How to Patrol a Network against an Unknown Attack.

Steven Alpern
LSE

with Alec Morton
and Katerina Papadaki*

Outline

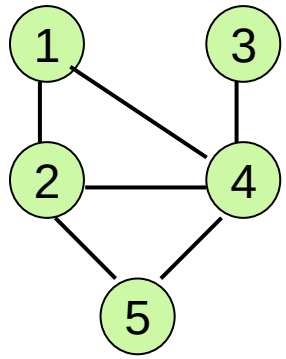
- Introduce Patrolling Games on a graph.
- Applications and types of games.
- Results for all graphs.
- Strategy reduction techniques.
- Solutions for special graphs.

Idea: Think of planning to steal a painting from the Louvre – or defending against it.

Patrolling Game on a Graph

Graph: Q=(N,E)
Nodes: N ={1,2,…,n}
Edges: E

T = time horizon of the game
t = 1,…,T



Players

Attacker: picks a node i and first time τ to perform the attack and needs m uninterrupted periods at the node for the attack to be successful

Patroller: picks a walk w on the graph that lasts T time periods and is successful if the walk intercepts the Attacker during the attack.

Pure Strategies

Attacker: (i, τ)
Patroller: w

Mixed Strategies:

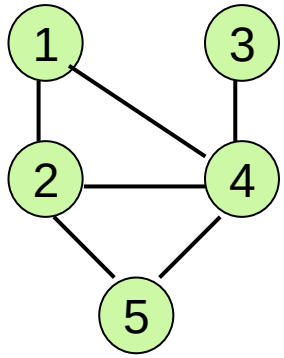
Playing (i, τ) with probability p(i, τ)
Playing w with probability p(w)

We assume: $T \geq m$

Patrolling Game on a Graph

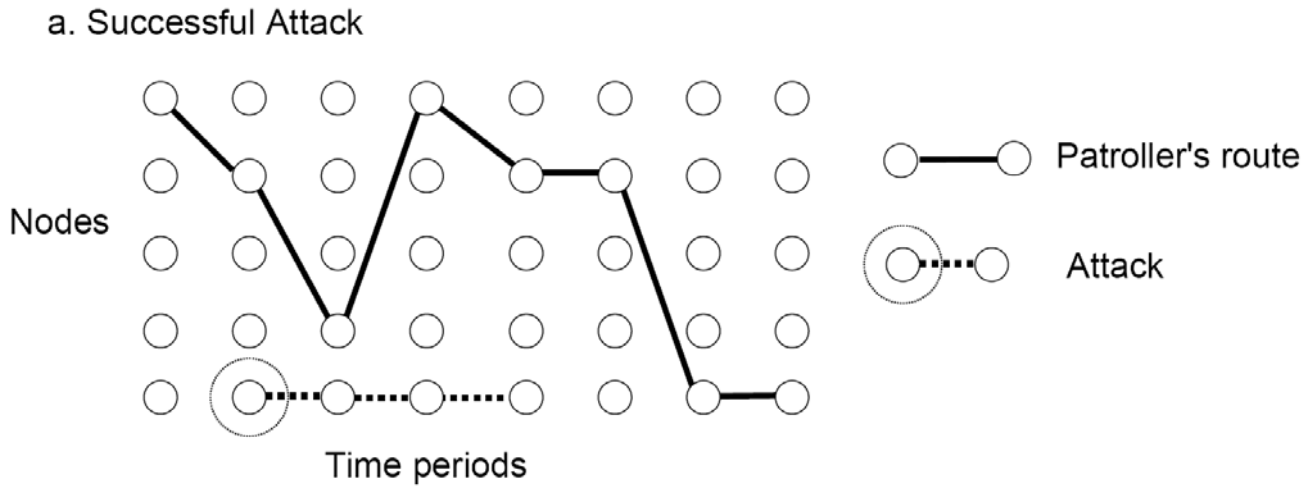
Space-time Network:

n=5, T=8, m=4



patroller picks: w = 1-2-4-1-2-2-5-5

attacker picks: (i, τ) =(5,2)

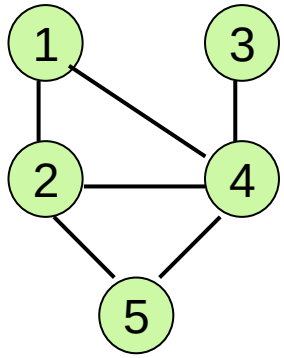


Since the patroller's walk does not intercept the attacker the attack is successful.

Patrolling Game on a Graph

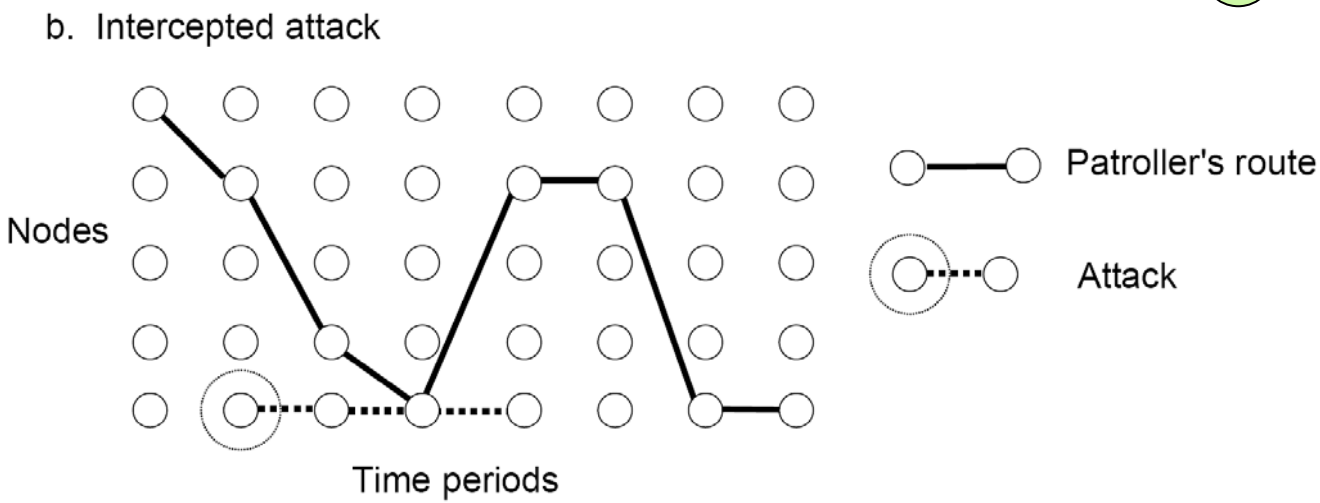
Space-time Network:

n=5, T=8, m=4



patroller picks: w = 1-2-4-5-2-2-5-5

attacker picks: (i, τ) =(5,2)



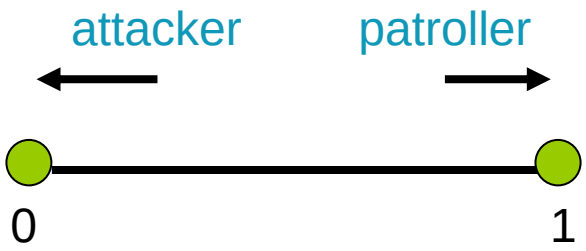
Since the patroller's walk intercepts the attacker the attack is not successful.

