The Role of Network Packet Loss Modeling in Reliable Transport of Broadcast Audio

April 14, 2015

NAB Show 2015

Featuring GatesAir's

Junius Kim
Hardware Engineer

Keyur Parikh
Architect / Software Lead

you live,
breathe and
eat this stuff

CONFERENCES: APRIL 11–16, 2015 • EXHIBITS: APRIL 13–16
LAS VEGAS CONVENTION CENTER • LAS VEGAS, NEVADA USA

NABSHOW Where Content Comes to Life

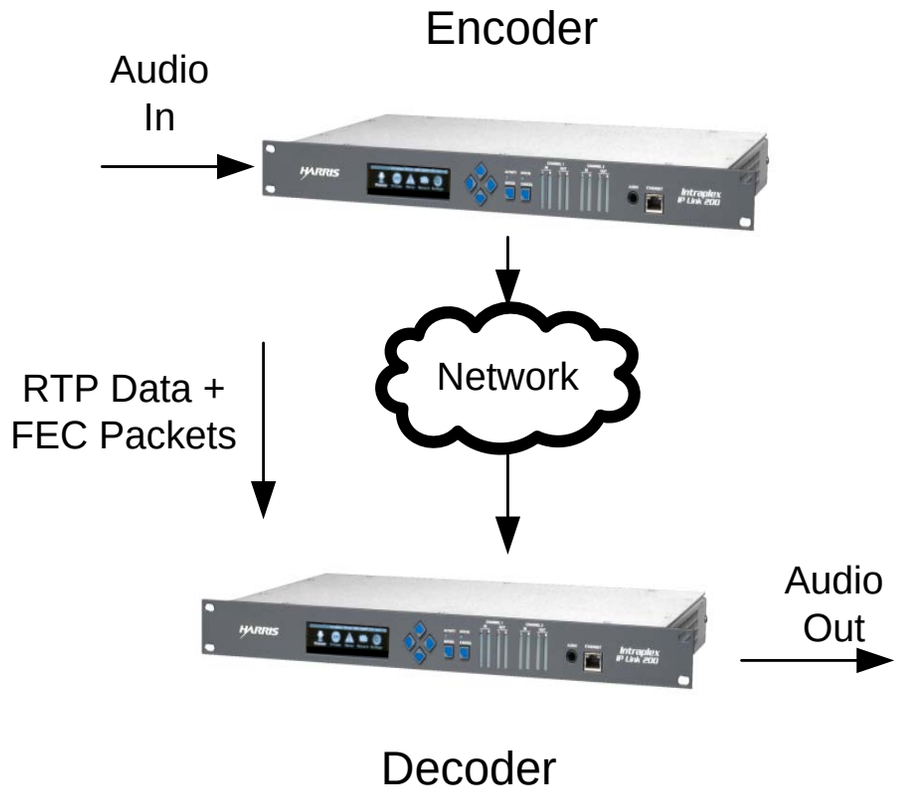
CRAVE MORE

The Role of Network Packet Loss Modeling in Reliable Transport of Broadcast Audio

Junius Kim and Keyur Parikh
GatesAir
Mason, OH

Overview

- Network Impairments
- Packet Loss Modeling
- Packet Loss Analysis
- Packet Loss Simulation
- Packet Loss Mitigation



