To Be Proactive or Not: A Framework to Model Cyber Maneuvers for Critical Path Protection in MANETs

Zhuo Lu
University of Memphis

Lisa Marvel
Army Research Laboratory

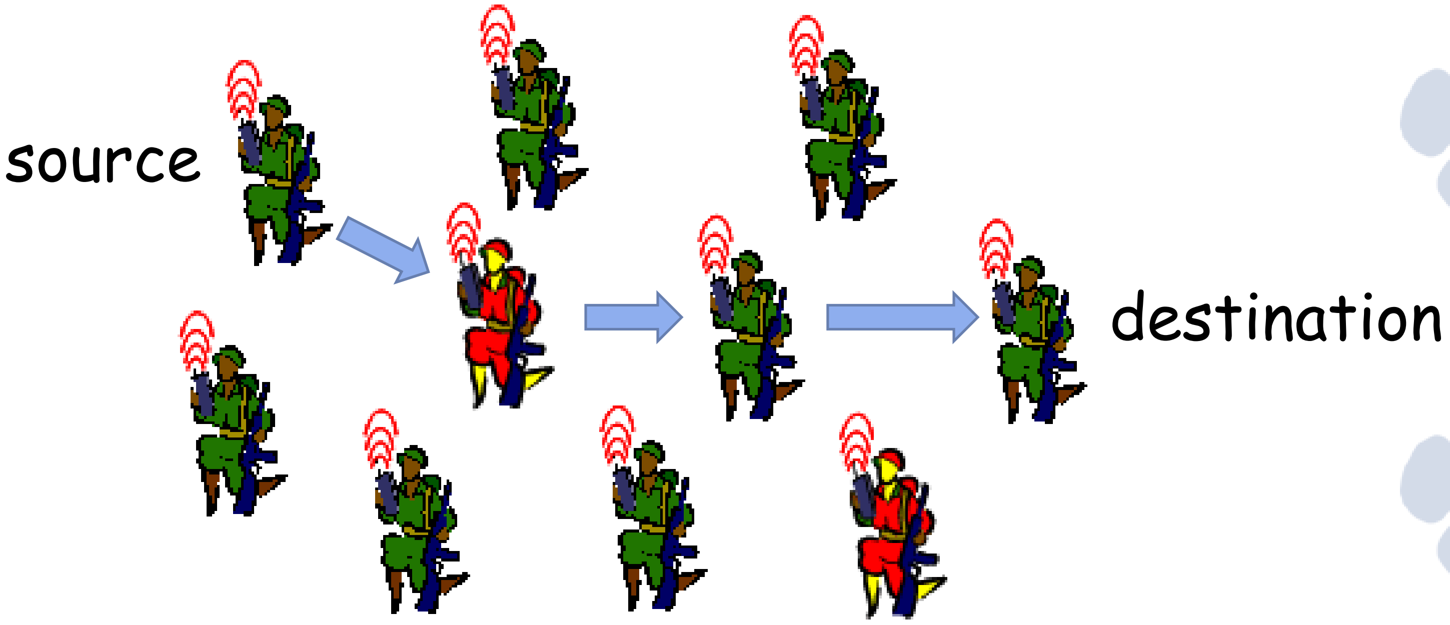
Cliff Wang
North Carolina State University / Army Research Office

Outline

- Background
  - Cyber maneuvers in tactical MANETs
- Framework
  - Models
  - Optimization approach
- Evaluation and simulation results
- Conclusions

Tactical MANETs

- Mobile Ad-Hoc Network (MANET)
  - infrastructure-less network of mobile wireless devices for military operations



Goals vs Issues in Cyber Missions

- Issues / Constraints:
  - Limited energy budget
  - Limited power/bandwidth
  - Distributed deployed in battlefields, may be easy to be compromised by cyber attacks

We must optimally design/coordinate cyber maneuvers to achieve security goals under constraints!

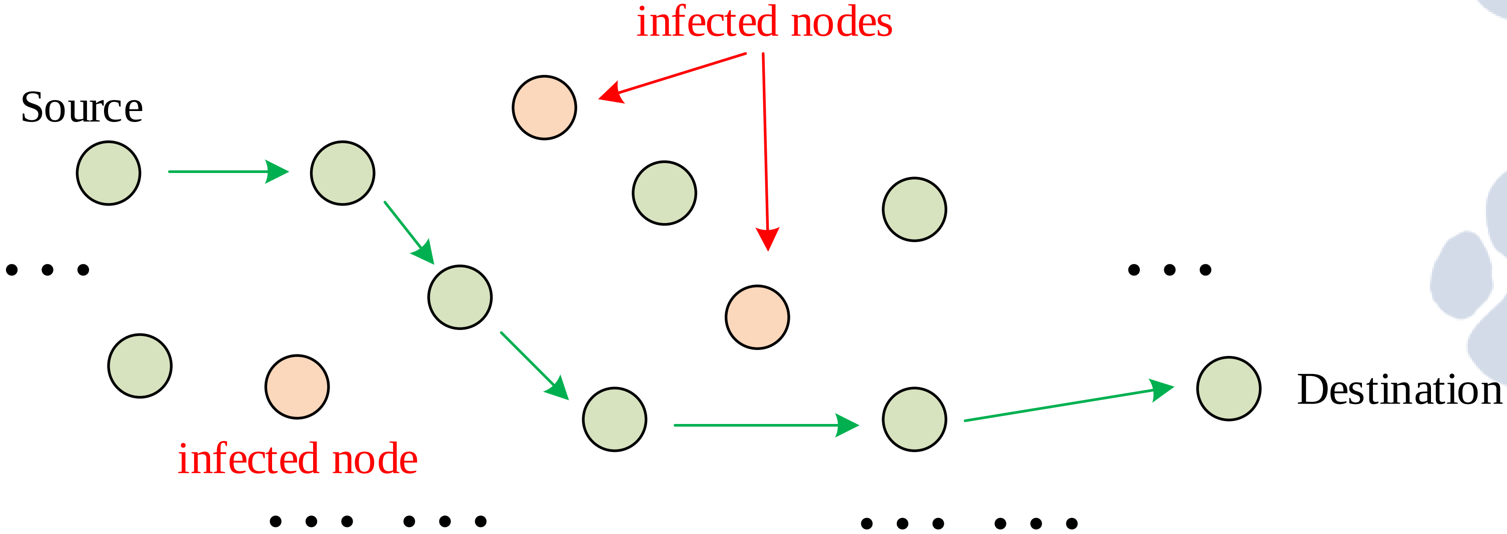
- To achieve successful army operations:
  - Protecting a critical path
  - Prolonging the network lifetime
  - Securing critical nodes
  - …

Cyber Maneuvers

- Cyber maneuver
  - an action in the cyber space towards achieving the goal in a mission
  - e.g., software upgrade, patching, node isolation/blocking, …
- Reactive or Proactive
  - reactive: face security issues then solve!
    - E.g., traditional intrusion detection
  - proactive: prevent security issues from happening (now and in the future)
    - e.g., MTD.

