NSL

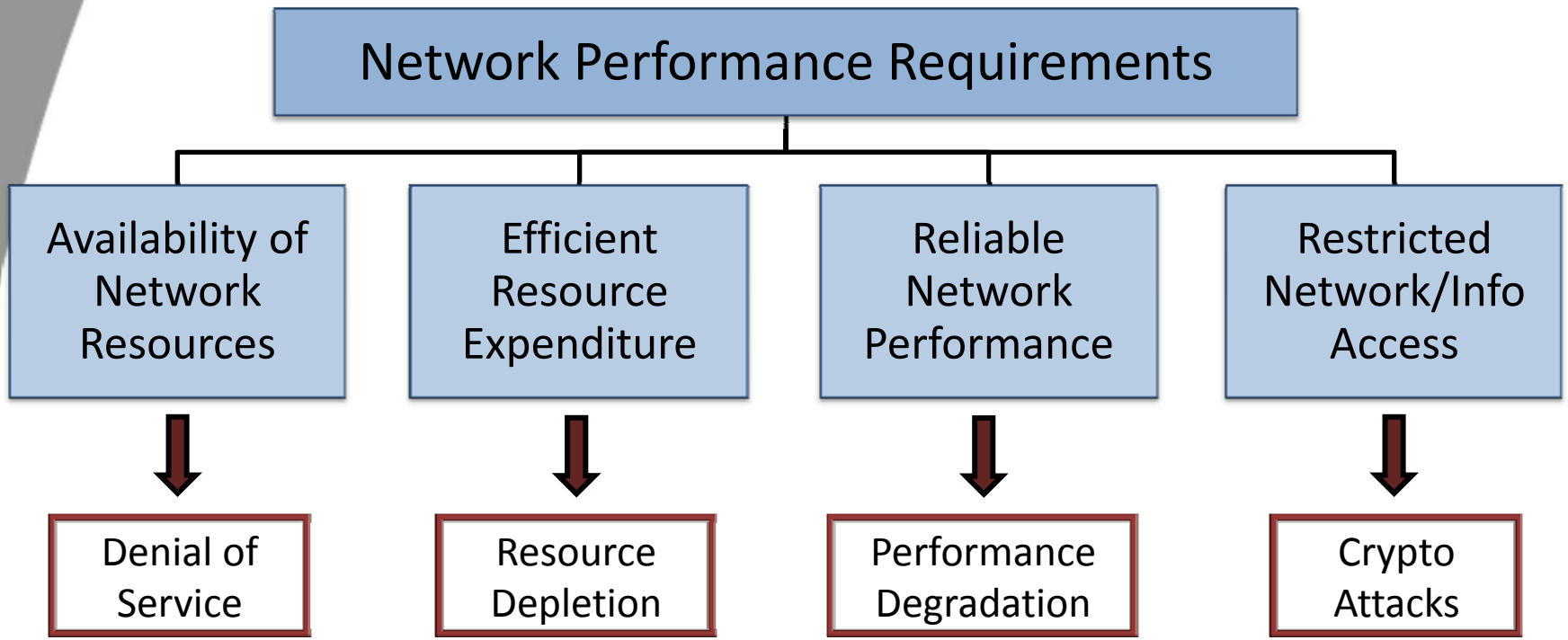
UNIVERSITY OF WASHINGTON

Network Flow Modeling of Jamming Attack

Bertinoro PhD. Summer School, July 2009

Radha Poovendran
Network Security Lab
Electrical Engineering Department
University of Washington, Seattle, WA
http://www.ee.washington.edu/research/nsl

