論文進度報告

Advisor: Prof. Frank Yeong-Sung Lin
Presented by: Tim, Quen Ting Chen

Title

- Recovery and Resource Reallocation Strategies to Maximize Network Survivability for Multi-Stage Defense Resource Allocation under Malicious Attacks

- 考量惡意攻擊情況下多階段防禦資源分配以最大化網路存活度之修復與資源重分配策略

Key Issue

- Multi-Stage Network Attack and Defense
- Resource Reallocation
- Network Recovery

Agenda

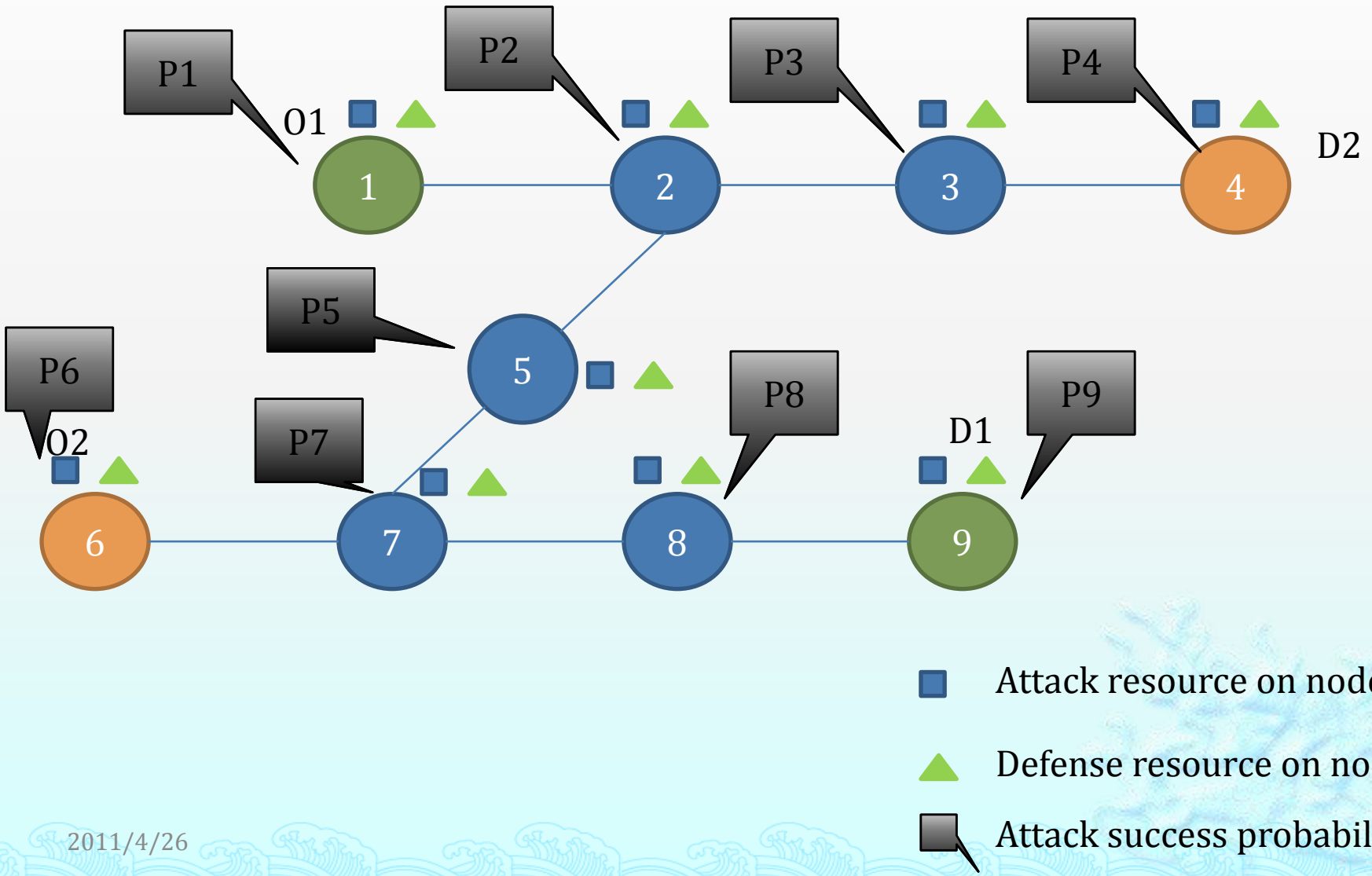
- Average Degree of Disconnectivity(Average DOD)
- Problem Description
- Problem Formulation
- Solution Approach
- Experiment(On stage)