Our Scenario and Objective

- In a MANET deployed in adversary environment
  - Nodes can be affected by virus from an attacker because of new software vulnerability
  - **Goal: Make sure a critical path is always protected! Should we be proactive or not?**
    - **Be proactive: immediately patch a vulnerable node.**
    - **Be reactive: patch a vulnerable node when it faces threats**

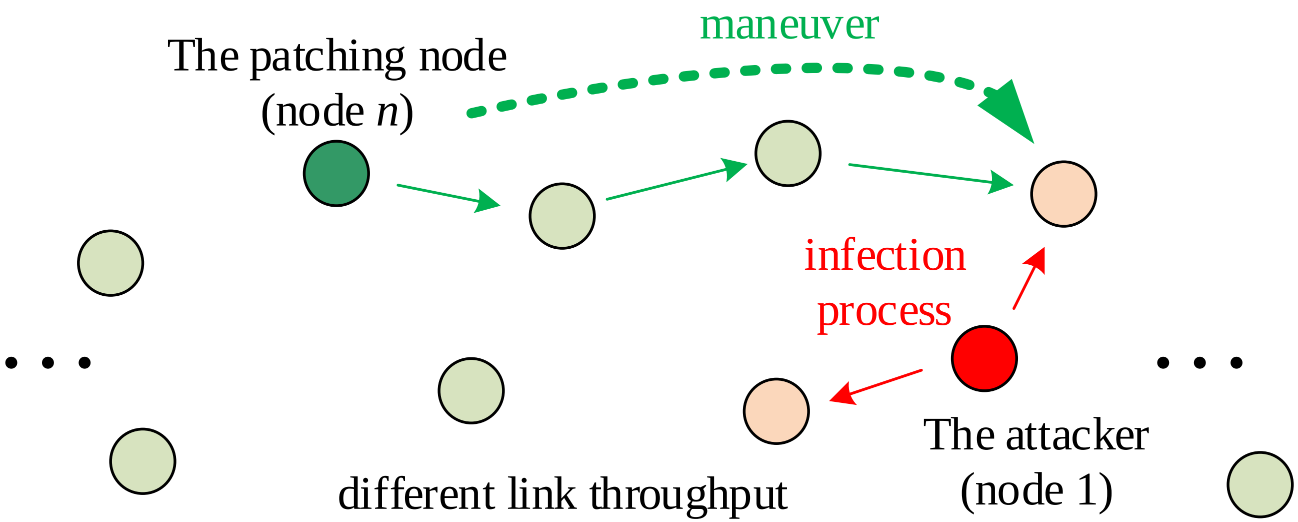


Our Analytical Framework

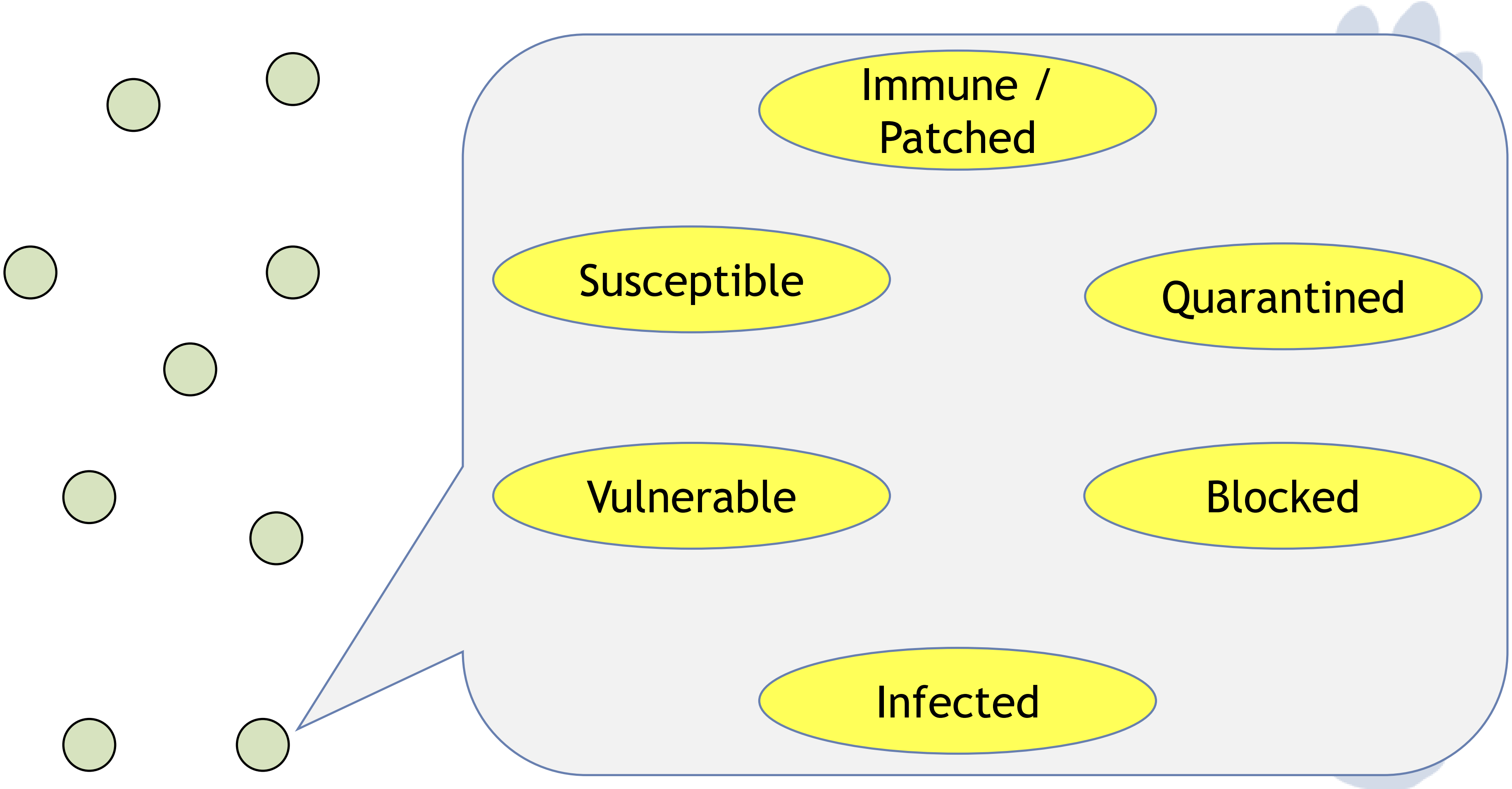
- A new framework to model the effectiveness and costs of cyber maneuvers, it integrates
  - Network model
  - Attack model
  - Cyber maneuver model
  - Cost model
  - Optimization framework

Network and Attack Scenario

- MANET: *n* nodes
  - Node 1: the attacker that infect other nodes.
  - Node *n*: patching node that performs a maneuver on nodes, e.g., patching an infected node
    - Assumption: patching node knows all info (e.g., node/link states)
  - Nodes 2-*n*: legitimate nodes that can be infected, patched.



