論文進度報告

Advisor: Frank, Y.S. Lin

Presented by Q.T. Chen

2010/12/24

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

Agenda

- Problem Description
- Problem Formulation
- Solution Approach

Problem Description

Problem Description

- Role
  - Defender
  - Attacker

- The network survivability is measured by **average DOS**.

Defender

- Objective

  The defender tried to minimize the damage of the network (Average DOS).

- Budget Constraint (reallocating & new allocated budget)
  - deploying the defense budget in nodes
  - repairing the compromised node

Attacker

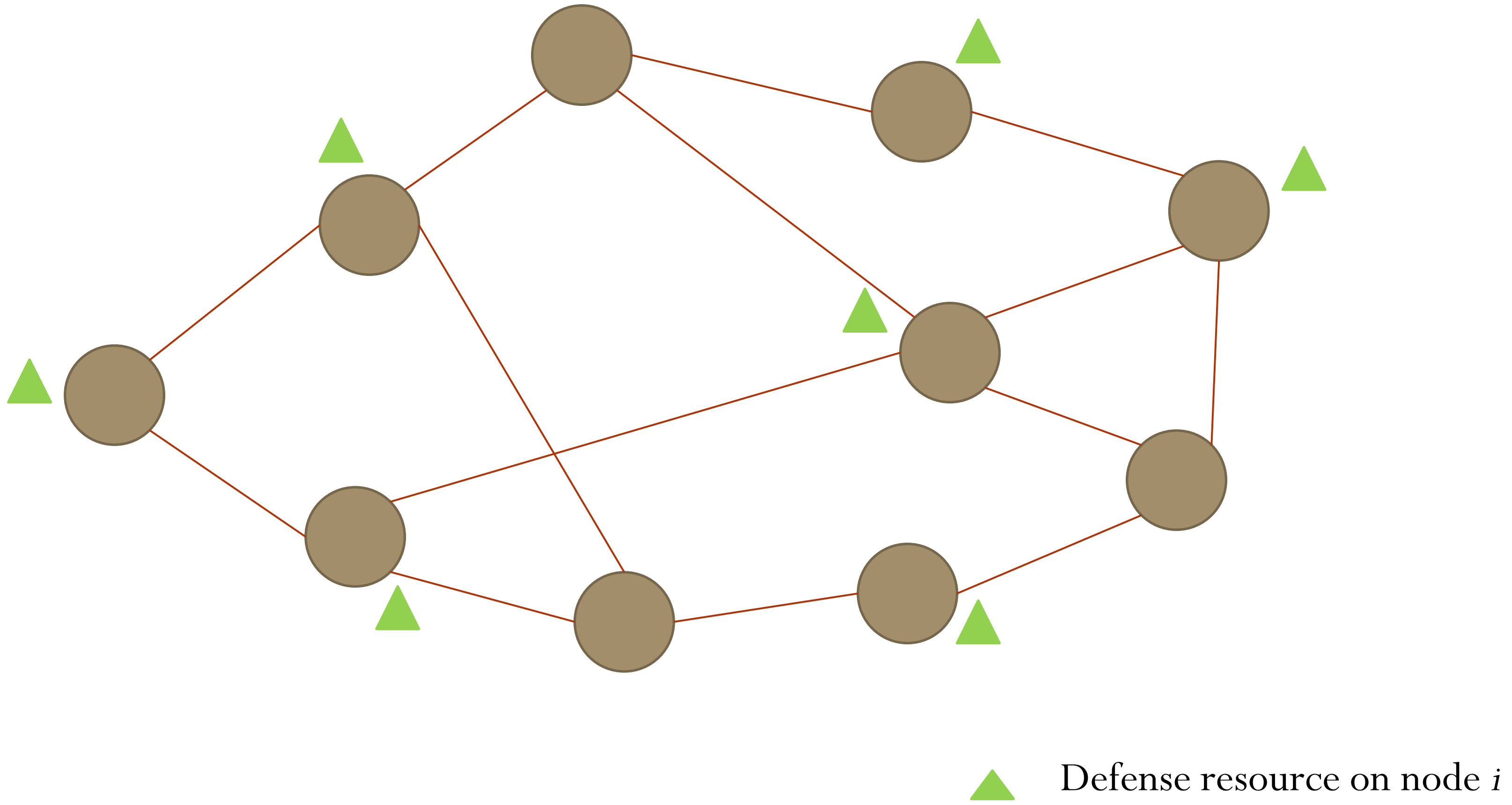
- Objective

  The attacker tried to maximize the damage of the network (Average DOS)

