evidence identifier, are sent to the noise filter. The α-cuts based fuzzy Bayesian approximate inference engine receives the evidences without noise caused by system faults, then calculates the fuzzy probabilities of all asset nodes $\widetilde{p}(z)$. At last, the current cybersecurity risk can be assessed by the following equation.

$$\widetilde{\mathscr{R}} = \sum_{z \in \mathscr{B}} \widetilde{p}(z) \cdot v(z),$$

Risk Assessment

The evidences generated by attack evidence pool, invalidation evidence identifier, and incident evidence identifier, are sent to the noise filter. The α-cuts based fuzzy Bayesian approximate inference engine receives the evidences without noise caused by system faults, then calculates the fuzzy probabilities of all asset nodes $\widetilde{p}(z)$. At last, the current cybersecurity risk can be assessed by the following equation.

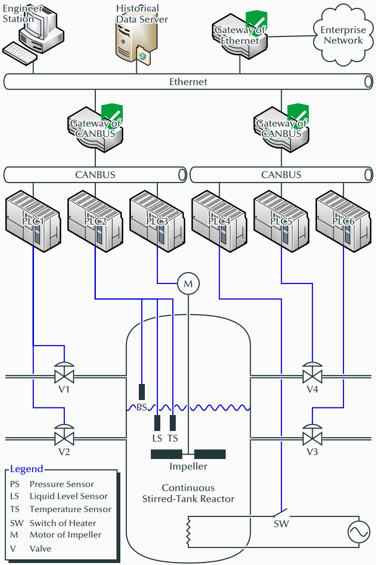
$$\widetilde{\mathscr{R}} = \sum_{z \in \mathscr{B}} \widetilde{p}(z) \cdot v(z),$$

where $v(z)$ is the value of the asset z.

Performance Analysis

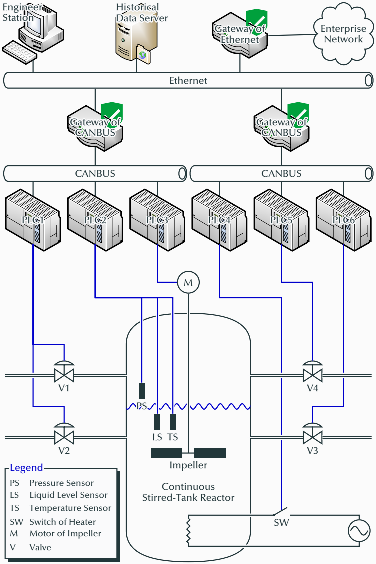
Performance Analysis

There are several cybersecurity vulnerabilities in the control system.



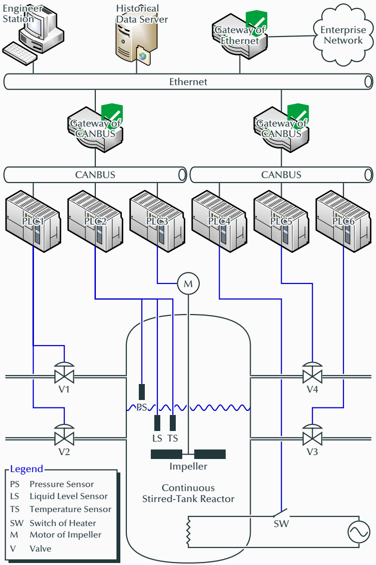
Performance Analysis

There are several cybersecurity vulnerabilities in the control system. The HDS has three vulnerabilities which may be utilized by attackers: the buffer overflow vulnerability (CVE-2007-4060), the FTP-bounce vulnerability (CVE-1999-0017), and the improper restriction of excessive authentication attempts (CVE-2015-6029).



Performance Analysis

There are several cybersecurity vulnerabilities in the control system. The HDS has three vulnerabilities which may be utilized by attackers: the buffer overflow vulnerability (CVE-2007-4060), the FTP-bounce vulnerability (CVE-1999-0017), and the improper restriction of excessive authentication attempts (CVE-2015-6029). The ES has two vulnerabilities: the buffer overflow vulnerability (CVE-2007-4060), and an authentication vulnerability.



