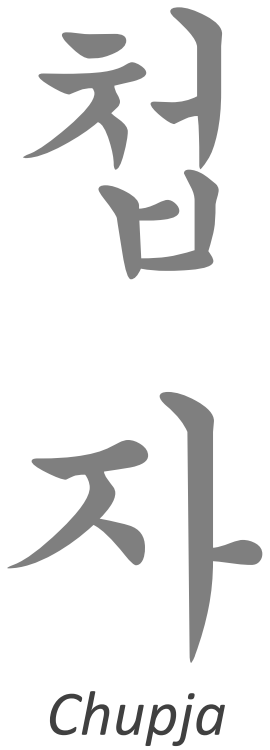
PHY Covert Channels: Can you see the Idles?

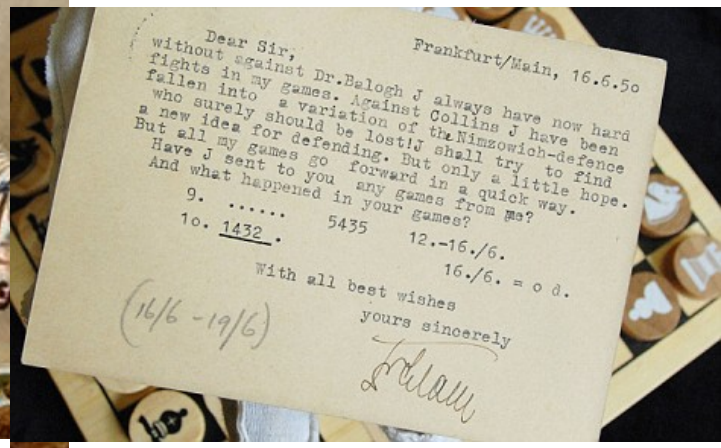


Ki Suh Lee
Cornell University

Joint work with Han Wang, and Hakim Weatherspoon

첩자 (chupja)


Goguryeo 고구려
Baekje 백제
Silla 신라


Dear Sir,
Frankfurt/Main, 16.6.5o
without against Dr.Balogh J always have now hard
fights in my games. Against Collins J have been
fallen into a variation of the Nimzowich-defence
who surely should be lost! J shall try to find
a new idea for defending. But only a little hope.
But all my games go forward in a quick way.
Have J sent to you any games from me?
And what happened in your games?
9. .....
1o. 1432. 5435 12.-16./6.
16./6. = o d.
With all best wishes
yours sincerely
(16/6 -19/6)

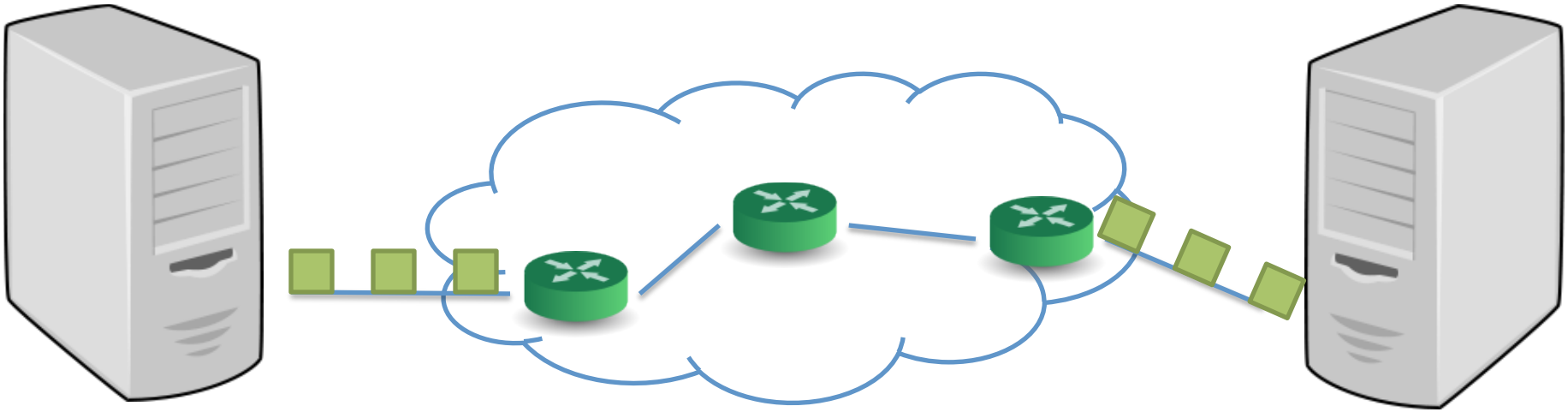

Setauket ★ Long Island ★ New York ★ 1778-1781
SPIES!

Covert Channels

- Hiding information
  - Through communication not intended for data transfer

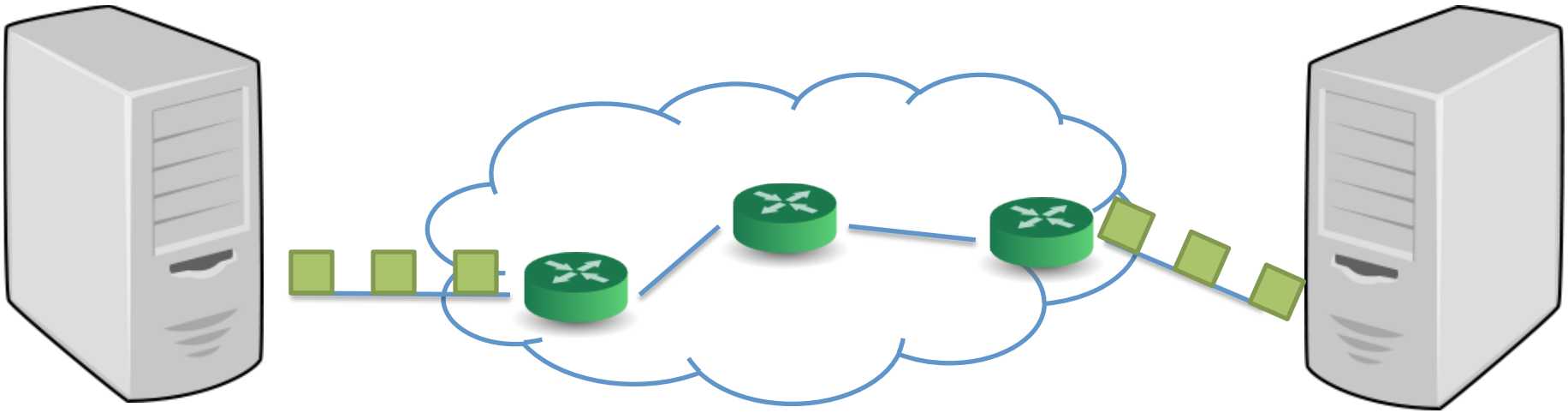
Network Covert Channels

- Hiding information
  - Through communication not intended for data transfer
  - Using legitimate packets (Overt channel)
    - Storage Channels: Packet headers
    - Timing Channels: Arrival times of packets