Average Degree of Disconnectivity (Average DOD)

Average DOD

- A metric of network survivability
- **Nothing is one hundred percent successful.**
- Therefore, we introduce the concept of the probability(using the **contest success function**)into the **DOD.**

Average DOD


P1
P2
P3
P4
O1
D2
1
2
3
4
P5
P6
5
P8
P9
P7
D1
O2
6
7
8
9
Attack resource on node *i*
Defense resource on node *i*
Attack success probability

Average DOD

Network Configuation	Probability(P)	DOD	P *DOD
1,2,3,4,5,6,7,8,9	(1-P1)*(1-P2)(1-P3)(1-P4)(1-P5)(1-P6)(1-P7)(1-P8)(1-P9)	0	0
1,2,3,4,5,6,7,8,9	P1*(1-P2)(1-P3)(1-P4)(1-P5)(1-P6)(1-P7)(1-P8)(1-P9)	(1+0)/2	(1/2)*P1*(1-P2)(1-P3)(1-P4)(1-P5)(1-P6)(1-P7) (1-P8)(1-P9)
. . . . .			
1,2,3,4,5,6,7,8,9	P1*P2*P3*P4*P5*P6*P7*P8*P9	(6+6)/2	6*P1*P2*P3*P4*P5*P6*P7*P8*P9

Average DOD

Average DOD

- The greater value of Average DOD, the smaller the network survivability.

Problem Description

Problem Description

- The network survivability is measured by **Average DOD**

- Role
  - Defender
  - Attacker

Defender

- Objective
  - The defender tried to minimize the damage level of network (Average DOD)
- Constraint
  - The total budget of defender
- To determine
  - The defender's budget allocation in each node in each round
  - Whether to reallocate budget or not
  - Whether to repair the compromised node or not

The Reallocation Budget Policy

- The reallocation policy
  - The discount factor (0~100%)
  - 1. All nodes
  - 2. Partial nodes reallocation
    - Recycle the budget only of the compromised node
    - Recycle the budget according to the discount rate
    - Recycle the budget of the node which across the less OD pair
  - 3.Non-reallocated

The Repaired Node Policy

- The repaired node policy
  - 1. All nodes which are compromised
  - 2. Partial compromised nodes
    - Repair the compromised node according to the passing number of the OD pair
    - Repair the compromised node according to the compromised probability of last round (CSF Value)
    - Repair the compromised node according to the repair cost
  - 3. Non-repaired

Attacker

- Objective
  - The attacker tried to maximize the damage of the network (Average DOD)
- Constraint
  - The total budget
- To determine
  - The attacker's budget allocation in each node in each round

The Strategy of Attacker

- The accumulated experience strategy of attacker：
  - Exist the accumulated experience ability
    - Positive
    - Negative
  - Non existed accumulated experience ability

Problem Formulation

Given

- The network topology
- Attacker’s total budget
- Defender’s total budget

Objective

- To minimize the maximum damage of the network (Average DOD)

Subject To

- Budget constraint for attacker
- Budget constraint for defender

To Determine

- Attacker
  - How to allocate attacker's budget to each node in each round
- Defender
  - How to allocate defender's budget to each node in each round
  - Whether to repair the compromised node in each round
  - Whether to reallocate budget or not

Given Parameter

Given parameter	
Notation	Description
V	Index set of nodes
R	Index set of rounds in the attack and defense actions
$\hat{A}$	Total budget of attacker
$\hat{B}$	Total budget of defender
w_r	The weight of the Average DOD in round r , where $r \in R$

