

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

Zhang Qi

qiqi@hust.edu.cn

October 8, 2015



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

Outlines

Introduction

Architecture

Hazardous Incident Prediction

- The Bayesian Network Based Knowledge Modeling

- Incident Prediction

Dynamic Risk Assessment

- Classification of Incident Consequences

- Quantification of Incident Consequences

- Calculation of Dynamic Risk

Simulation

- Knowledge Modeling and Simulation Platform

- Simulation and Result Analysis

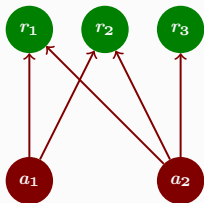
Hazardous Incident Prediction

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



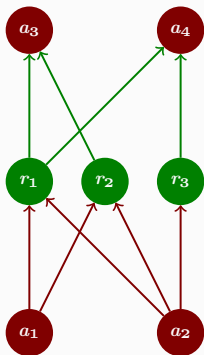
Attack Level

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



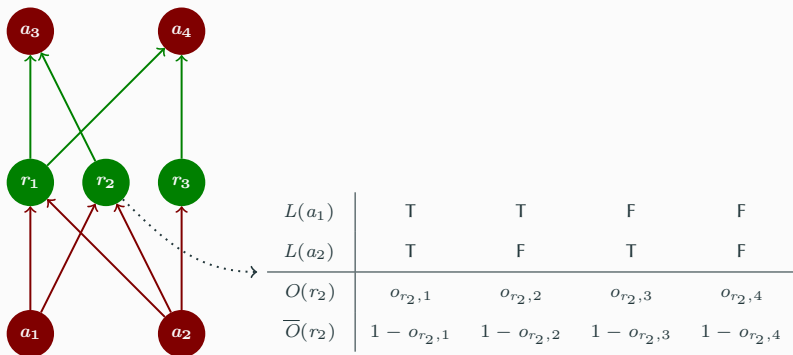
Attack Level

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



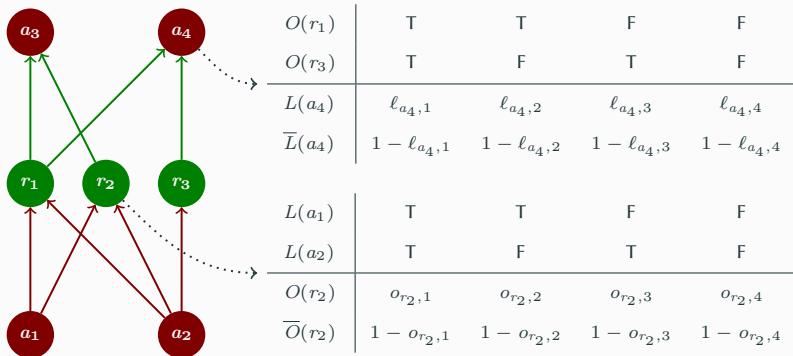
Attack Level

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



Attack Level

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



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

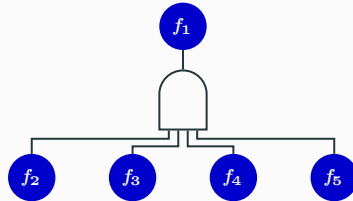
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

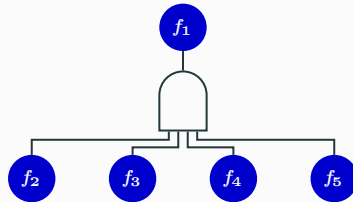
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



$$F_1 = F_2 F_3 F_4 F_5$$

Function Level

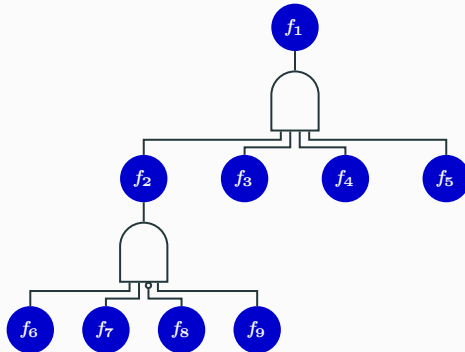
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

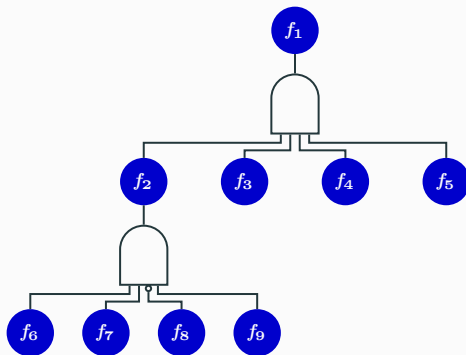
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

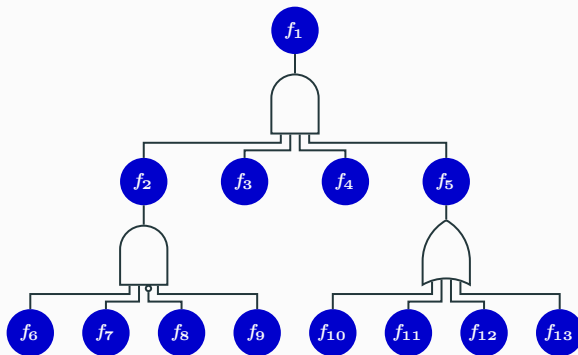
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

Function Level

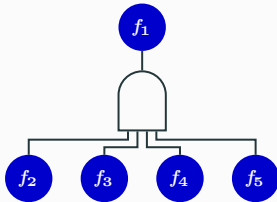
Function Tree Analysis is widely used to analyze the stability of control system, a typical function tree is shown in following figure.