Patrolling Game on a Graph

The game is a zero-sum game with the following payoff:

$$\text{Payoff to the patroller} = \begin{cases} 1 & \text{if } (i, \tau) \text{ is intercepted by } w \\ 0 & \text{otherwise} \end{cases}$$

Value of the game = probability that the attack is intercepted



We denote that game: G(Q, T, m) and the value of the game V(Q, T, m)

Assumptions

We make some simplifying assumptions:

- The attacker will attack during the time interval:

  By patrolling as if an attack will take place, the patroller deters the attack on this network and gives an incentive to the attacker to attack another network.

- The nodes have equal values:

  Nodes with different values can be easily modelled in the mathematical programming formulations of the game. All games that can be solved computationally, can also be solved using different valued nodes.

- The nodes on the network are equidistant:

  This can also be modelled in the mathematical programming formulations.

Applications and Game Types

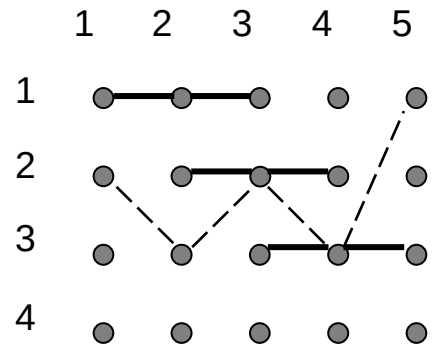
- Patrolling a Gallery:

  T = fixed shift

  (e.g. one working day)

  We call this the one-off game and denote it G^o with value V^o.

one-off (open) game:



attacker can only start attack at nodes 1,2,3.

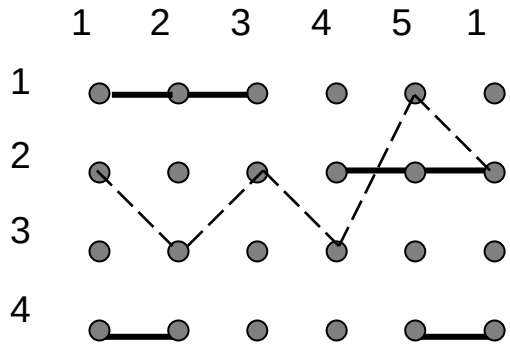
- Patrolling an Airport or a virtual network:

  continuous patrolling

  We call this the periodic game and we let T be the period.

  We denote it with G^p, V^p.

periodic game:



patroller must return to starting node.

Results for all Graphs

Monotonicity Results

1. The Value of the game is non-decreasing in m:

$$V(Q,T,m) \leq V(Q,T,m') \quad \text{for } m \leq m'$$

- the longer the attacker takes to complete the attack, the higher the probability to the attack being intercepted.

2. The Value of the game is non-decreasing in the edge set |E|:

$$V(Q,T,m) \leq V(Q',T,m) \qquad E \subseteq E' \quad N = N'$$

- with additional edges there are more patrolling paths and thus it is better for the patroller

Results for all Graphs

Monotonicity Results

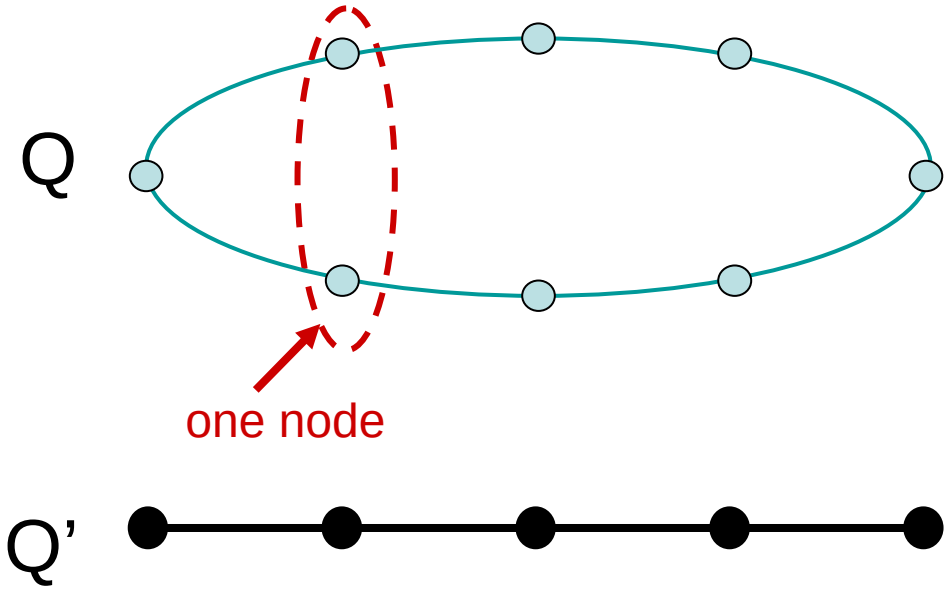
3. The Value of the periodic game is less than or equal to the value of the one-off game:

$$V^p(Q,T,m) \leq V^o(Q,T,m)$$

- the one-off game has more patrolling strategies.

