Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming

Zhuo Lu†, Wenye Wang†, and Cliff Wang‡

† Department of Electrical and Computer Engineering
North Carolina State University, Raleigh NC, US.

‡ Army Research Office
Research Triangle Park NC, US.

Outline

Outline

Smart Grid Vision

The Smart Grid: the next-generation power grid.

- Power infrastructures with information technologies.
- National Institute of Standards and Technology (NIST): Roadmap and Guidelines. [NIST'09,10,11]

Smart Grid Vision

The Smart Grid: the next-generation power grid.

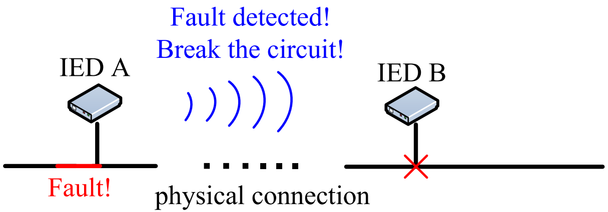
- Power infrastructures with information technologies.
- National Institute of Standards and Technology (NIST): Roadmap and Guidelines. [NIST'09,10,11]

Wireless networks for power control applications [NIST'11].

- Efficient
- Low-cost
- Convenient network access

Power Applications over Wireless

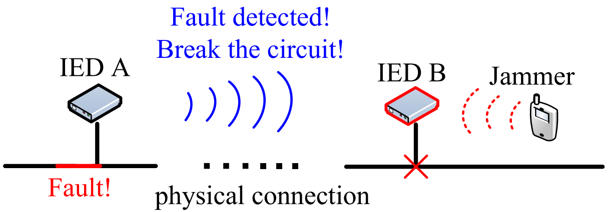
Example: A generic protection scenario over wireless networking [Cleverland'07,Kanabar'09,El-Khattam'10].



- IED: Intelligent electronic devices
- A needs to tell B: break your circuit!
- The message has a strict delay requirement.
  - Example: 3ms/10ms for substation protection [IEC 61580].

Threat of Jamming Attacks on Power Applications

Example: A generic protection scenario over wireless networking [Cleverland'07,Kanabar'09,El-Khattam'10].



A jammer can disrupt the time-critical messaging, leading to

- denial-of-service, as it does in conventional wireless networks.
- physical damages to power infrastructures.

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Conventional results cannot be used in the smart grid.

- How a message can be finally delivered (improving message delivery ratio) [Chiang'08, Strasser'09, Liu'10].

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Conventional results cannot be used in the smart grid.

- How a message can be finally delivered (improving message delivery ratio) [Chiang'08, Strasser'09, Liu'10].
  100% messages delivered $\neq$ messages arrived on time

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Conventional results cannot be used in the smart grid.

- How a message can be finally delivered (improving message delivery ratio) [Chiang'08, Strasser'09, Liu'10].

  100% messages delivered $\neq$ messages arrived on time
- Case-by-case methodologies when analyzing attacks.
  - Widely-adopted models: memoryless, periodic, reactive, *et al* [Xu'02, Bayraktaroglu'08].

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Conventional results cannot be used in the smart grid.

- How a message can be finally delivered (improving message delivery ratio) [Chiang'08, Strasser'09, Liu'10].
  100% messages delivered $\neq$ messages arrived on time
- Case-by-case methodologies when analyzing attacks.
  - Widely-adopted models: memoryless, periodic, reactive, *et al* [Xu'02, Bayraktaroglu'08].

  NIST requires that *power system operations must be able to continue during any security attack or compromise (as much as possible) [NIST'10].*

Existing Anti-Jamming Works: Methods and Issues

Communication theory: Spread spectrum technologies

- frequency hopping (FH) or direct sequence (DS)
- building multiple frequency and code channels.
- a practical jammer cannot jam all the channels at the same time.

Conventional results cannot be used in the smart grid.

- How a message can be finally delivered (improving message delivery ratio) [Chiang'08, Strasser'09, Liu'10].

  100% messages delivered $\neq$ messages arrived on time
- Case-by-case methodologies when analyzing attacks.
  - Widely-adopted models: memoryless, periodic, reactive, *et al* [Xu'02, Bayraktaroglu'08].