Network Covert Channels

- Hiding information
  - Through communication not intended for data transfer
  - Using legitimate packets (Overt channel)
    - Storage Channels: Packet headers
    - Timing Channels: Arrival times of packets

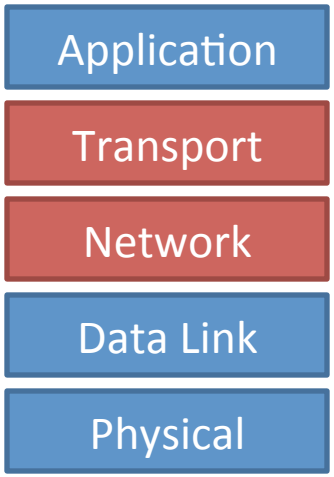


Goals of Covert Channels

- Bandwidth
  - How much information can be delivered in a second
- Robustness
  - How much information can be delivered without loss / error
- Undetectability
  - How well communication is hidden

Goals of Covert Channels

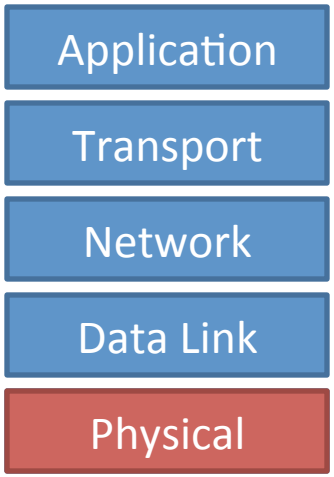
- Bandwidth
  - How much information can be delivered in a second
  - 10~100s bits per second
- Robustness
  - How much information can be delivered without loss / error
  - Cabuk'04, Shah'06
- Undetectability
  - How well communication is hidden
  - Liu'09, Liu'10



Current network covert channels
are implemented in L3~4 (TCP/IP) layers
and are *extremely* ***slow***.

Chupja: PHY Covert Channel

- Bandwidth
  - How much information can be delivered in a second
  - ~~10~100s bits per second~~ -> 10s~100s ***Kilo*** bits per second
- Robustness
  - How much information can be delivered without loss / error
  - Bit Error Rate < 10%
- Undetectability
  - How well communication is hidden
  - Invisible to detection software



Chupja is a network covert channel
which is faster *than priori art*.

It is implemented in L1 (PHY),
robust and virtually invisible to software.

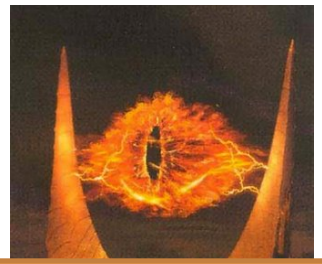
Outline

- Introduction
- Design
- Evaluation
- Conclusion

Outline

- Introduction
- Design
  - Threat Model
  - 10 Gigabit Ethernet
- Evaluation
- Conclusion

Threat Model



Passive Adversary

Commodity Server
Commodity NIC

Application
Transport
Network
Data Link
Physical

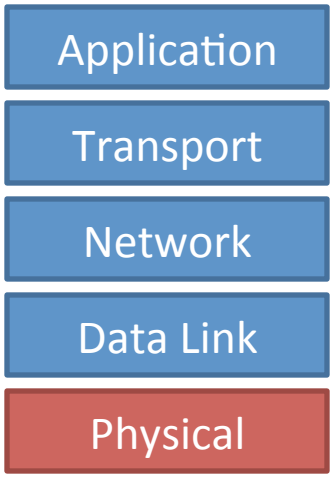
Sender

Application
Transport
Network
Data Link
Physical

Receiver

10 Gigabit Ethernet

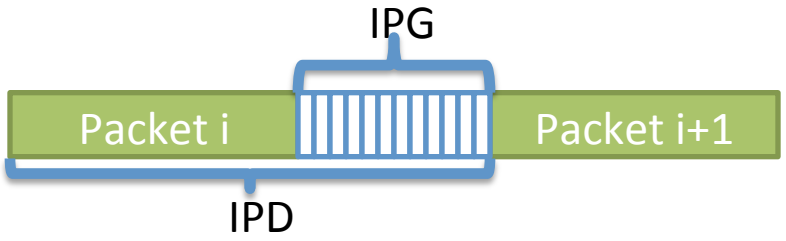
- Idle Characters (/I/)



  - Each bit is ~100 picosecond wide
  - 7~8 bit special character in the physical layer
  - 700~800 picoseconds to transmit
  - Only in PHY

Terminology

- Interpacket delays (D) and gaps (G)

