From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time-Critical Traffic

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.

April 13, 2011

Outline

Outline

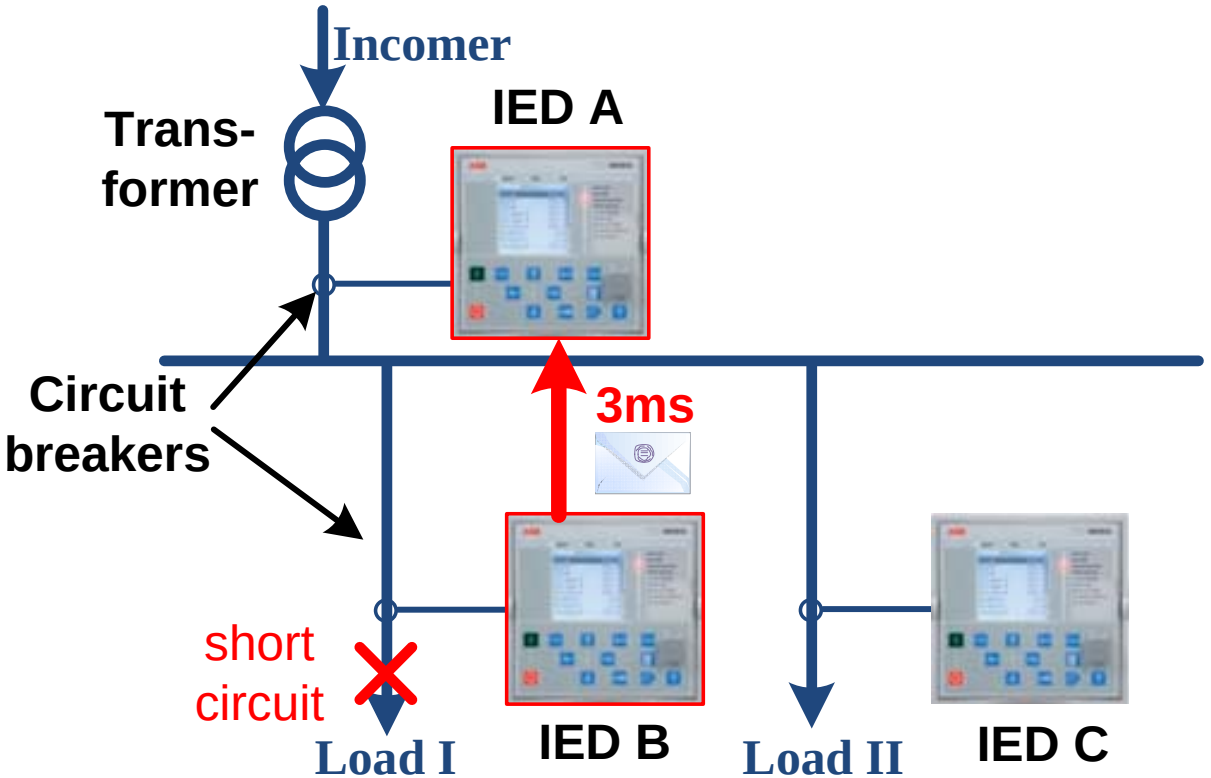
Time-Critical Wireless Networks

Emerging cyber-physical systems (notably the smart grid) have provided a new paradigm for wireless network design.

- Time-critical wireless networks.

Why Time-Critical?

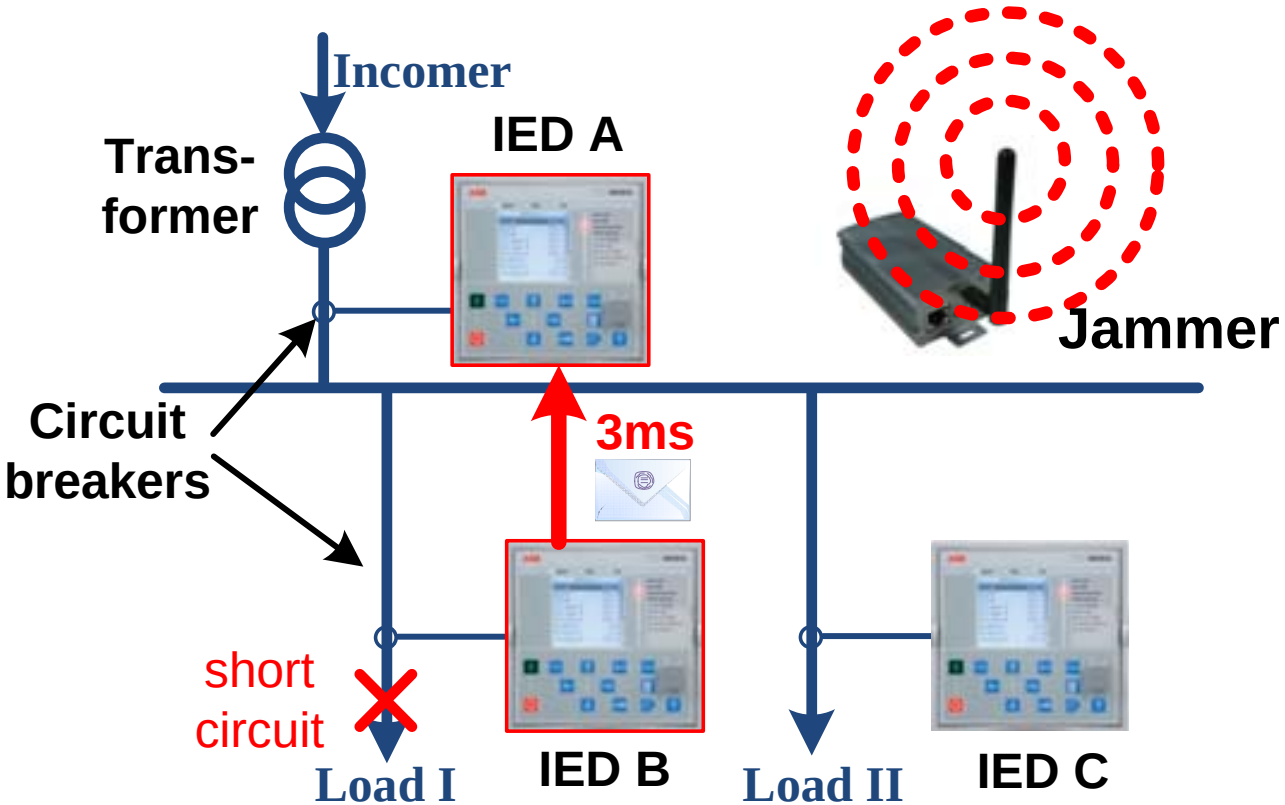
Example: A substation protection scenario.



- IED: Intelligent electronic devices
- B needs to tell A: Do not break your circuit!

Jamming Issue in Time-Critical Networks

Example: A substation protection scenario.



- A jammer can severely disrupt time-critical communication.