Results for all Graphs

Node Identification



4. If Q' is obtained from Q by node identification, then

$$V(Q') \geq V(Q)$$

since any patrol on Q that intercepts an attack, has a corresponding patrol on Q' that intercepts the same attack

Results for all Graphs

Bounds on Value

5. We have: $$\frac{1}{n} \leq V \leq \frac{m}{n}$$

The patroller can guarantee the lower bound by:

- picking a node equiprobably and waiting there

The attacker can guarantee the upper bound by:

- fixing an attack time interval and
- attacking at a node equiprobably during that interval;

Out of these n pure strategies, the patroller can intercept at most m of them (since the walk during the attack interval can visit at most m nodes)

The lower bound can be achieved for the disconnected graph D_n with n nodes:

$$V(D_n, T, m) = \frac{1}{n}$$

Results for all Graphs

Game with m=1

6. For the special case where K_n is the complete graph with n nodes, Ruckle (1983) has shown that:

$$V^o(K_n, T, 1) = \frac{1}{n}$$

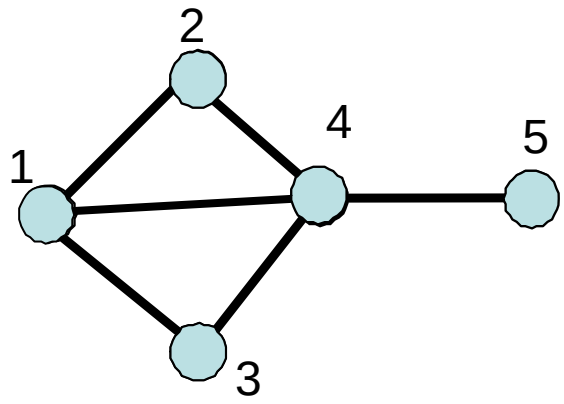
Hence, $$\frac{1}{n} = V^o(K_n, T, 1) \geq V(Q, T, 1) \geq \frac{1}{n}$$

Result: For m=1: $V(Q, T, 1) = \frac{1}{n}$ for all Q and T

Henceforth we assume $m \geq 2$

Strategy Reduction Techniques

Symmetrization

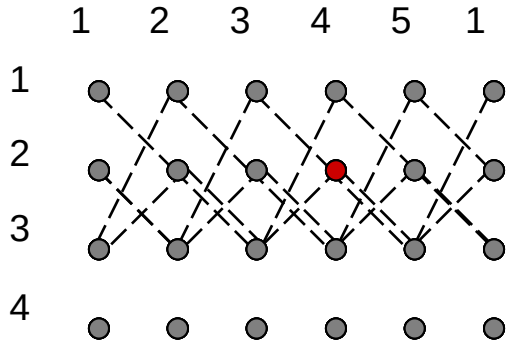


Graph symmetrization:

Adjacency preserving bijections on Q:

- Nodes 2 and 3 are equivalent
- There exists an optimal attack strategy that attacks nodes 2 and 3 equiprobably

Time symmetrization:



For the periodic game,

- the time shifted patrols are equivalent
- the attack intervals are equivalent under some rotation of the time cycle.
- we only need to consider the attack node not the attack interval.

Symmetrical Strategies: mixed strategies which give equal probability to equivalent strategies

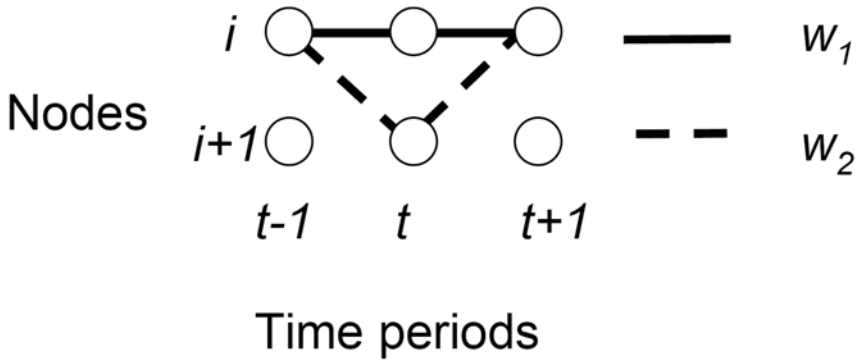
Strategy Reduction Techniques

Dominance for T>=3

For $m \geq 2$:

Walks w_1, w_2 same except on (t-1, t, t+1).

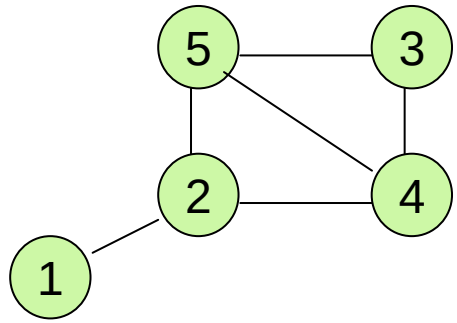
- walk w_2 dominates w_1:
  If w_1 intercepts an attack (i, τ) then w_2 also intercepts (i, τ) .



For $m \geq 3$:

Let 1 be a leaf node connected to node 2:
We call node 2 a penultimate node.

- the attacker should not attack at penultimate nodes.



From above, walk w does not stay at a node for 3 consecutive periods.

If w intercepts (1, τ) then it must intercept (2, τ).

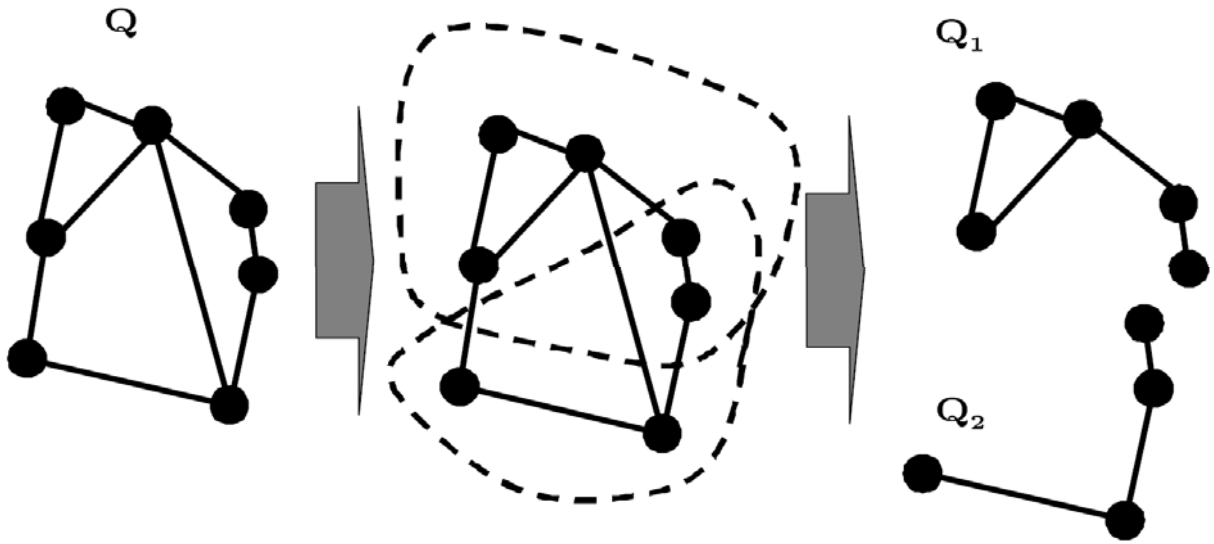
Strategy Reduction Techniques

Decomposition

The set of graphs $Q_k = (N_k, E_k)$, $k = 1 \ldots K$ is a decomposition of graph Q if:

$\cup N_k = N$

If both $i, j \in N_k$ and $(i, j) \in E$, then $(i, j) \in E_k$.