- Budget Constraint
  - deploying the attack budget in nodes

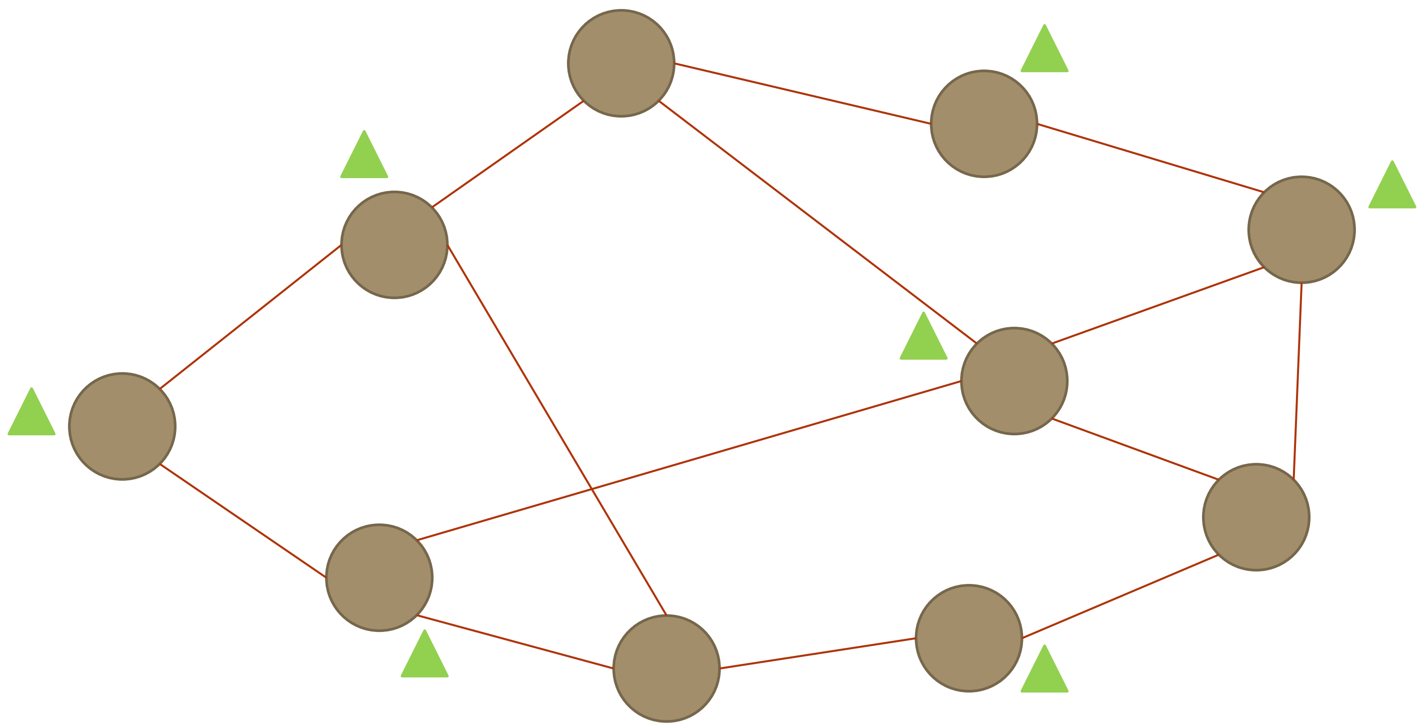
Scenario In Each Round

Scenario (Defender)



Scenario (Defender)