Robust Ad-Hoc Networking



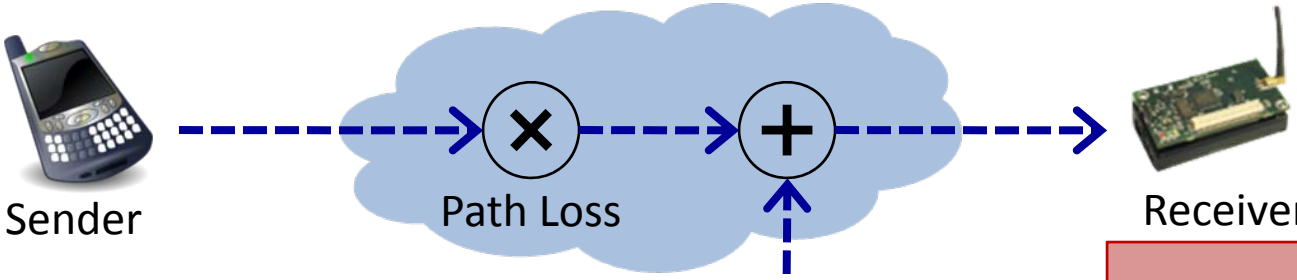
How can we enable robust network performance in the presence of adversaries?

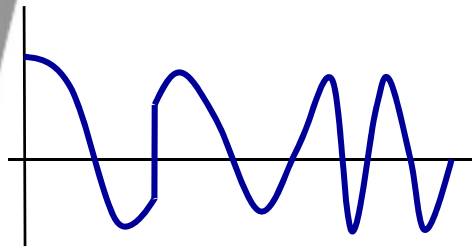
NSL

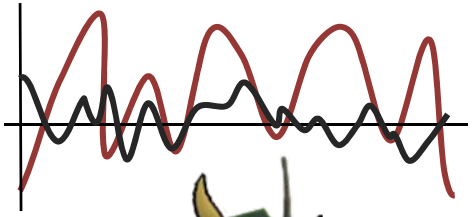
Outline for the first part

- Viewing Jamming as a network flow problem
- Linear programming models for the impact of attacks with jamming succeeds with probability one

