Science-Based Metrics for Network Topology Resilience Against Attacks

Assane Gueye

Dept. of Electrical and Computer Engineering
University of Maryland, College Park

Information Technology Laboratory
National Institute of Standards and Technology

Director of Research, IPROSI
Institut Professionnel pour la Securité

Colloque sur la Cryptographie et les Codes Correcteurs d'Erreurs
Université Cheikh Anta Diop, Dakar-SN
December 3-11, 2015

Joint work with:

Dr. Aron Lazska (Vanderbilt University), Prof. Jean C. Walrand, Prof. Venkat Anantharam (UC Berkeley)

Disclaimer!

- **Top-Down approach**
  - **Daily operations and management, access control, patches & upda**
  - **Short term**
- **Bottom-Up Approach**
  - **Mathematical models and Analysis**
  - **Science for (cyber)security**
  - **Long term**

Source: T. Alpcan, T. Basar; Network Security: A Decision and Game Theoretic Approach

Motivations

Our Nation's cybersecurity strategy is twofold: **(1) improve our resilience to cyber incidents** and **(2) reduce the cyber threats**
Source: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

However…

*"**When you can measure** what you are speaking about, and express it in numbers, **you know something** about it; but **when you cannot measure** it, when you cannot express it in numbers, **your knowledge is of a meagre and unsatisfactory kind**; it may be the beginning of knowledge, but you have scarcely in your thoughts advanced to the state of Science, whatever the matter may be."*

Need: Quantification of security risk
Develop sound security/robustness metrics

Motivations

- Quantification of security risk, Security metrics

  - **Some people think it is infeasible!**

    On the Brittleness of Software and the Infeasibility of Security Metrics

    Steven M. Bellovin, IEEE Security & Privacy, (Volume:4 , Issue: 4), July-Aug. 2006

  - **Common attempts…**
    - **Vendors**: Critical, High, Medium, Low
    - NVD+CVSS

Motivations

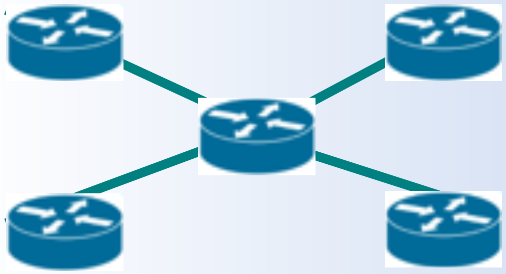
- Deriving **sound security/robustness metrics** is challenging!

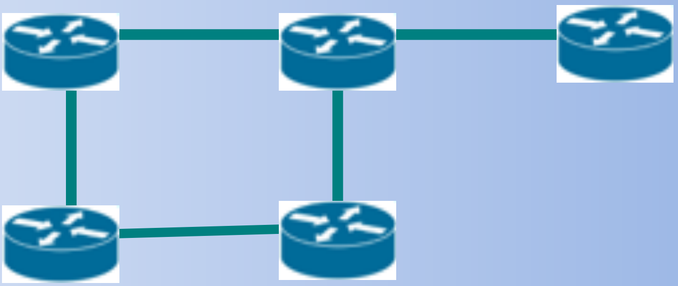
Example: **robustness of network topology**

- Conventional wisdom

  connectivity = *minimum number of nodes (or edges) whose removal disconnects the graph (**min-cut**)*

- **Simple**, but...





- Both networks **have a node-connectivity of 1**

  ➔ Equally robust!

  Right?

Motivations

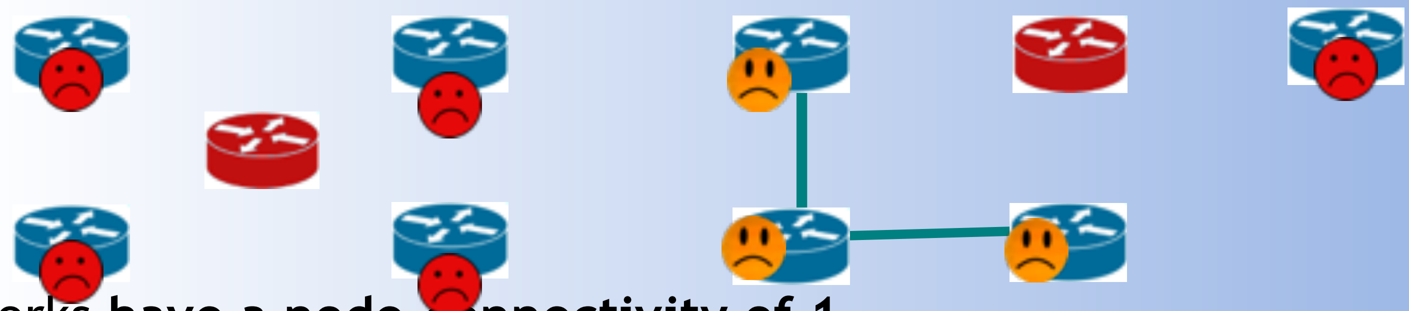
- Deriving **sound security/robustness metrics** is challenging!

Example: **robustness of network topology**

- Conventional wisdom

  connectivity = *minimum number of nodes (or edges) whose removal disconnects the graph (**min-cut**)*

- **Simple**, but...



- Both networks **have a node-connectivity of 1**

  ➔ Equally robust!

  ~~Right~~? **Not Really!**

Motivations

- Deriving **sound security/robustness metrics** is **challenging**!