Performance Analysis

In this paper, the α-cuts based fuzzy Bayesian approximate inference engine is implemented with C++ language, and the build environment is Microsoft Visual Studio 2015.

Performance Analysis

In this paper, the α-cuts based fuzzy Bayesian approximate inference engine is implemented with C++ language, and the build environment is Microsoft Visual Studio 2015.

To demonstrate the ability to adjust the risk value in real-time with the launching of multi-step attacks, in the first simulation, an imaginary attack scenario is proposed.

Performance Analysis

In this paper, the α-cuts based fuzzy Bayesian approximate inference engine is implemented with C++ language, and the build environment is Microsoft Visual Studio 2015.

To demonstrate the ability to adjust the risk value in real-time with the launching of multi-step attacks, in the first simulation, an imaginary attack scenario is proposed. From the 49th minute to the 81st minute, the attacker scans the network of the Ethernet;

Performance Analysis

In this paper, the α-cuts based fuzzy Bayesian approximate inference engine is implemented with C++ language, and the build environment is Microsoft Visual Studio 2015.

To demonstrate the ability to adjust the risk value in real-time with the launching of multi-step attacks, in the first simulation, an imaginary attack scenario is proposed. From the 49th minute to the 81st minute, the attacker scans the network of the Ethernet; from the 90th minute to the 142nd minute, the attacker scans the vulnerabilities of the devices in the Ethernet;

Performance Analysis

In this paper, the α-cuts based fuzzy Bayesian approximate inference engine is implemented with C++ language, and the build environment is Microsoft Visual Studio 2015.

To demonstrate the ability to adjust the risk value in real-time with the launching of multi-step attacks, in the first simulation, an imaginary attack scenario is proposed. From the 49th minute to the 81st minute, the attacker scans the network of the Ethernet; from the 90th minute to the 142nd minute, the attacker scans the vulnerabilities of the devices in the Ethernet; from the 163rd minute to the 204th minute, the attacker launches the DoS attack to the HDS.

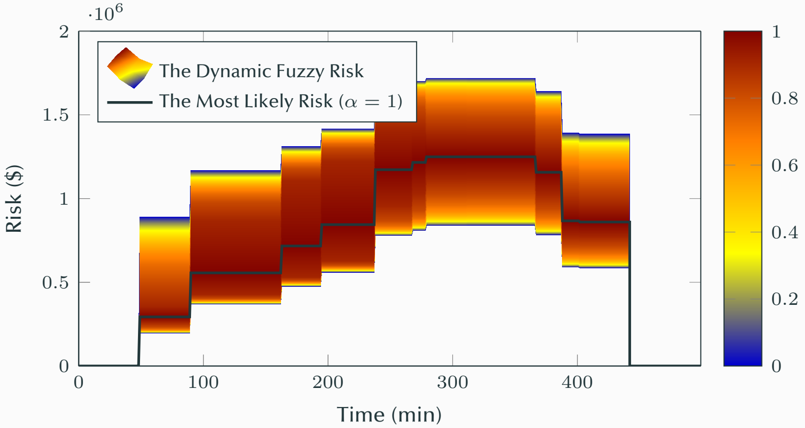
Performance Analysis

The evidence list are shown in the following table.

Start Time	End Time	Evidence Decription
49	81	attacker launches network scanning attack a_1
90	142	attacker launches vulnerability scanning attack a_2
163	204	attacker launches DoS attack a_6 on HDS
195	205	attacker launches spoofing attack a_8 on ES
238	260	attacker reconfiguration of PLC6
268	367	traffic control function f_3 of V3 is failed
279	388	temperature control function f_{11} is failed
312	402	incident temperature anomaly e_3 occurs

Performance Analysis

The following figure shows the curve of dynamic cybersecurity risk from 1st minute to 498th minute.



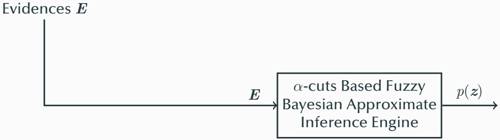
Performance Analysis

To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.