Network Layer Impact of Jamming Attacks

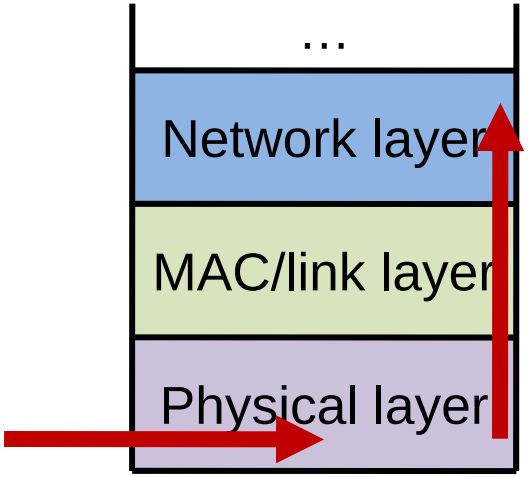






Jamming decreases *SINR*, causes ***decoding failure*** and ***packet loss***

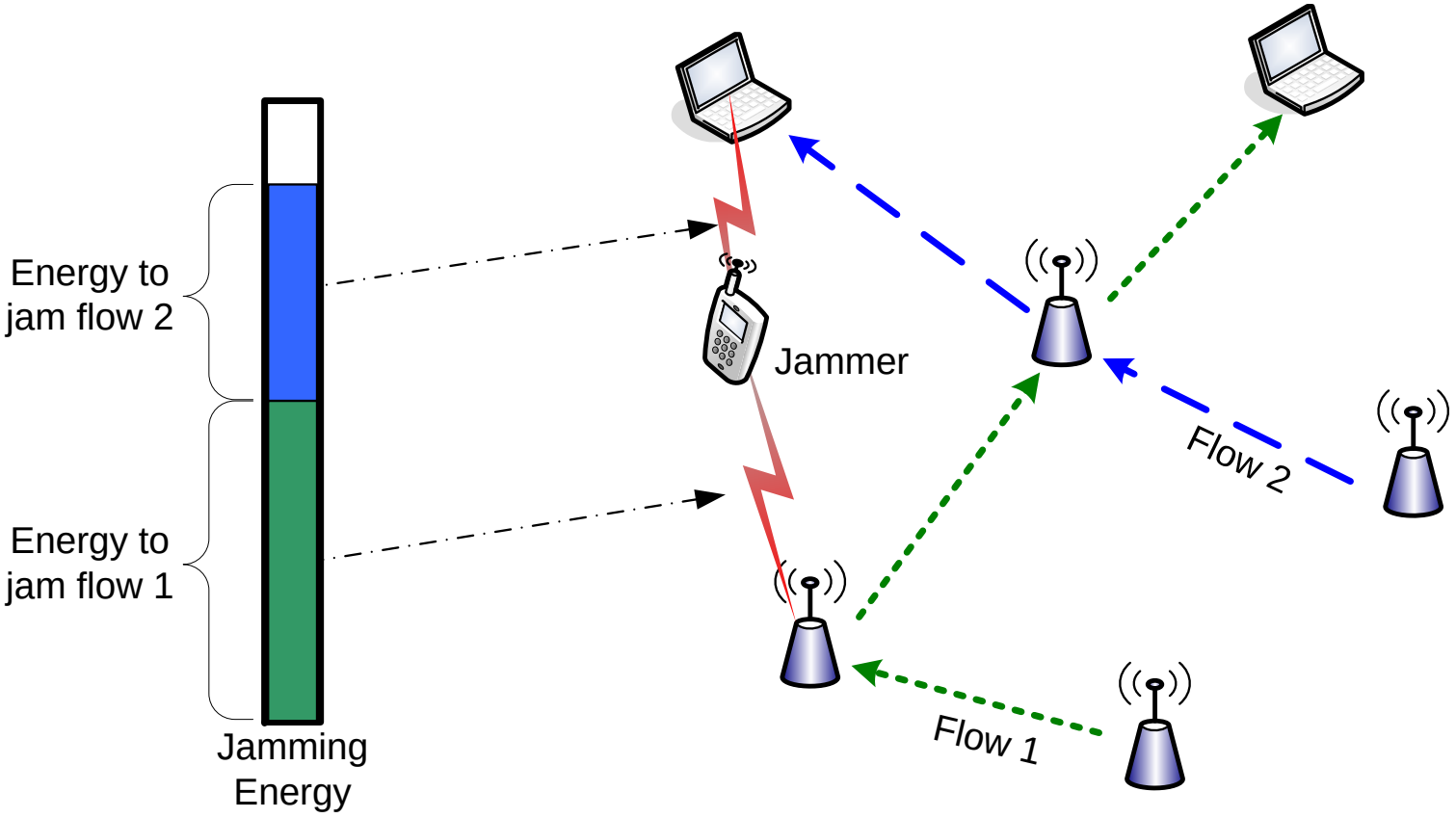
Effects of jamming, a *physical layer attack,* can be captured in the *network layer metric* of goodput



Jamming Network Flows

- **Adversary goal**: reduce network throughput via coordinated jamming
  - Constraints: finite energy, device capability, physical restrictions
- How should the jamming energy be allocated to best throttle the network flows?

Modeling Jamming Attacks



Note: we assume a single jamming transmission is required to jam each packet.

Modeling Jamming Attacks

- For jammer *j*, flow *f*:
  - r_f = data rate of *f*
  - x_{jf} = fraction of data in *f* jammed by *j*
    - Assume: jamming succeeds *w.p.* 1
  - c_{jf} = jamming energy per-unit data rate for flow *f*
  - c_j = total energy available to jammer *j*

Constraint: Total flow

$$\sum_j x_{jf} \leq 1, \ \forall f$$

Constraint: Total energy

$$\lambda_j(\mathbf{x}) = \sum_f \frac{c_{jf} r_f x_{jf}}{c_j} \leq 1, \ \forall j$$