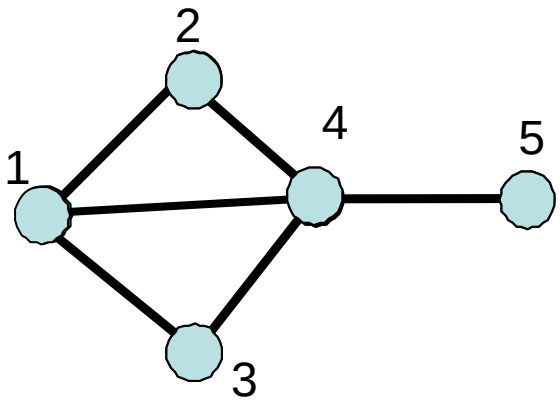
Decomposition Result: We have $V(Q) \geq \dfrac{1}{\sum_k 1/V(Q_k)}$,

which holds with equality if the Q_k are disjoint in Q .

Example

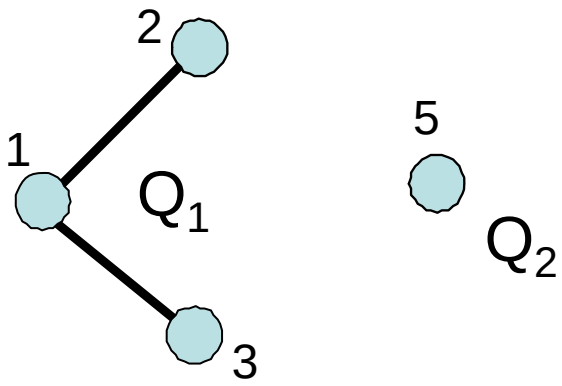
Kite Graph

Periodic game on Q, with T=3 and m=3:



From dominance, we know that attacker would never attack at penultimate node 4, since it is always better to attack at the adjacent leaf node.

Without node 4 the graph decomposes into two graphs Q_1 and Q_2 shown below.

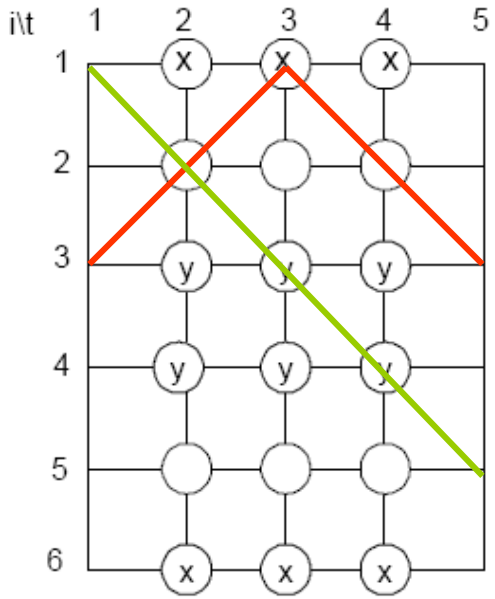


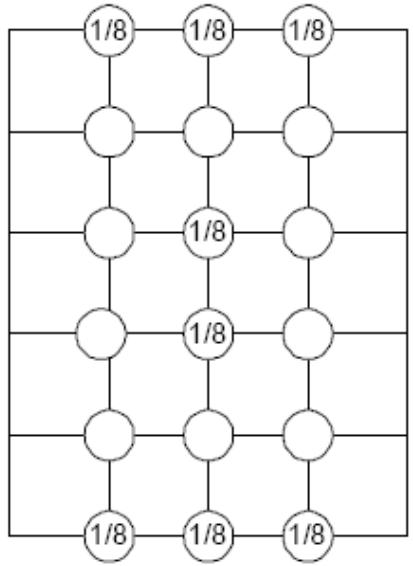
From decomposition we have:

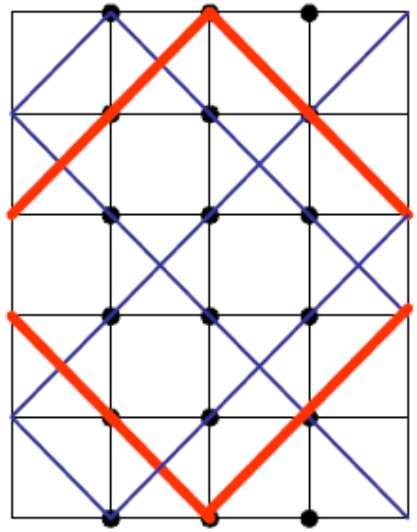
$$V^p(Q) = \frac{1}{1/V^p(Q_1) + 1/V^p(Q_2)} = \frac{1}{2+1} = \frac{1}{3}$$

$$V^p(Q_1) = \frac{1}{2} \qquad V^p(Q_2) = 1$$

Timing of Attack:G^o (L_6),T= 5,m= 3)







Left: time-equiprob.
3x+2y=x+5y,
x=1/10,y=1/15
And V=13/30

Middle:, 8 equiprobable attacks.
No patrol can intercept >3 attacks,
so V<=3/8<13/30.
Right: Play blue 1/8, red ¼. All attacks intercepted by by 3 patrols out of 8, counting reds as 2.

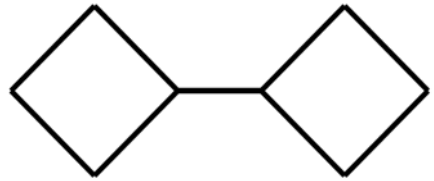
Generic Strategies

Uniform Attacker Strategy

The attacker fixes a time interval of length m.
Attacks at each node of Q equiprobably

Attacker's Diametrical Strategy

d(i,j) = minimum number of edges between nodes i and j
d = diameter of Q = maximum d(i,j) for all pairs i, j.



The attacker attacks equiprobably nodes i and j that have distance d.

We have: $V \leq \max\left[m/2d, 1/2\right]$

The diametrical strategy guarantees the above upper bound:

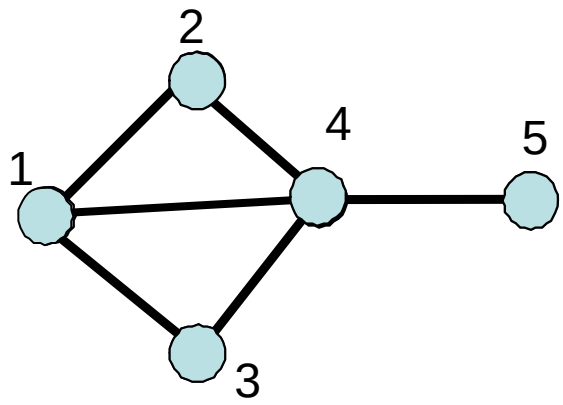
- If m, T are large as compared to d, the best the patroller can do against the diametrical strategy is to go back and forth across the graph diameter (m/2d)

- If d is large as compared to m, T, the best the patroller can do against the diametrical strategy is to stay at the diametrical nodes and win half the time (1/2).