  NIST requires that *power system operations must be able to continue during any security attack or compromise (as much as possible) [NIST'10].*

- Worst-case methodology is vital to smart grid security design.

Research Question and Our Contribution

Open research question

How to minimize the worst-case message delay to provide performance guarantee for smart grid applications under jamming?

Research Question and Our Contribution

Open research question

How to minimize the worst-case message delay to provide performance guarantee for smart grid applications under jamming?

A trivial solution

1. Increase the number of channels $\longrightarrow$ reliability.
2. Increase the bandwidth of each channel $\longrightarrow$ timing guarantee.

Research Question and Our Contribution

Open research question

How to minimize the worst-case message delay to provide performance guarantee for smart grid applications under jamming?

A trivial solution

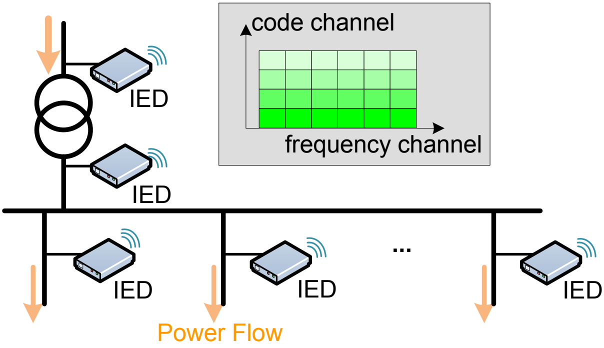
1. Increase the number of channels $\longrightarrow$ reliability.
2. Increase the bandwidth of each channel $\longrightarrow$ timing guarantee.

In this paper, given fixed network setups, we find a new way to minimize the message delay under worst-case jamming attacks.

Outline

Network Model

A local-area power system over a wireless network with m nodes, N_f frequency and N_c code channels.



Time-Critical Message Transmission Model

How to transmit a time-critical message for an IED? [IEC 61850]

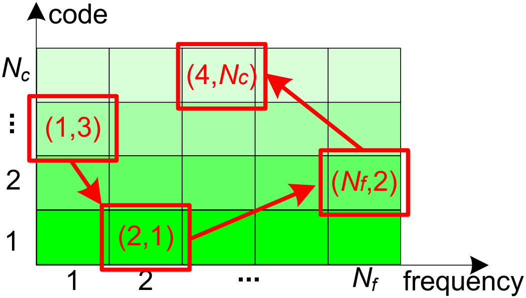
- be transmitted multiple times to ensure reliability.
- stop re-transmission after the deadline is passed.

Time-Critical Message Transmission Model

How to transmit a time-critical message for an IED? [IEC 61850]

- be transmitted multiple times to ensure reliability.
- stop re-transmission after the deadline is passed.

We adopt such a simple transmission scheme, and assume

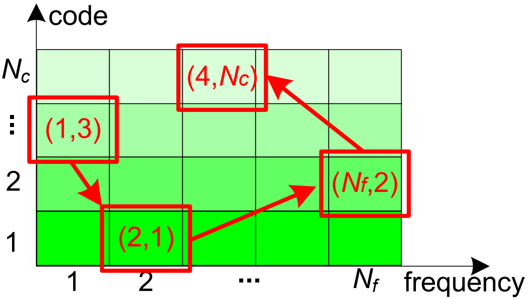


Time-Critical Message Transmission Model

How to transmit a time-critical message for an IED? [IEC 61850]

- be transmitted multiple times to ensure reliability.
- stop re-transmission after the deadline is passed.

We adopt such a simple transmission scheme, and assume



The secret channel selection pattern is not known to the attacker.

Jamming Attack Model

It's vital to use worst-case analysis rather than case-by-case one in the smart grid.

- no particular jamming model.

Jamming Attack Model

It's vital to use worst-case analysis rather than case-by-case one in the smart grid.

- no particular jamming model.

Question: How to adopt the worst-case analysis of jamming attacks

1. Define a generic model to cover most existing models.
2. Find out what is the worst case induced by the generic model.