AoIP Application

Network Impairments

- Jitter
- Out-of-Order Packets
- Duplicate Packets

  Well defined solution for above impairments…

- Packet Loss

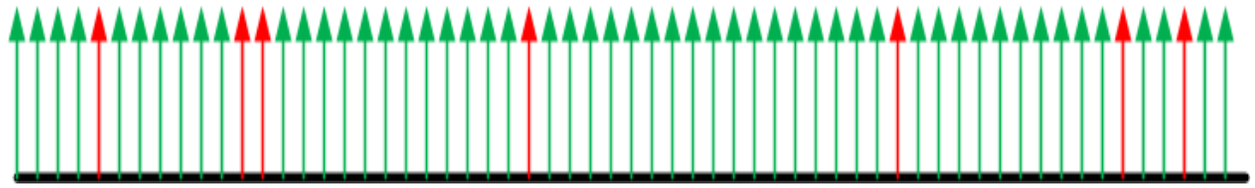
  More difficult problem to solve…

Packet Loss

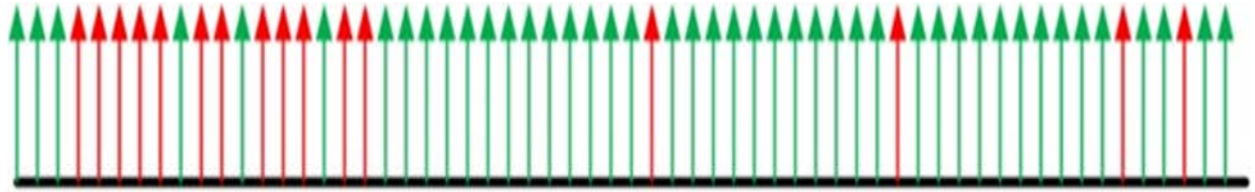
- Causes of IP packet loss: route flapping, transmission errors, congestion
- Unmanaged vs. managed network services
- Packet loss concealment methods: energy interpolation, noise substitution, replaying previous frame
- Concealment works well at very low packet losses
- Need to use correction techniques along with concealment for higher level packet losses
- Correction techniques are based on standard RTP over UDP protocol

Packet Loss Patterns

- Random vs. Burst Packet Loss
- Random Losses
  - Uncorrelated
  - Appear to be spread out
- Burst Losses
  - Correlated



Random

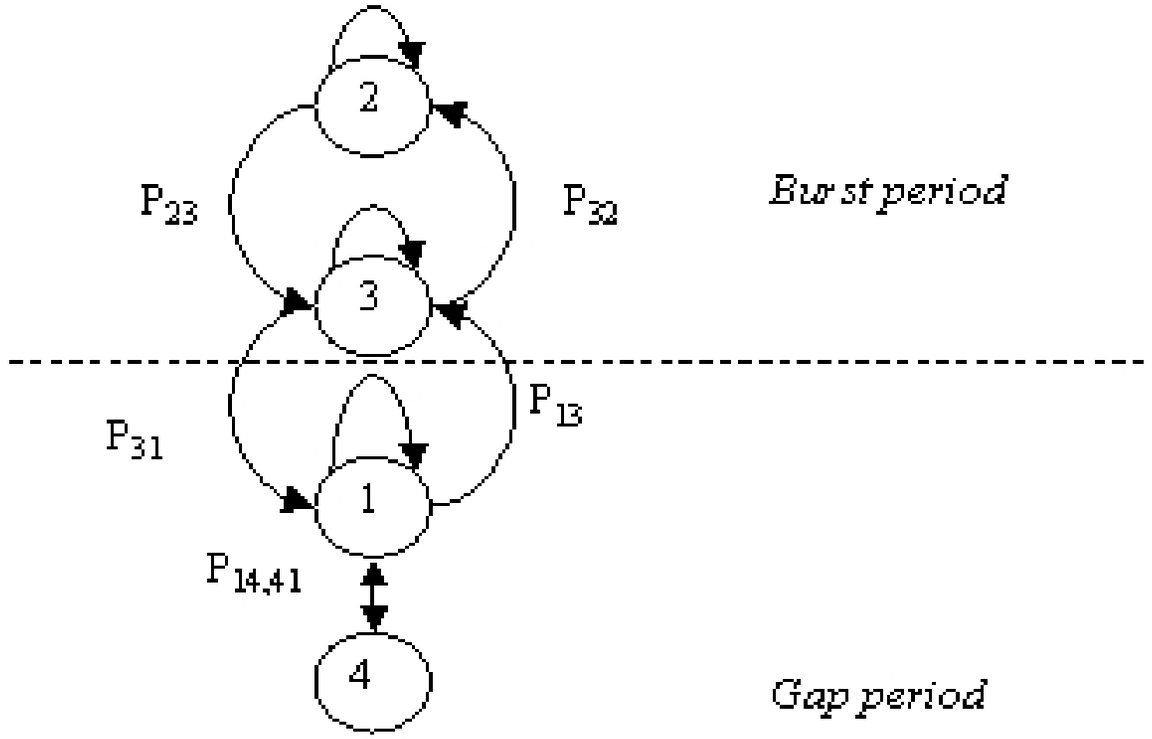


Burst + Random

Four State Markov Model

- Multi-state model
- Transition between states with a transition probability
- 4-state model represents burst periods, during which packets are received and lost according to a first 2-state model and gap periods during which packets are received and lost according to a second 2-state model