Generic Strategies

Independent strategies

Independent set: set of nodes where no simultaneous attacks at any two nodes of the set can be intercepted by the same patrol. Depends on T,m and game type



Periodic Game for Kite Graph with T=3, m=3.

Independent Sets: {2,3} {1,5} {2,3,5}
(since the patrol needs to return to the initial node)

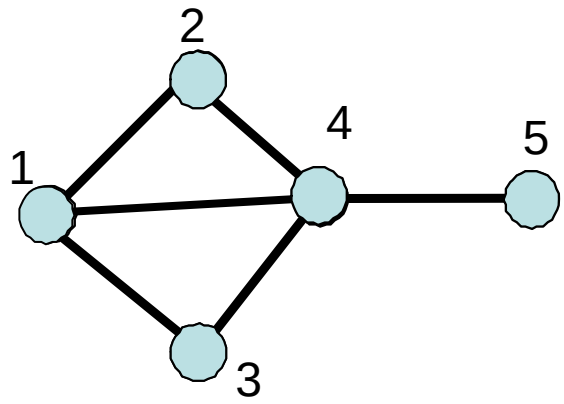
Independence number I : the size of the maximal independent set (3).

Independent attack strategy: attack equiprobably nodes in the maximal independence set in a common attack interval.

Generic Strategies

Covering strategies

Intercepting Patrol: a patrol w that intercepts every attack on a node that it contains.



Periodic Game for Kite Graph with T=3, m=3.

Intercepting patrols: 1-1-2-1
1-3-4-1
4-5-5-4
} covering set

Covering set of Q: a set of intercepting patrols such that every node of Q is contained in at least one of the patrols.

Covering number J: the size of the minimal covering set.

Covering patrol strategy: choose equiprobably from the minimal set of covering patrols.

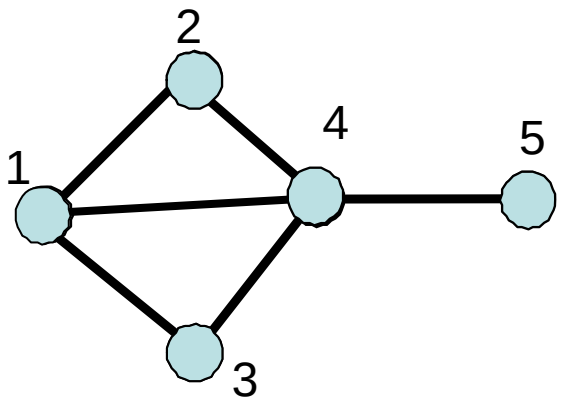
Generic Strategies

Independent and Covering strategies

$$\frac{1}{\mathcal{J}} \leq V \leq \frac{1}{\mathcal{I}}$$

Upper bound: independent attack strategy
Lower bound: covering patrol strategy

When $\mathcal{I} = \mathcal{J}$ we can determine the value of the game:



Periodic Game for Kite Graph with T=3, m=3.

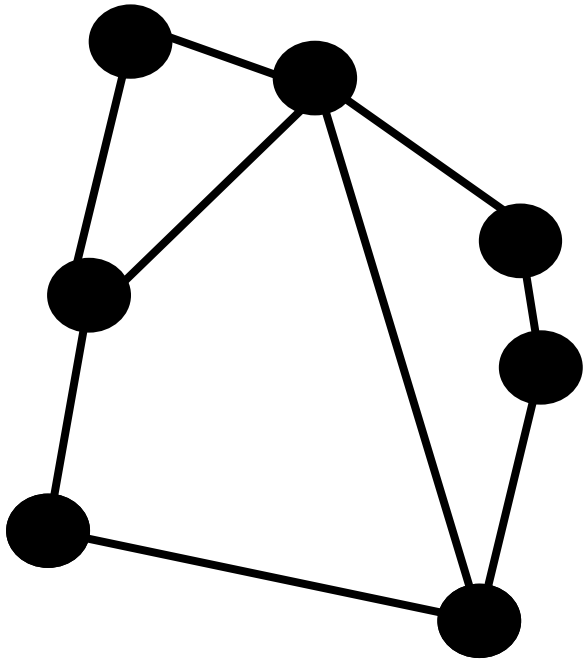
Maximal Independent Set = {2,3,5}
Minimal Covering Set = {1-1-2-1, 1-3-4-1, 4-5-5-4}

We have $\mathcal{I} = \mathcal{J} = 3$:

V(Q) = 1/3

Solutions for Special Graphs

Hamiltonian Graph



Any graph with a Hamiltonian cycle:

- value $\frac{m}{n}$
- Patroller - Random Hamiltonian patrol: pick a node at random and follow the Hamiltonian cycle in a fixed direction
- Attacker - uniform attacking strategy

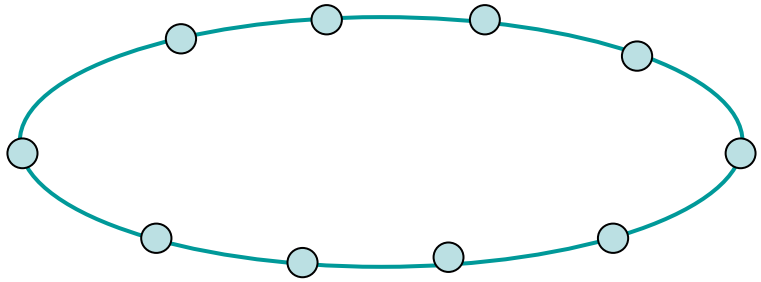
1. $V^o = \frac{m}{n}$;
2. $V^p \leq \frac{m}{n}$ *with equality if* T *is a multiple of* n, *and* $V^p \to m/n$ *as* $T \to \infty$.