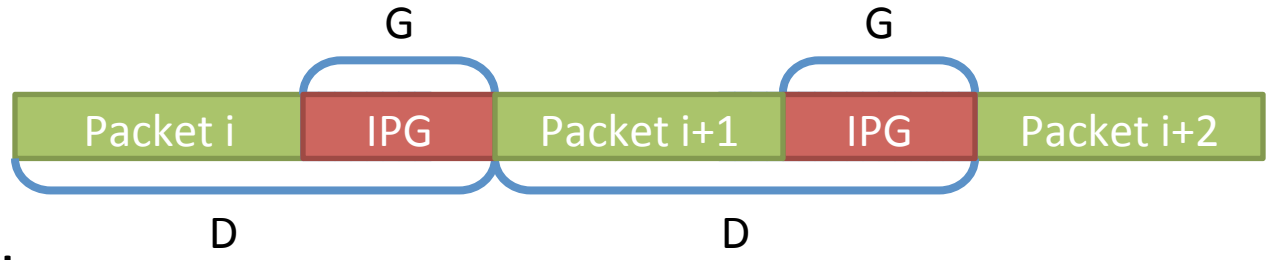


- Homogeneous packet stream

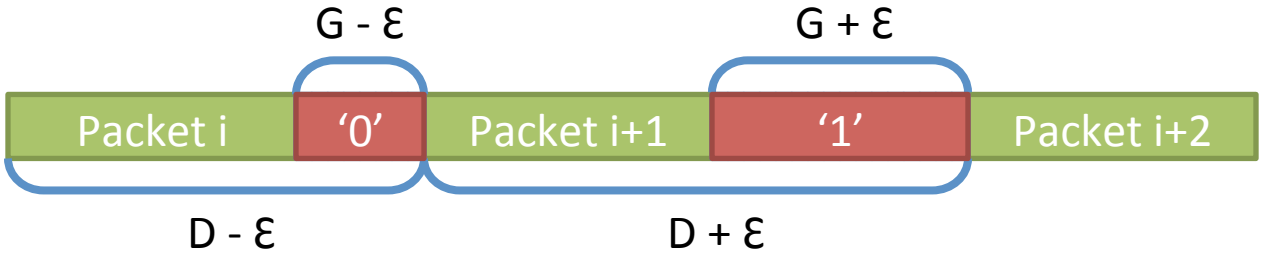
  - Same packet size,
  - Same IPD (IPG),
  - Same destination

Chupja: Design

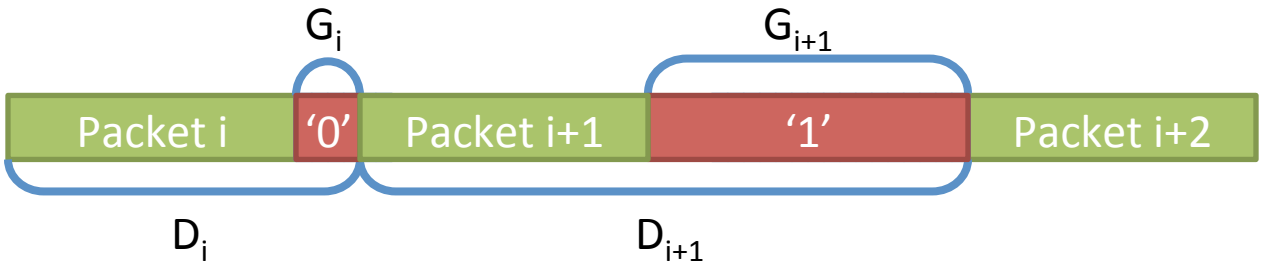
- Homogeneous stream



- Sender

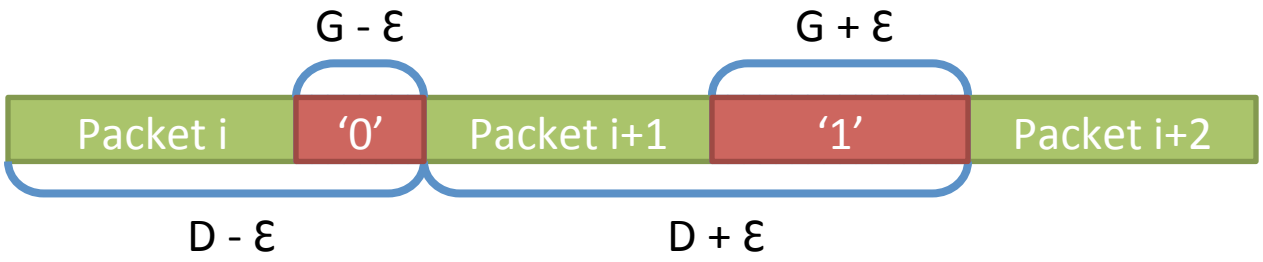


- Receiver



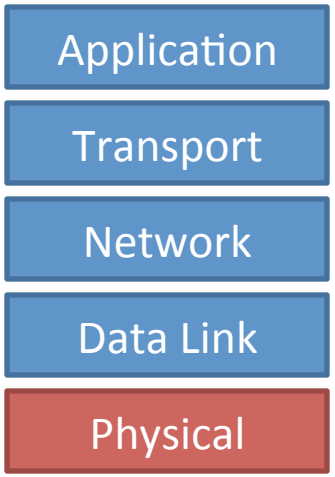
Chupja: Design

- With shared *G*
  - Encoding ‘1’: $G_i = G + \varepsilon$
  - Encoding ‘0’: $G_i = G - \varepsilon$



Implementation

- SoNIC [NSDI '13]
  - Software-defined Network Interface Card
  - Allows control and access *every bit* of PHY
    - In realtime, and in software
- 50 lines of C code addition



Outline

- Introduction
- Design
- Evaluation
  - Bandwidth
  - Robustness
  - Undetectability
- Conclusion