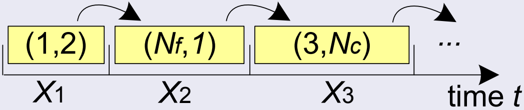
Jamming Attack Model

It's vital to use worst-case analysis rather than case-by-case one in the smart grid.

- no particular jamming model.

Definition (Generic Jamming Process)

A jammer's jamming process is denoted as a Markov-renewal process $((F, C), X) = \{(F_k, C_k), X_k | k = 1, 2, \cdots\}$.

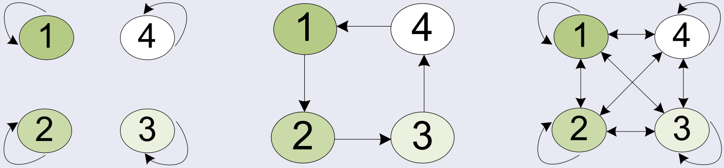


- X_k is the interval for the k status.
- (F_k, C_k) is the targeted frequency-code channel.

Generic Jamming Model: Markov-Renewal Process

Why is $((F, C), X)$ Markovian?

- Two associated transition matrices $\mathbf{Q}_F$ and $\mathbf{Q}_C$.

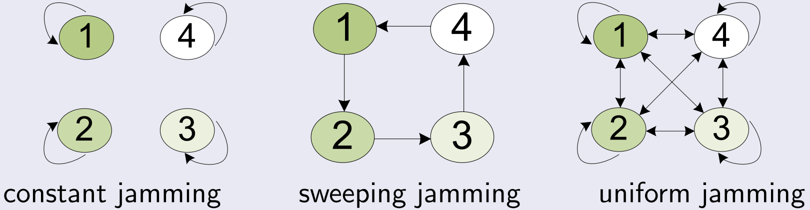


constant jamming sweeping jamming uniform jamming

Generic Jamming Model: Markov-Renewal Process

Why is $((F, C), X)$ Markovian?

- Two associated transition matrices $\mathbf{Q}_F$ and $\mathbf{Q}_C$.



Reactive or non-reactive? Manipulate the jamming interval X_k

- Non-reactive (jam all the way): X_k is randomly distributed.
- Reactive (sense then jam): $X_k = \tau + S_k \mathbf{1}_A$.
  - τ: constant channel sensing time.
  - $\mathbf{1}()$ is the indicator function.
  - A: event that the channel is busy, S_k the jamming interval.

Problem Formulation

1. Under the generic jamming model, find out the worst-case performance;

Problem Formulation

1. Under the generic jamming model, find out the worst-case performance;
   - Delay is critical for measuring the performance of power systems. A message becomes invalid as long as its delay D is larger than the timing requirement σ.

Problem Formulation

1. Under the generic jamming model, find out the worst-case performance;
   - Delay is critical for measuring the performance of power systems. A message becomes invalid as long as its delay D is larger than the timing requirement σ.
   - Metric: message invalidation probability $\mathbb{P}(D > \sigma)$ denoting the probability that the message is not delivered on time

Problem Formulation

1. Under the generic jamming model, find out the worst-case performance;
   - Delay is critical for measuring the performance of power systems. A message becomes invalid as long as its delay D is larger than the timing requirement σ.
   - Metric: message invalidation probability $\mathbb{P}(D > \sigma)$ denoting the probability that the message is not delivered on time
   - We try to find out the worst-case message invalidation probability $\mathbb{P}(D > \sigma)$.

Problem Formulation

1. Under the generic jamming model, find out the worst-case performance;
   - Delay is critical for measuring the performance of power systems. A message becomes invalid as long as its delay D is larger than the timing requirement σ.
   - Metric: message invalidation probability $\mathbb{P}(D > \sigma)$ denoting the probability that the message is not delivered on time
   - We try to find out the worst-case message invalidation probability $\mathbb{P}(D > \sigma)$.
2. Attempt to minimize the worst-case $\mathbb{P}(D > \sigma)$.