Solutions for Special Graphs

Hamiltonian Graphs: example

Periodic game on Q, T=10, m=4:

Q



C_{10} has a Hamiltonian cycle and T=10 is a multiple of n=10:

$$V(C_{10}) = \frac{m}{n} = \frac{4}{10}$$

Solutions for Special Graphs

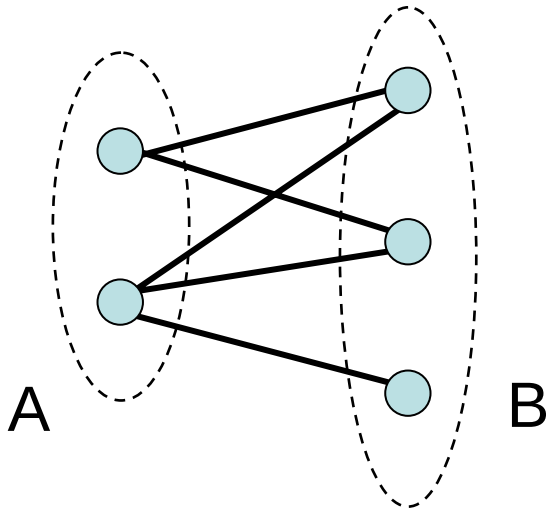
Bipartite Graphs

$K_{a,b}$

- No odd cycles

$$a = |A|, b = |B|, a \leq b$$

We assume: $m \leq 2b$



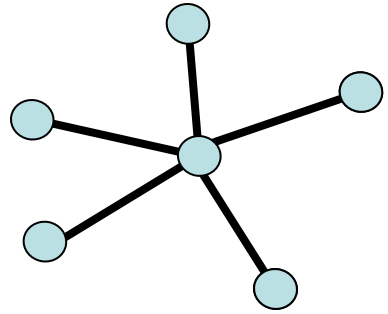
1. $V^o \leq m/(2b)$, *with equality if* Q *is complete bipartite*
2. $V^p \leq m/(2b)$, *with equality if* Q *is complete bipartite and* T *is a multiple of* $2b$.
   if Q *is complete bipartite then* $V^p \to m/(2b)$ *as* $T \to \infty$.

Attacker can guarantee $m/2b$, if he attacks equiprobably on each node of the larger set B.

When Q is complete bipartite and a=b, there exists a Hamiltonian cycle and the value is achieved.

Solutions for Special Graphs

Bipartite Graphs: The Star Graph



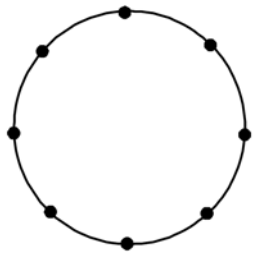
S_n : star graph with n nodes

$C_{2(n-1)}$: cycle graph with 2(n-1) nodes

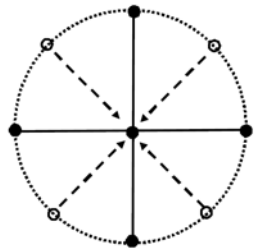
a = 1, b = n-1
T is a multiple of 2(n-1)

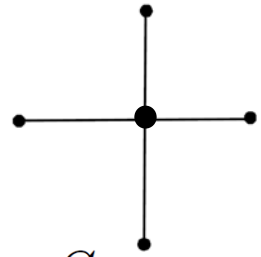
By node identification:

$$V(S_n) \geq V(C_{2(n-1)}) = \frac{m}{2(n-1)}$$



C_8





S_5

Since S_n is bipartite:

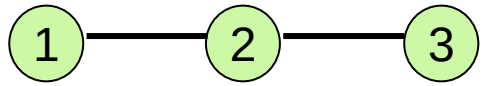
$$V(S_n) \leq \frac{m}{2b} = \frac{m}{2(n-1)}$$

Thus, $V(S_n) = \frac{m}{2(n-1)}$

- attack leaf nodes equiprobably
- patrols leaf nodes every second period

Solutions for Special Graphs

Line Graph



If Q is a line and $n \leq m+1$, then

1) $V^o = \frac{m}{2(n-1)}$;

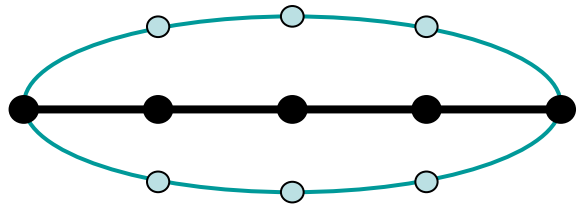
2) $V^p \leq \frac{m}{2(n-1)}$ with equality if T a multiple of $2(n-1)$;

$V^p \to \frac{m}{2(n-1)}$ as $T \to \infty$.

- d = diameter = n-1
  The diametrical attacker strategy guarantees the upper bound for the attacker

- We use node identification, to show that the upper bound is achieved:

$$V(L_n) \geq V(C_{2(n-1)}) = \frac{m}{2(n-1)}$$

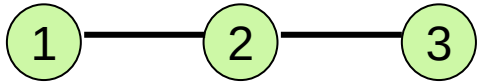


The Hamiltonian patrol on the cycle graph is equivalent to walking up and down the line graph (oscillation strategy).

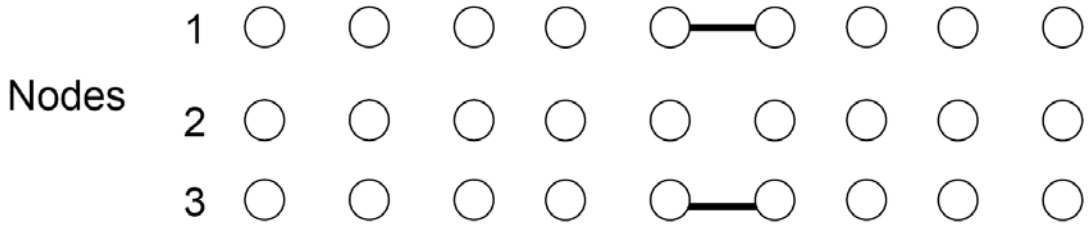
Solutions for Special Graphs

Line Graph

Consider L_3 the line graph with n=3. Let m=2.

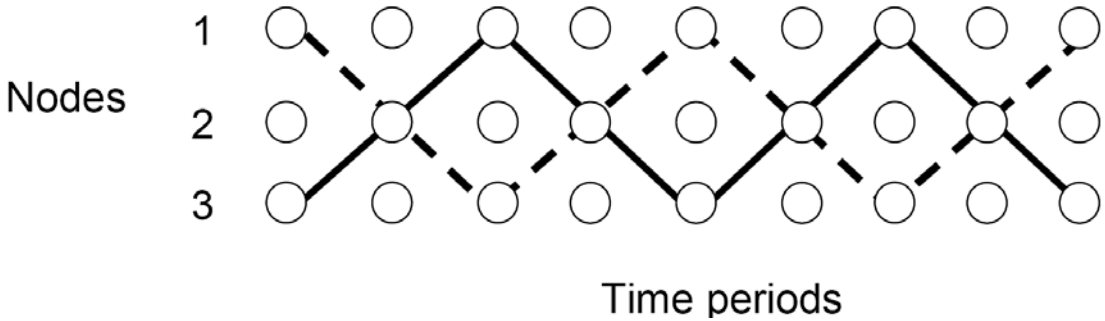


Attacker can guarantee ½ by attacking at the endpoints equiprobably:
no walk can intercept both.