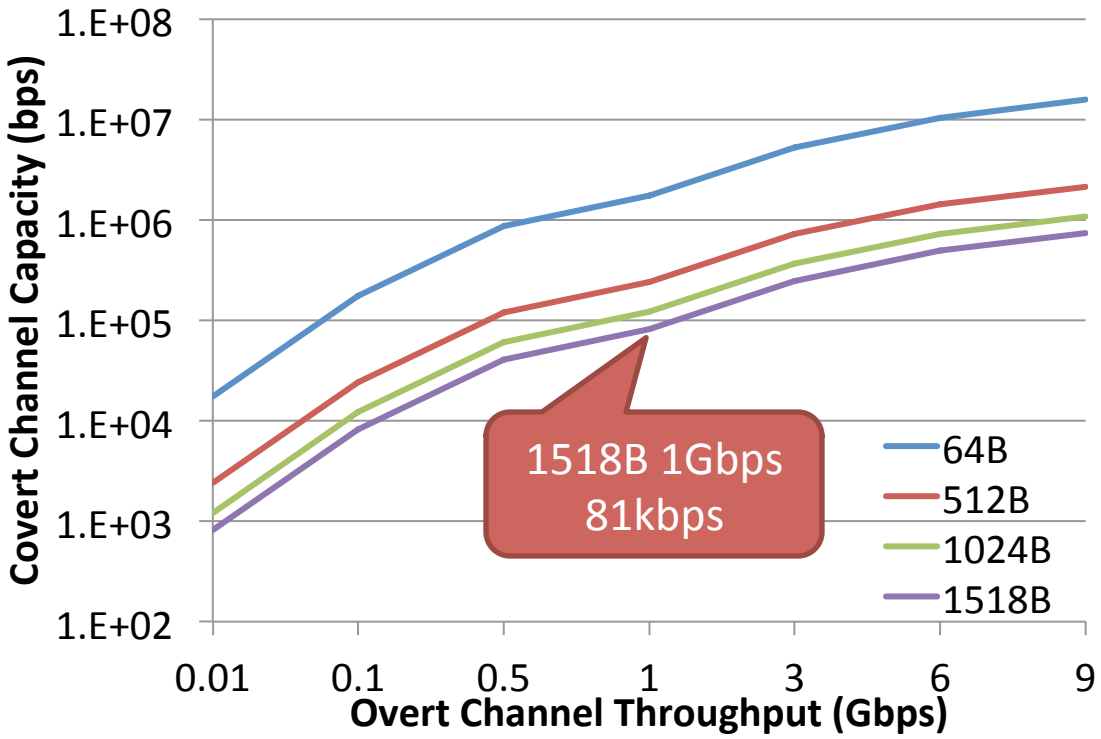
Evaluation

- What is the *bandwidth* of *Chupja*?
- How *robust* is *Chupja*?
  - *Why* is *Chupja* robust?
- How *undetectable* is *Chupja*?

What is the *bandwidth* of *Chupja*?

Evaluation: Bandwidth

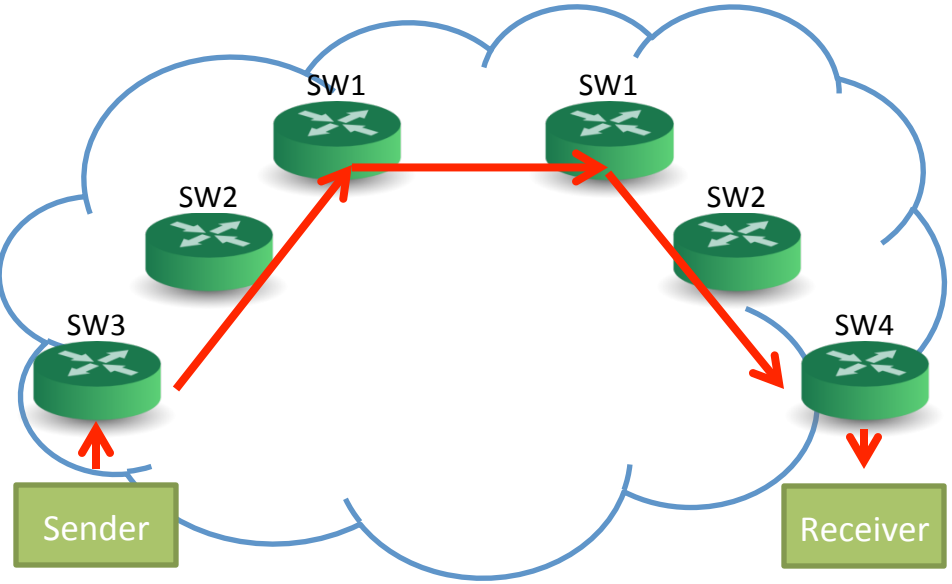
- Covert bandwidth equals to ***packet rate*** of overt channel

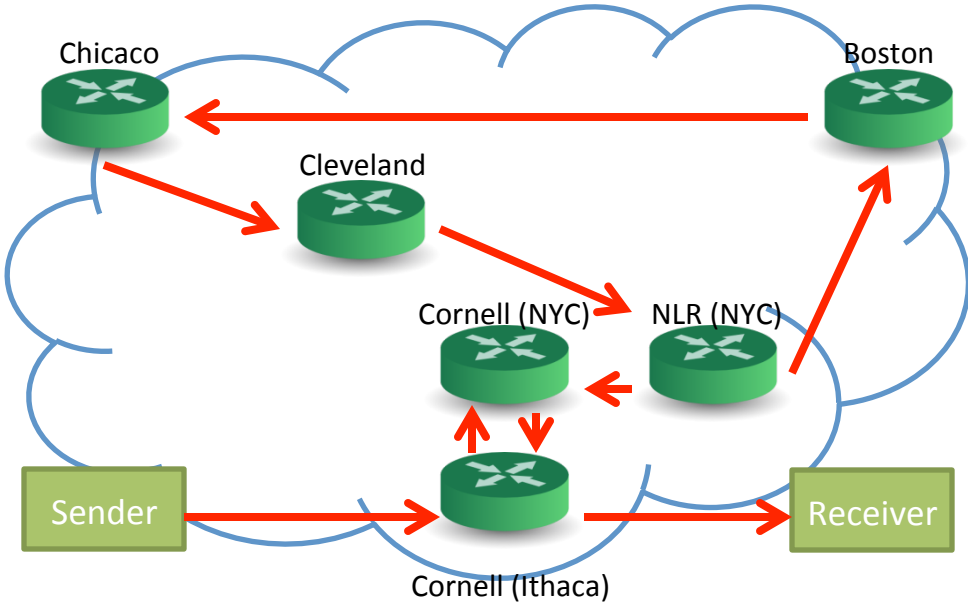


How *robust* is *Chupja*?