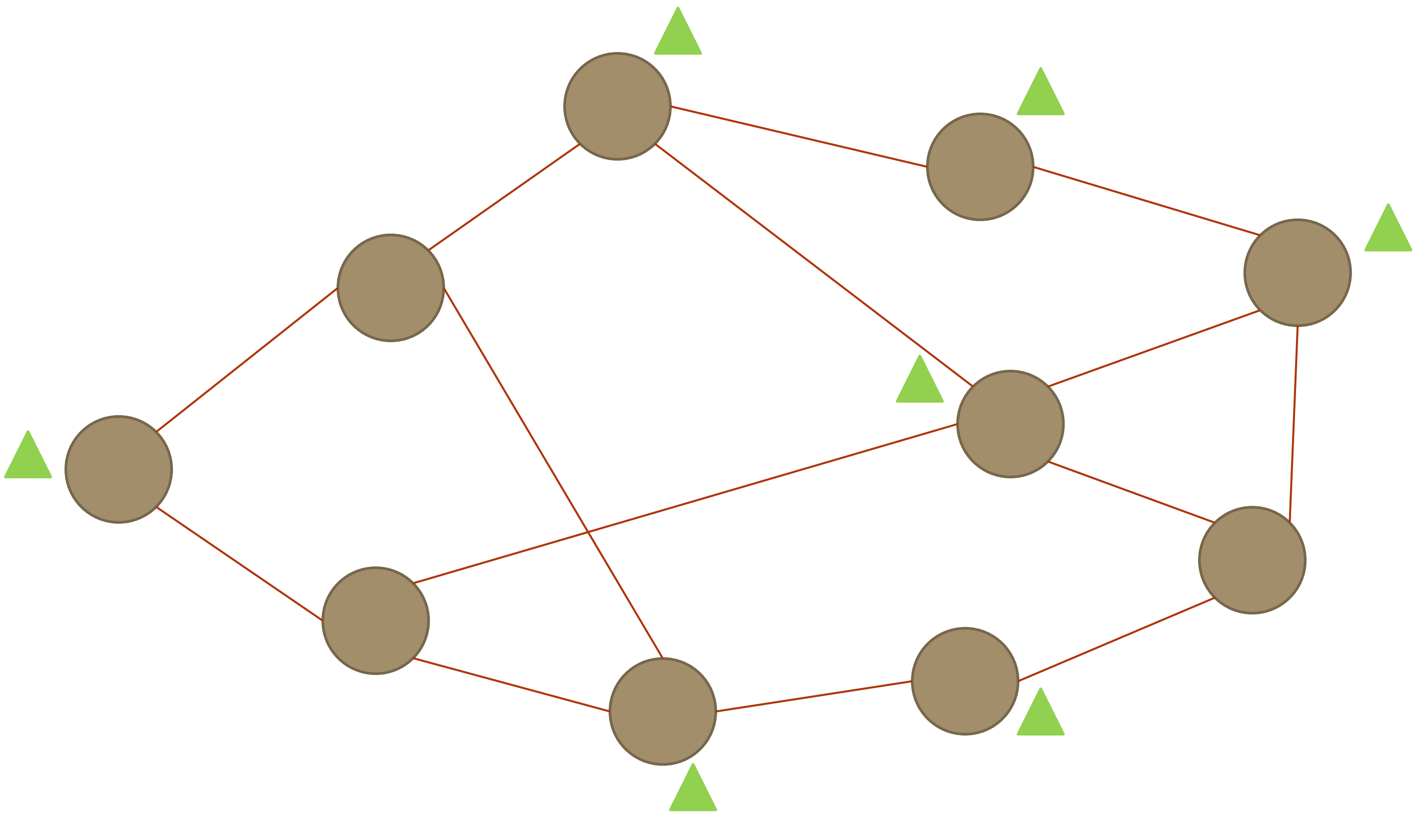
withdraw the resources



Defense resource on node i

Scenario (Defender)