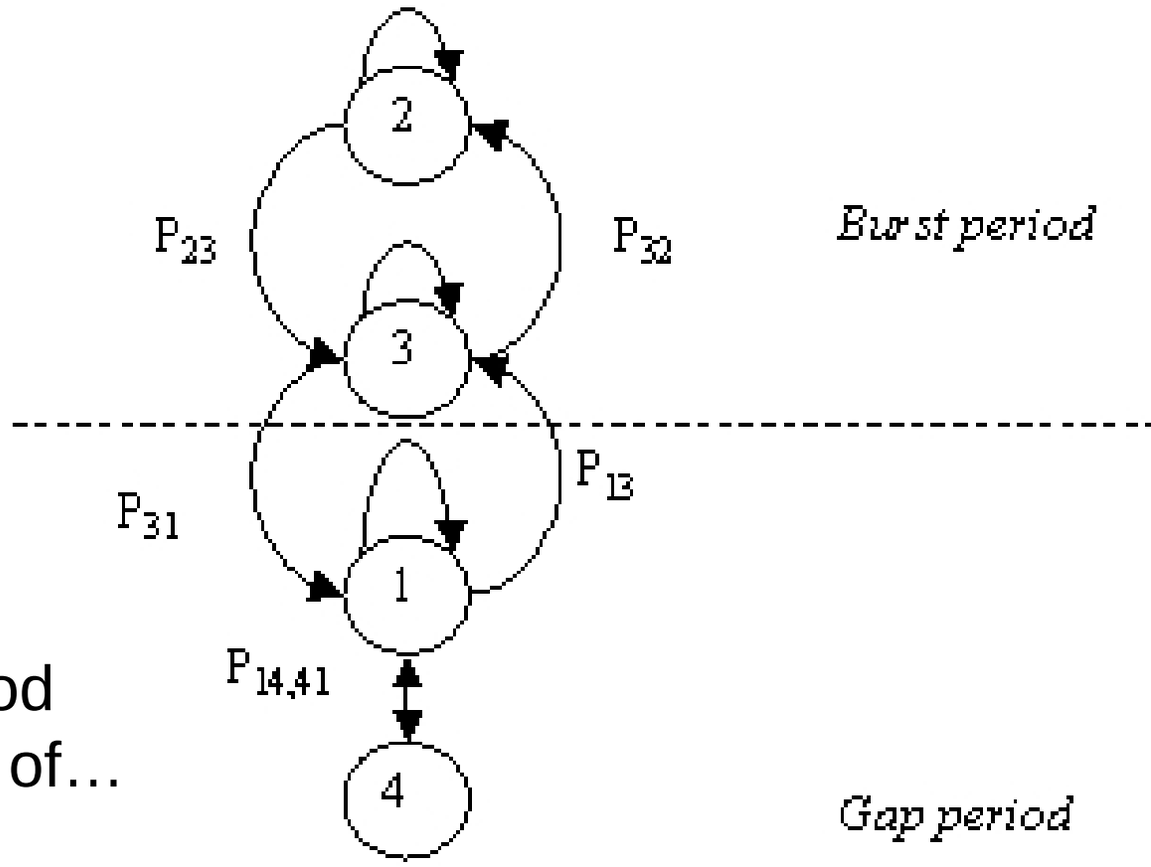
Packet Loss Model



Four-State Markov Model

Four-State Markov Model

State 1 - Packet is successfully received
State 2 - Packet is received within a burst
State 3 - Packet is lost within a burst
State 4 - Isolated packet lost within a gap