The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list,

Performance Analysis

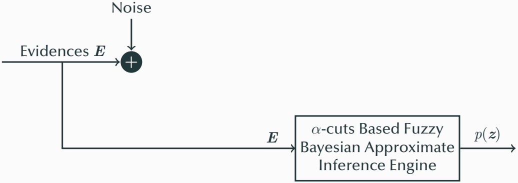
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list,

Performance Analysis

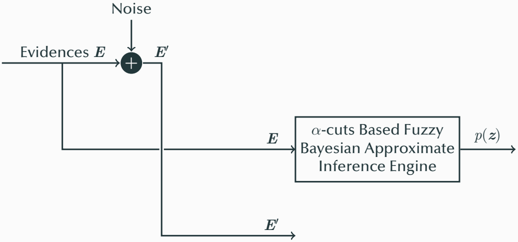
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list,

Performance Analysis

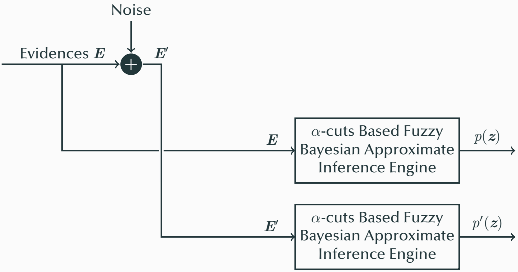
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise,

Performance Analysis

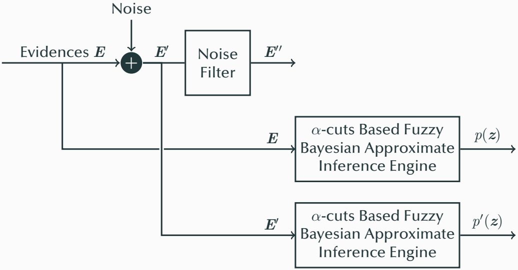
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise,

Performance Analysis

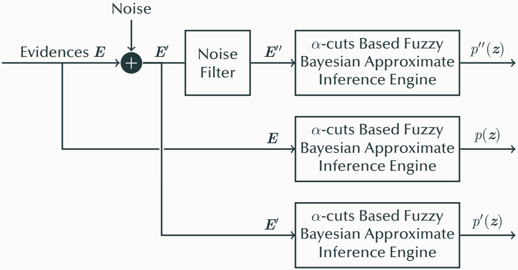
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

Performance Analysis

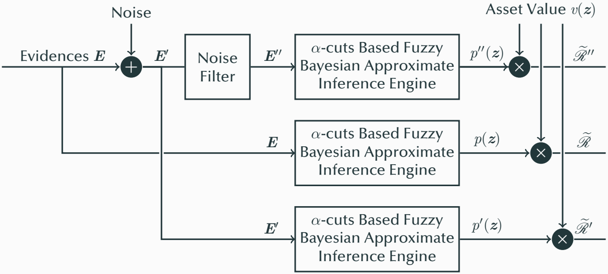
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

Performance Analysis

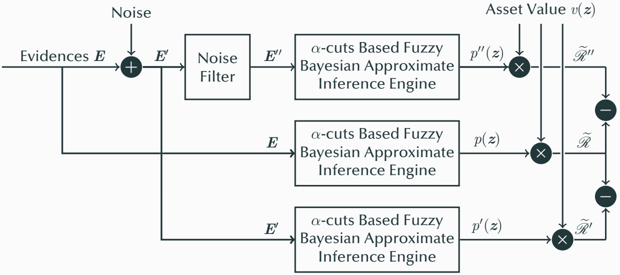
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

Performance Analysis

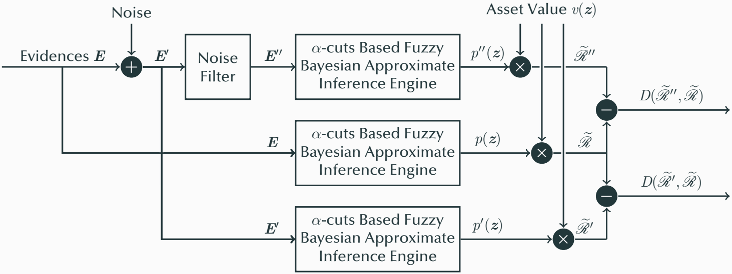
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