Attack Evaluation Metrics

- **F = Total number of flows**
- **Impact** of attack
  - Average reduction in flow rate
- Attack **Gain** (Efficiency)
  - Average reduction in flow rate per energy expenditure per jammer
- Energy **Variation**
  - Relative variation in resource expenditure

$$I(\mathbf{x}) = \frac{1}{F}\sum_{j,f} x_{jf}$$

$$E(\mathbf{x}) = \frac{\frac{1}{F}\sum_{j,f} x_{jf}}{\frac{1}{J}\sum_{j} \lambda_j(\mathbf{x})}$$

$$V(\mathbf{x}) = 1 - \frac{\min_j \lambda_j(\mathbf{x})}{\max_j \lambda_j(\mathbf{x})}$$

Attack Formulations

- Constrained optimization formulation
  - Assume allocation is done by centralized adversary
  - Optimize with respect to evaluation metrics individually or jointly

Maximize Jamming Impact

- Maximize impact ***I(x)*** and gain ***E(x)***
  - First, constrain ***I(x)=1*** and minimize energy expenditure (denominator of ***E(x)***)
  - If no feasible solution, maximize impact ***I(x)***
  - Both ***I(x)*** and denominator of ***E(x)*** are linear in **x**, so each formulation is LP

$$\begin{aligned} \min \quad & \|\Lambda(\mathbf{x})\|_1 \\ \text{s.t.} \quad & \lambda_j(\mathbf{x}_j) \leq 1 \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 = 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \leq x_{jf} \leq 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}. \end{aligned}$$

$$\begin{aligned} \max \quad & \|\mathbf{x}\|_1 \\ \text{s.t.} \quad & \lambda_j(\mathbf{x}_j) \leq 1 \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 \leq 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \leq x_{jf} \leq 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}. \end{aligned}$$

Maximize Jamming Gain

- Maximize gain ***E(x)***
  - Inherently tries to maximize impact ***I(x)***, but makes tradeoffs for energy savings
  - ***E(x)*** is rational in **x**, can be approximated by an LP to within an additive constant $\varepsilon>0$

$$\begin{aligned} \max \quad & \frac{|\mathcal{F}|^{-1}\|\mathbf{x}\|_1}{|\mathcal{J}|^{-1}\|\Lambda(\mathbf{x})\|_1} \\ \text{s.t.} \quad & \lambda_j(\mathbf{x}_j) \le 1 \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 \le 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \le x_{jf} \le 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}. \end{aligned}$$

$$\begin{aligned} \min \quad & |\mathcal{J}|^{-1}\|\Lambda(\mathbf{x})\|_1 - \epsilon^{-1}|\mathcal{F}|^{-1}\|\mathbf{x}\|_1 \\ \text{s.t.} \quad & \lambda_j(\mathbf{x}_j) \le 1 \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 \le 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \le x_{jf} \le 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}. \end{aligned}$$

Minimize Variation

- Minimize variation ***V(x)*** with max ***I(x)***
  - First, constrain ***I(x)=1*** and minimize maximum energy expenditure
  - If no feasible solution, maximize minimum energy expenditure

$$\begin{aligned} \min \quad & \lambda \\ \text{s.t.} \quad & \lambda_j(\mathbf{x}_j) \leq \lambda \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 = 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \leq x_{jf} \leq 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}, \\ & 0 \leq \lambda \leq 1. \end{aligned}$$

$$\begin{aligned} \max \quad & \lambda \\ \text{s.t.} \quad & \lambda \leq \lambda_j(\mathbf{x}_j) \leq 1 \text{ for all } j \in \mathcal{J}, \\ & \|\mathbf{x}_f\|_1 \leq 1 \text{ for all } f \in \mathcal{F}, \\ & 0 \leq x_{jf} \leq 1 \text{ for all } j \in \mathcal{J}, f \in \mathcal{F}, \\ & 0 \leq \lambda \leq 1. \end{aligned}$$