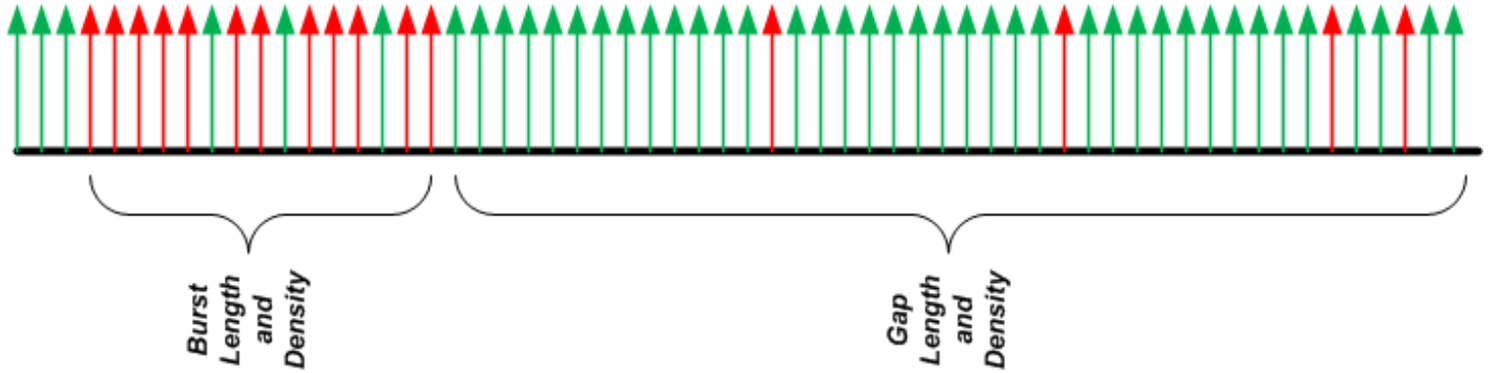


For example, using the loss pattern:
0000011001010101101100000000100

where 1 represents a lost packet and 0 is a good received packet, correlates to the state pattern of…

1111133223232332331111111411

Burst Packet Loss Model



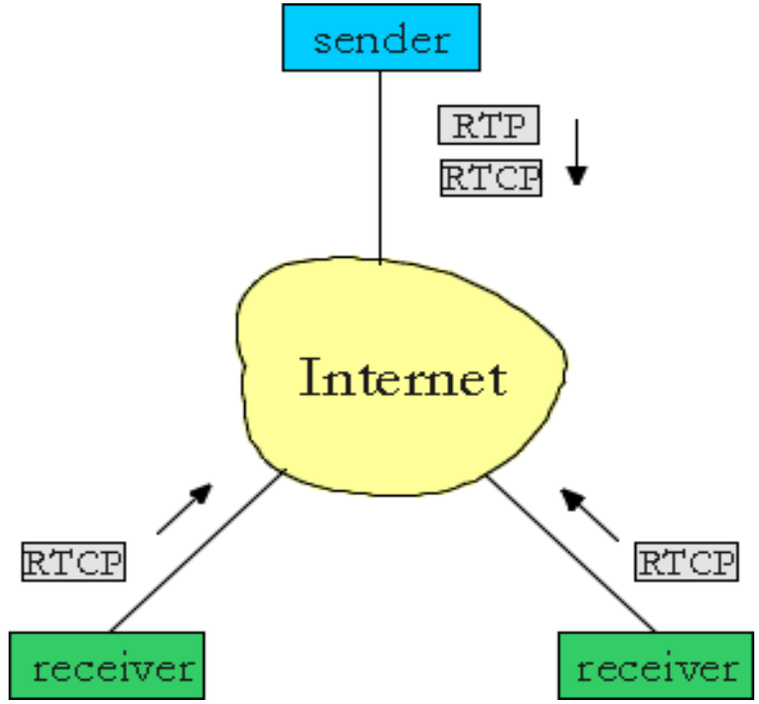
- Gap state: isolated or random losses
- Burst state: correlated packet losses in burst
- Density: probability of loss
- Period/Length: time within a state
- Gap Length and Gap Density
- Burst Length and Burst Density
- Objective of modeling is to characterize and fit “real world” network behavior

RFC 3611

- RFC 3611 defines an Extended Report (XR) packet type for the RTP Control Protocol (RTCP)
- RTP Control Protocol (RTCP) is a companion protocol of the Real-time Transport Protocol (RTP)
- XR supplements the reports in RTCP
- Intended for VoIP applications for monitoring of performance metrics

RTCP

- RTCP specifies report PDUs exchanged between sources and destinations of multimedia information
  - Receiver reception report
  - Sender report
- Reports contain statistics such as the number of RTP-PDUs sent, packet jitter, packet loss, round trip delay
- Used to provide feedback on QoS by periodically sending statistics