Performance Analysis

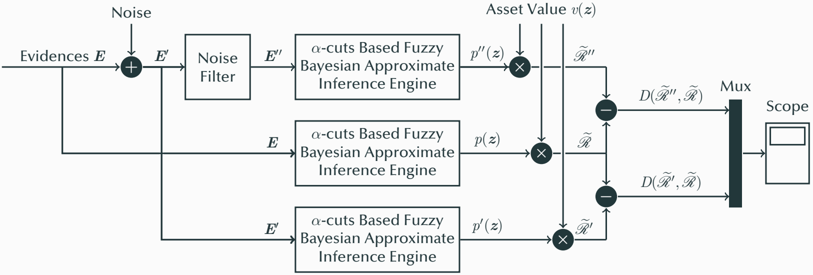
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

Performance Analysis

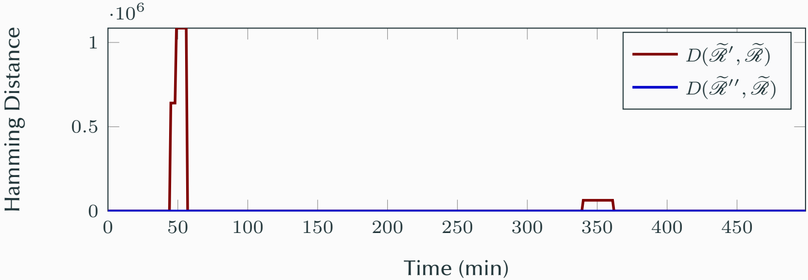
To verify the efficiency of noise reduction, a contrast simulation is designed. The following figure shows the program of the contrast simulation.



The symbol $\boldsymbol{E}$ is the evidence sequence which is shown in the evidence list, the symbol $\boldsymbol{E}'$ is the evidence sequence $\boldsymbol{E}$ which is added noise, and the symbol $\boldsymbol{E}''$ is the evidence sequence which is filtered by the noise filter.

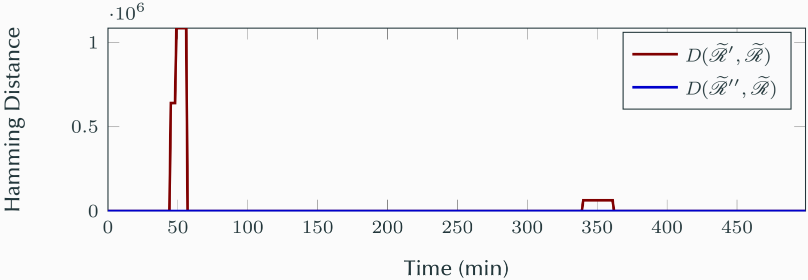
Performance Analysis

The following figure shows that the curve of the Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ has two disturbances from 45th minute to 56th minute and from 340th minute to 361st minute.



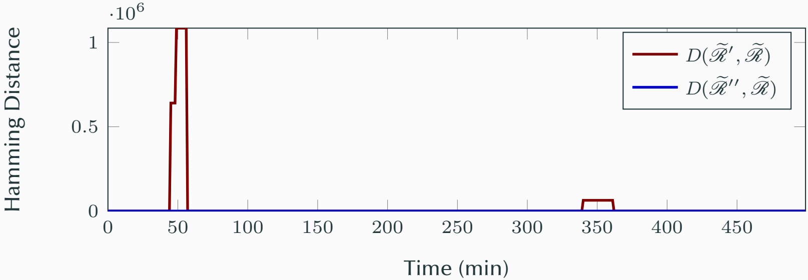
Performance Analysis

The following figure shows that the curve of the Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ has two disturbances from 45th minute to 56th minute and from 340th minute to 361st minute. The maximum distance between $\widetilde{\mathscr{R}}'$ and $\widetilde{\mathscr{R}}$ is $1.08488 \cdot 10^6$.