Evaluation Setup

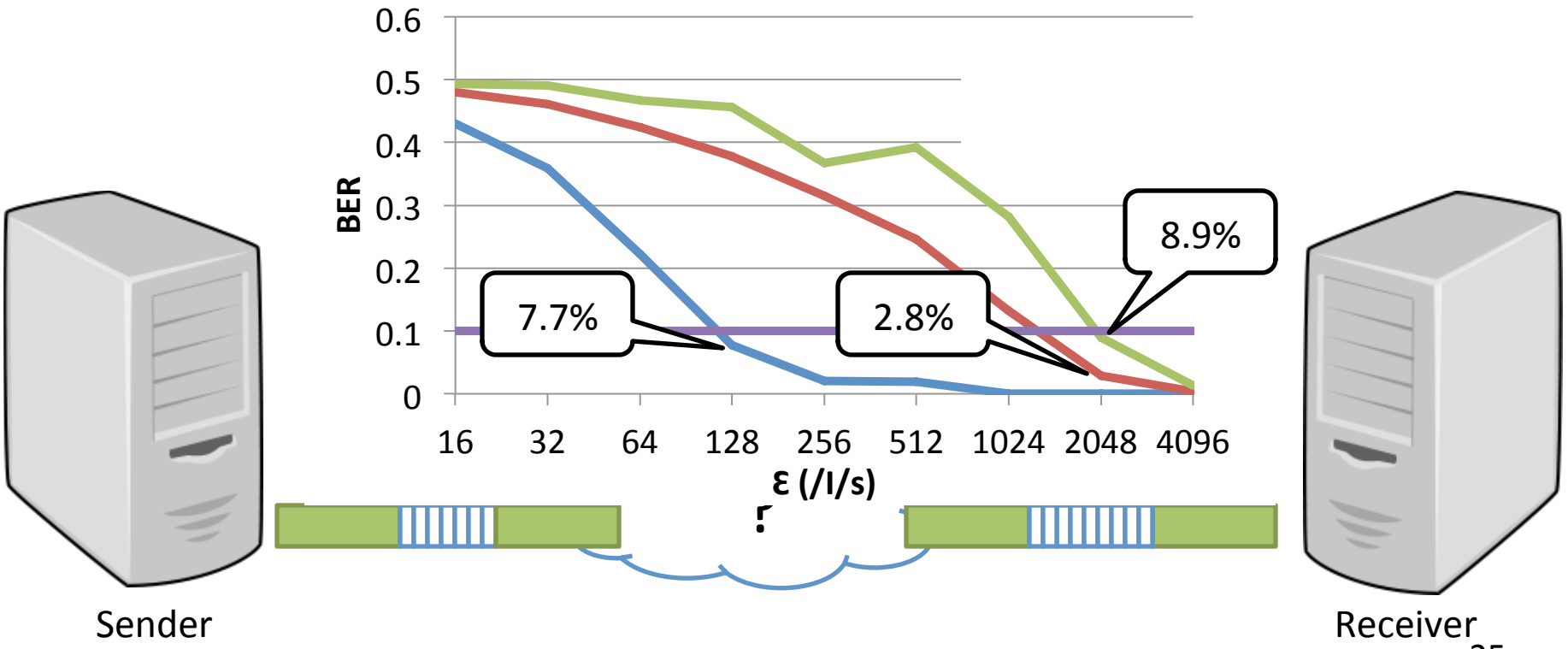
- Small Network
  - Six commercial switches
  - Average RTT: 0.154 ms
- National Lambda Rail
  - Nine routing hops
  - Average RTT: 67.6ms
  - 1~2 Gbps External Traffic





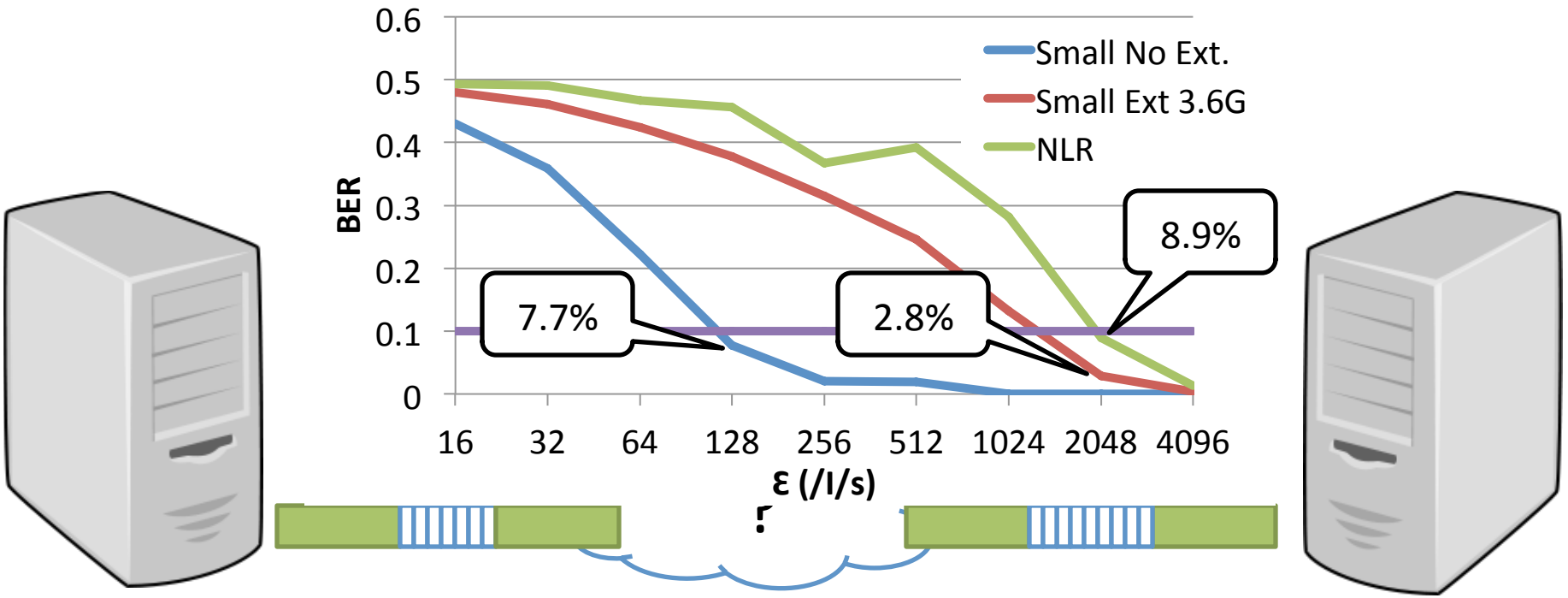
Evaluation: Robustness

- Overt Channel at 1 Gbps (D = 12211ns, G=13738 /l/s)
- Covert Channel at 81 kbps