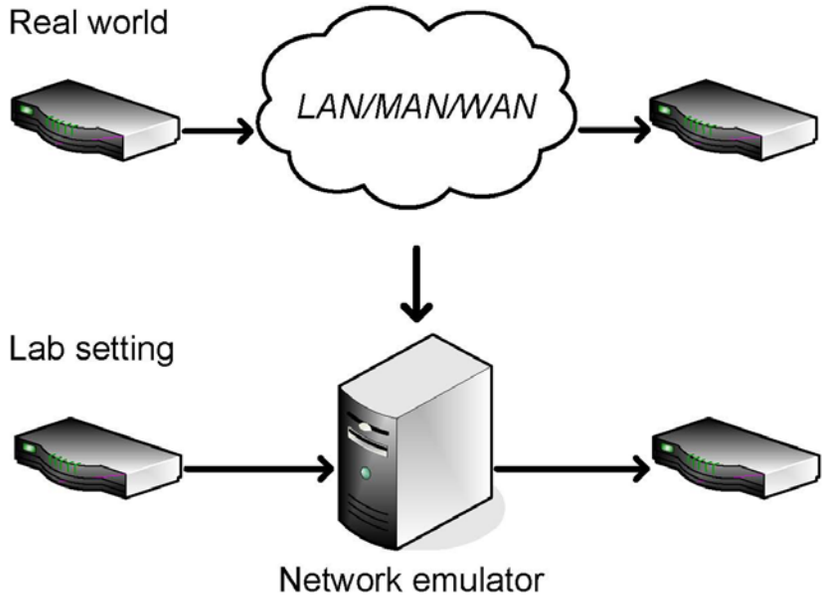
RFC 3611 Metrics

The VoIP Metrics payload is shown below:

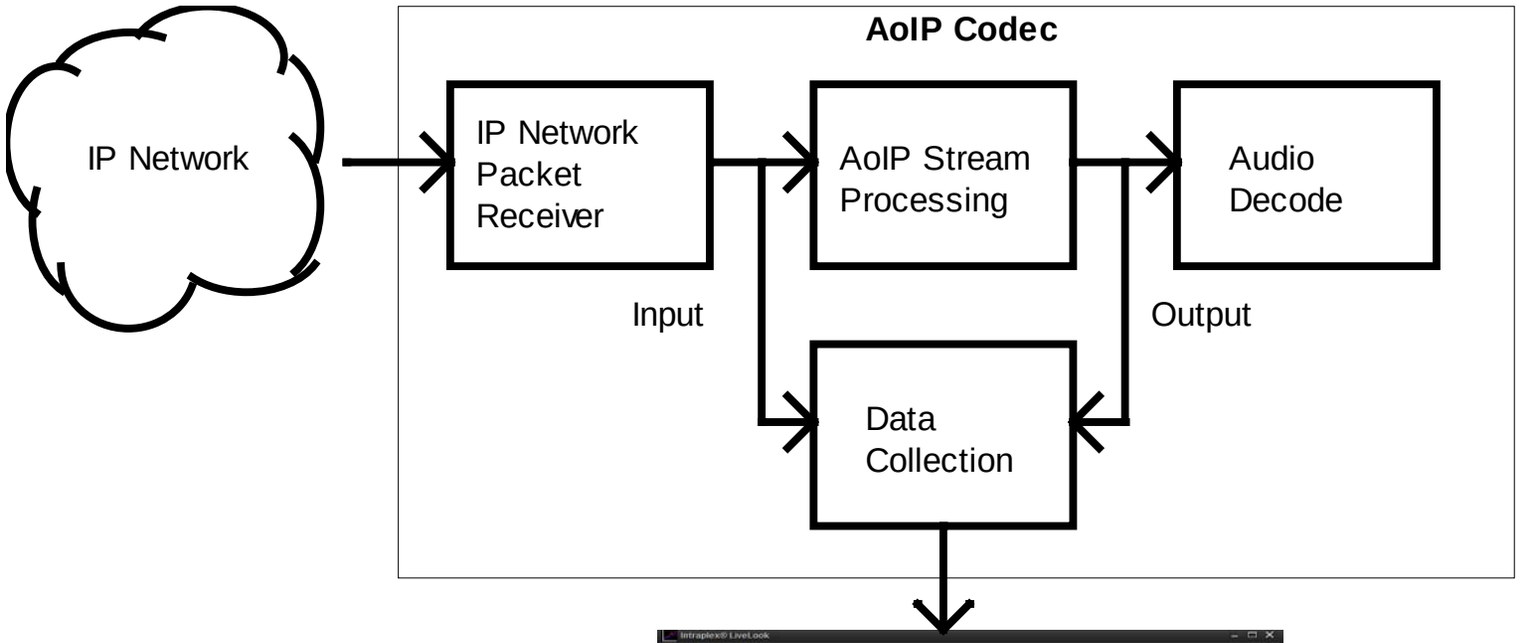
Network Packet Loss	Packets discarded due to jitter	Density of lost/ discarded packets in burst periods	Density of lost/ discarded packets in gap periods
Average duration of burst periods (mS)		Average duration of gap periods (mS)	
RTP Round Trip Delay (mS)		End System Delay (mS)	
Signal Level (dBm)	Noise Level (dBm)	Residual Echo Return Loss (dB)	Gmin - typically 16, which classifies >5% loss as burst
R factor	External R factor	MOS LQ	MOS CQ
PLC and Jitter Buffer Config	Reserved	Average jitter buffer delay (mS)	
Current max jitter buffer delay (mS)		Max jitter buffer size (mS)	