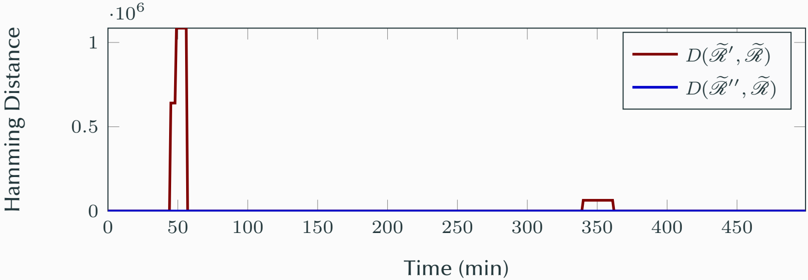
Performance Analysis

The following figure shows that the curve of the Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ has two disturbances from 45th minute to 56th minute and from 340th minute to 361st minute. The maximum distance between $\widetilde{\mathscr{R}}'$ and $\widetilde{\mathscr{R}}$ is $1.08488 \cdot 10^6$. It indicates that without the noise filter, the value of dynamic cybersecurity risk will be disturbed by the noise from system faults.



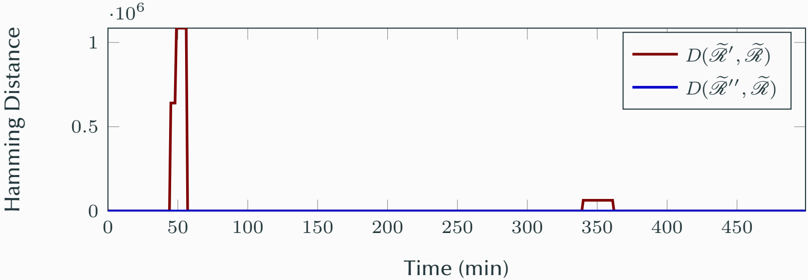
Performance Analysis

The following figure shows that the curve of the Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ has two disturbances from 45th minute to 56th minute and from 340th minute to 361st minute. The maximum distance between $\widetilde{\mathscr{R}}'$ and $\widetilde{\mathscr{R}}$ is $1.08488 \cdot 10^6$. It indicates that without the noise filter, the value of dynamic cybersecurity risk will be disturbed by the noise from system faults. The curve of Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ is always equal to 0.



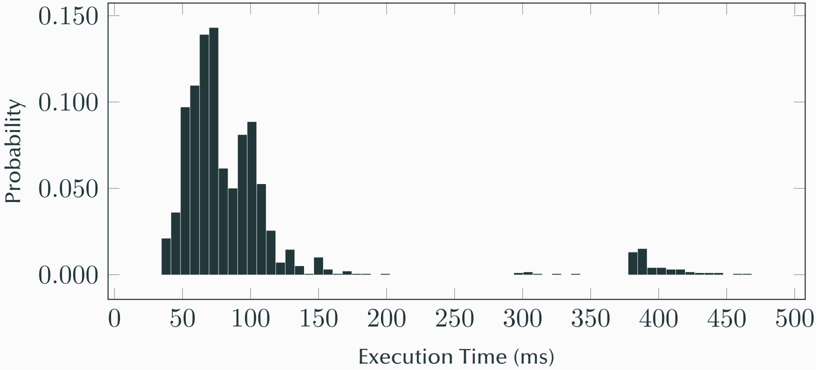
Performance Analysis

The following figure shows that the curve of the Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ has two disturbances from 45th minute to 56th minute and from 340th minute to 361st minute. The maximum distance between $\widetilde{\mathscr{R}}'$ and $\widetilde{\mathscr{R}}$ is $1.08488 \cdot 10^6$. It indicates that without the noise filter, the value of dynamic cybersecurity risk will be disturbed by the noise from system faults. The curve of Hamming distance $D(\widetilde{\mathscr{R}}', \widetilde{\mathscr{R}})$ is always equal to 0. This contrast simulation shows that with the noise filter, the noise from system faults can be reduced, largely.