NSL

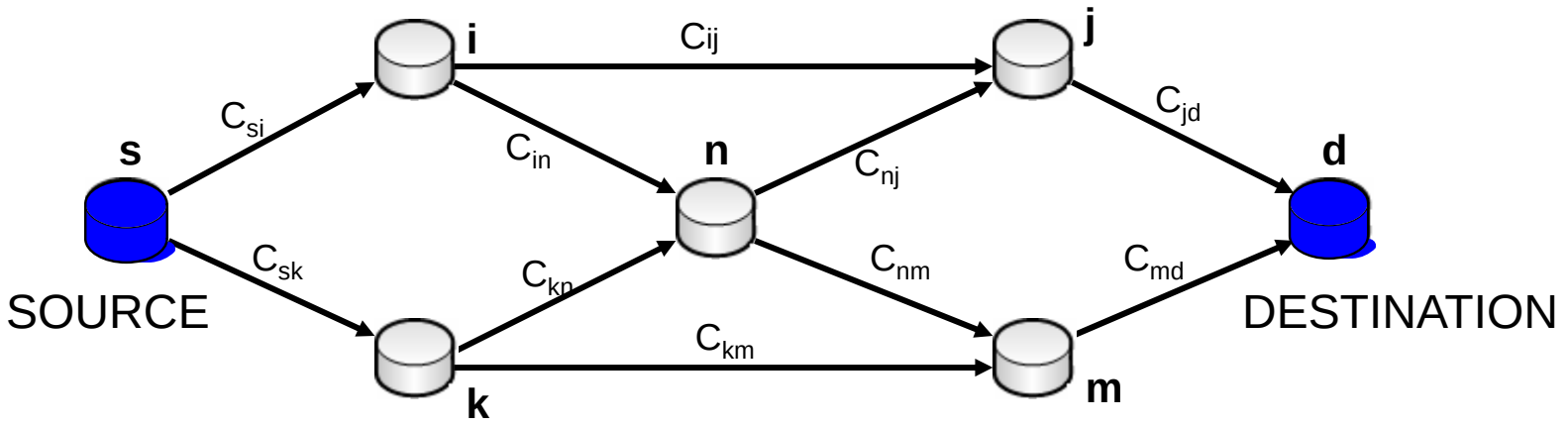
Traffic Allocation using Portfolio Selection under Stochastic Jamming Attacks

Outline

- Overview
- Wireless Network model
- Dynamic jamming & Recursive Estimation
- Markowitz portfolio optimization
- NUM Optimization of traffic allocation
- Simulation & Results
- Contributions and future work

Network Model

- Collection of wireless nodes.
- Source, destination, links, paths.
- Individual links have constant capacities.
- Graph model: Vertex set Q, edge-set H, set of sources $V \subseteq Q$