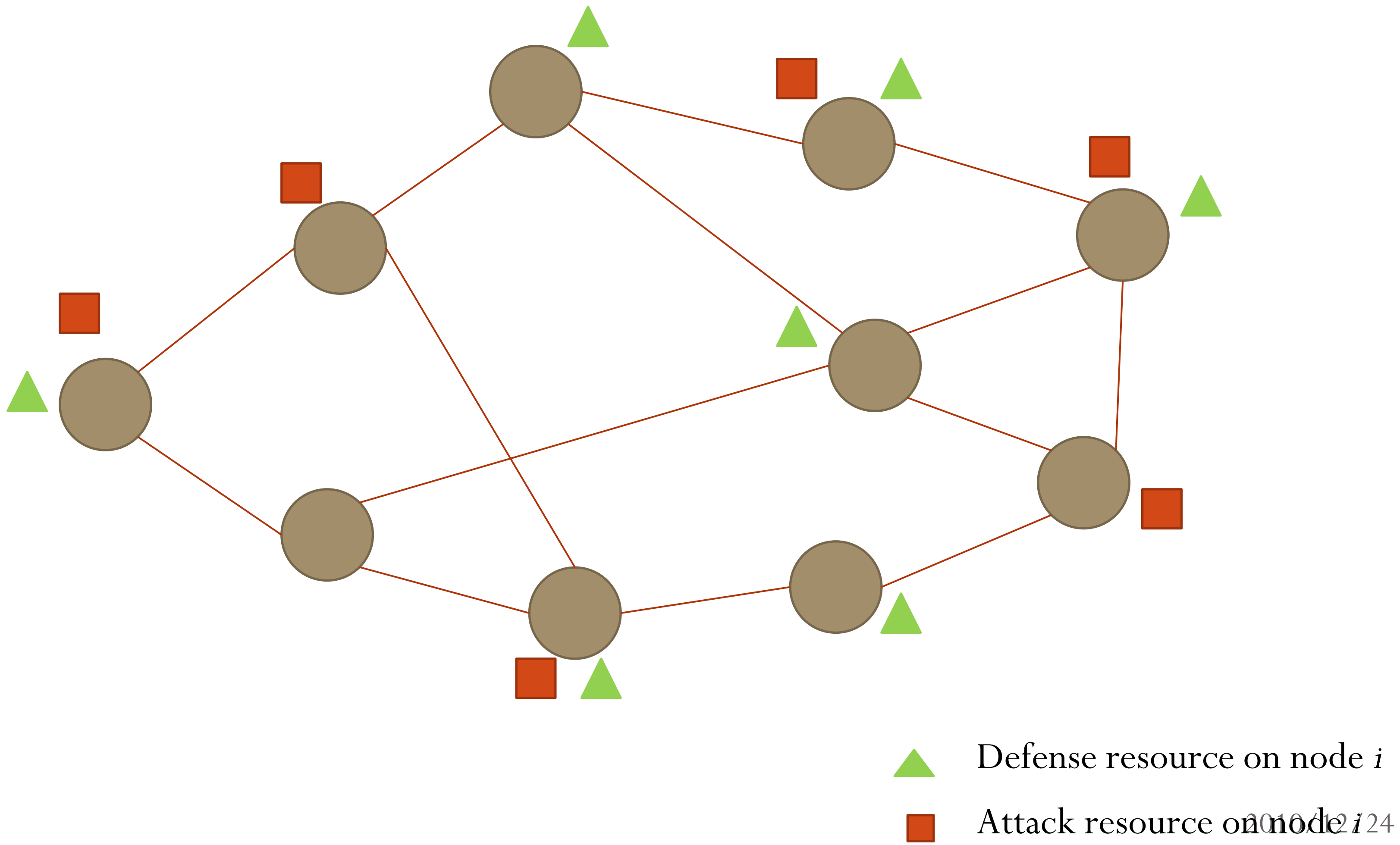
reallocating & new allocated budget



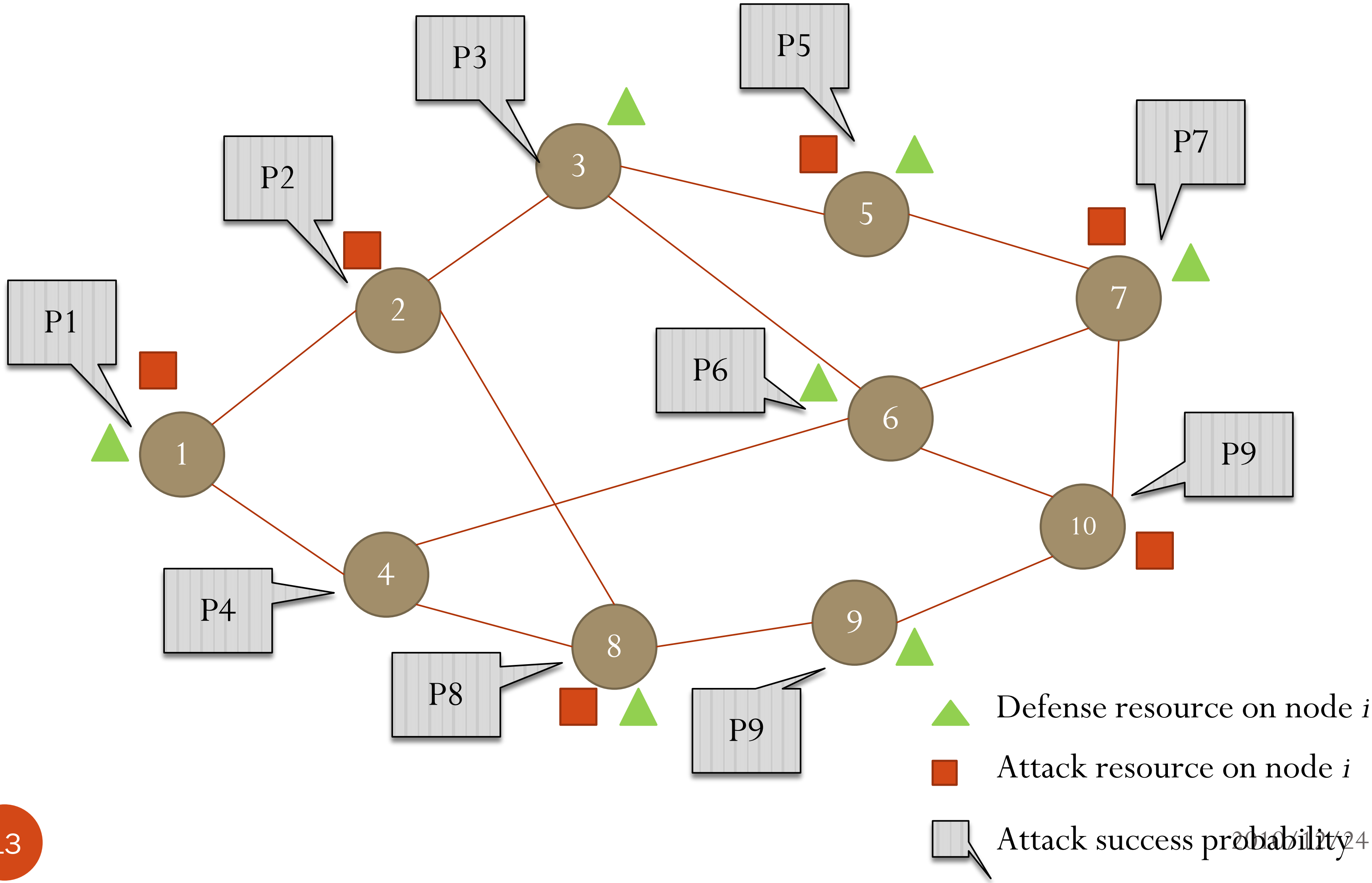
Defense resource on node *i*

2010/12/24

Scenario (Attacker)



Scenario


P1
P2
P3
P4
P5
P6
P7
P8
P9
P9
1
2
3
4
5
6
7
8
9
10
Defense resource on node *i*
Attack resource on node *i*
Attack success probability

Problem Formulation

Problem Assumption

- 1. The problem involves attacker and defender.
- 2. Both attacker and defender have **complete information about the network topology**.
- 3. Both attacker and defender are limited by budget.
- 4. Only node attack is considered. (Link attack is not considered)
- 5. Only malicious attack is considered. (We do not consider random error)
- 6. The attacker can accumulate experience.

Problem Assumption

- 7. For the defender, the budget can be **reallocated** and the **discount factor** is considered.
- 8. For the defender, the compromised node can be repaired.
- 9. Only static network is considered. (We do not consider the growth of network overtime)
- 10. The network survivability is measured by average DOS.
- 11. Any two nodes of the network can form an OD pair.
- 12. We determined the attack success probability using by **contest success function**, considering the resource allocation of both parties.