  - **Adversarial nature of the problem**

    "… uses knowledge about network to design strategy in anticipation to adversary action...

  - **Our approach:**

    Game theory-based

Security & Game Theory

Rational: Mathematical formulation to capture interaction between defender and attacker

Illustrations:

(a) PROTECT is being used in Boston (b) Extending PROTECT to NY

Figure 1: USCG boats patrolling the ports of Boston and NY

Game Theory for Airport Security

ARMOR (LAX)

Airports create security systems and terrorists seek out breaches.

Placing checkpoint

Allocate canine units

Outline

1. **Game Theory 101**
2. **Robustness of Sensor and Access Networks**
3. **Vulnerability Metric**
4. **Summary**

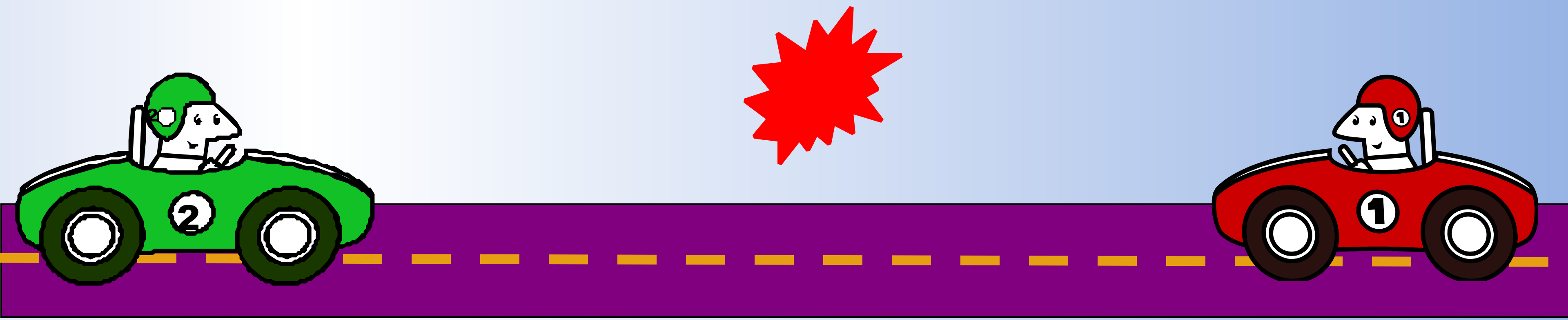
What is Game Theory?

Game theory studies the strategies people use when
making decisions.

Assumptions:

- Rationality
- Interdependency
- Selfishness
- Maliciousness
- Conflict of Interest

Example 1:
Game of Chicken

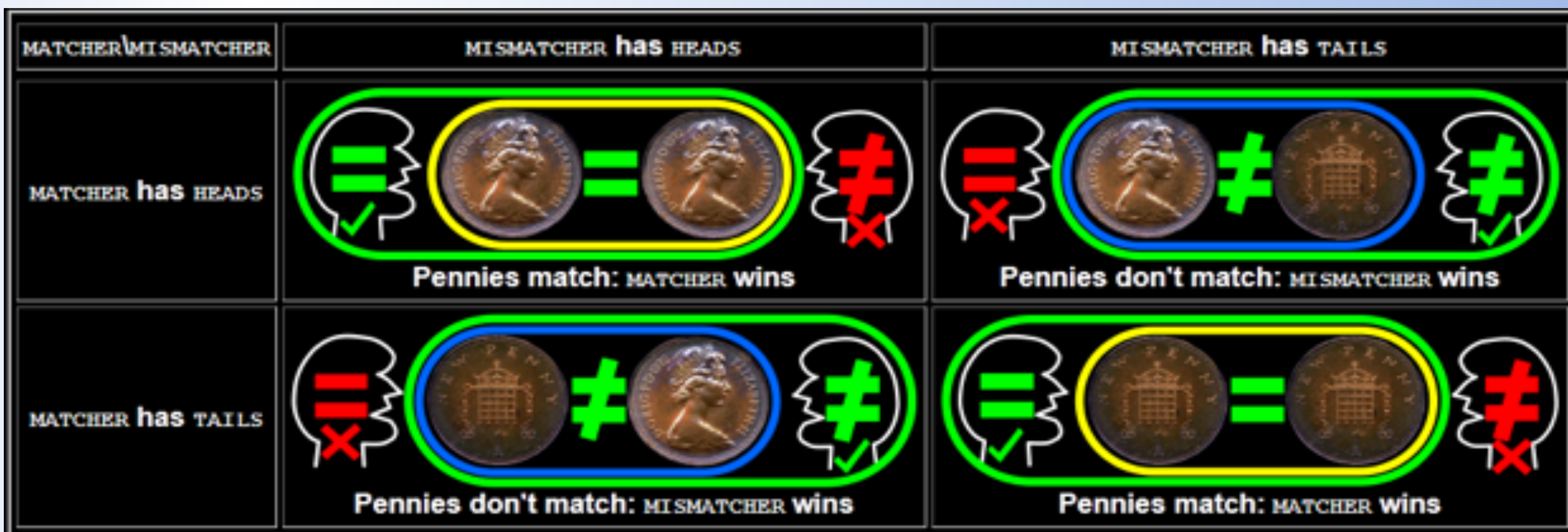


- First driver who steers away loses
- If they both stay on the road: CRACH

- What would you do?