Outline

Theorem: Worst-Case Delay Bound

Theorem (Worst-Case Delay Performance)

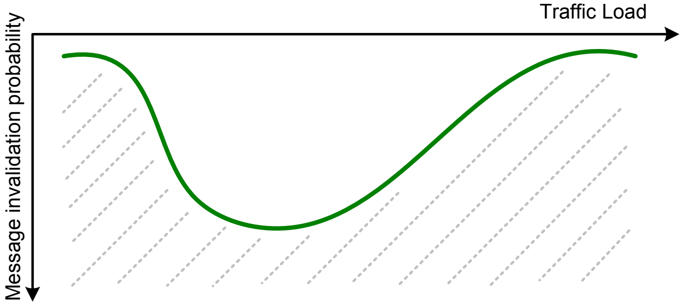
For a wireless local-area network $\mathcal{N}(m, N_f, N_c)$, the worst-case delay performance at node k is always induced by the reactive jamming and bounded by

$$\mathbb{P}(D_k > \sigma) \leq \left(1 - \left(1 - \frac{1}{N_f N_c}\right)^{T_L(1-\rho)\gamma_k} \left(1 - \frac{T_L}{\frac{\tau N_f N_c}{1-\rho} + \rho T_L^2 \gamma_k}\right)\right)^{\sigma/T_L},$$

where T_L is the message transmission duration, σ is the message delay threshold, $\gamma_k = \sum_{j=1, j\neq k}^{m} \lambda_j$, and λ_j is the traffic rate at node j.

Theoretical Indication for Practical Security Design

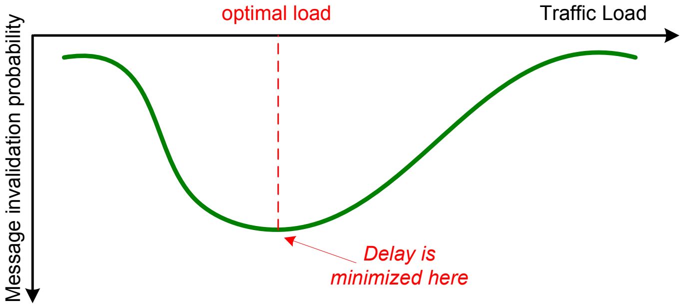
Theoretical results tell us



Jammer's achievable region

Theoretical Indication for Practical Security Design

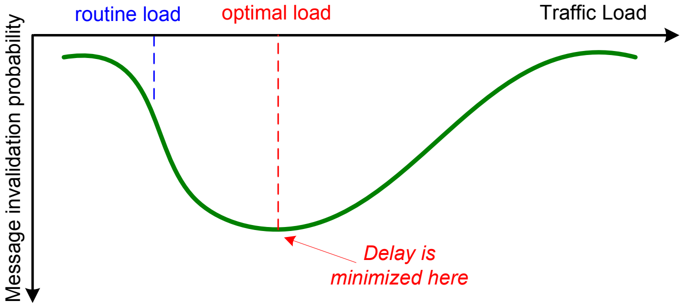
Theoretical results tell us



There exists an optimal network traffic load to minimize worse-case delay/message invalidation probability.

Theoretical Indication for Practical Security Design

Theoretical results tell us

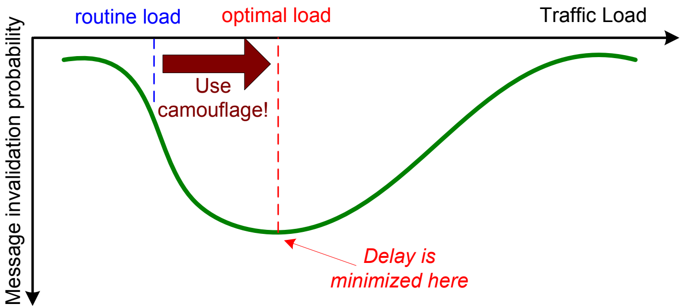


In the smart grid, network traffic is usually highly unsaturated for reliable monitoring and control.

- Example: wireless monitoring for substation transformers only needs to transmit a message every second [Cleverland'07].