Given Parameter

Given parameter	
Notation	Description
θ_i	Existing defense resource allocated on node i , where $i \in V$
e_{ri}	Repair cost of defender when node i is dysfunctional in round r , where $i \in V$ and $r \in R$
d_{ri}	The discount rate of defender reallocate resources on node i in round r , where $i \in V$ and $r \in R$

Decision Variable

Decision variable	
Notation	Description
$\vec{a}_r$	Attacker's budget allocation, which is a vector of defense resource $a_{r1,}$ a_{r2} to $a_{ri,}$ in round r, where $i \in V$ and $r \in R$
$\vec{b}_r$	Defender's budget allocation, which is a vector of attack cost $b_{r1,}$ b_{r2} to $b_{ri,}$ in round r, where $i \in V$ and $r \in R$.
a_{ri}	Attacker's budget allocation on node i in round r, where $i \in V$ and $r \in R$.
b_{ri}	Defender's budget allocation on node i in round r, where $i \in V$ and $r \in R$.
A_r	Attacker's total budget in round r, where $r \in R$
B_r	Defender's defense budget in round r, where $r \in R$

Decision Variable

Decision variable	
Notation	Description
$\overrightarrow{z_r}$	Defender's recovery budget allocation, which is a vector of repaired status z_{r1} , z_{r2} to z_{ri} in round r , where $i \in V$ and $r \in R$
z_{ri}	1 if node i is repaired by defender in round r , 0 otherwise where and $i \in V$ *and* $r \in R$
$\bar{D}(\vec{a}_r, \vec{b}_r)$	The average DOD, which is considering under attacker's and defender's budget allocation are $\vec{a}_r$ and $\vec{b}_r$ in round r , where $r \in R$

Formulation

Objective function:

$$\min_{\vec{b}_r, \vec{z}_r} \max_{\vec{a}_r} \sum_{r \in R} w_r \bar{D}(\vec{a}_r, \vec{b}_r) \qquad \text{(IP 1)}$$

Subject to:

$$\sum_{i \in V} b_{ri} + \sum_{i \in V} e_{ri} z_{ri} \le B_r + \sum_{i \in V} \theta_i d_{ri} \qquad \forall\, r \in R \qquad \text{(IP 1.1)}$$

$$\sum_{i \in V} a_{ri} \le A_r \qquad \forall\, r \in R \qquad \text{(IP 1.2)}$$

$$\sum_{r \in R} B_r \le \hat{B} \qquad \text{(IP 1.3)}$$

$$\sum_{r \in R} A_r \le \hat{A} \qquad \text{(IP 1.4)}$$

Solution Approach

Gradient Method

- In our problem, we use the gradient method to solve our inner and outer problem.
- The type of the gradient method
  - Gradient descent (Solve minimization problem)
  - Gradient ascent(Solve maximization problem)

The Algorithm of Gradient

1) Get a start point

2) Determine a direction which could be positive or negative

3) Determine a step size

4) Repeat

   a. Find the most impact dimension of all dimensions

   b. Move a step of the most impact dimension

   c. Update the start point

   Until stopping criterion is satisfied

The Impact Calculation

- The derivative of the Average DOD is difficult to calculating, so the following method could be used to calculate it：

$$\lim_{h \to 0} \frac{\overline{D}(r_i + h) - \overline{D}(r_i)}{h}$$

$\overline{D}()$ means the Average DOD value

r_i means the resources on node i

Solution Procedure

- In each round, both cyber attacker and network defender have budget constraint.
- The **attacker** uses the **Gradient ascent** to adjust the budget of attacker in each round.
- The **defender** uses the **Gradient descent** to adjust the budget of defender in each round.
- Until both attacker and defender are not adjust their budget resource.

Accelerating Calculation of The Average DOD

- The calculation of the Average DOD value, we need to get：
  - **DOD value** of each configuration (Difficult)
  - **Probability value** of each configuration (Easy)
- Therefore, we could use the probability value of each configuration to accelerate calculation of the Average DOD.

Accelerating Calculation of The Average DOD

- Once the probability is too small, the impact of the Average DOD value is almost same.
- For example：

  The probability is 0.0000000001

  The DOD value is 1000 or 1

  The Average DOD of this configuration is almost same.