- **Game Theory helps predict each driver’s decision**

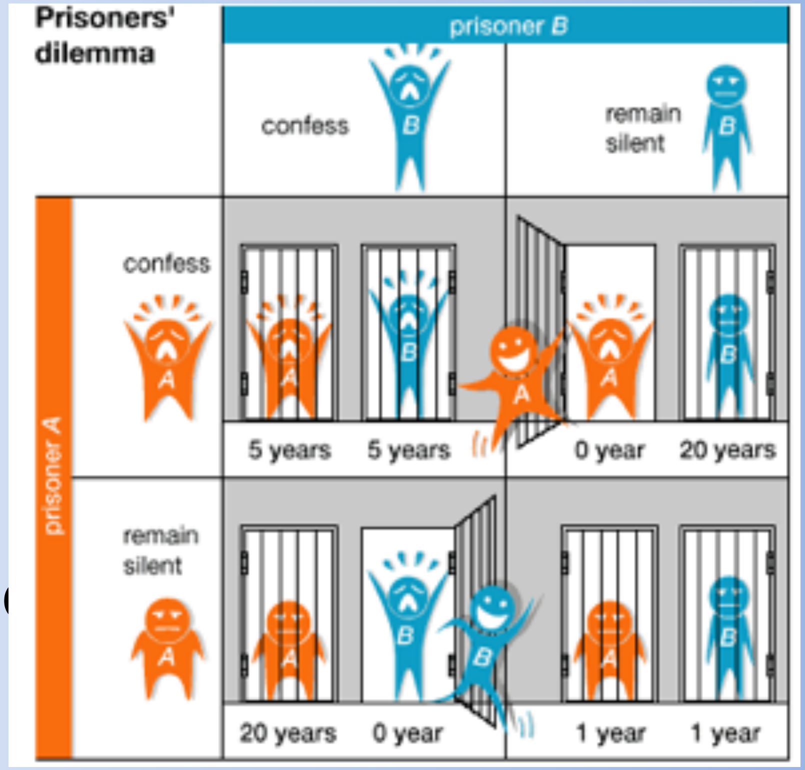
Example 2: Matching Pennies



- **Game Theory helps predict players' decision**

Example 3: Prisoners' Dilemma

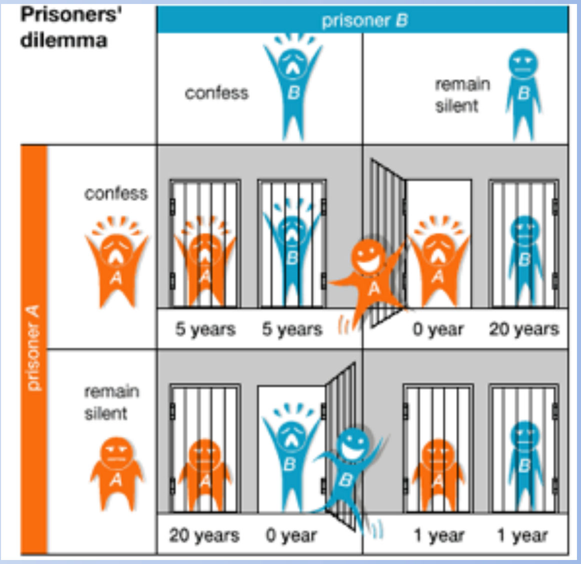
- If both confess,
  - ➔ each gets 5 years
- If both remain silent,
  - ➔ each gets 1 year
- If one confesses and one remains sil
  - ➔ 0 years for "confessee"
  - ➔ 20 year for silent



- **Game Theory helps predict prisoners' decision**

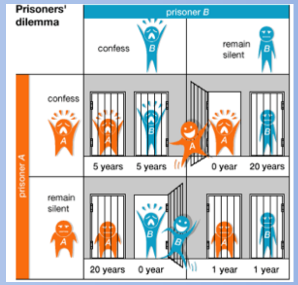
How do you predict?

- Prisoners' Dilemma
  - **Step 1: 2-by-2 Matrix Representation**
    - If PA confesses & PB confesses
      ➔ 5 years for PA and 5 years for PB
    - If PA confesses & PB remains silent
      ➔ 0 years for PA and 20 years for PB
    - If PA is silent & PB confesses
      ➔ 20 years for PA and 0 years for PB
    - If PA is silent & PB is silent
      ➔ 1 year for PA and 1 year for PB



		Prisoner B	
		confess	silent
Prisoner A	confess	(5 , 5)	(0 , 20)
	silent	(20 , 0)	(1 , 1)

How do you predict?



- Prisoners' Dilemma
  - **Step 2: Analyze the matrix**

Prisoner B

Prisoner A	confess	silent
confess	(5 , 5)	(0 , 20)
silent	(20 , 0)	(1 , 1)

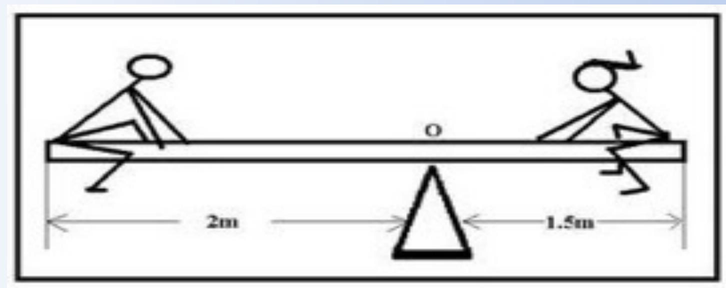
- **Suppose PA chooses "silent"**
  ➔ PB's best response if to choose "confess"
- **Suppose PA chooses "confess"**
  ➔ PB's best response if to choose "confess"

Conclusion: Both prisoners will confess (and get 5 years each)!