Node States and Capabilities



The capability of a node can be defined based on its state. E.g., capability= 0 if infected

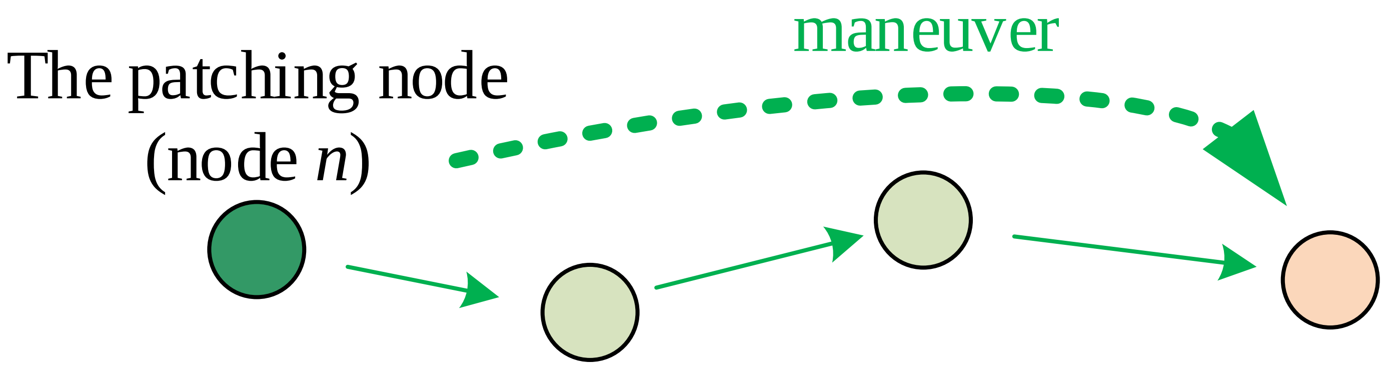
Example: Node Capability

Immune:	4
Vulnerable:	2
Susceptible:	1
Infected:	0
Blocked:	0

Positive values

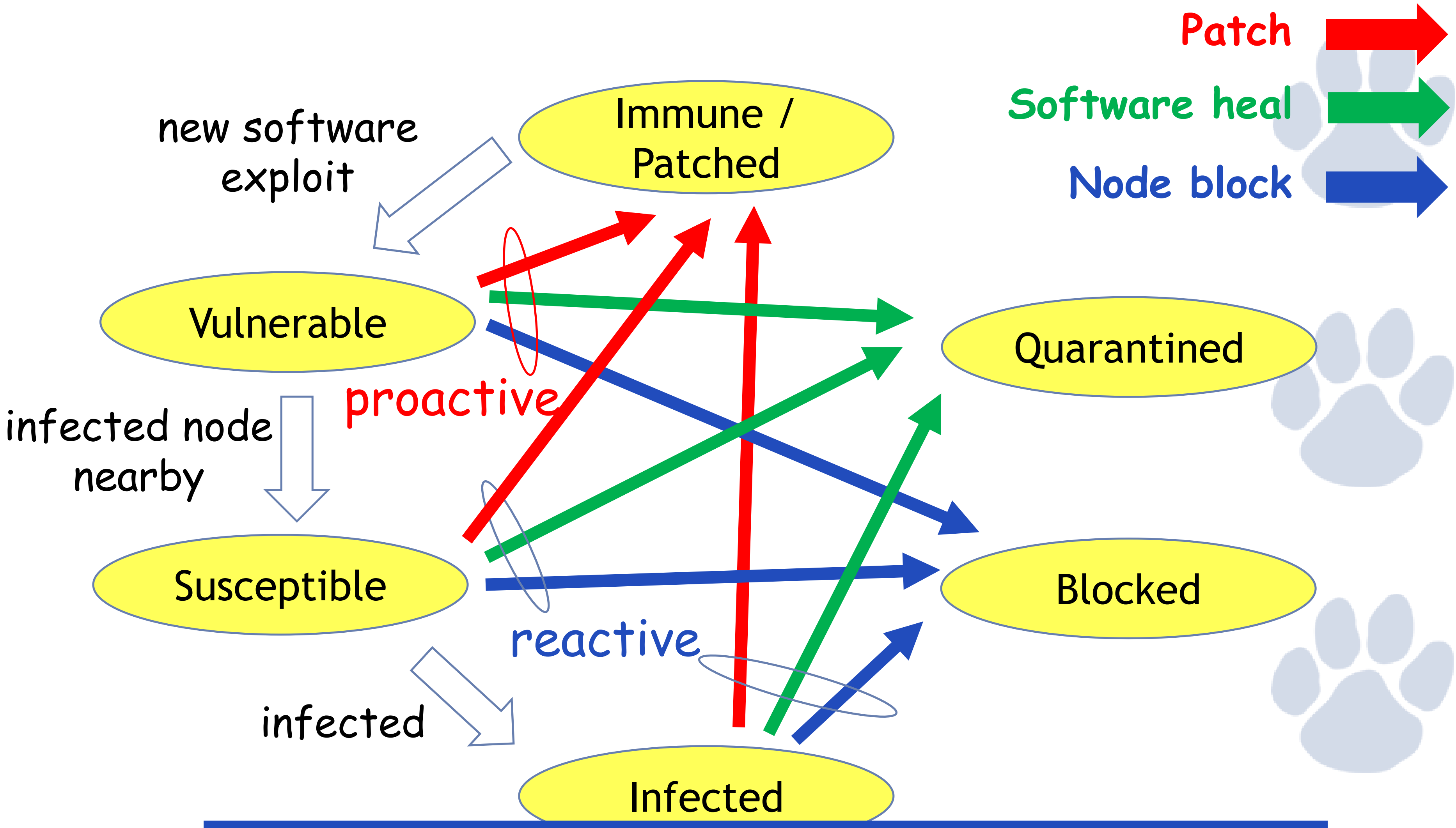
Cyber Maneuvers

- Set of cyber maneuvers



  - No Action
  - Patch ➔ Completely upgrade a node’s software
  - Software Heal ➔ partly recover the routing function
  - Node Block ➔ completely disable a node