Evaluation: Robustness

- Overt Channel at 1 Gbps (D = 12211ns, G=13738 /I/s)
- Covert Channel at 81 kbps
- *Modulating IPGS at 1.6us scale (=2048 /I/s)*



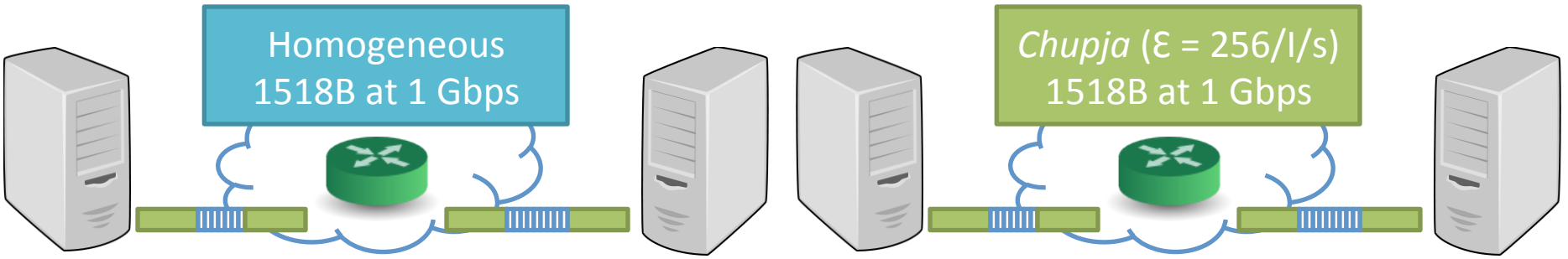
Why is *Chupja* robust?

Evaluation: Why?

- Switches do not add significant perturbations to IPDs
- Switches treat ‘1’s and ‘0’s as *uncorrelated*
  - *Over multiple hops* when there is *no external traffic*.
  - *With external traffic*

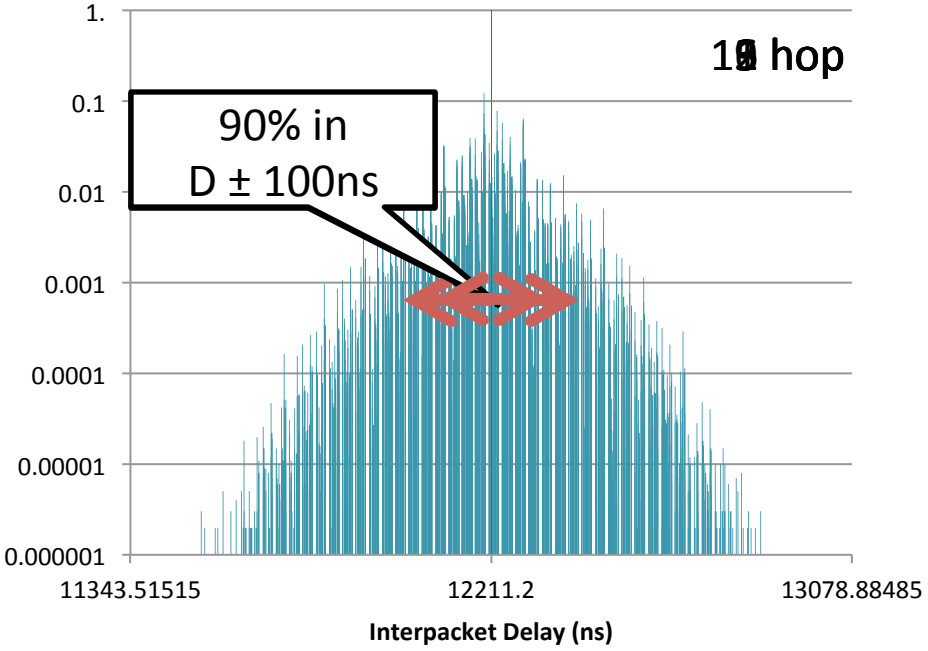
Evaluation: Why?

- Switches do not add significant perturbations to IPDs
- Switches treat '1's and '0's as *uncorrelated*
  - *Over multiple hops* when there is *no external traffic*.
  - *With external traffic*

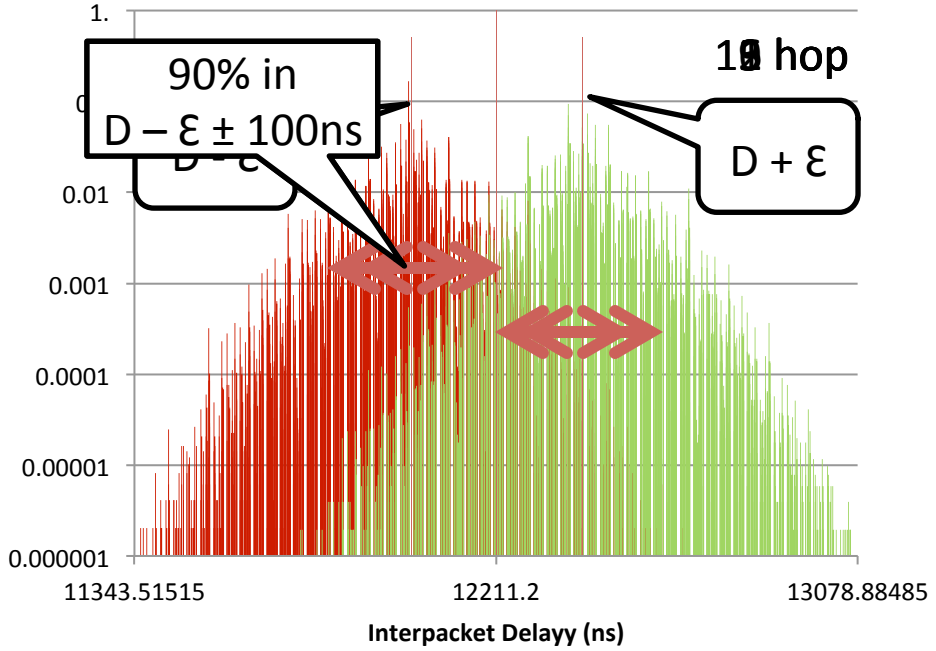


Evaluation: Why?