Remark: No matter what PA does, PB will always confess

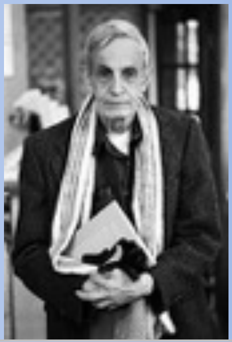
Similarly: No matter what PB does, PA will always confess

Nash equilibrium



"...a point of the game, in which no player has anything to gain by unilaterally changing his own strategy..."

		Prisoner B	
		confess	silent
Prisoner A	confess	(5 , 5)	(0 , 20)
	silent	(20 , 0)	(1 , 1)



John F. Nash

Security & Game Theory

Rational: Mathematical formulation to capture interaction between defender and attacker

Illustrations:

Network Blocking Game
Intelligent Virus Game
Intruder Game

SSI

A Framework for Analyzing Network Resilience Against Attacks

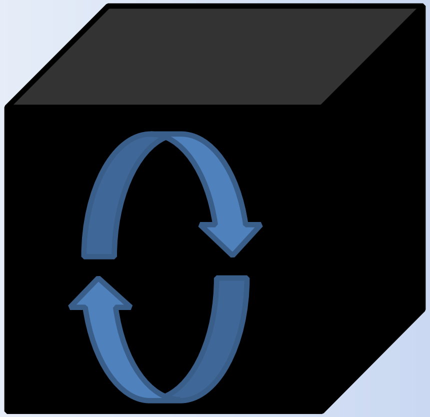
Assane Gueye, Jean Walrand: A Game Theoretic Approach to Communication Security, CDC 2008, Cancun, Mexico

Network Blocking Games

Network topology

Network operation

Loss in connectivity



2-Player game

Payoff function

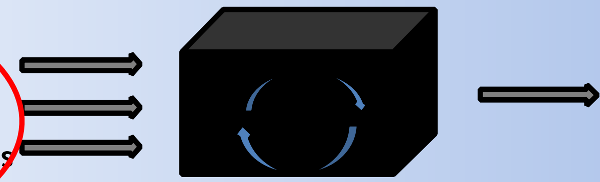
Nash equilibrium characterization

Vulnerability metrics

Identification of most critical links

NBG (1)

Network Topology
Network Operation
Network value model/Usage loss



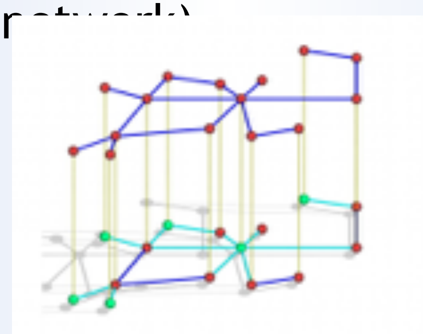
2-Player Game
Payoffs definition, NE characterization

- Vulnerability metric
- Critical subsets of links

Framework

- **Network topology**
- Network Operation
  - Connectivity
  - Loss in connectivity

  how the network functions (e.g., sensor network, backbone network)

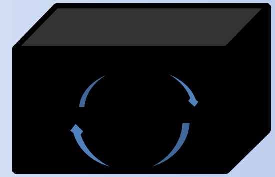


SSI*

Network topology = { Set of nodes connected by set of links

NBG (2)

Network Topology
Network Operation
Network value model/Usage loss



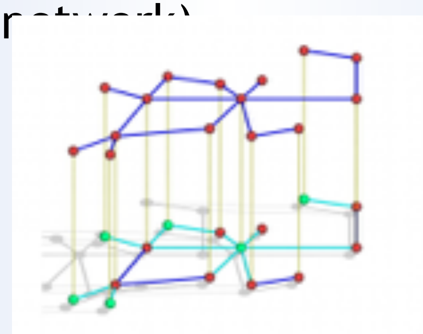
2-Player Game
Payoffs definition, NE characterization