Node State Transition



Patch

Software heal

Node block

new software exploit

Immune / Patched

Vulnerable

Quarantined

infected node nearby

proactive

Susceptible

Blocked

reactive

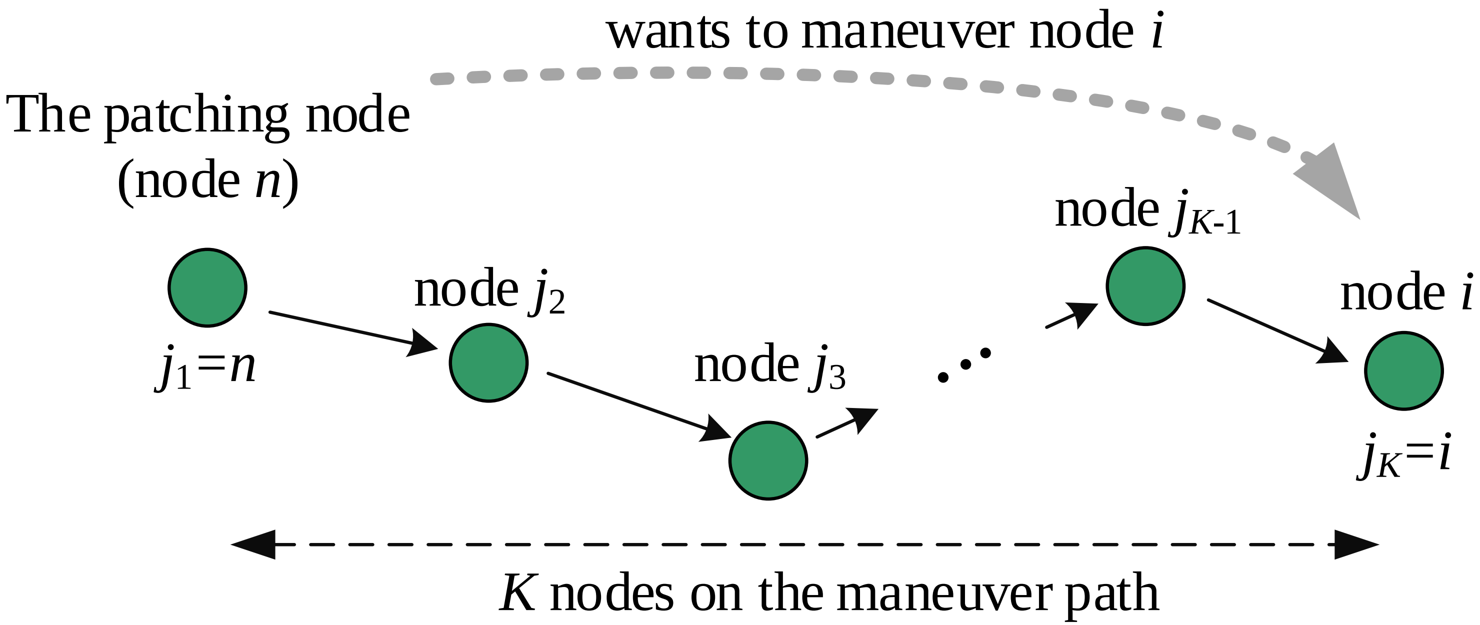
infected

Infected

Q: Should we be proactive or reactive?

Cost Model

- Energy Cost in MANETs
  - A cyber maneuver costs energy at all involved nodes.
    - Patch > Software Heal > Node Block > No Action



Optimization Goals

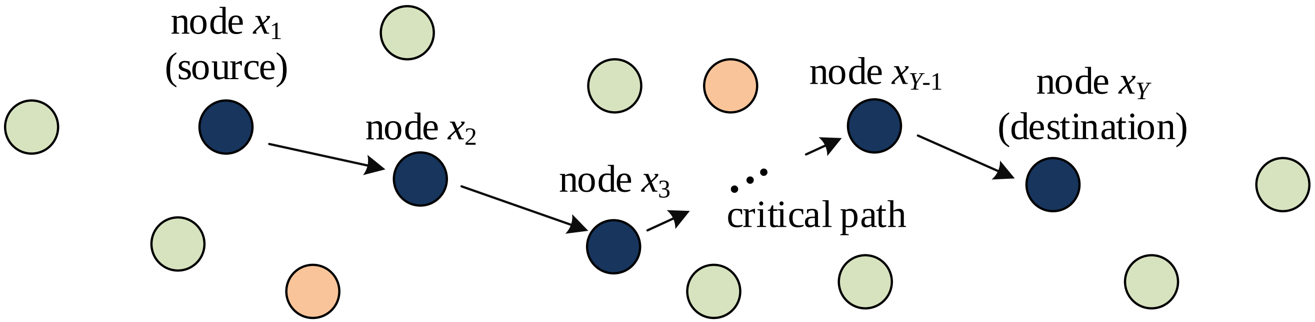
- Lots of objectives, e.g.:
  - All nodes on the path must not be infected;
  - The overall capability of the path (i.e., the sum of capabilities of all nodes on the path) should be maximized;
  - The overall capability of the network (i.e., the sum of capabilities of all nodes in the network) should be maximized;
  - The cost to protect such a path should be minimized.
- Cannot be all met at the same time!

Our Strategy

- Maximize one objective: (primary focus)
  - maximize the lifetime of a critical path
- Add multiple constraints:
  - E.g., the total capability in the network, on the path, the cost of the maneuver.
- Based on two views:
  - Current view (cannot predict the future).
  - Statistical view (can somehow predict the future)
    - e.g., statistical consumption of energy, node mobility, …

Our Formulation I

- Based on current view of the network: have all node info (e.g., remaining energy, link rate), but no future info (e.g., who nodes will move)



$$
\begin{array}{rl}
\text{maximize:} & \min\{E_{x_y} - e_{m,x_y}\}_{y\in[1,Y]} \\
\text{choose maneuver } M_m & \\
\text{subject to} & s^*_{x_y} \in \mathcal{S}^* \text{for all } y \in [1,Y], \\
& \Sigma_{y=1}^{Y} C(s^*_{x_y})/Y \geq C^*_{path}, \\
& \Sigma_{i=2}^{n-1} C(s^*_i)/Y \geq C^*_{network}, \\
& c_{m,q} \leq c^*, \\
& M_m \text{ is energy-feasible},
\end{array}
$$