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

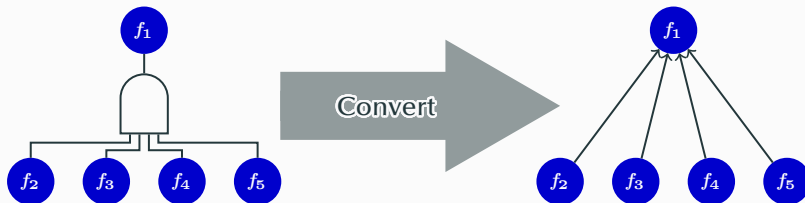
Function Level

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



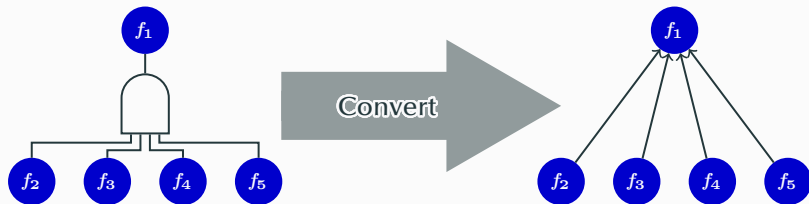
Function Level

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



Function Level

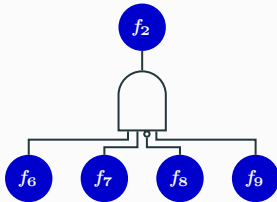
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_2)$	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

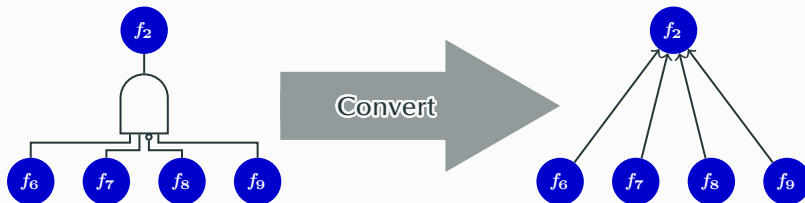
Function Level

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



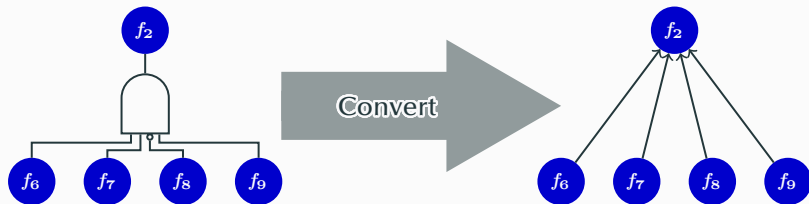
Function Level

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



Function Level

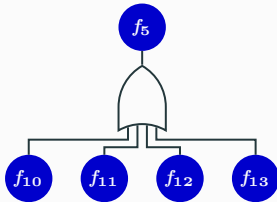
To simplify the inference, the function tree is converted into Bayesian network, which is shown in following figure.



$F(f_6)$	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

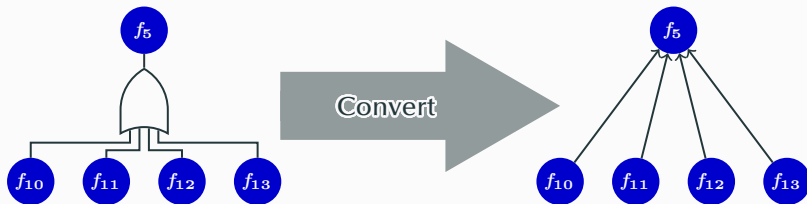
Function Level

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



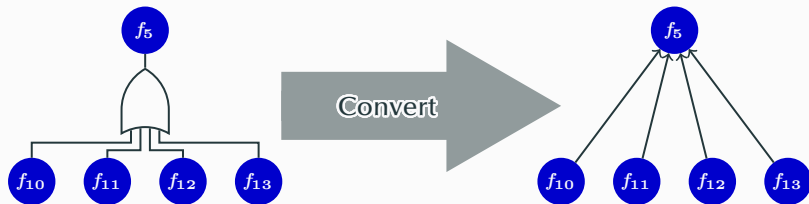
Function Level

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



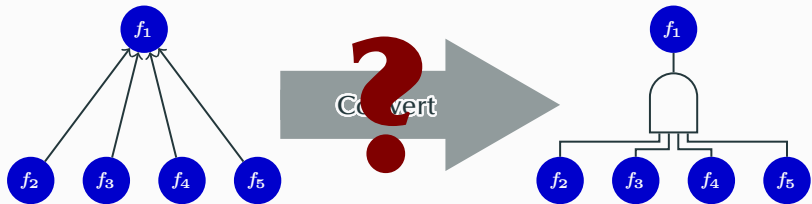
Function Level

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

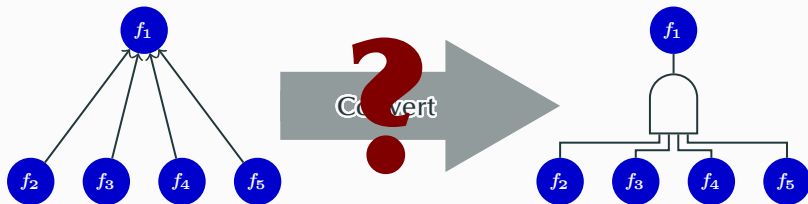


$F(f_{10})$	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
$F(f_{11})$	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F
$F(f_{12})$	T	T	F	F	T	T	F	F	T	T	F	F	T	T	F	F
$F(f_{13})$	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
$F(f_5)$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$\overline{F}(f_5)$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

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

Collection of Evidence

Calculation of Incident Probability

Questions?