Given

- 1.The network topology
- 2.Attacker's total budget
- 3.Defender's total budget

Objective

- To minimize the maximum damage of the network (i.e. the average DOS)

Subject To

- Budget constraint for attacker
- Budget constraint for defender

To Determine

- Attacker
  - How to allocate attack budget to each node in each round

- Defender
  - How to allocate defense budget to each node in each round
  - Whether to repair the compromised node in each round

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
θ_i	Existing defense resource allocated on node i, where $i \in V$
e_i	Repair cost of defender when node i, is dysfunctional, where $i \in V$
d_{ri}	The discount rate of defender reallocate resources on node i, 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
$\vec{z}_r$	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 DOS, 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:

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

Subject to:

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

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

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

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

Solution Approach

Gradient

- In vector calculus, the gradient of a scalar field is a vector field which points in the direction of the greatest rate of increase of the scalar field, and **whose magnitude is the greatest rate of change**. (from Wikipedia)

- We could use the **partial deviation** to get the increase rate of each variable.

ex. F(X,Y)= 2X+3Y

$$\frac{\partial F(X,Y)}{\partial X} = 2 \qquad \frac{\partial F(X,Y)}{\partial Y} = 3$$

Gradient

- It is almost impossible to calculate the partial-deviation of **Average DOS of each node**, because it is too complicated.

- So.....

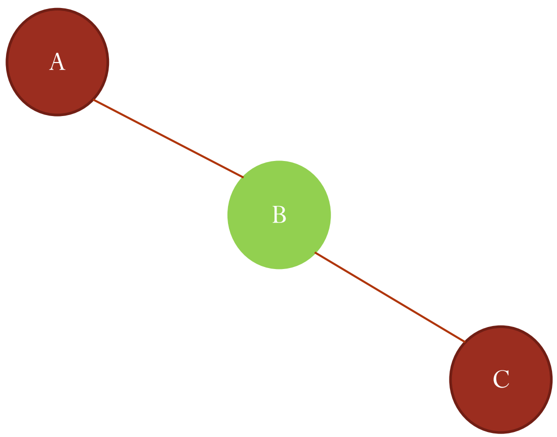
  We calculate the partial-deviation by

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

r_i means the resources on node *i*

Example1

- There are three nodes in the network. (AC link is an O-D pair)



Experience

	A	B	C
defender resource	1	1	1
attacker resource	1	1	1
Contest intensity(m)	1		

成功機率	0.50	0.50	0.50

Experience

A	B	C	機率(P)	DOS	P*DOS
0	0	0	0.125	0	0
0	0	1	0.125	1	0.125
0	1	0	0.125	1	0.125
0	1	1	0.125	2	0.25
1	0	0	0.125	1	0.125
1	0	1	0.125	2	0.25
1	1	0	0.125	2	0.25
1	1	1	0.125	3	0.375
				平均DOS	1.5

平均 DOS =1.5

Experience

	A	B	C
defender resource	2	1	1
attacker resource	1	1	1
Contest intensity(m)	1		

Experience

A	B	C	機率(P)	DOS	P*DOS
0	0	0	0.166667	0	0
0	0	1	0.166667	1	0.166667
0	1	0	0.166667	1	0.166667
0	1	1	0.166667	2	0.333333
1	0	0	0.083333	1	[illegible]
1	0	1	0.083333	2	[illegible]
1	1	0	0.083333	2	[illegible]
1	1	1	0.083333	3	0.25
				平均DOS	1.333333