Maximize the minimum

All nodes on the critical

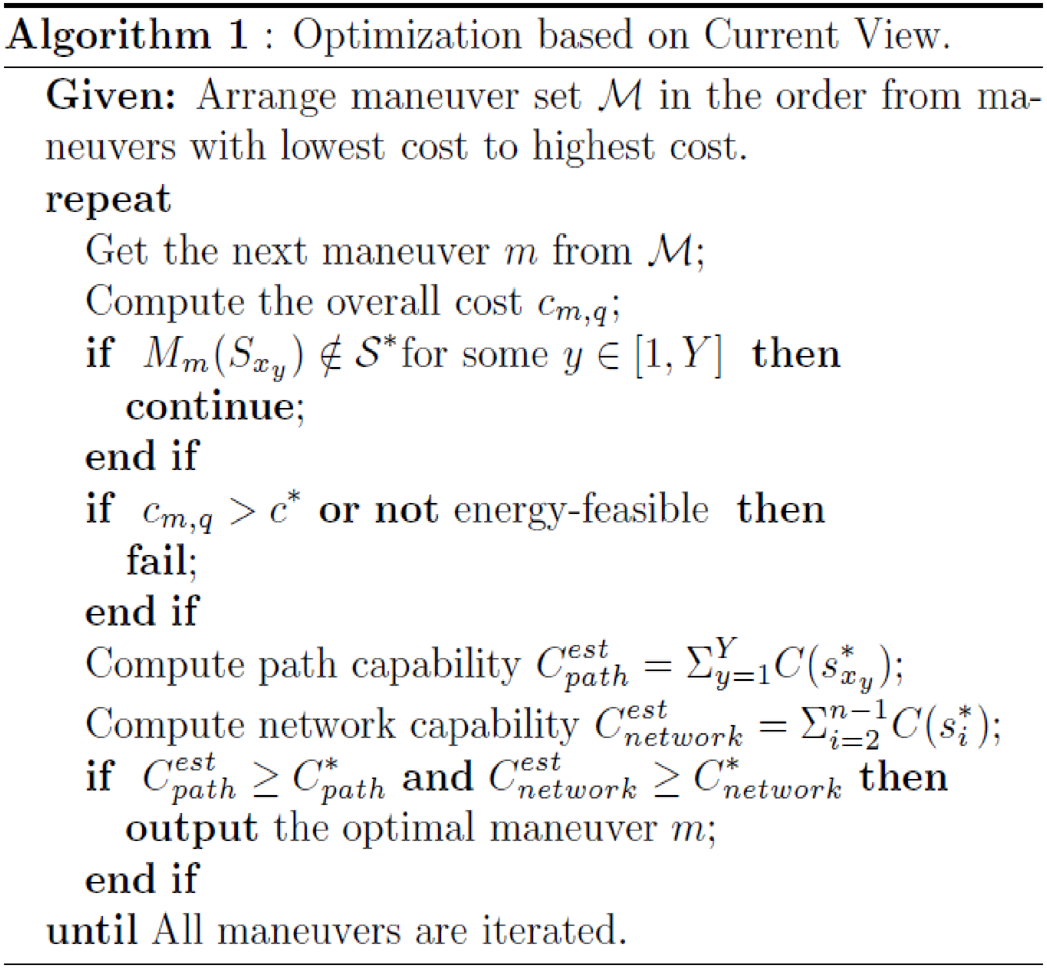
The total capability on

The total capability in

All nodes involved in a cyber maneuver must have enough energy.

Solution

- Indications:
  - defer cyber maneuver (i.e., choose No Action) as much as possible unless we have to act (when the constraints do not hold)
  - Because we only have the current view, and cannot predict the future.
  - Try not to be proactive unless we have to!

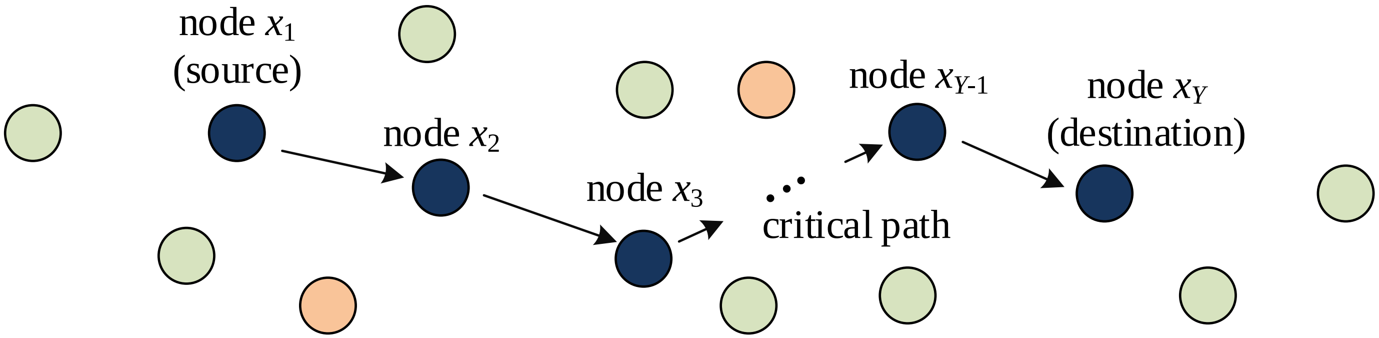


Algorithm 1 : Optimization based on Current View.

```
Given: Arrange maneuver set $\mathcal{M}$ in the order from maneuvers with lowest cost to highest cost.
repeat
    Get the next maneuver $m$ from $\mathcal{M}$;
    Compute the overall cost $c_{m,q}$;
    if $M_m(S_{x_y}) \notin \mathcal{S}^*$ for some $y \in [1, Y]$ then
        continue;
    end if
    if $c_{m,q} > c^*$ or not energy-feasible then
        fail;
    end if
    Compute path capability $C^{est}_{path} = \Sigma_{y=1}^{Y} C(s^*_{x_y})$;
    Compute network capability $C^{est}_{network} = \Sigma_{i=2}^{n-1} C(s^*_i)$;
    if $C^{est}_{path} \geq C^*_{path}$ and $C^{est}_{network} \geq C^*_{network}$ then
        output the optimal maneuver $m$;
    end if
until All maneuvers are iterated.
```

Formulation II

- Based on statistical view of the network:
  - Node distribution, mobility statistics, energy consumption



$$\begin{array}{ll}
\text{maximize:} & \mathbb{P}(A_\tau) \\
\text{choose } M_{m_z} \text{ on node } q_z & \\
\text{for all } z \in [1, Z] & \\
\text{subject to} & s^*_{x_y} \in \mathcal{S}^* \text{for all } y \in [1, Y], \\
& \Sigma_{y=1}^{Y} C(s^*_{x_y})/Y \geq C^*_{path}, \\
& \Sigma_{i=2}^{n-1} C(s^*_i)/Y \geq C^*_{network}, \\
& \Sigma_{z=1}^{Z} c_{m,q_z}/Z \leq c^*, \\
& M_{m_z} \text{ is energy-feasible,}
\end{array}$$