Vulnerability metric
Critical subsets of links

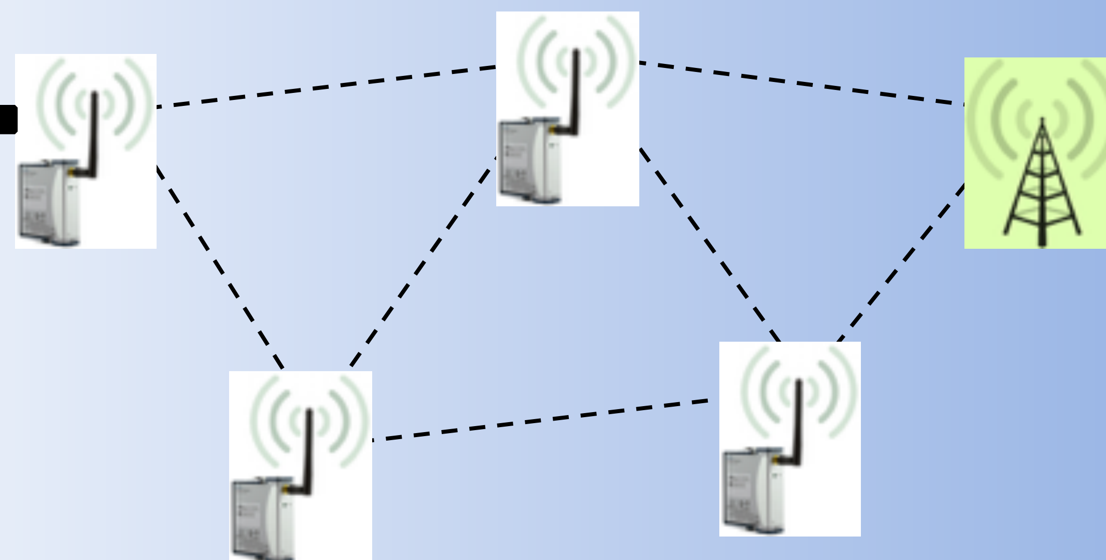
Framework

- Network topology
- **Network Operation**
  - Connectivity
  - Loss in connectivity

  how the network functions (e.g., sensor network, backbone network)



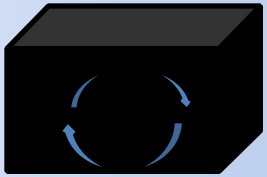
Example: Sensor and access networks



Each node has to be able to reach the gateway.

NBG (3)

Network Topology
Communication model
Network value model/Usage loss



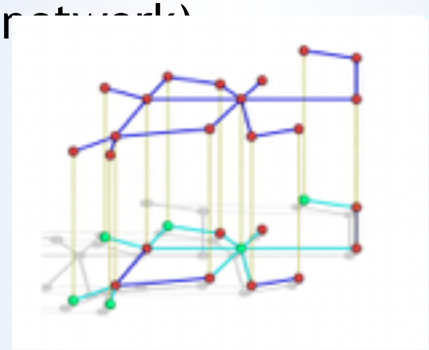
2-Player Game
Payoffs definition, NE characterization

Vulnerability metric
Critical subsets of links

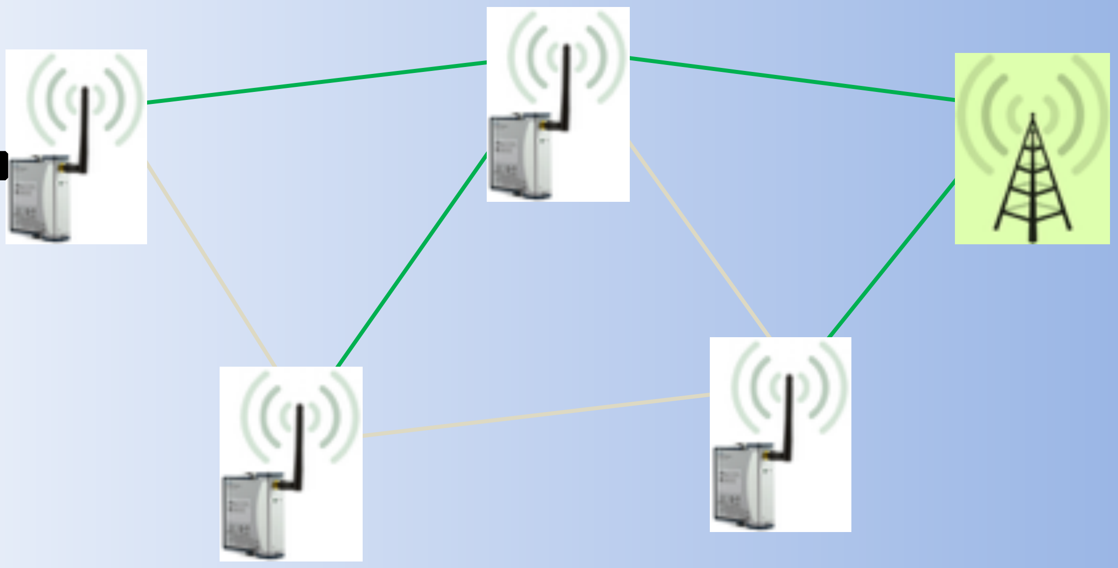
Framework

- Network topology
- **Network Operation**
  - **Connectivity**
  - Loss in connectivity

  how the network functions (e.g., sensor network, backbone network)



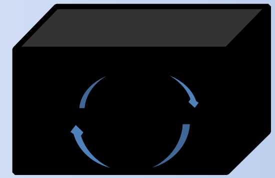
Example: Sensor and access networks



Spanning tree (rooted at gateway) (routing tables)

NBG (4)

Network Topology
Communication model
Network value model/Usage loss



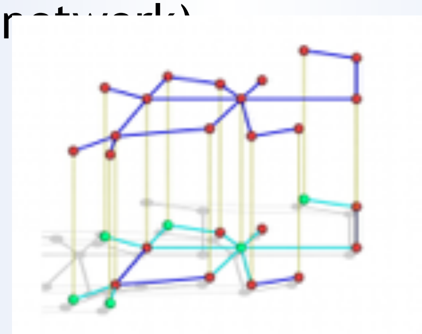
2-Player Game
Payoffs definition, NE characterization