0.166667

平均 DOS =1.33333

Experience

	A	B	C
defender resource	1	2	1
attacker resource	1	1	1
contest intensity(m)	1		

0.166667

平均 DOS =1.33333

Experience

	A	B	C
defender resource	1	1	2
attacker resource	1	1	1
contest intensity(m)	1		

0.166667

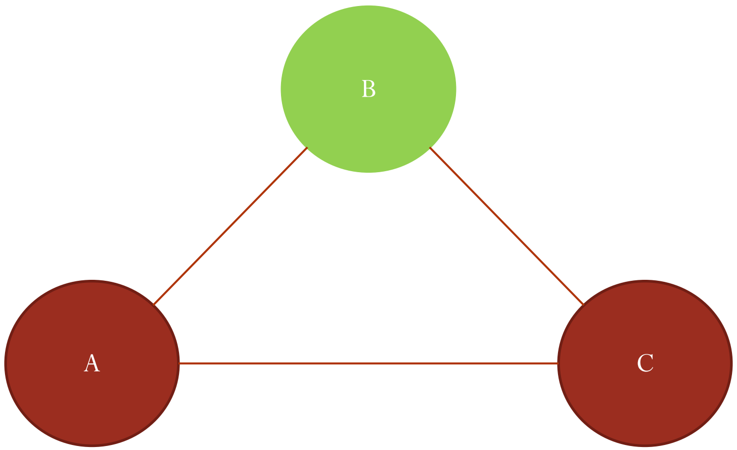
平均 DOS = 1.33333

Result1

- Therefore we could know that the important degree of node 1 , 2 , 3 are same for defender, we need to put the same amount of resources into those node.

Example2

- There are three nodes in the network. (AC link is an O-D pair)



Experience

	A	B	C
defender resource	1	1	1
attacker resource	1	1	1
Contest intensity(m)	1		

平均 DOS =1

Experience

	A	B	C
defender resource	2	1	1
attacker resource	1	1	1
contest intensity(m)	1		

平均 DOS = 0.833333

0.166667

Experience

	A	B	C
defender resource	1	2	1
attacker resource	1	1	1
contest intensity(m)	1		

0

平均 DOS = 1

Experience

	A	B	C
defender resource	1	1	2
attacker resource	1	1	1
contest intensity(m)	1		

0.166667

平均 DOS = 0.833333

Result2

- Therefore we could know that the node 1,3 are more important than node 2, we could recycle the resource of node 2 and distribute those resources to the node 1,3.

	A	B	C
defender resource	1.5	0.000001	1.5
attacker resource	1	1	1
contest intensity(m)	1		

0.2

平均 DOS = 0.8

Gradient

- As a result, we could use the concept of gradient to distribute resources more effectively.

Thank you for your listening！

Average DOS Calculating Method

- The more number of the nodes of network, the more difficult to calculate the Average DOS.

- Because we need to consider all of the possible network statuses,

Number of nodes	Network Status
4	2^4
10	2^{10}
100	2^{100}

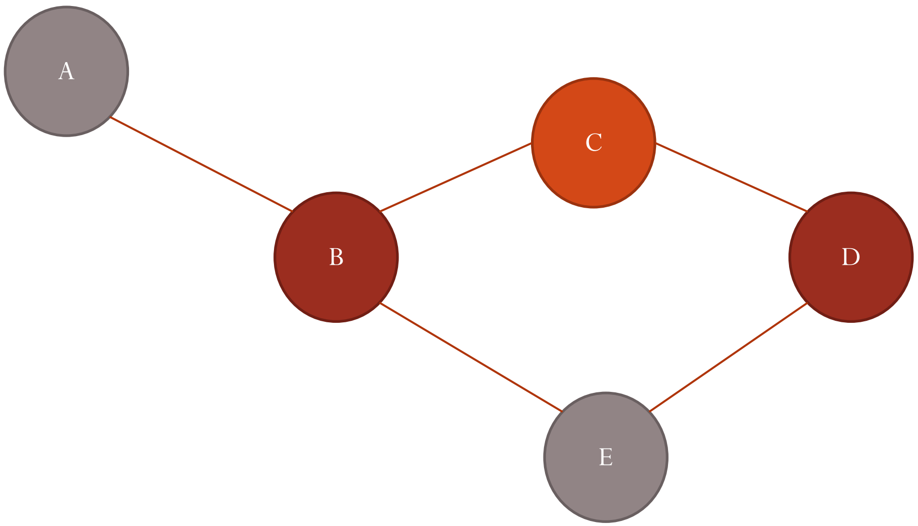
Average DOS Calculating Method

- In order to calculate the Average DOS, we need to calculate the **DOS value** and **probability** of each kind of network status.

- However, in order to calculate DOS value of each kind of network status, it need to take lots of time to calculate those value.

Example

- There are five nodes of the network and there exists two O-D pairs in the network(AE and BD)



Experience

- As a result, we need to consider 64 possible network statuses.