$$V \leq \frac{1}{2}$$

Patroller can guarantee ½ by playing equiprobably the following oscillations:
every attack is intercepted by at least one oscillation.



$$V \geq \frac{1}{2}$$

Solutions for Special Graphs

Line Graph

	m=2	m=3	m=4	m=5	m=6	m=7	m=8	m=9	m=10
n=1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
n=2	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
n=3	**1/2**	**3/4**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
n=4	**1/2**	**1/2**	**4/6**	**5/6**	**1**	**1**	**1**	**1**	**1**
n=5	**1/3**	3/7	**4/8**	**5/8**	**6/8**	**7/8**	**1**	**1**	**1**
n=6	**1/3**		4/8	**5/10**	**6/10**	**7/10**	**8/10**	**9/10**	**1**
n=7	**1/4**			5/11	**6/12**	**7/12**	**8/12**	**9/12**	**10/12**
n=8	**1/4**				6/12	**7/14**	**8/14**	**9/14**	**10/14**
n=9	**1/5**					7/15	**8/16**	**9/16**	**10/16**
n=10	**1/5**						8/16	**9/18**	**10/18**
n=11	**1/6**							9/19	**10/20**
n=12	**1/6**								10/20

Mathematical Programming

LP Formulation

Let A be the set of attacker strategies for G(Q,T,m)

Patroller's game:

$$\max_{x,v} v$$

$$s.t. \quad \sum_{w \in \mathcal{W}} P(w,a)x(w) \geq v \quad \text{for all} \quad a \in \mathcal{A}$$

$$\sum_{w \in \mathcal{W}} x(w) = 1$$

$$x(w) \geq 0, \quad \text{for all} \quad w \in \mathcal{W}$$

Num. of attacker strategies:	n	(periodic game)
(constraints)	n(T-m+1)	(one-off game)
Num. of patroller strategies:	number of circuits of length T	(periodic game)
(variables)	number of paths of length T	(one-off game)

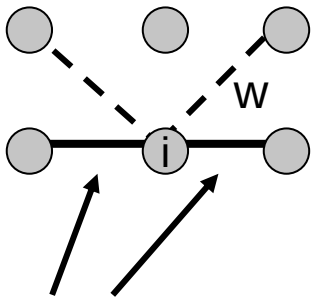
Flow formulation

Case: Periodic game, Q bipartite, m=2, T even

Proposition: A walk that dwells at a node for more than one period is dominated by walks that do not dwell at a node.

Thus, we can count the number of attacks intercepted:

- each visit at a node will intercept exactly two attacks
- the attacks intercepted from visits to different nodes are disjoint

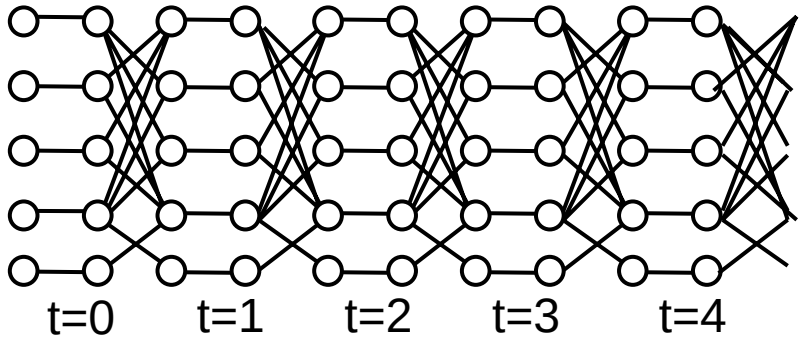


attacks intercepted from the visit of walk w to node i and not intercepted by any other visit of w

Flow formulation

Case: Periodic game, Q bipartite, m=2, T even

kite graph, T=5



Split space-time network Q_S:
- introduce split arcs
- no arc joining the same node in consecutive time periods

$$N(i,e) = \begin{cases} 1 & \text{if } e \text{ is a split arc for node } i, \\ 0 & \text{otherwise.} \end{cases}$$

- i nodes in Q
- e arc of Q_S:

$$B(e,w) = \begin{cases} 1 & \text{if arc } e \text{ of } Q_S \text{ is on the walk } S \text{ of } Q_S, \\ 0 & \text{otherwise.} \end{cases}$$

$NB(i,w)$ = number of visits of walk w to node i during the time horizon

$2NB(i,w)$ = number of attacks at node i intercepted by walk w

Probability attack at node i is intercepted by w = $\frac{2}{T}NB(i,w)$

Flow formulation

Case: Periodic game, Q bipartite, m=2, T even

$$\max_{x,v} v$$

$$s.t. \quad \frac{2}{T} NBx \geq v$$

$$\sum_{w} x(w) = 1$$

$$x(w) \geq 0$$

size of x: no. of walks
x gives probability of each walk
x is a flow on each walk

- Substitute: Bx with z
- Then z(e) is the probability flow on arc e.
- Using flow conservation constraints: $Fz = 0$ we can guarantee that the flow z forms walks

$$\max_{z,v} v$$

$$s.t. \quad Fz = 0$$

$$\frac{2}{T} Nz \geq v$$

$$\sum_{e \in \mathcal{S}} z(e) = 1$$

flow value equals 1

$$z(e) \geq 0$$

Flow formulation

Case: Periodic game, Q bipartite, m=2, T even

$$\max_{z,v} v$$

$$s.t. \quad Fz = 0$$

$$\frac{2}{T} N z \geq v$$

$$\sum_{e \in \mathcal{S}} z(e) = 1$$

$$z(e) \geq 0$$

num. of variables: (2E+n)T + 1
num of constraints: 2nT+n+1

Linear in the problem parameters.

We can solve games with large n and T.

Further, it is easy to introduce different attack values at each node.