Vulnerability metric
Critical subsets of links

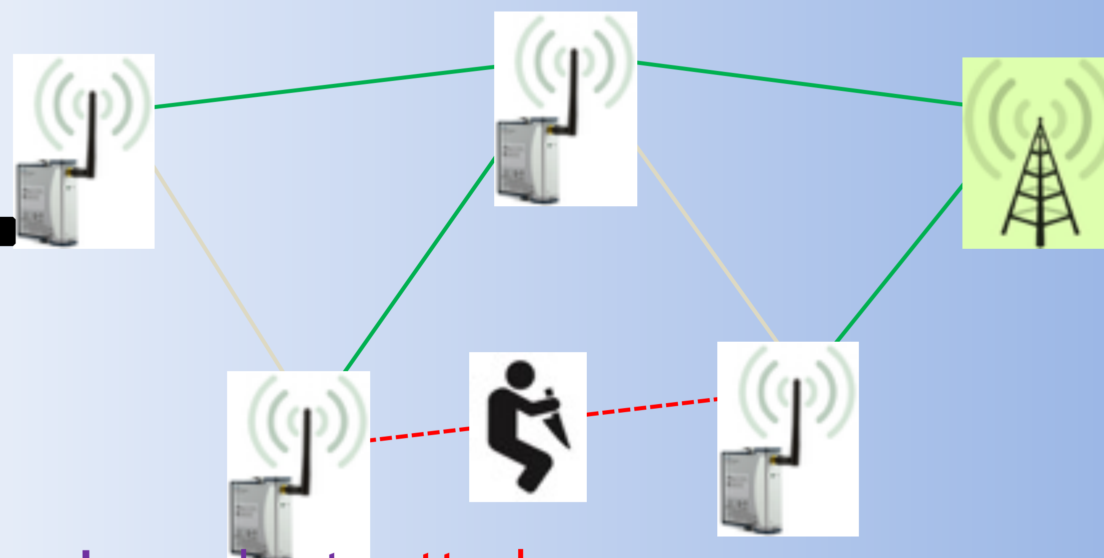
Framework

- Network topology
- **Network Operation**
  - Connectivity
  - **Loss in connectivity**

how the network functions (e.g., sensor network, backbone network)



Example: Sensor and access networks

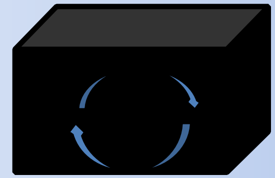


- **Loss**: due to attack
- **Attacker**: targets links to disrupt connectivity

If miss → no loss loss in connectivity (LiC)

NBG (5)

Network Topology
Communication model
Network value model/Usage loss



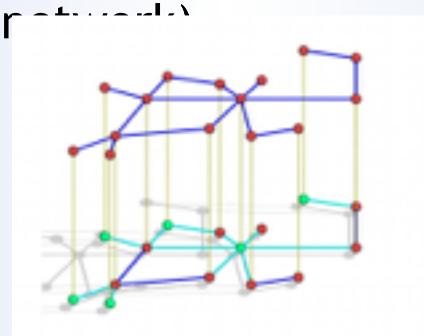
2-Player Game
Payoffs definition, NE characterization

Vulnerability metric
Critical subsets of links

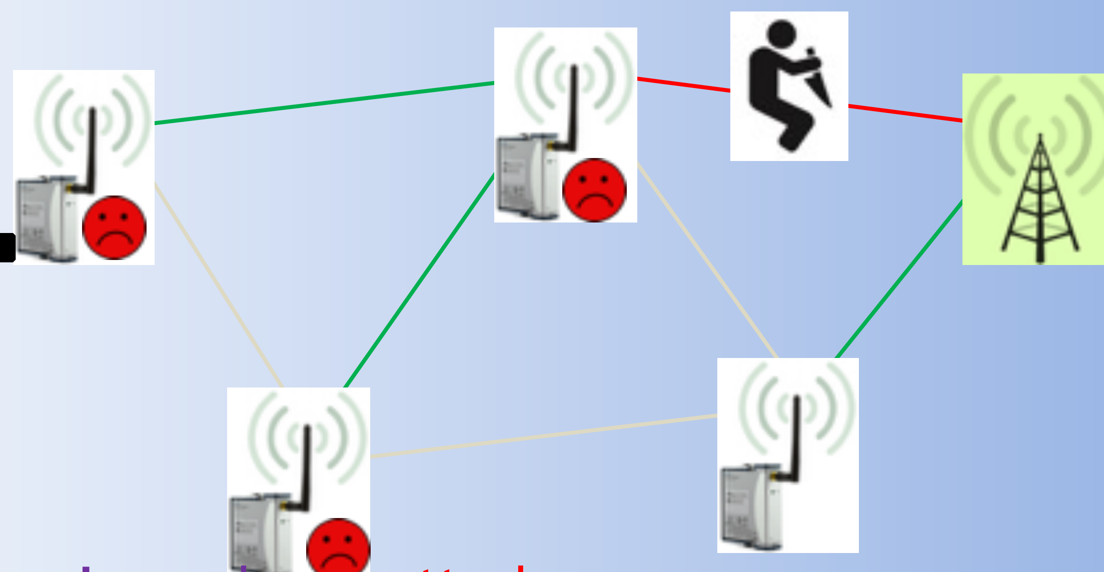
Framework

- Network topology
- **Network Operation**
  - Connectivity
  - **Loss in connectivity**

  how the network functions (e.g., sensor network, backbone network)