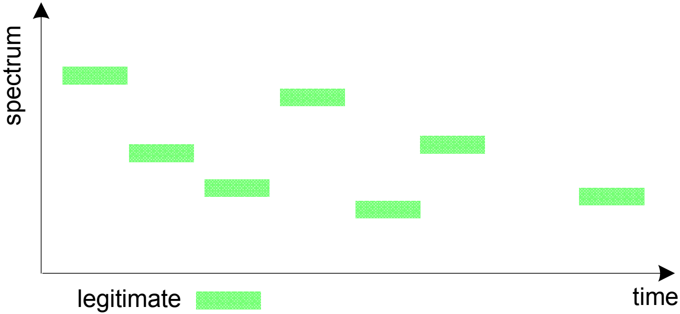
Theoretical Indication for Practical Security Design

Theoretical results tell us



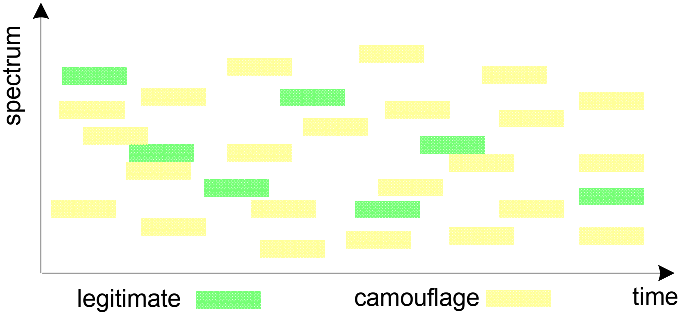
This implies that we need to transmit redundant traffic to optimize the traffic load. We call such traffic camouflage.

Intuition of the U-shaped Phenomenon



A reactive jammer can sense channels every fast: if there is no traffic, then go to next channel!

Intuition of the U-shaped Phenomenon



A reactive jammer is busy in jamming camouflage, giving a chance for legitimate traffic to pass through.

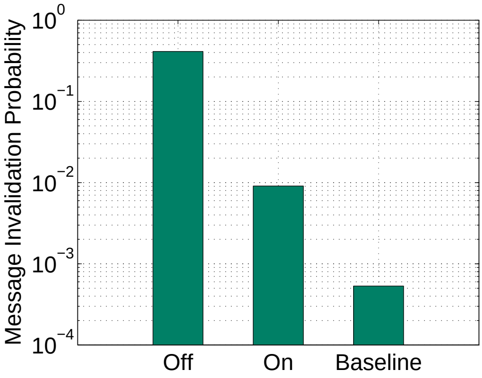
Experimental Setups

We set up an wireless anti-islanding network in the FREEDM systems center in North Carolina State University.

- Spread spectrum: frequency hopping with 8 channels.
- Bandwidth: 125KHz per channel.
- Number of nodes: 5 USRP-based IEDs.
- Jammer: USRP-based reactive jammer, scanning channel one by one.
- Routine traffic: 1 message/second.
- Message length: 400 bytes.
- Anti-islanding message timing requirement: 150ms.

Experimental Results

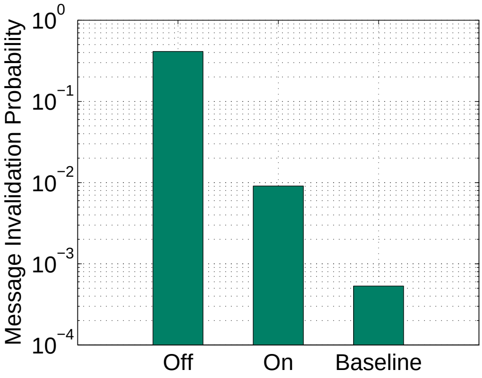
Routine traffic: 1 message/second.
Optimal camouflage traffic load: 14 messages/second.



Experimental Results

Routine traffic: 1 message/second.

Optimal camouflage traffic load: 14 messages/second.



Transmitting camouflage traffic will improve the performance in order of magnitude!