- Switches do not add significant perturbations to IPDs
- Switches treat encoded '0' and '1' as uncorrelated
  - *Over multiple hops* when there is *no* external traffic.



Homogeneous stream

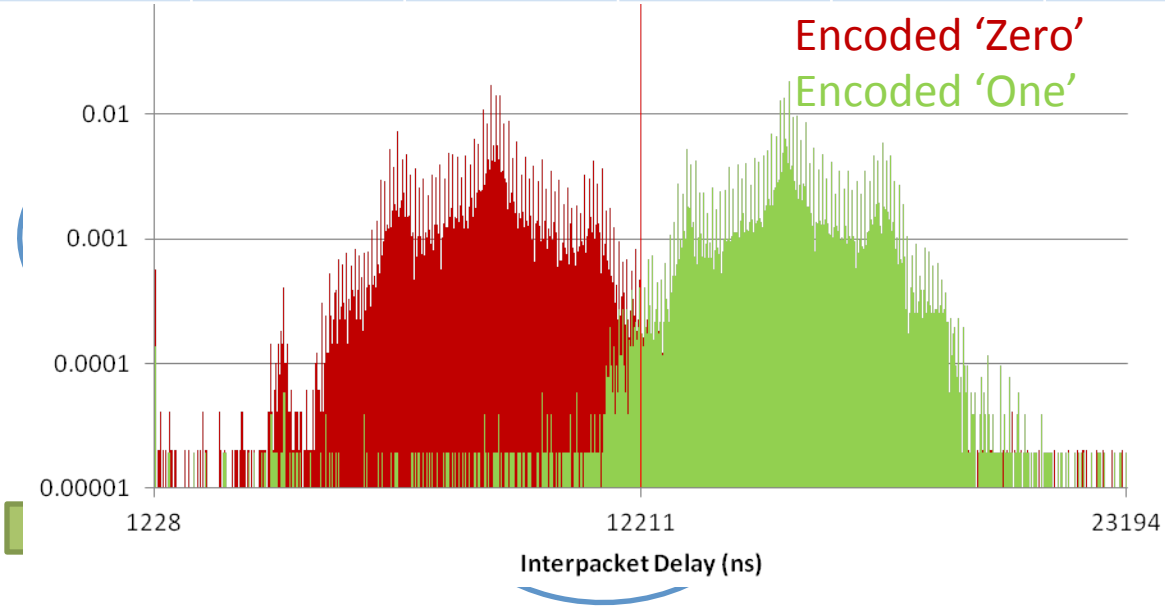


Chupja stream (Ɛ=256/l/s)

Evaluation: Why?

- Most of IPDs are within some range from original IPD
  - Even when there is *external traffic*.

Ɛ (/I/s) (ns)	256 (=204.8ns)	512 (=409.6)	1024 (=819.2)	2048 (=1638.4)	4096 (=3276.8)
BER					



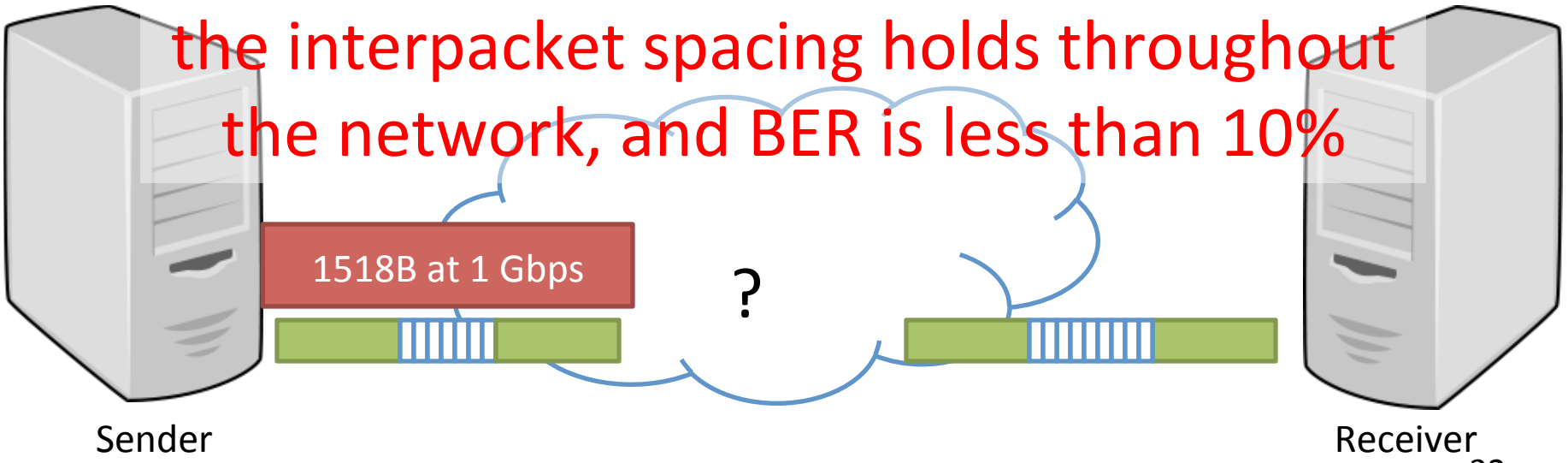
Sender

Receiver

Evaluation: Why?