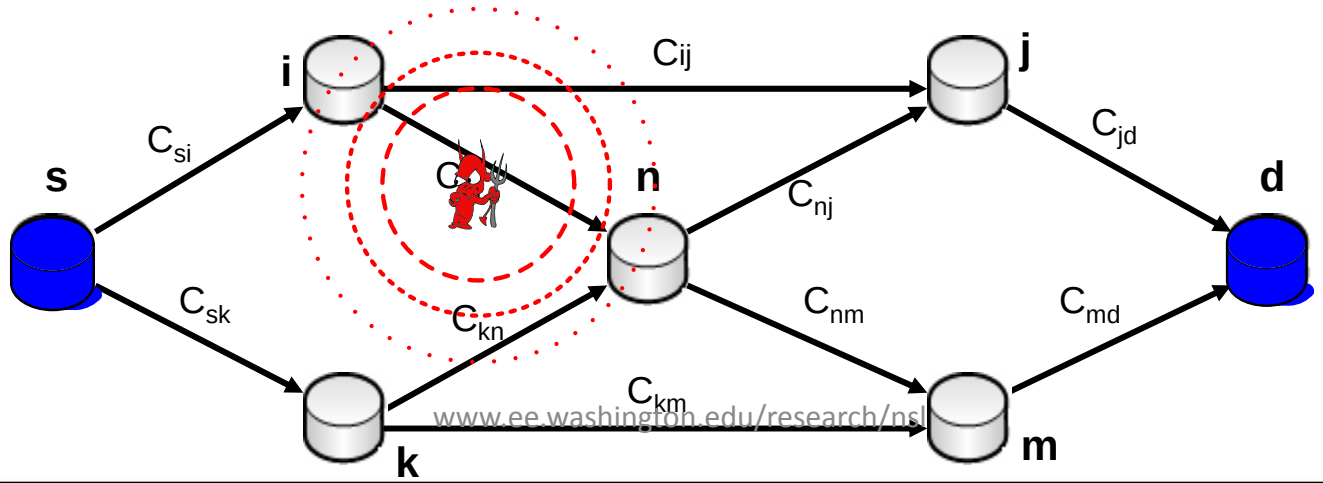


Routing

- Source Routing:
  - Source discovers path to destination.
  - Stores path information.
  - Intermediate nodes help in **route maintenance**.
- Multi-path Routing:
  - Source maintains multiple paths to destination.
  - Multiple paths are more robust to link failures.
  - Paths are preferably **diverse** and **disjoint**.

Jamming

- Deliberate transmission of radio signals to disrupt the communication in a wireless network by decreasing the signal-to-noise ratio (SNR).
- Several types: constant, deceptive, random, reactive. Emphasis on the impact, not the type
- Mobile/Reactive jammers have greater impact.



Anti-jamming methods

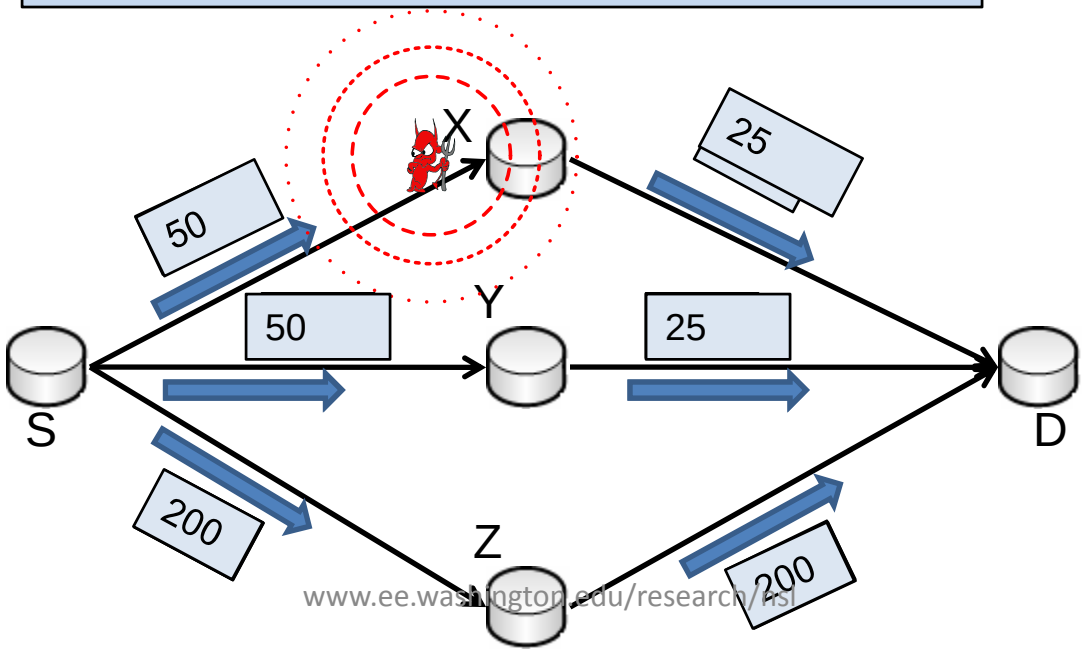
- Physical Layer methods:
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)
  - Beam-forming and Interference Rejection
- MAC and Network Layer methods:
  - Channel Switching
  - Routing around jammed areas
  - Spatial retreats
- Our approach: Multi-path routing (spatial route diversity)