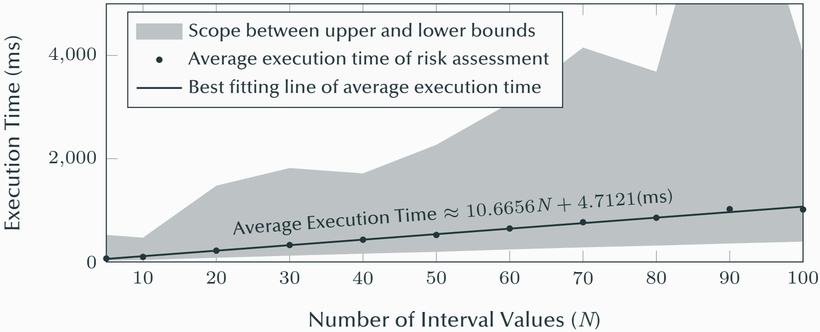
Performance Analysis

To demonstrate the execution time of our approach, another simulation is designed. In the second simulation, the set $\boldsymbol{\alpha}$'s size $n = 10$, the maximum number of iterations $t_{\max} = 100$, the accuracy $D_{\min} = 1 \times 10^{-4}$, the inference process is repeated 5,000 times. The distribution curve of the execution time is shown in the following figure.



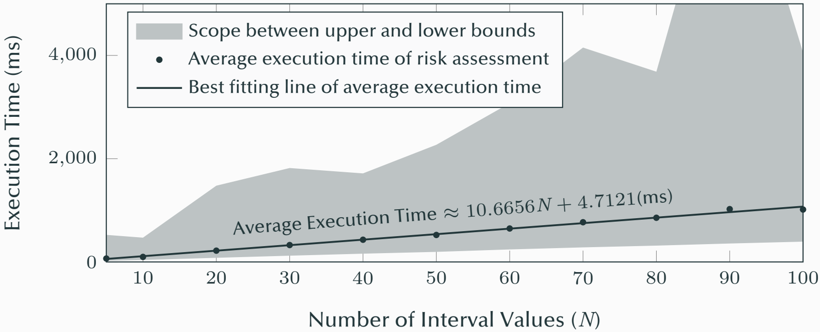
Performance Analysis

To show the possible upper/lower bounds and the scalability of our approach, the fourth simulation is implemented.



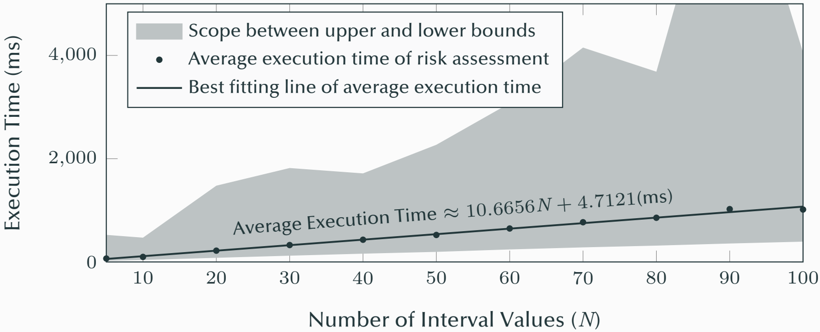
Performance Analysis

To show the possible upper/lower bounds and the scalability of our approach, the fourth simulation is implemented. In this simulation, for each number of interval values $N \in \{5, 10, 20, 30, \cdots, 100\}$, the Bayesian network is inferred 5,000 times with stochastic evidence set.



Performance Analysis

To show the possible upper/lower bounds and the scalability of our approach, the fourth simulation is implemented. In this simulation, for each number of interval values $N \in \{5, 10, 20, 30, \cdots, 100\}$, the Bayesian network is inferred 5,000 times with stochastic evidence set. All the execution times are recorded, and the following figure shows the possible upper/lower bounds and the scalability of the proposed risk assessment approach.



Thanks to Li Xuan & Chu Zhongtao.

Task Planning

Task Planning

- Finish the simulation of 2^{nd} paper.
- Finish the outline of 4^{th} paper.