Exiting Works and Issues

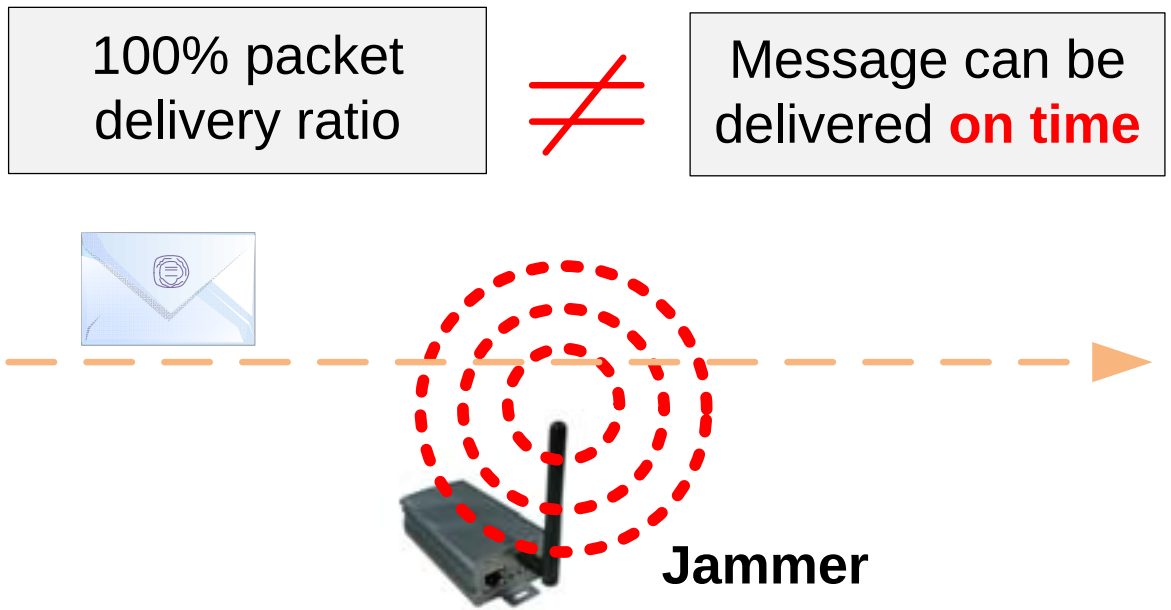
Existing results can not be readily adopted in time-critical networks.

- Jamming modeling and evaluation: packet delivery/transmission ratios (Xu'02), number of jammed packets (Li'07), network throughput (Bayraktaroglu'08).

Exiting Works and Issues

Existing results can not be readily adopted in time-critical networks.

- Jamming modeling and evaluation: packet delivery/transmission ratios (Xu'02), number of jammed packets (Li'07), network throughput (Bayraktaroglu'08).



Exiting Works and Issues

Existing results can not be readily adopted in time-critical networks.

- Jamming modeling and evaluation: packet delivery/transmission ratios (Xu'02), number of jammed packets (Li'07), network throughput (Bayraktaroglu'08).
- Jamming detection: requires the knowledge of the jamming impact to accurately identify significant attacks. (Xu'02, Wood'07)

Exiting Works and Issues

Existing results can not be readily adopted in time-critical networks.

- Jamming modeling and evaluation: packet delivery/transmission ratios (Xu'02), number of jammed packets (Li'07), network throughput (Bayraktaroglu'08).
- Jamming detection: requires the knowledge of the jamming impact to accurately identify significant attacks. (Xu'02, Wood'07)
  With no understanding of jamming impact, it is hard to design efficient detection methods.

Exiting Works and Issues

Existing results can not be readily adopted in time-critical networks.

- Jamming modeling and evaluation: packet delivery/transmission ratios (Xu'02), number of jammed packets (Li'07), network throughput (Bayraktaroglu'08).
- Jamming detection: requires the knowledge of the jamming impact to accurately identify significant attacks. (Xu'02, Wood'07)

A fundamental question:

How to model and detect jamming attacks against time-critical traffic in wireless networks?

Outline

Requirements for Time-Critical Transmission

Time-critical messages require

- Highest priority,
- Low processing delay,
- No buffering and queuing.

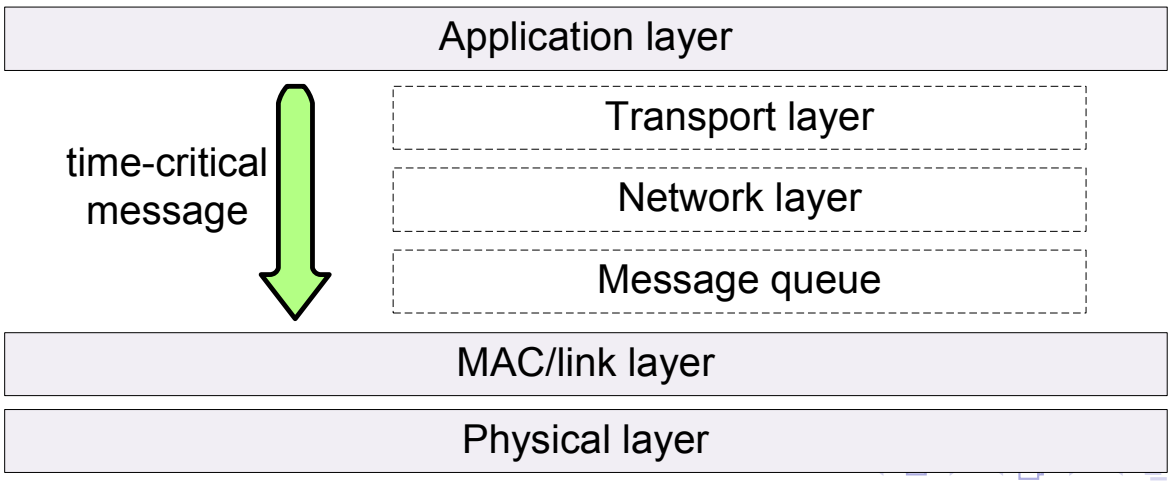
Requirements for Time-Critical Transmission

Time-critical messages require

- Highest priority,
- Low processing delay,
- No buffering and queuing.

IEC 61850 is a recent standard for power substation communication.

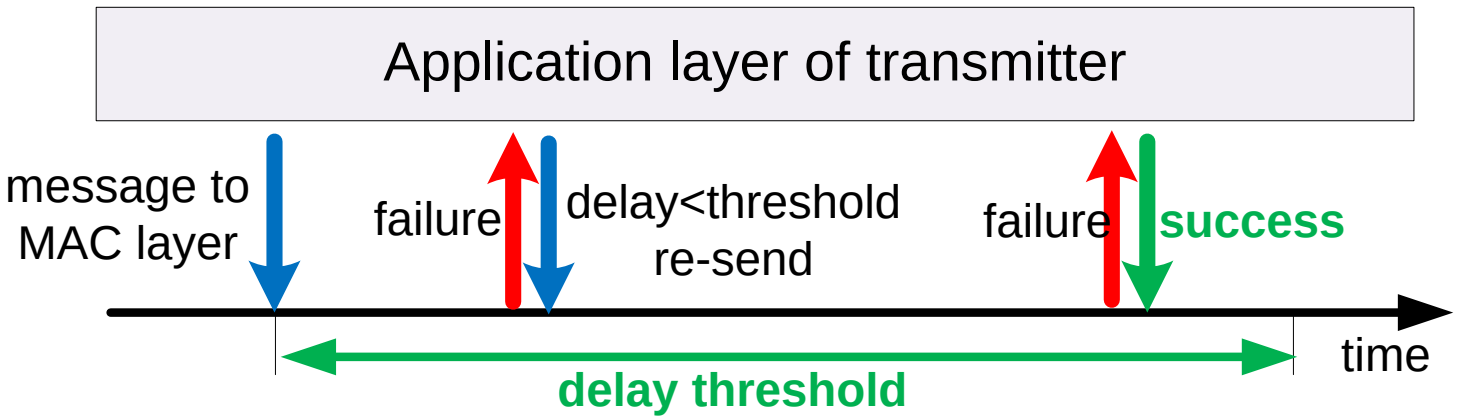
- GOOSE (Generic Object Oriented Substation Events) messages have 3ms and 10ms delay requirements for power device protection.
  - Simple retransmission mechanism: no any flow control.