Accelerating Calculation of The Average DOD

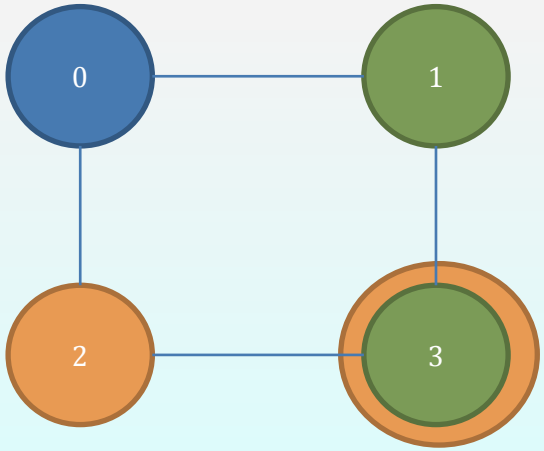
- So the algorithm is as below：
  - Calculating the probability of each possible network configuration
  - Sorting all the possible network configurations by the probability value from large to small value
  - Setting a threshold of cumulative probability

  Once the cumulative probability larger than the threshold, setting the corresponding DOD value as the largest DOD in the network

Experiment(One stage)

The Network Environment

- The number of node：4
- The number of OD pair of the network：2
- The topology (1,3) and (2,3)



The Result

m=1

攻擊者 \ 防禦者	2000	4000	6000	8000
2000	1	0.666667	0.5	0.4
4000	1.333333	1	0.8	0.666667
6000	1.5	1.2	1	0.857143
8000	1.6	1.333333	1.142857	1

The Result

m=1

	攻擊	防禦		攻擊	防禦		攻擊	防禦		攻擊	防禦
節點0	0	0	節點0	0	0	節點0	0	0	節點0	0	0
節點1	500	500	節點1	500	1000	節點1	500	1500	節點1	500	2000
節點2	500	500	節點2	500	1000	節點2	500	1500	節點2	500	2000
節點3	1000	1000	節點3	1000	2000	節點3	1000	3000	節點3	1000	4000
總資源	**2000**	**2000**		**2000**	**4000**		**2000**	**6000**		**2000**	**8000**

The Result(2000/2000)

m=1

Configuration	Probability	Configuration	Probability
0000(3,2,1,0)	0.125	1000	0.125
0001	0	1001	0
0010	0.125	1010	0.125
0011	0	1011	0
0100	0.125	1100	0.125
0101	0	1101	0
0110	0.125	1110	0.125
0111	0	1111	0

The Result(2000/4000)

m=1

Configuration	Probability	Configuration	Probability
0000(3,2,1,0)	0.296296	1000	0.148148
0001	0	1001	0
0010	0.148148	1010	0.0740741
0011	0	1011	0
0100	0. 148148	1100	0.0740741
0101	0	1101	0
0110	0.0740741	1110	0.037037
0111	0	1111	0

The Result(2000/6000)

m=1

Configuration	Probability	Configuration	Probability
0000(3,2,1,0)	0.421875	1000	0.140625
0001	0	1001	0
0010	0.140625	1010	0.046875
0011	0	1011	0
0100	0.140625	1100	0.046875
0101	0	1101	0
0110	0.046875	1110	0.015625
0111	0	1111	0

The Result(2000/8000)

m=1

Configuration	Probability	Configuration	Probability
0000(3,2,1,0)	0.512	1000	0.128
0001	0	1001	0
0010	0.128	1010	0.032
0011	0	1011	0
0100	0.128	1100	0.032
0101	0	1101	0
0110	0.032	1110	0.008
0111	0	1111	0

The Result

m=1				
防禦者 / 攻擊者	2000	4000	6000	8000
2000	1	0.666667	0.5	0.4

m=4				
防禦者 / 攻擊者	2000	4000	6000	8000
2000	1	0.117647	0.0243902	0.0077821

m=8				
防禦者 / 攻擊者	2000	4000	6000	8000
2000	1	0.00778209	0.00030478	0.00003

Thank you for your listening!!