Effect of Jamming on Network Throughput

Jamming → Packet errors → Packet Retransmission

↓

Decrease in Throughput

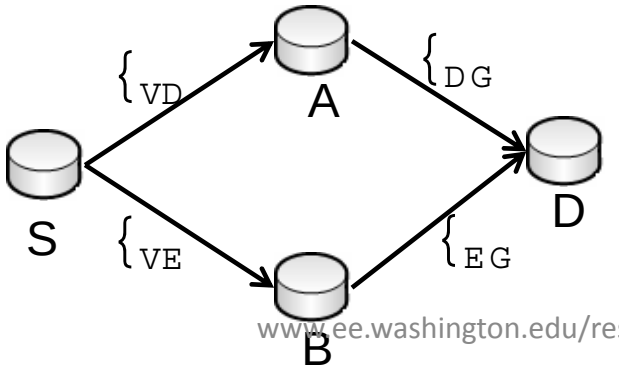


Impact of Jamming – Probabilistic View

- Analytical measurements are not possible
  - Jammer locations, signal power are unknown.
  - We use Heuristics -- Packet Delivery Ratio (PDR)
- Packet Delivery Rates vary over time:
  - Dynamic jammer strategy.
  - Mobility of jammer.
- Due to uncertainty from jamming, we model the PDR at a node as a **random process.**

Include Jamming Impact into Network Flow

- Network flow formulation
  - Suppose flow of rate ϕ_p is sent over a single source-destination path s_p.
  - Let $\{_{lm}$ be the fraction of correctly received packets over link (l,m) i.e. packet success rate. Mean of $\{_{lm}$ *is* μ_{lm} and variance is σ_{lm}^2.
  - $|_p$ is the fraction of ϕ_p successfully received at destination *d along path* s_p and is the product of the $\{_{lm}$'s on path s_p. Mean of $|_p$ is γ_p and variance is ω_p^2.
  - $|_m$*'s* for multiple paths are correlated due to overlapping links.



Path 1: S – A – D

$|_4 = \{_{VD} * \{_{DG}$

Path 2: S – B – D

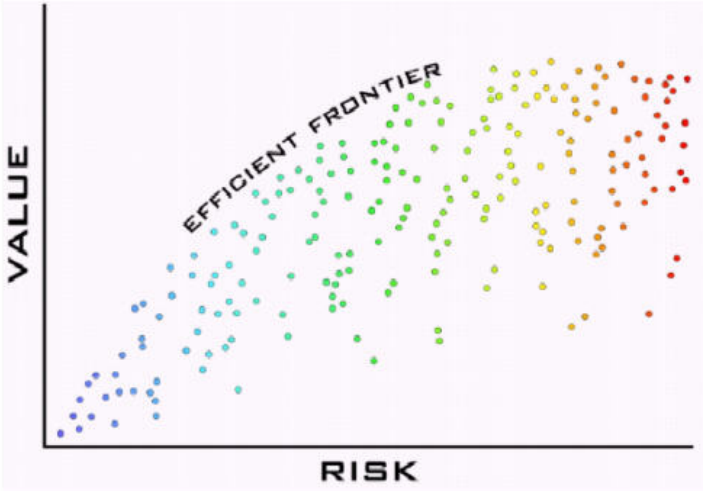
$|_5 = \{_{VE} * \{_{EG}$

Reviewing the Problem Setup

- The traffic allocation problem for a source:
  - Resources available: Multiple paths
  - Performance metrics for each path:
    - Estimated mean end-to-end packet success rate
    - Estimated var in end-to-end packet success rate
  - Goal: Achieve optimal throughput performance
    - Maximize average throughput
    - Minimize variance in the achieved throughput
  - "Intelligent" traffic allocation among paths.
  - What is the role of uncertainty on link weights?