Example: Sensor and access networks



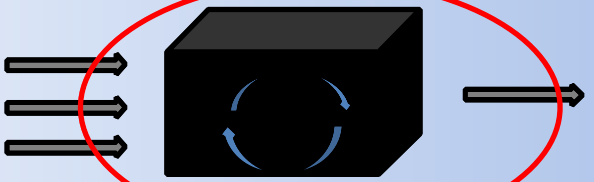
- **Loss:** due to attack
- **Attacker**: targets links to disrupt connectivity

  If miss → no loss in connectivity (LiC)

  Else → LiC = number of disconnected nodes

NBG (6)

Network Topology
Communication model
Network value model/Usage loss



2-Player Game
Payoffs definition, NE characterization

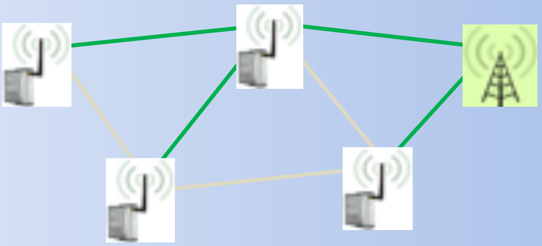
Vulnerability metric
Critical subsets of links

Framework

Players and strategies

Players:

Network Operator



Attacker

Strategies:

- **Operator**

  T∈T: feasible set of resources

  E.g.: Spanning trees, feasible flows

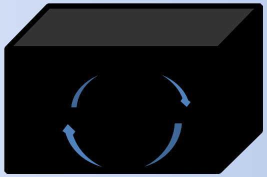
- **Attacker**

  e∈E: resource

  E.g.: links, nodes

NBG (7)

Network Topology
Communication model
Network value model/Usage loss



2-Player Game
Payoffs definition, NE characterization

- Vulnerability metric
- Critical subsets of links

Framework

- **Nash equilibrium**
- **Vulnerability metric**
- **Critical links**

Defender model + Adversary model

Network Blocking Game

Equilibrium solution

Equilibrium payoff → **Metric for vulnerability**

Computing equilibrium solution can be challenging!

Vulnerability Metrics

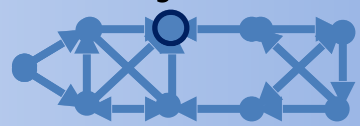
Vulnerability Metric & Graph Theory (1/4)

All-to-One Networks (e.g., Sensor Network) [3]

❖ Game

- Operator: choose a *rooted spanning arborescence*
- Attacker: Attack a link

Payoff $= \lambda(T, e) = \#$ of nodes disconnected from S associated with T and e

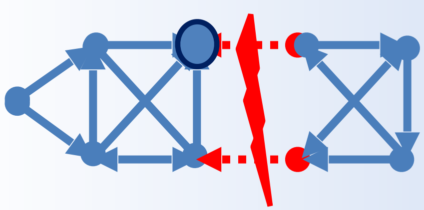


❖ **Vulnerability Metric** (= Average # of disconnected nodes per attacked link)

$$\boxed{\theta^* = max\left\{\frac{\lambda(E) - \mu(E)}{|E|} : E \subseteq \mathcal{E}(G)\right\}}$$

$\lambda(E) = \#$ *of nodes disconnected by removing links in* E

(Inverse) Directed Strength of Graph (Cunningham 1982)



$|E|=2$

$\lambda(E)=4$

❖ **Critical subset of links**: E* achieving θ^*

Uniform attack in each critical subset

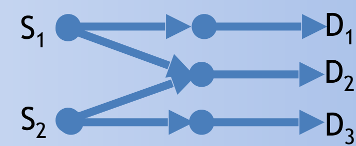
Vulnerability Metric & Graph Theory (2/4)

Many-to-Many Networks (e.g., Supply chain network)

❖ **Game**

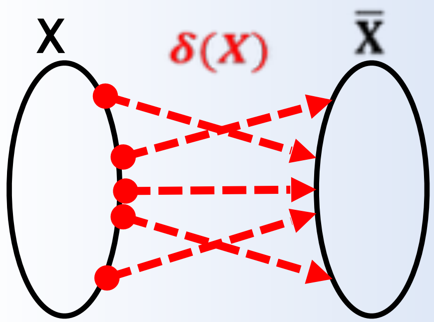
- Operator: choose a *feasible flow*
- Attacker: Attack a link

$\lambda(T, e)$ = amount of goods T carries over e



❖ **Vulnerability Metric (= Average excess demand per attacked link)**

$$\theta^* = max\left\{\frac{d(\bar{X}) - s(\bar{X}) - \mu(\delta(X))}{|\delta(X)|} : \emptyset \subset X \subseteq V\right\}$$



$\bar{X} = V - X$
$\delta(X)$= edges from X to $\bar{X}$
$d(\bar{X})$ = total demand in $\bar{X}$
$s(\bar{X})$ = Total supply in $\bar{X}$
$d(\bar{X}) - s(\bar{X})$ = excess demand in $\bar{X}$

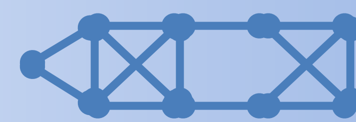
❖ **Critical subset of links: $\delta(X)^*$ for X achieving θ^***
Uniform attack in each critical subset

Vulnerability Metric & Graph Theory (3/4)