Modeling for Time-Critical Transmission

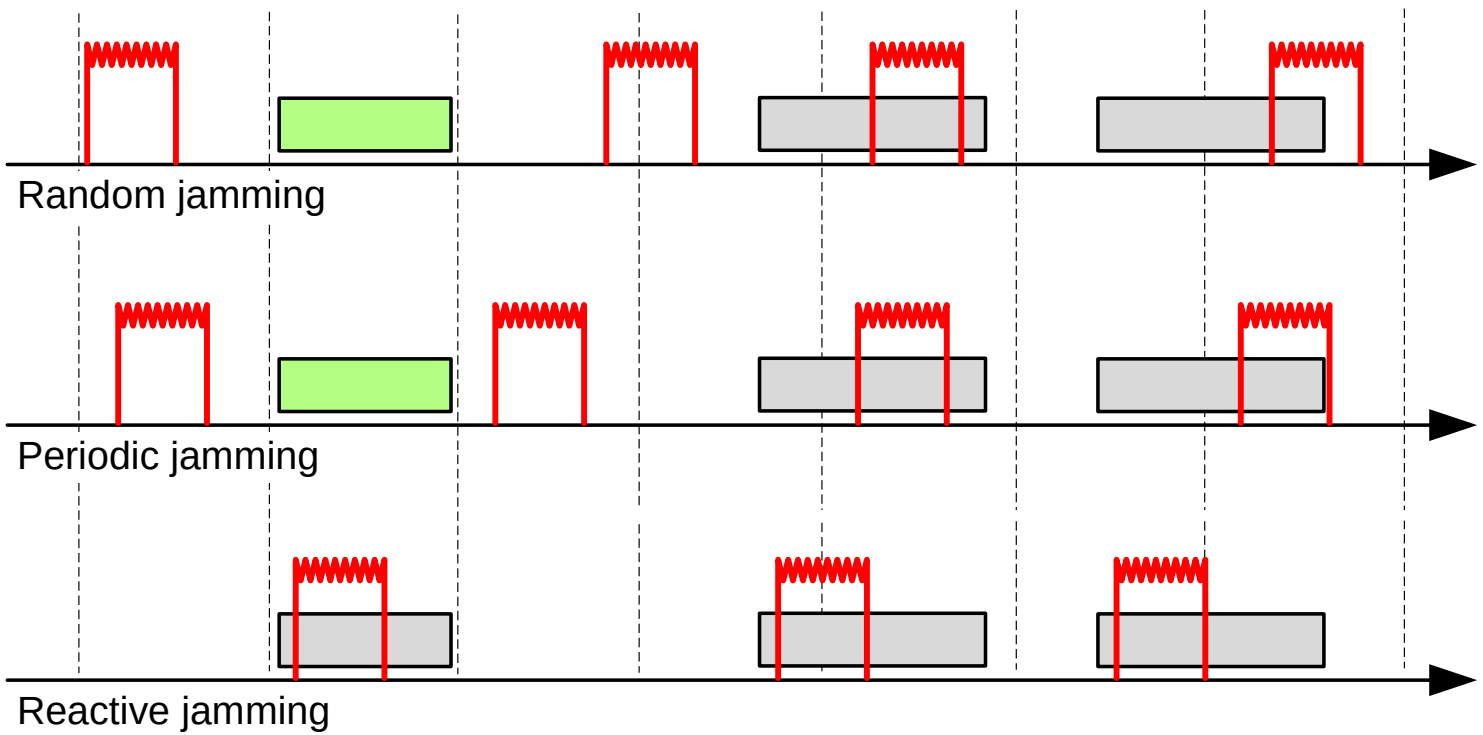
Modeling for time-critical transmission.

- A direct map from the application layer to MAC layer.
- Retransmission of a failed packet until the deadline.