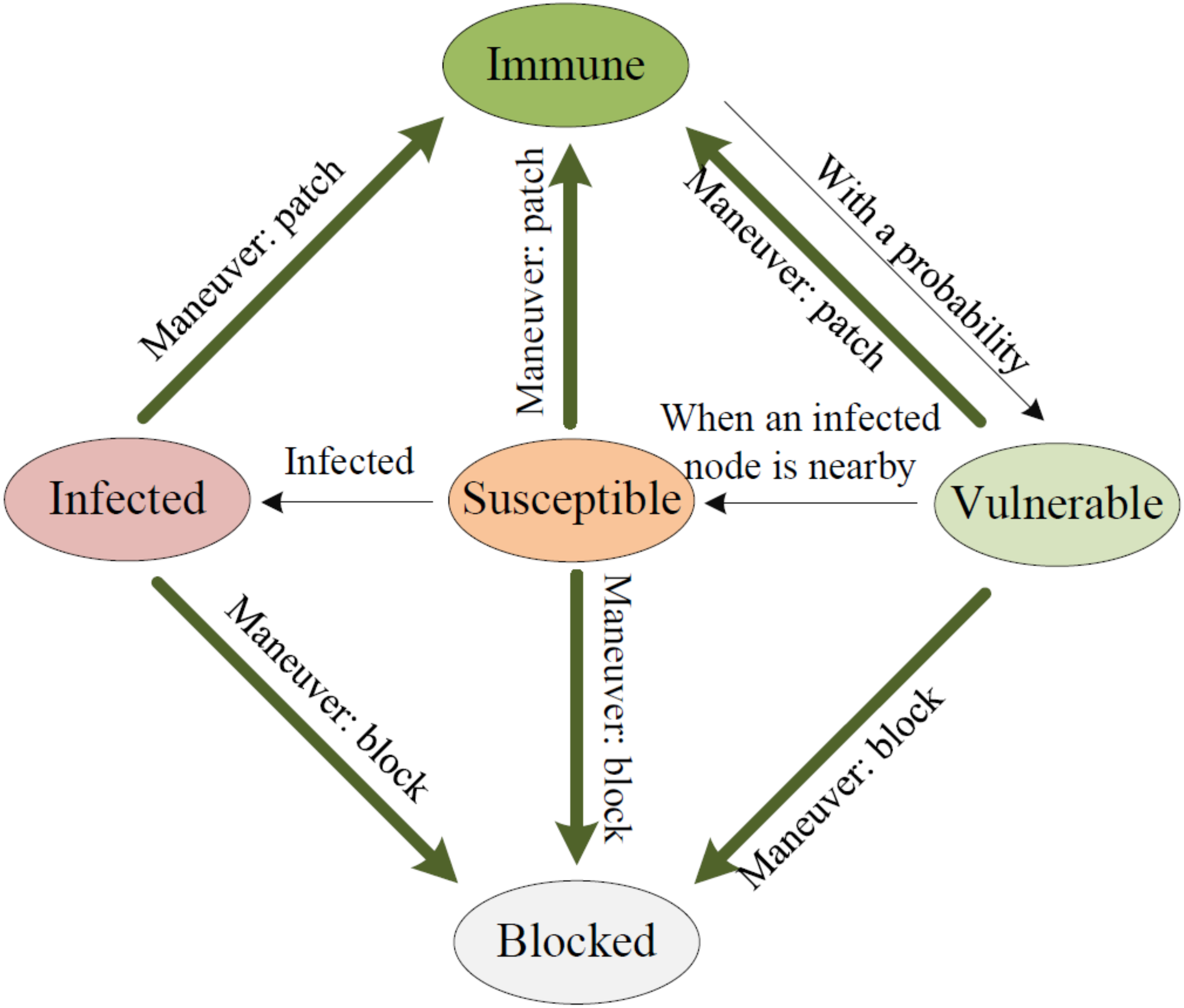
Maximize the probability that there still exists a secure critical path after time duration τ

Solution: Sufficient information gives us the best proactive solutions!

Simulation Setups

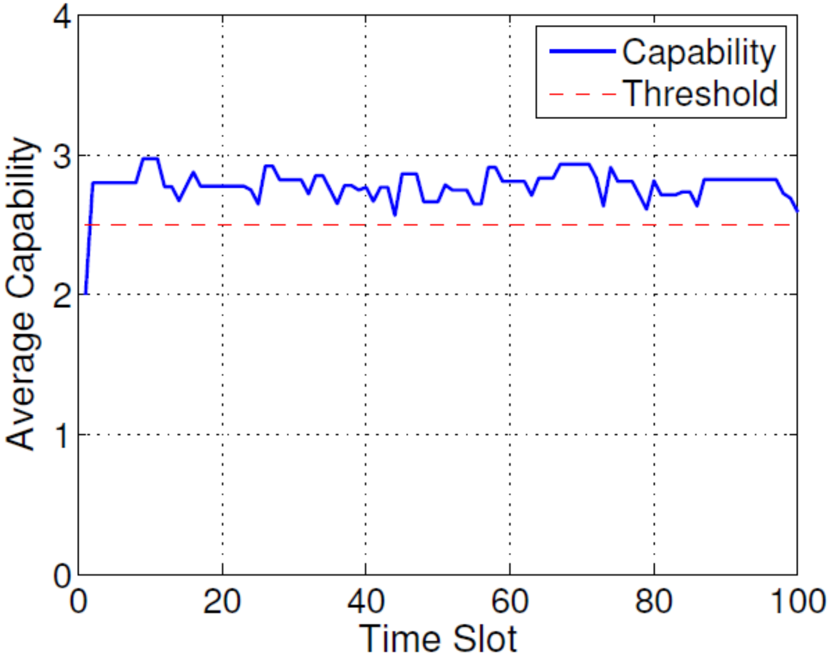
- A MANET:
  - Network size: a 1000-meter by 1000-meter region.
  - Node setups: Transmission range of 100 meters, uniformly distributed with independent mobility.
  - Energy mode: the energy consumption is a linear function of the number of traffic transmissions of each node.
  - Critical path: we randomly choose two nodes as the source and the destination
  - Attack and defense:
    - There exists an adversary in the network that attempts to infect other nodes as long as they meet.
    - The patching node aiming to make the best decision to maneuver other nodes in the network in order to maximize the lifetime of the critical path between the source and the destination.