All-to-All Networks (e.g., Bridged Ethernet—linear loss), [3]

- **Game**
  - Operator: choose a *spanning tree*
  - Attacker: Attack a link

  $\lambda(T, e)$ = size of smallest connected component

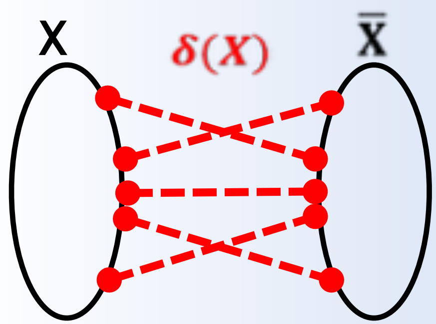


- **Vulnerability Metric** **(=Average # of disconnected nodes per links)**

$$\theta^* = \max\left\{\frac{|X| - \mu(\delta(X))}{|\delta(X)|} : \ \emptyset \subset X \subseteq V, 0 < |X| \le \frac{|V|}{2}\right\}$$

(inverse) Cheeger's constant,
Edge expansion factor of G

Note: In general the Cheeger constant is an upperbound, however, bound is tight for infinite number of graphs



$\bar{X} = V - X$
$\delta(X)$= edges between X and $\bar{X}$

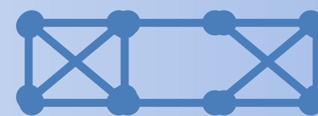
- **Critical subset of links:** $\delta(X)^*$ for X achieving θ^*
  Uniform attack in each critical subset

Vulnerability Metric & Graph Theory (4/4)

All-to-All Networks (e.g., Bridged Ethernet—constant loss) [3]

- Game
  - Operator: choose a *spanning tree*
  - Attacker: Attack a link

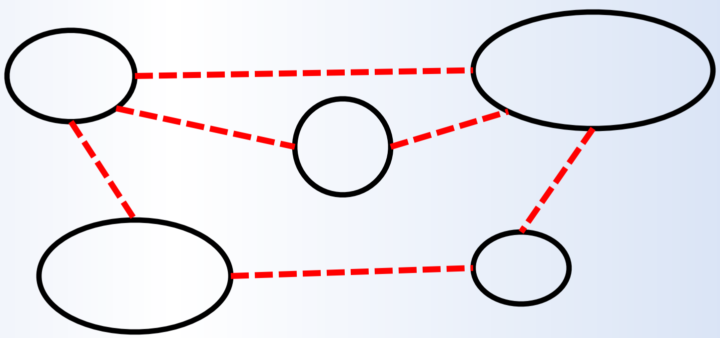
  $LiV(T,e) = \text{total value} \quad (\text{if } e \in T)$



- **Vulnerability Metric** (= Average # of (dis)connected components per attacked link)

$$\theta^* = \max\left\{\frac{Q(G\backslash E) - 1 - \mu(E)}{|E|} : E \subseteq \mathcal{E}(G)\right\}$$

Spanning Tree Packing (SPT) Number
(Tutte & Nash-Williams 1961)



E = Set of edges going across the partitions
$Q(G\backslash E)$ = number of connected components

- **Critical subset of links**: E* achieving θ^*
  Uniform attack in each critical subset

Summary

- Network topology resilience under adversarial environment
- Game theoretic framework

  - Network Topology
  - Network Operation
  - Loss in Connectivity

  2-Player Game
  - Payoff function
  - Nash equilibrium

  - Vulnerability metrics
  - Critical links

- Vulnerability metrics
  – Related to known graph theory notions
  – More suitable to adversarial environment (compared to existing ones)
  – Identification of Critical links
- Analysis tools
  – Theory of blocking pairs of polyhedron

Conclusion from Game Theory Approach

….the ability of a malicious/selfish agent to acquire and exploit system information may alter conclusions drawn by using conventional predictive security metrics…

References

[1] Assane Gueye, Aron Lazska. Network Topology Vulnerability/Cost Tradeoff: Model, Application, and Computational Complexity. *Internet Mathematics 2015* (To Appear, submitted 2014).

[2] Aron Lazska, Assane Gueye. Quantifying Network Topology Robustness Under Budget Constraints. In *4th Conference on Conference on Decision and Game Theory for Security*, November 11-12, 2013, Dallas, TX

[3] Assane Gueye, Aron Lazska, Jean C. Walrand, Venkat Anantharan. A Polyhedral-Based Analysis of Nash Equilibria of Quasi-Zero-Sum Games and its Applications to Communication Network Security. *ACM Transactions of Economics and Computation*, 2013 (In review)

[4] Assane Gueye, Vladimir Marbukh. A Game Theoretic Framework for Network Vulnerability Assessment and Mitigation, In *3rd Conference on Conference on Decision and Game Theory for Security*, November 5-6, 2012, Budapest, Hungary

[5] Assane Gueye, Jean C. Walrand, Venkat Anantharam. Design of Network Topology in an Adversarial Environment, 1st *Conference on Conference on Decision and Game Theory for Security (GameSec)*, November 22-23, 2010, Berlin

[6] Aron Laszka, Dávid Szeszlér, Levente Buttyán. Linear Loss Function for the Network Blocking Game: An Efficient Model for Measuring Network Robustness and Link Criticality. 3rd Conference on Decision and Game Theory for Security (GameSec), November 2012

Contact: agueye@umd.edu, assane.gueye@nist.gov