Markowitz Portfolio Optimization

- Input:
  - Past performance of each asset
    - Expected return for each asset.
    - Risk involved in each asset.
    - Correlation between assets.
- Output:
  - Set of portfolios giving:
    - Highest returns for a given risk.
    - Lowest risk for given returns.
- History projects the known past to an uncertain future, quantified into risk.



Correspondence between Portfolio Theory and Traffic Allocation

Principal to be invested	⟺	Source Data to be sent
Investment options	⟺	Potential Paths
Mean return for each asset	⟺	Mean packet delivery rate γ for each path
Overall mean return	⟺	Mean throughput
Risk	⟺	Standard deviation of throughput

Constraints

Non-negative traffic rates → $\phi_v \geq 0$

Data generation rate at source → $1^W \phi_v \leq U_v$

Link Capacity constraint → $\sum_{s \in \mathcal{S}} \sum_{\ell:(i,j) \in p_{s\ell}} \phi_{s\ell} y_{s\ell}^{(i)} \leq c_{ij}$

$$\sum_{s \in \mathcal{S}} \boldsymbol{W}_s \boldsymbol{\phi}_s \leq \boldsymbol{c}$$

All constraints are linear in ϕ_v

Utility Functions

Analogous to Markowitz Portfolio Theory, for a given source v, we define utility function as:

$$x_v(\phi_v) = \underbrace{\gamma_v^T \phi_v}_{\text{Mean}} - \underbrace{n_v \phi_v^T \Omega_v \phi_v}_{\text{Variance}}$$

$n_v = 0$ gives **max-mean** case

$n_v > 0$ gives **optimal risk-return** case

Optimization Problem Setup

- Considering the combined utility function and constraints for all sources $v \in S$, we get:

Optimal Jamming-Aware Traffic Allocation

$$\boldsymbol{\phi}^* = \arg\max_{\{\boldsymbol{\phi}_s\}} \sum_{s \in \mathcal{S}} \boldsymbol{\gamma}_s^T \boldsymbol{\phi}_s - k_s \boldsymbol{\phi}_s^T \boldsymbol{\Omega}_s \boldsymbol{\phi}_s$$

$$\text{s.t.} \quad \sum_{s \in \mathcal{S}} \boldsymbol{W}_s \boldsymbol{\phi}_s \leq \boldsymbol{c}$$

$$\mathbf{1}^T \boldsymbol{\phi}_s \leq R_s \text{ for all } s \in \mathcal{S},$$

$$\mathbf{0} \leq \boldsymbol{\phi}_s \text{ for all } s \in \mathcal{S}.$$

Distributed Solution

- Centralized method is not suited for large multi-source networks.
- Enable each source to compute ϕ_v^* independently.
- Links are used by multiple sources and hence the capacity constraints are coupled.
- Problem setup is similar to Network Utility Maximization (NUM).
- Use Lagrangian method for decomposition.[1]

Distributed Solution

- Use link prices λ_{lm} to convert the link capacity constraints into a Lagrangian price term.
- At each iteration, sources use links based on their current price.
- Price is then updated based on link utilization and capacity.

$$L(\boldsymbol{\phi}, \boldsymbol{\lambda}) = \sum_{s \in \mathcal{S}} \boldsymbol{\gamma}_s^T \boldsymbol{\phi}_s - k_s \boldsymbol{\phi}_s^T \boldsymbol{\Omega}_s \boldsymbol{\phi}_s + \boldsymbol{\lambda}^T \underbrace{\left(\boldsymbol{c} - \sum_{s \in \mathcal{S}} \boldsymbol{W}_s \boldsymbol{\phi}_s \right)}_{\text{Link capacity}}$$

Reading list for the 2nd lecture

- From NSL Website
  - Throughput Optimization for Multipath Unicast Routing Under Probabilistic Jamming
  - Linear Programming Models for Jamming Attacks on Network Traffic Flows

NSL

Acknowledgements

- Collaborators: Profs. Jim Ritcey, Guevara Noubir; Students Patrick Tague, David Slater, Sid Nabar
- http://www.ee.washington.edu/research/nsl