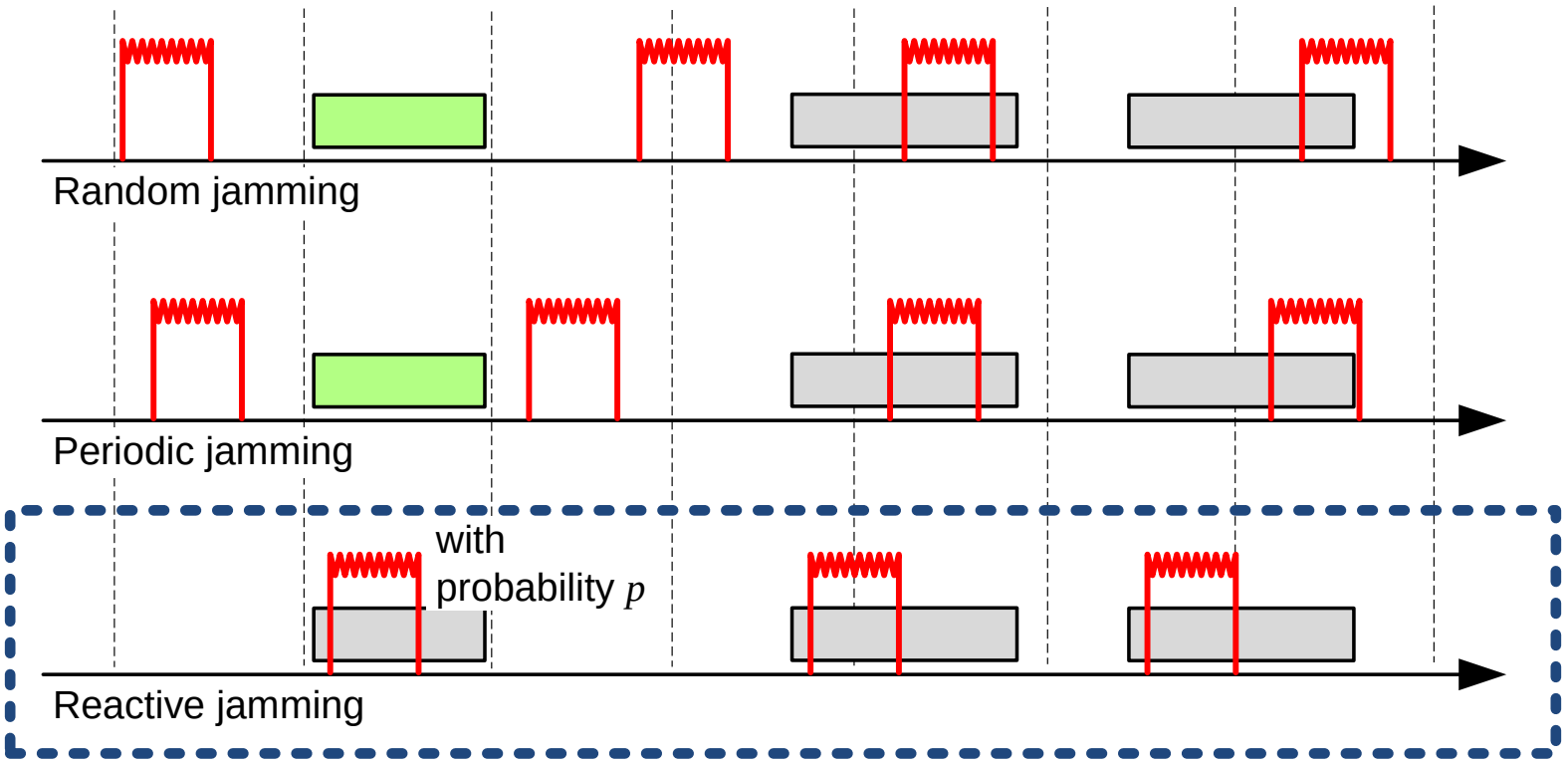
Models for Jamming Attacks

Various jamming models available in the literature (Xu'02, Bayraktaroglu'08)



Models for Jamming Attacks

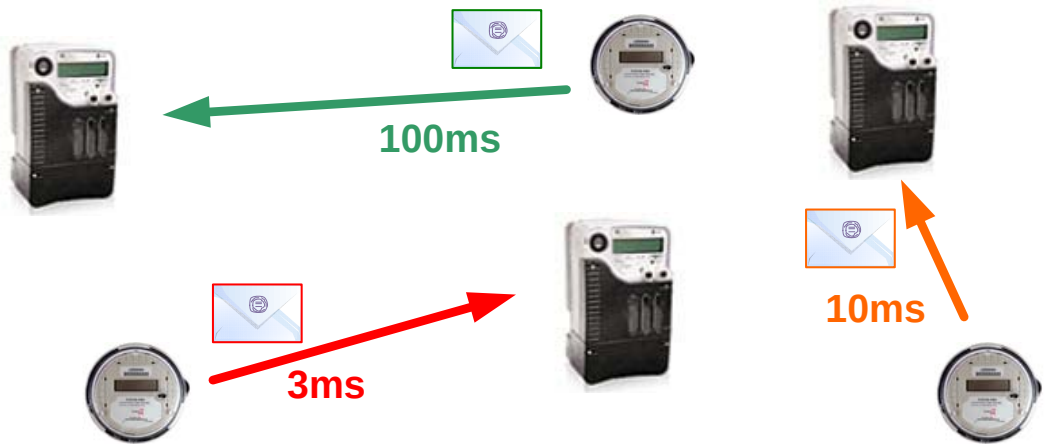
Various jamming models available in the literature (Xu'02, Bayraktaroglu'08)



In this paper, we consider reactive jamming as it is the primary focus in existing work.

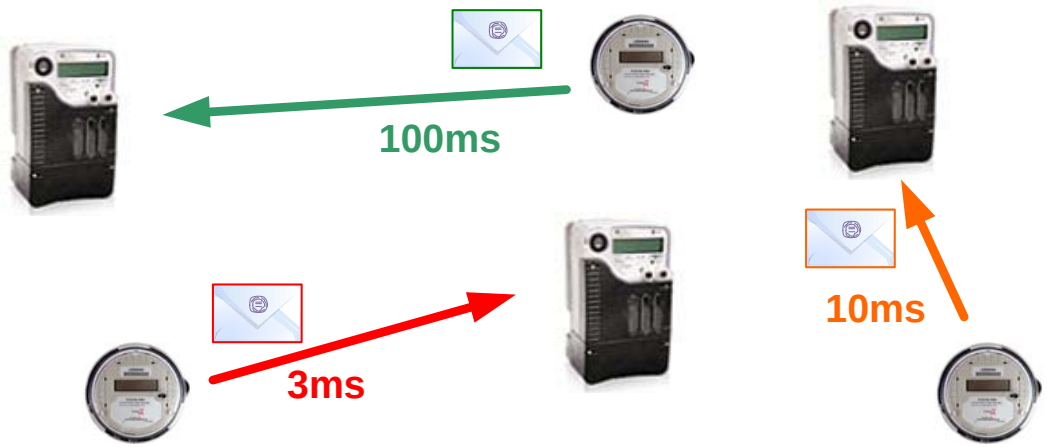
Performance Metric

The goal of time-critical network is to deliver time-critical messages with specific delay thresholds.



Performance Metric

The goal of time-critical network is to deliver time-critical messages with specific delay thresholds.

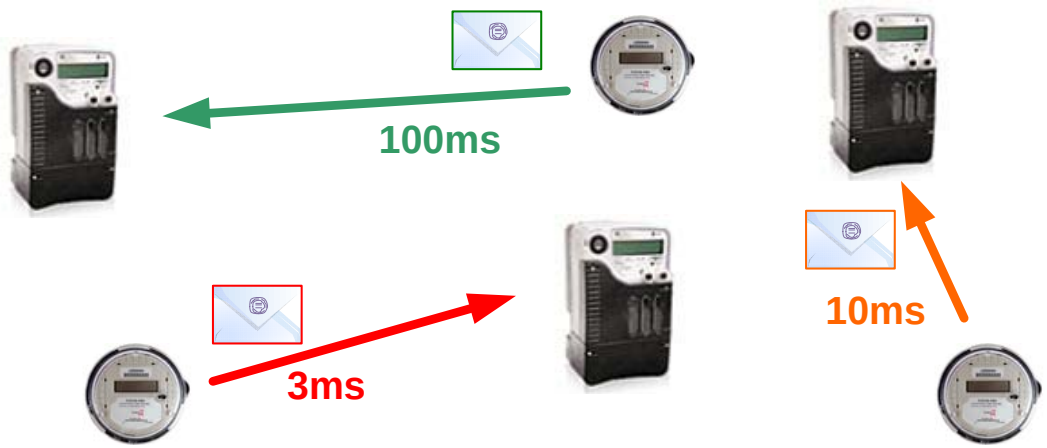


The metric should

1. be message-oriented.
2. directly reflect the delay constraints.

Performance Metric

The goal of time-critical network is to deliver time-critical messages with specific delay thresholds.