- Switches do not add significant perturbations to IPDs
- Switches treat '1's and '0's as *uncorrelated*
  - *Over multiple hops* when there is *no external traffic*.
  - *With external traffic*

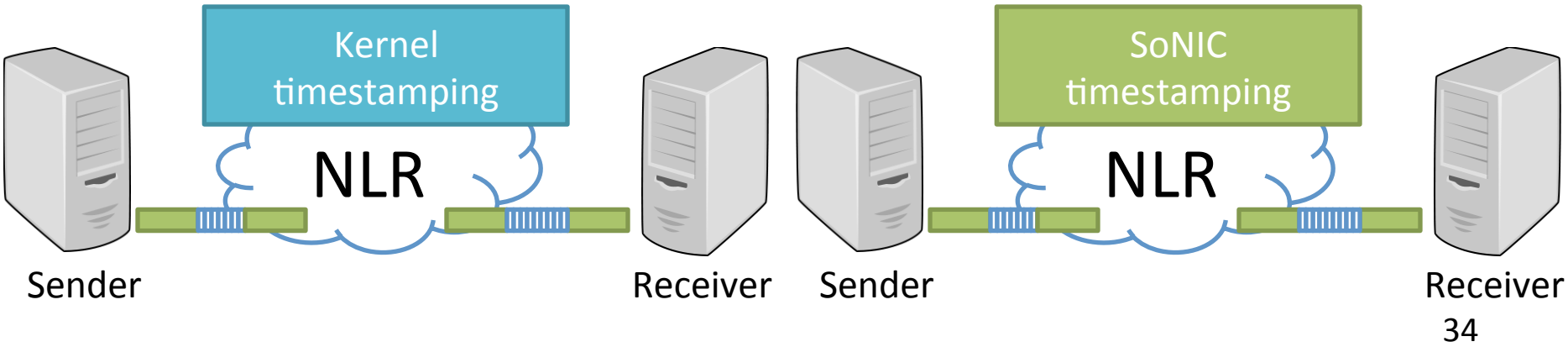
With sufficiently large Ɛ,
the interpacket spacing holds throughout
the network, and BER is less than 10%



How *undetectable* is *Chupja*?

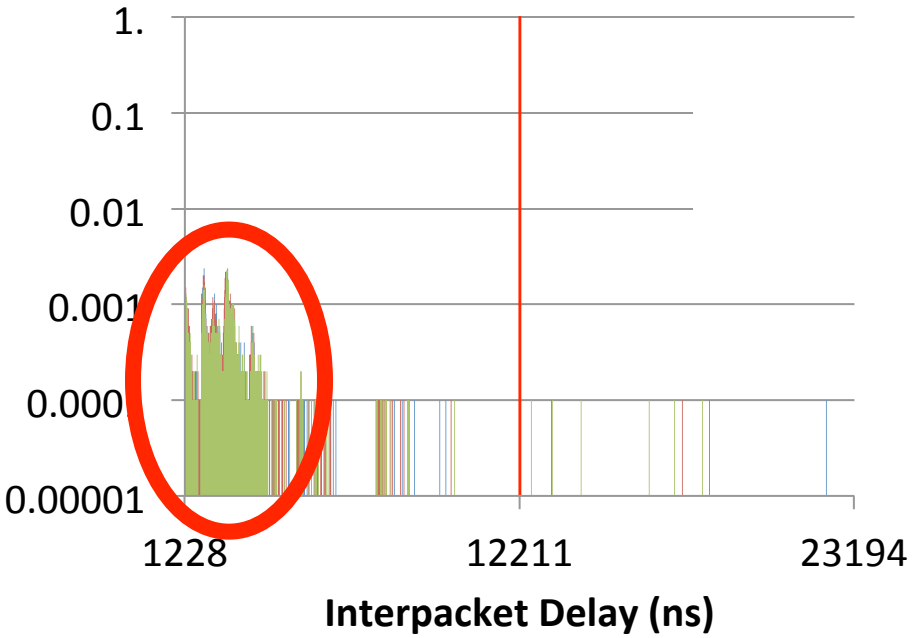
Evaluation: Detection Setup

- Commodity server with 10G NIC
  - Kernel timestamping

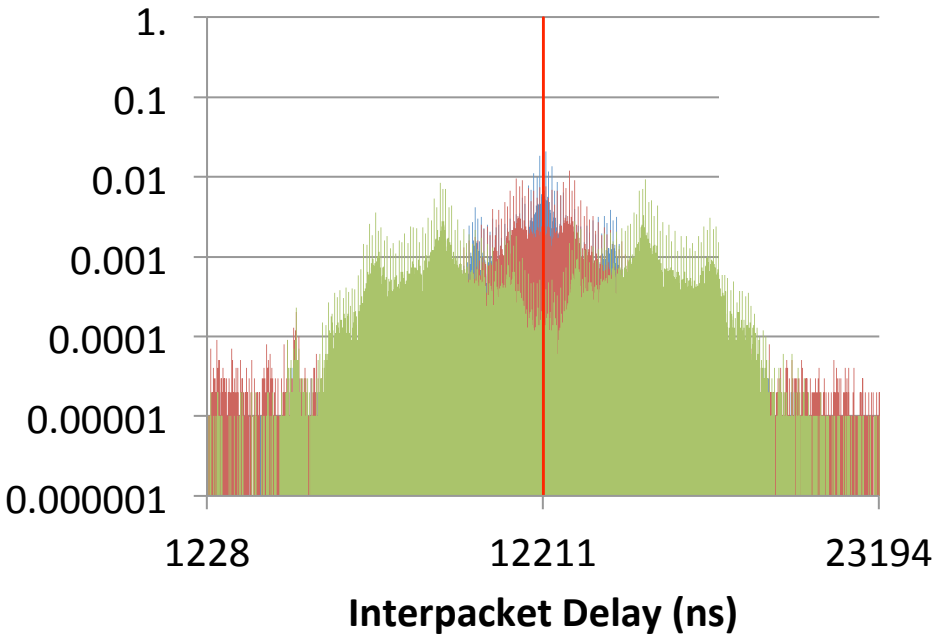


Evaluation: Detection

- *Adversary cannot detect patterns of Chupja*



Kernel Timestamping



SoNIC Timestamping

Evaluation: Summary

- What is the *bandwidth* of *Chupja*?
  - 10s~100s Kilo bits per second
- How *robust* is *Chupja*?
  - BER < 10% over NLR
  - *Why* is *Chupja* robust?
    - Sufficiently large Ɛ holds throughout the network
- How *undetectable* is *Chupja*?
  - Invisible to software

Conclusion

- *Chupja*: PHY covert channel
  - High-bandwidth, robust, and undetectable
- Based on understanding of network devices
  - Perturbations from switches
  - Inaccurate endhost timestamping
- http://sonic.cs.cornell.edu & GENI (ExoGENI)!!!

Thank you