Node States and Maneuvers

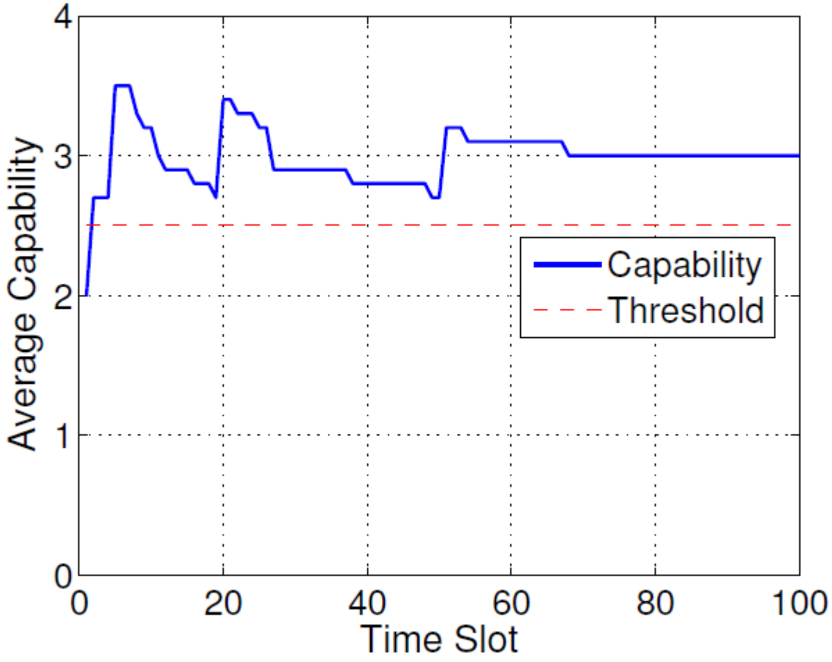


Result I

- Average capability on the critical path

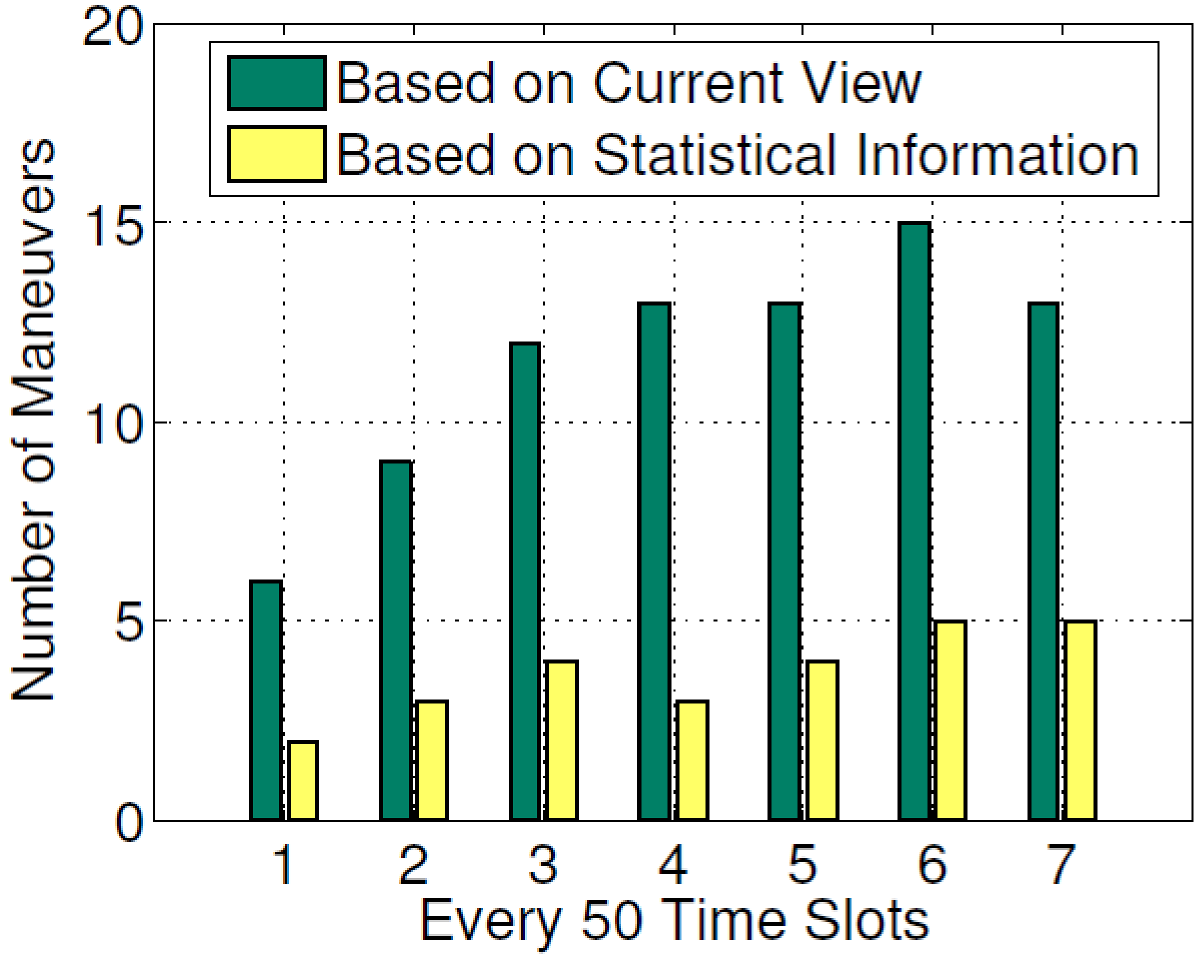


optimization based on current view

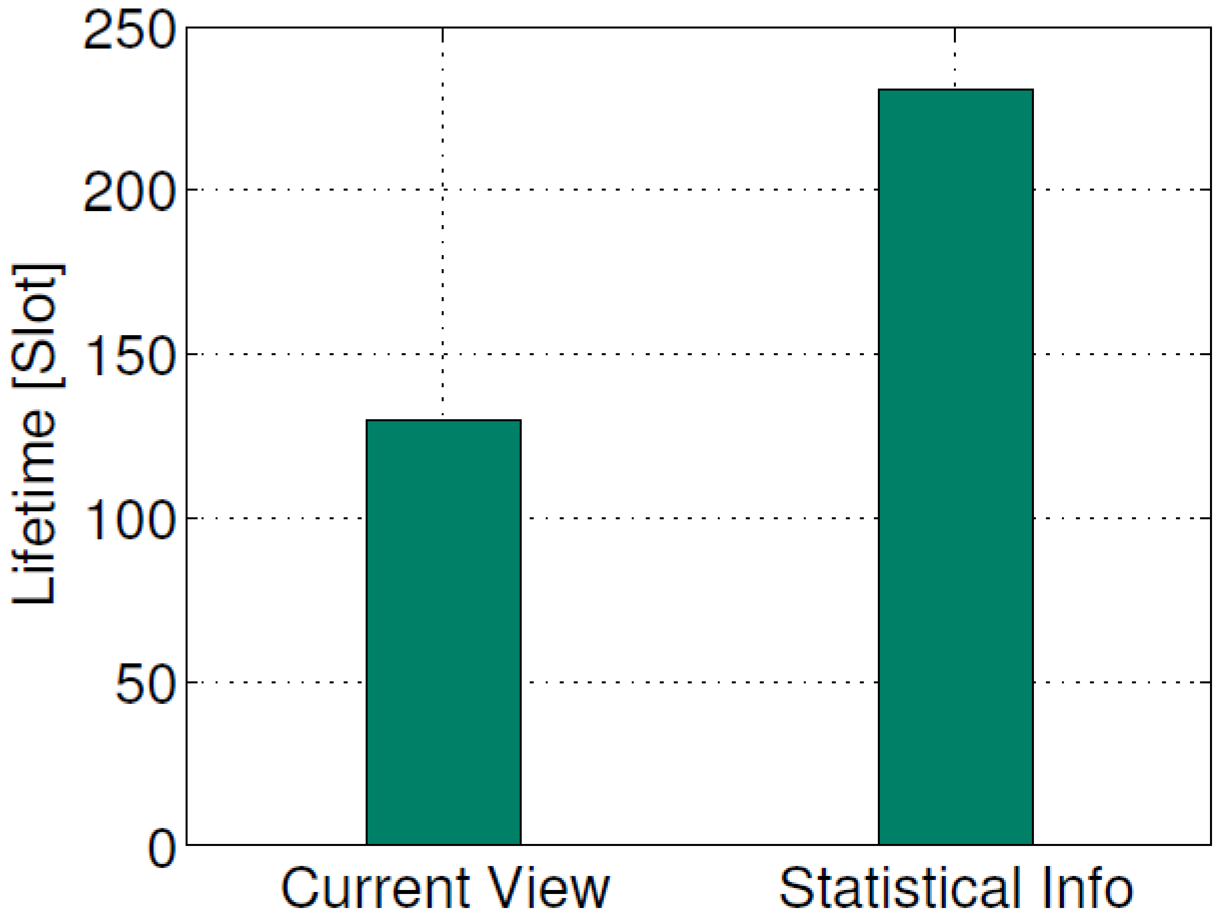


optimization based on statistical info

Result II

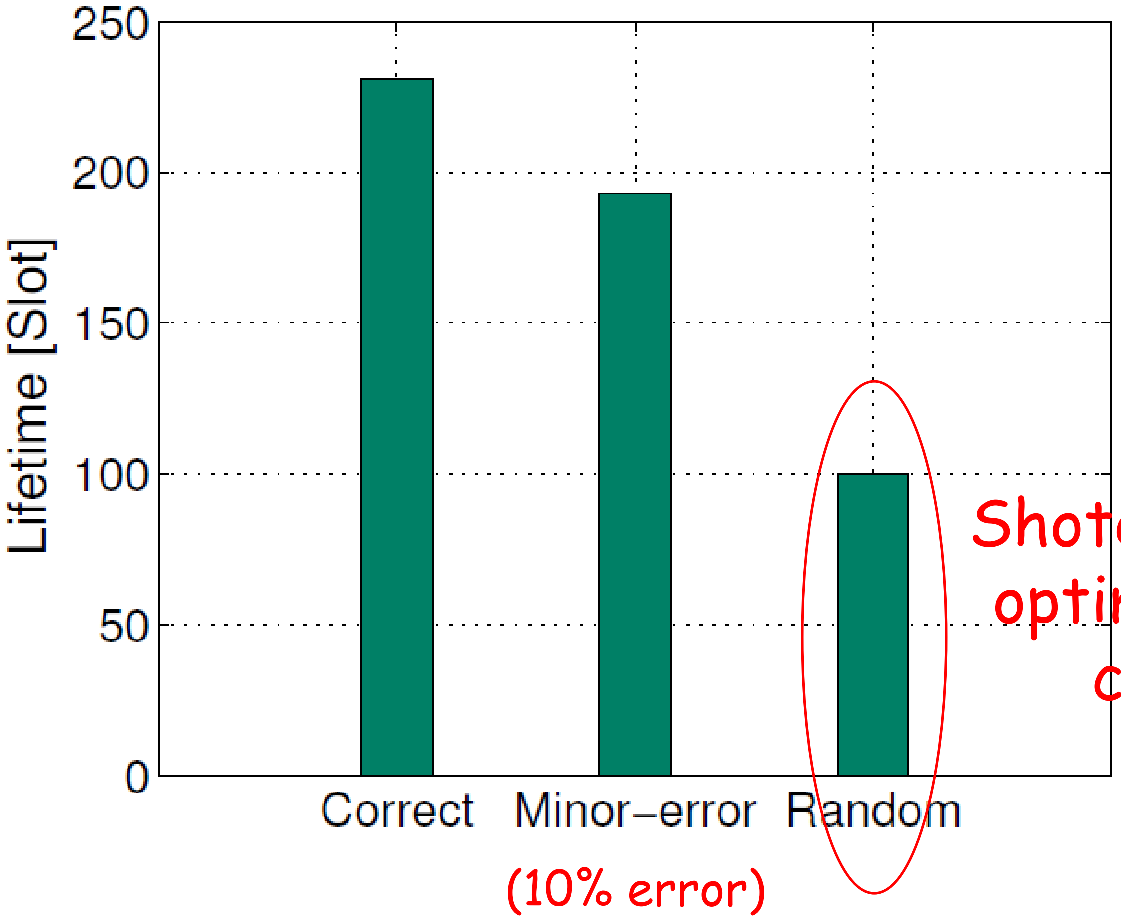

Based on Current View
Based on Statistical Information
Number of Maneuvers
0
5
10
15
20
1
2
3
4
5
6
7
Every 50 Time Slots

Result III


Lifetime [Slot]
250
200
150
100
50
0
Current View
Statistical Info

Result IV

- If there is an error in statistic info



(10% error)

Shoter than lifetime optimized based on current view

Conclusions

- A framework to model cyber maneuvers
  - Easily adopt more node states, maneuvers, cost models, …
- Accurate statistical info is a key enabler for proactive cyber maneuvers for critical path protection
  - If we only have current view, defer proactive strategies
  - If we have sufficient statistical info, choose the best proactive strategies based on the optimization framework.
  - Wrong statistical info may lead to worse performance
- More to improve:
  - Information collection.
  - Trust on a path.
  - Fine-grained statistical error analysis.

рахмат
danke
謝謝
spas
ngiyabonga
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
gracias
хвала
kiitos
dankie
nanni
nandri
dhanyavad
asante
manana
thank you
bedankt
bayarlalaa
gracie
hvala
mauruuru
köszönöm
dankon
ačiū
akun
obrigada
tenki
enkosi
djiere dieuf
tau
mochchakkeram
murakoze
shukriya
дякую
mamnun
dziękuję
chnorakaloutioun
gratias ago
gracies
sulpáy
taiku
go raibh maith agat
sobodi
děkuji
sagolun
sukriya
kop khun krap
obrigado
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
kam sah hamnida
rahmat
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
merce
мерси
তোমাকে ধন্যবাদ
감사합니다
xiexie
merci