Message Invalidation Ratio

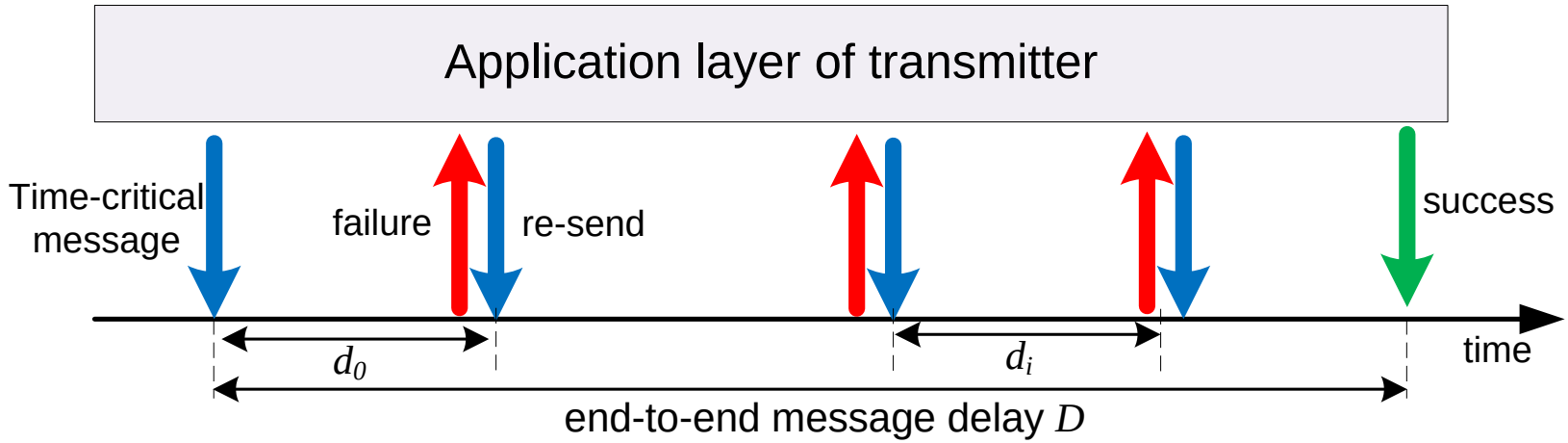
For a time-critical message with delay constraint σ, the message invalidation ratio is defined as

$$r = \mathbb{P}\{D > \sigma\},$$

where D is the end-to-end application-layer delay of the message.

Outline

Problem Formulation for End-to-End Delay



The end-to-end application delay:

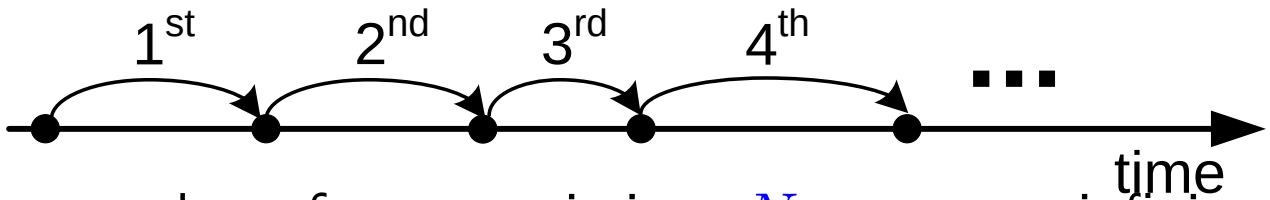
$$D = \sum_{i=0}^{N} d_i,$$

where d_i is the i.i.d. delay for i-th retransmission at the MAC layer, and N is the number of retransmissions.

The message invalidation ratio: $r = \mathbb{P}(D > \sigma)$.

Assumption: Dumb Transmitter

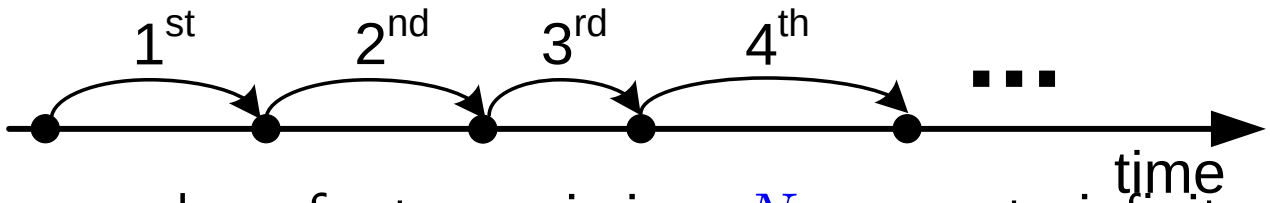
Assumption: A dumb transmitter always re-sends a transmission-failed packet until it is successfully delivered to the receiver.



- The number of retransmissions N can go to infinity.
  - enables asymptotic analysis. (Malone'07, Bayraktaroglu'08)

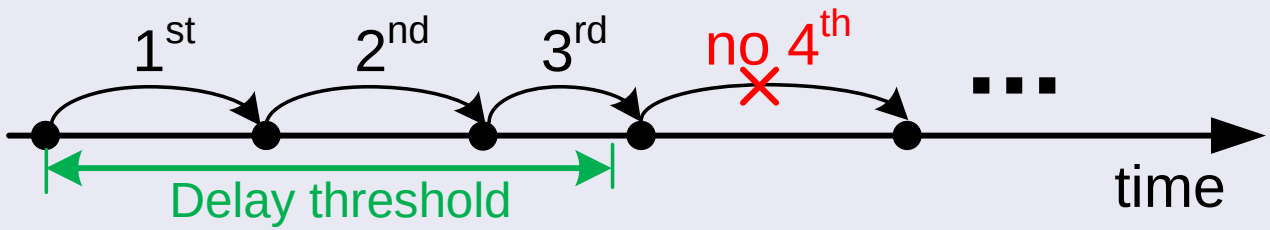
Assumption: Dumb Transmitter

Assumption: A dumb transmitter always re-sends a transmission-failed packet until it is successfully delivered to the receiver.



- The number of retransmissions N can go to infinity.
  - enables asymptotic analysis. (Malone'07, Bayraktaroglu'08)

Practical challenge: A message is retransmitted until the deadline.



- N is an upper-bounded random variable dynamically coupled with the cumulative delay in history.
- Mathematically, N is a stopping time. (need non-asymptotic tools!)

Martingale Theory

An effective tool to solve stopping time related mathematical problems.

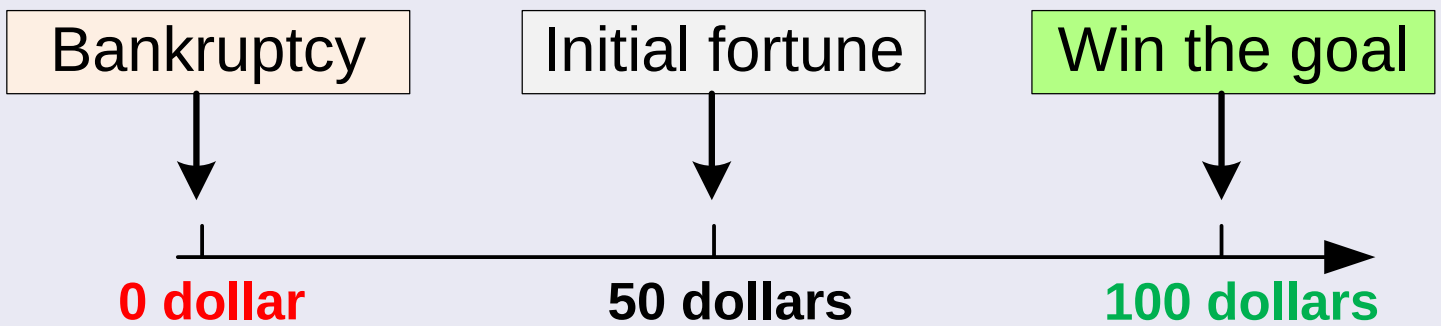
- Part of the motivation is to formulate some problems in gambling.