Outline

Conclusion

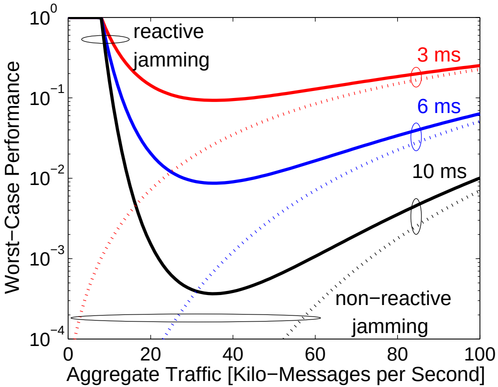
- We defined a generic jamming process, and show the worst-case delay bound is due to reactive jamming and exhibits a U-shaped function of network traffic load.
- There exists an optimal load to minimize the worst-case delay, therefore transmitting camouflage traffic can in fact help improve the delay performance.
- We illustrated via experiments that camouflage traffic can substantially improve the delay performance for smart grid applications under jamming attacks.

Conclusion

- We defined a generic jamming process, and show the worst-case delay bound is due to reactive jamming and exhibits a U-shaped function of network traffic load.
- There exists an optimal load to minimize the worst-case delay, therefore transmitting camouflage traffic can in fact help improve the delay performance.
- We illustrated via experiments that camouflage traffic can substantially improve the delay performance for smart grid applications under jamming attacks.
- Future work
  1. Consider the case of multiple attackers.
  2. Lift the assumption that the secret pattern between a transmit-receive pair is already set up.

Thank you!

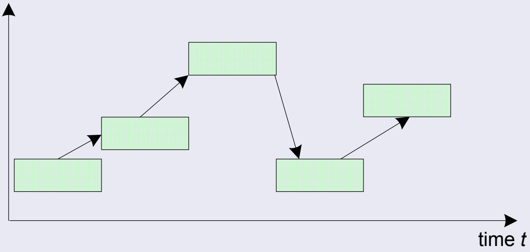
Backup 1: Reactive vs Non-reactive



The delay bound $\mathbb{P}(D_k > \sigma)$ versus aggregate traffic γ_k at node k for time-critical applications with delay thresholds of 3–10ms. ($N_f = N_c = 10$, $T_L = 1$ms, $\rho = 0.1$, and $\tau = 100\mu$s for reactive jamming)

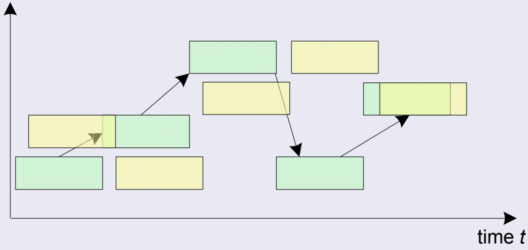
Backup 2: Interference Model

When a transmission fails



Backup 2: Interference Model

When a transmission fails



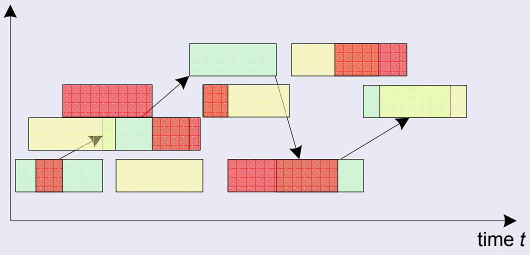
Interference model

A transmission on the (i, j)-th channel fails only if at least a portion $\rho \in (0, 1)$ of the transmission is

- either disrupted by jamming
- or collided by other legitimate traffic.

Backup 2: Interference Model

When a transmission fails



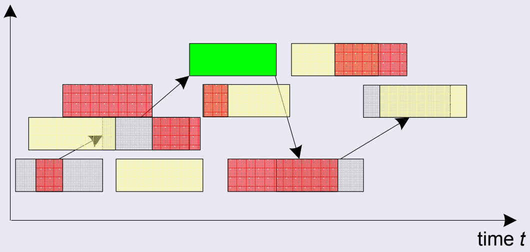
Interference model

A transmission on the (i, j)-th channel fails only if at least a portion $\rho \in (0, 1)$ of the transmission is

- either disrupted by jamming
- or collided by other legitimate traffic.

Backup 2: Interference Model

When a transmission fails



Interference model

A transmission on the (i, j)-th channel fails only if at least a portion $\rho \in (0, 1)$ of the transmission is

- either disrupted by jamming
- or collided by other legitimate traffic.