Flow formulation

Case: Periodic game, Q bipartite, m=2, T even

Multi-valued Nodes

$$\min_{z,v} v$$

$$s.t. \quad Fz = 0$$

$$d - \frac{2}{T} DNz \leq v$$

$$\sum_{e \in \mathcal{S}} z(e) = 1$$

$$z(e) \geq 0$$

d = vector of node values
D = diagonal matrix with d on the diagonal

Reverse the payoff:
0 when attack is intercepted
d(i) when attack at node i is successful

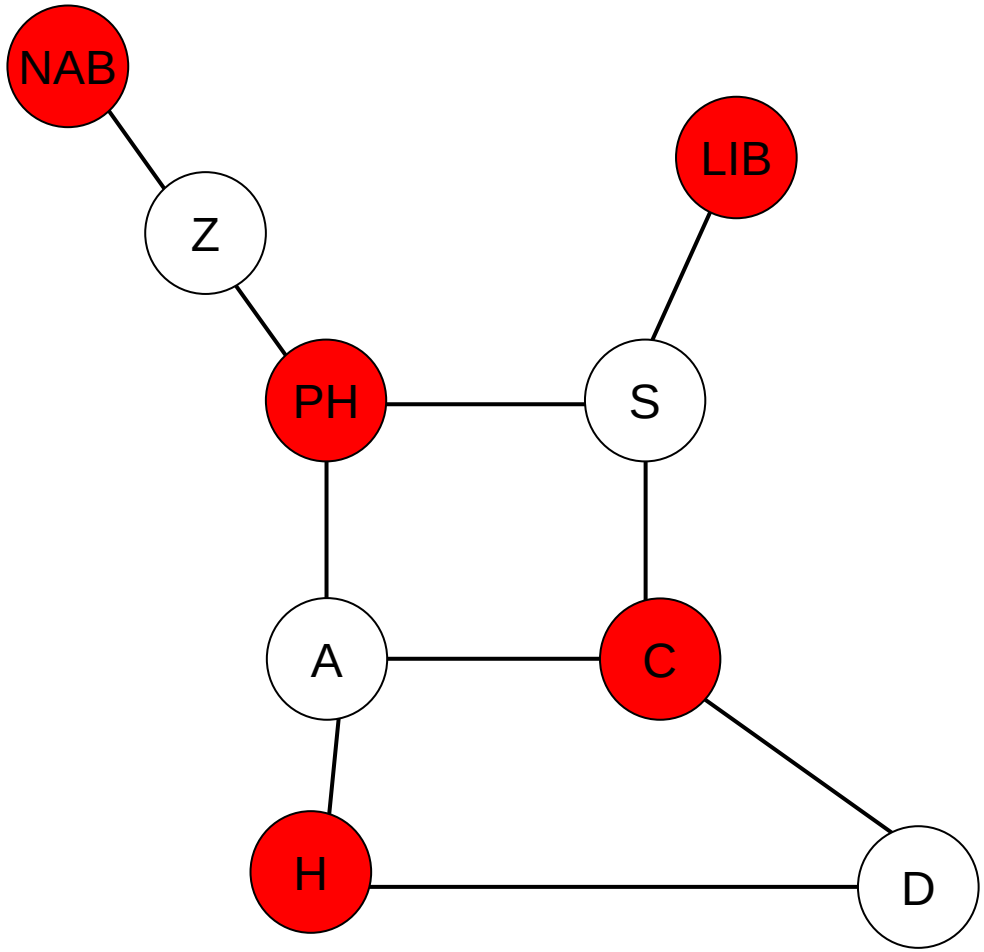
Flow formulation

Single-valued Nodes: (value = 0 attack intercepted)

Optimal Attacker strategy:
attack red nodes equiprobably
with probability 1/5

Game Value = 4/5
(1 is best for attacker)

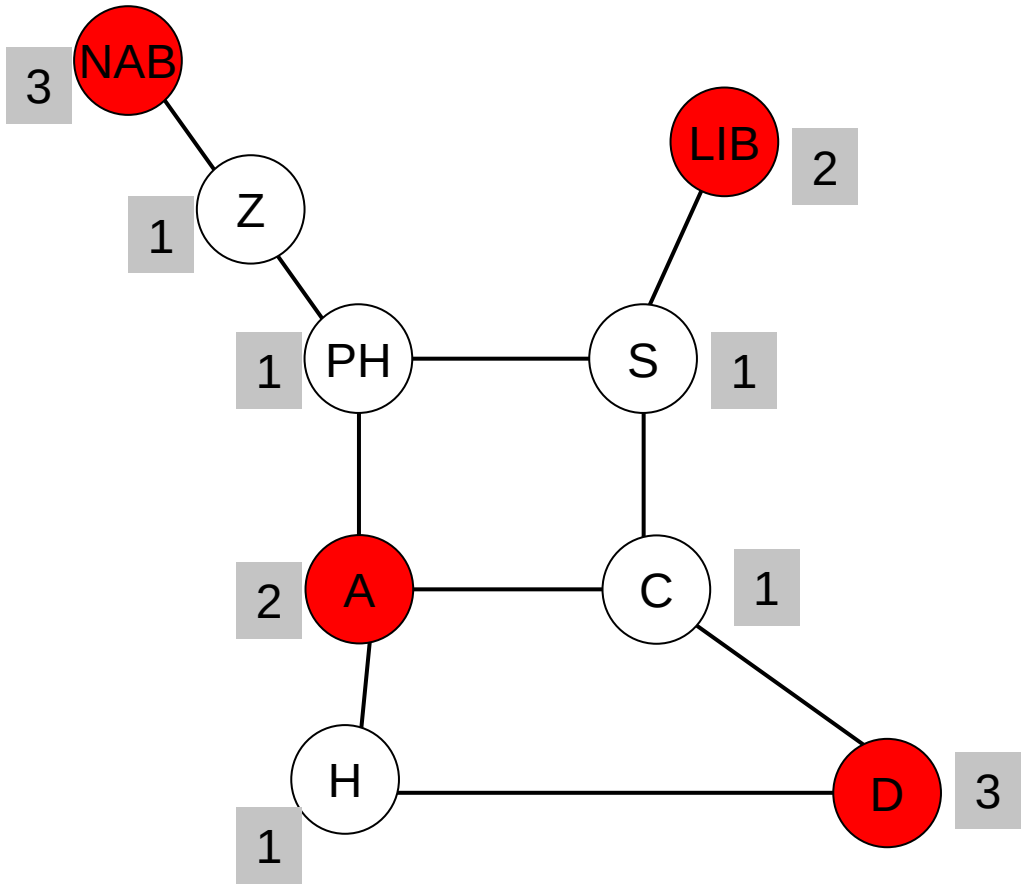
LSE network, m=2, T=20.



Flow formulation

Multi-valued Nodes (value = 0 attack intercepted)

LSE network, m=2, T=20.



Optimal Attacker strategy:
- attack NAB, D with prob. 2/10
- attack A, LIB with prob. 3/10

Game Value = 1.8
(0 is best for patroller)

Current and Future Work

Current work:

1. The Line Graph.
2. Network design: hardening nodes; adding edges.
3. Computational methods: constraint generation methods where the LP is solved with a subset of constraints and the most violated constraints are generated:
    - mixed integer programming is used to find the most violated constraint
    - a heuristic to find a violated constraint

Future work:

- Multiple attackers/ patrols
- Version with in-game observation

The End

Thank you.