An effective tool to solve stopping time related mathematical problems.

- Part of the motivation is to formulate some problems in gambling.

Gambler's ruin

In each play, he wins (or, loses) 1 dollar with probability p (or, $1-p$).



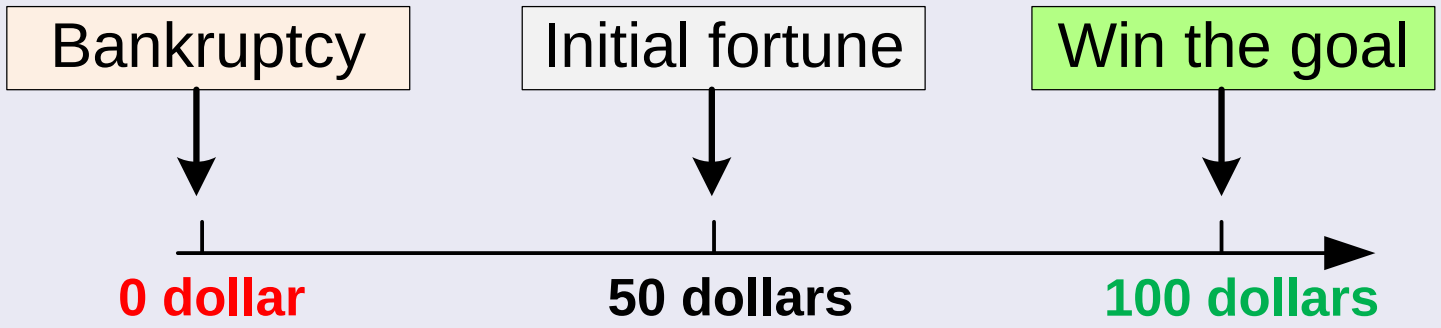
What is the probability that the gambler can win the game?

An effective tool to solve stopping time related mathematical problems.

- Part of the motivation is to formulate some problems in gambling.

Gambler's ruin

In each play, he wins (or, loses) 1 dollar with probability p (or, $1-p$).

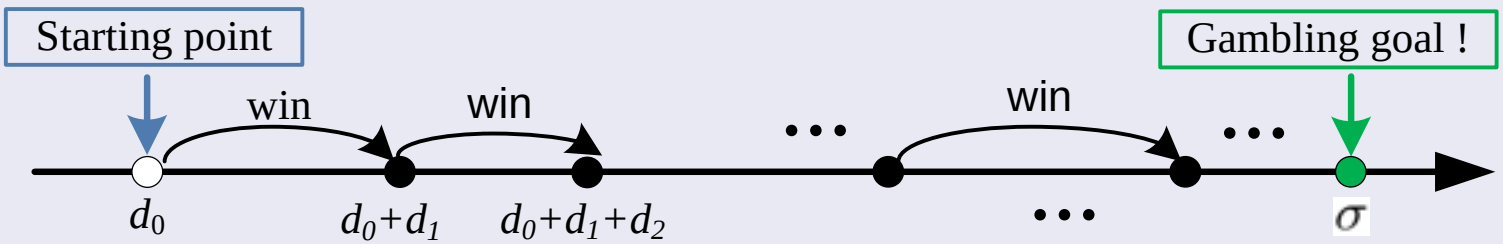


What is the probability that the gambler can win the game?

From Jammer to Gambler

The Jammer is a gambler

- Delay $\Rightarrow$ money
- Delay threshold $\Rightarrow$ gambler's winning goal.



- Message invalidation: the jammer keeps jamming each transmission of a message such that the cumulative delay is larger than the delay threshold.
- The gambler wins: the gambler keeps winning each play such that the cumulative money is larger than his goal.

Analytical Results Based on Martingale Theory

Theorem (Message invalidation ratio for general cases)

Given a jamming strategy $\mathcal{J}(p)$, the message invalidation ratio r is

$$r = \frac{\mathbb{E}(D_s) - \frac{c}{1-p_a}}{\mathbb{E}(D_s) - \frac{p_a c}{1-p_a} - \mathbb{E}(D_u)},$$

where $p_a = p^{N_{mac}}$, N_{mac} is the retry number at MAC layer, $c = \mathbb{E}(d_i)$ is the mean of the i.i.d. MAC-layer delay d_i, $D_s \leq \sigma$ is the end-to-end delay of a successfully delivered message, and $D_u > \sigma$ is the delay of failed message delivery.

Theorem (General upper bound)

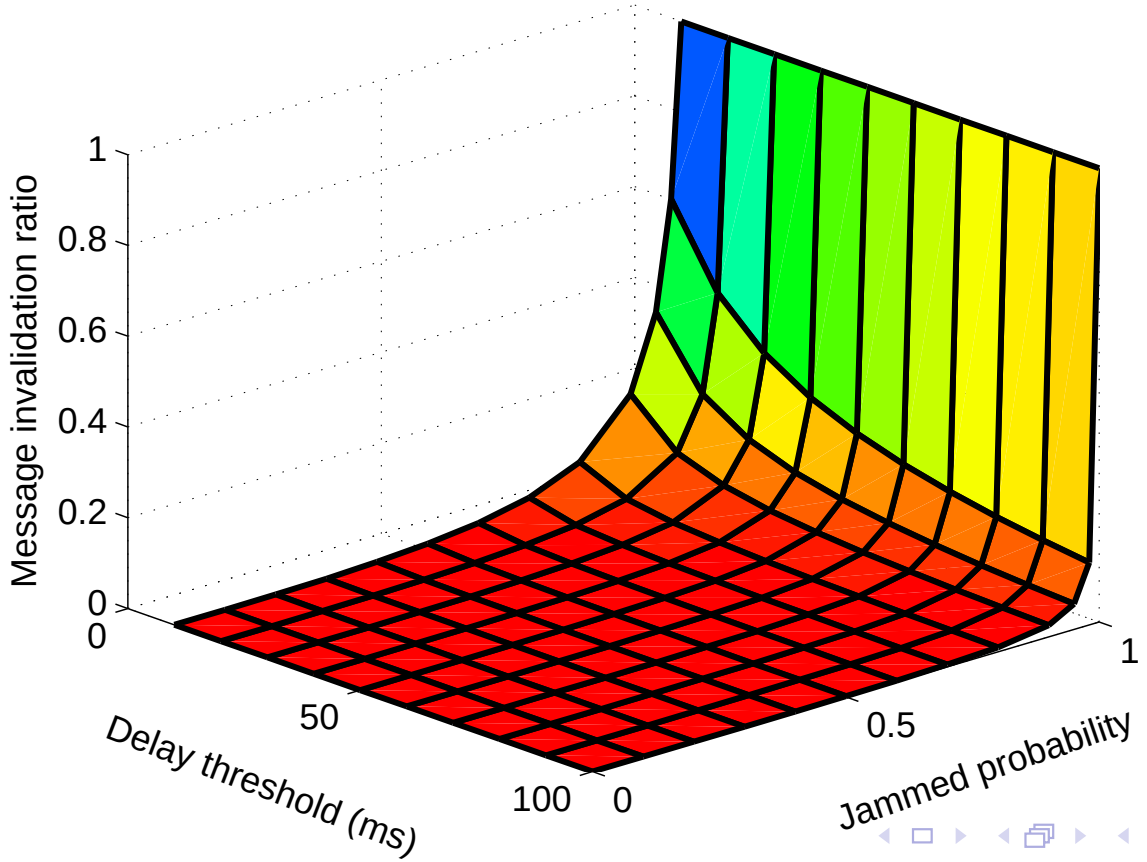
For the message invalidation ratio r in Theorem 1, it satisfies that

$$r \leq \frac{p^{N_{mac}} c}{(1 - p^{N_{mac}})(\sigma - c) + p^{N_{mac}} c}.$$

Indication of Analytical Results

Phase transition for message invalidation ratio:

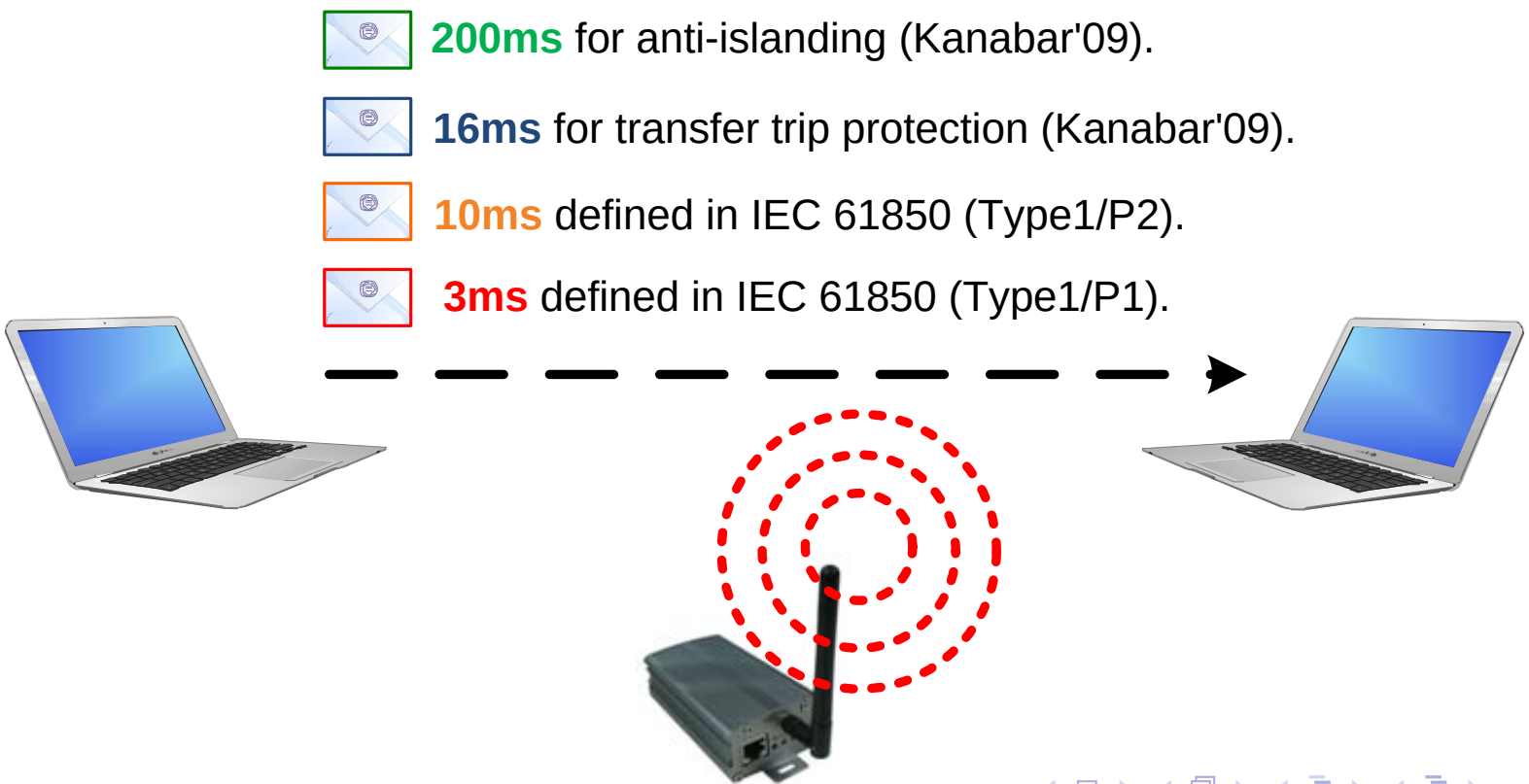
- Slightly-increasing phase: increases negligibly with the increasing of the jamming probability p.
- Dramatically-increasing phase: increases dramatically (and linearly) with the increasing of the jamming probability p.



Experimental Evaluation: Setups

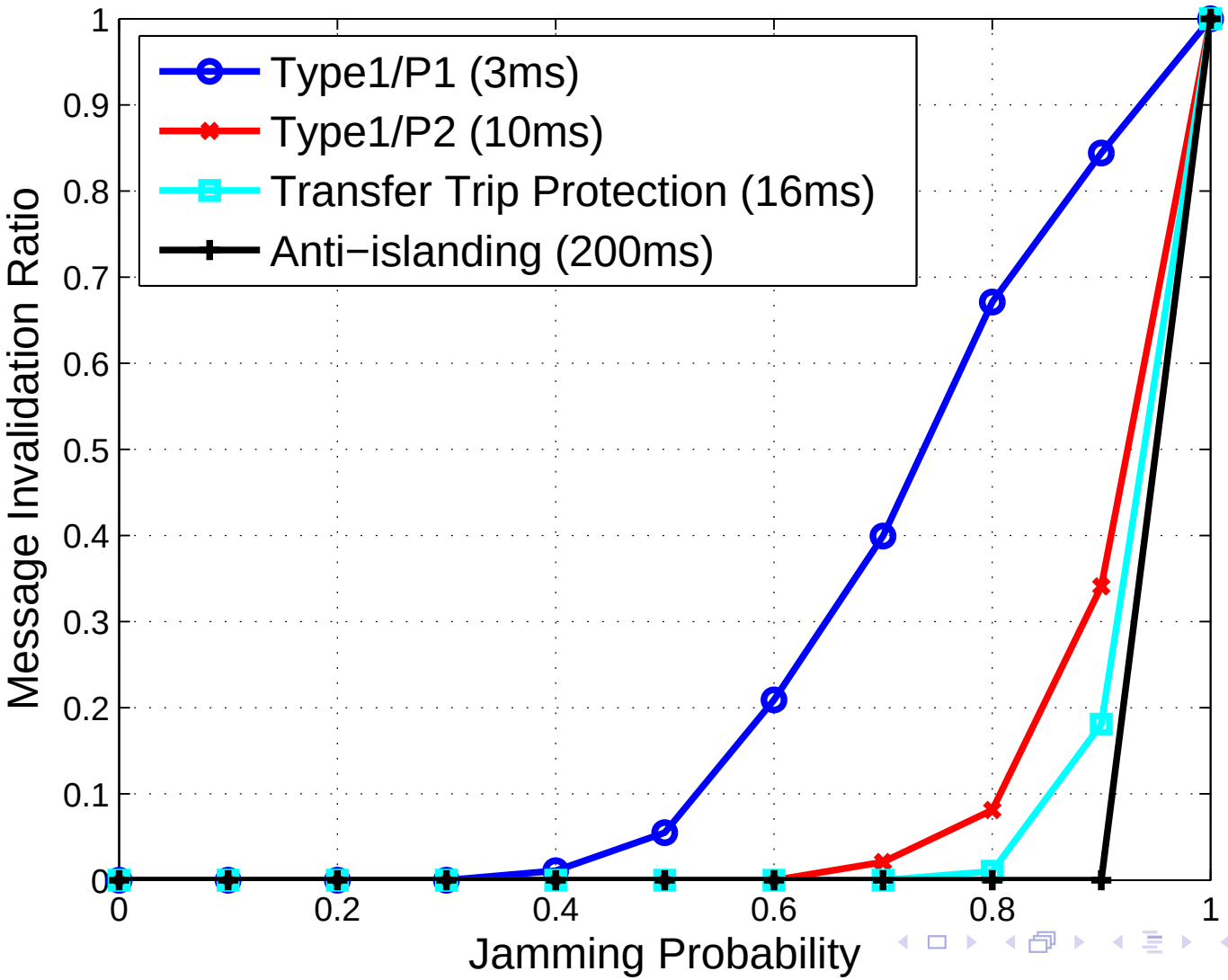
Setups:

- Network: a WiFi-based substation network. (WiFi Aliance'09, Kanabar'09, Akyol'10)
- Jammer: USRP with RNU Radio.
- Time-critical messages: 4 GOOSE applications.



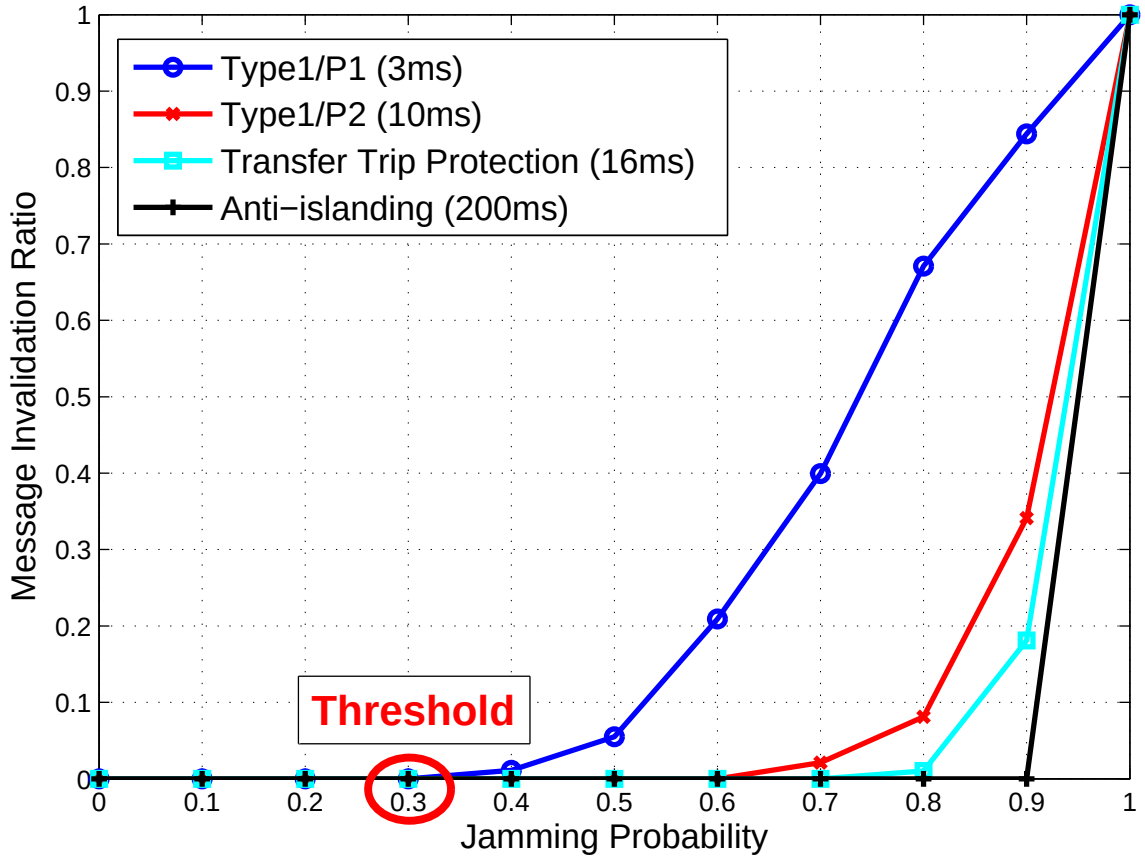
Experimental Results: Message Invalidation Ratio

GOOSE messaging between a transmit-receive pair under jamming.



Outline

JADE: Jamming Attack Detection based on Estimation



1. Transmit a number of packets.
2. Estimate the jamming probability $\hat{p}$ based on transmission results (e.g. no ACK)
3. if $\hat{p} > p^*$, jamming exists. The threshold p^* is chosen smaller than the transition point: $p^* = 0.3$.

Experimental Results of JADE

Jammer: time-varying with jamming probability p uniformly distributed on $[0.4, 0.9]$.

Benchmark: the Likelihood Ratio (LLR) Test (Li'07) is the theoretically optimal detector for deterministic models.

Experimental Results of JADE

Jammer: time-varying with jamming probability p uniformly distributed on $[0.4, 0.9]$.

Benchmark: the Likelihood Ratio (LLR) Test (Li'07) is the theoretically optimal detector for deterministic models.

Table: Detection Ratios of both JADE and LLR Test

Number of Samples:	50	100	150	200
Detection Time:	54ms	109ms	163ms	218ms
JADE:	98.6%	99.1%	100%	100%
LLR Test :	91.3%	92.1%	92.5%	91.6%

Experimental Results of JADE

Jammer: time-varying with jamming probability p uniformly distributed on $[0.4, 0.9]$.

Benchmark: the Likelihood Ratio (LLR) Test (Li'07) is the theoretically optimal detector for deterministic models.

Table: Detection Ratios of both JADE and LLR Test

Number of Samples:	50	100	150	200
Detection Time:	54ms	109ms	163ms	218ms
JADE:	98.6%	99.1%	100%	100%
LLR Test :	91.3%	92.1%	92.5%	91.6%

- The LLR Test has a model mismatching problem in dealing with a practical time-vary jammer.

Outline

Conclusion

1. Motivated by emerging time-critical wireless applications, we introduce the message invalidation ratio to quantify the impact of jamming attacks against time-critical traffic.
   - Theoretical results: Gambling based modeling.
   - Experimental results: GOOSE messaging in IEC 61850.
2. We show a phase transition phenomenon for the message invalidation ratio.
   - Slightly-increasing phase.
   - Dynamically-increasing phase.
3. We developed a JADE system to achieve simple, efficient and robust jamming detection for power substation networks.

Thank you!