Packet Loss Simulation

- Linux module netem for network emulation
- Simulation of packet delay, drops, duplicates, corrupted packets, and lost packets
- Linux router
- Usage of netem for WAN emulation
- Evaluation of performance of AoIP in a lab environment



AoIP Analysis Tool



Network Analyzer

Random Packet Loss

Packet Loss Rate

Gap Density

Burst Density

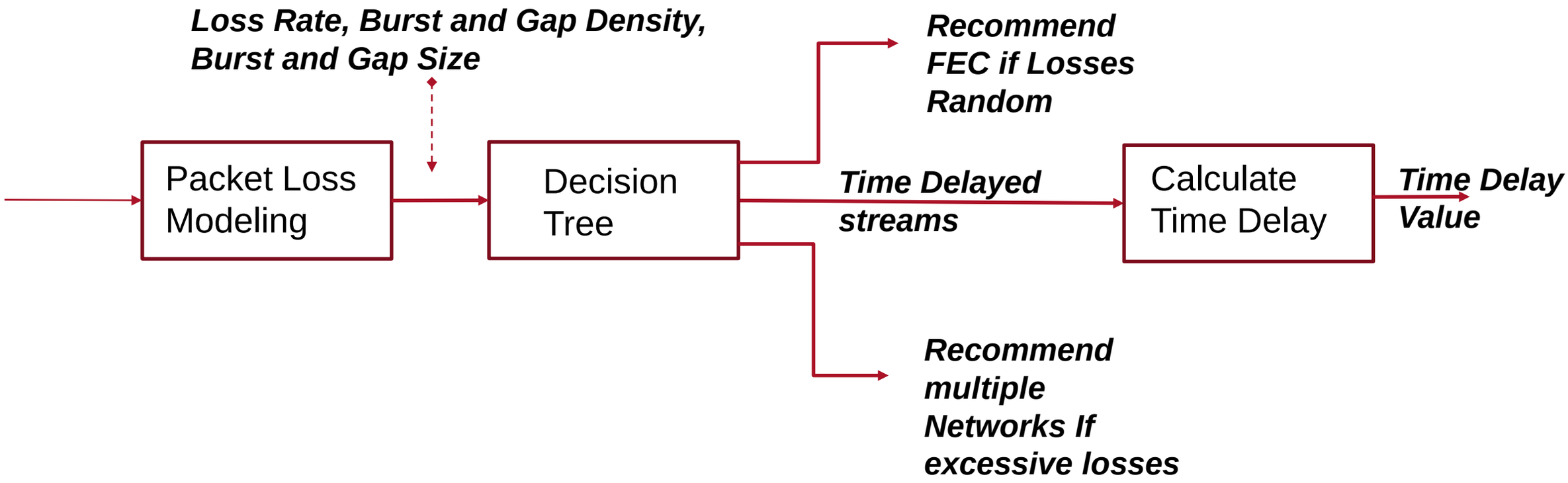
Burst Packet Loss

Packet Loss Rate

Burst Density

Burst Size

Network Analytics Flow



Report Generation

Stream Stats Summary

Loss Rate: 1.02
Loss Rate After Correction: 0.16
Packets Lost: 219101.00
Packets Lost(Group): 219101.00
Packets Recovered: 185049.00
Net Loss: 34052.00
Largest Loss Rate: 1.41

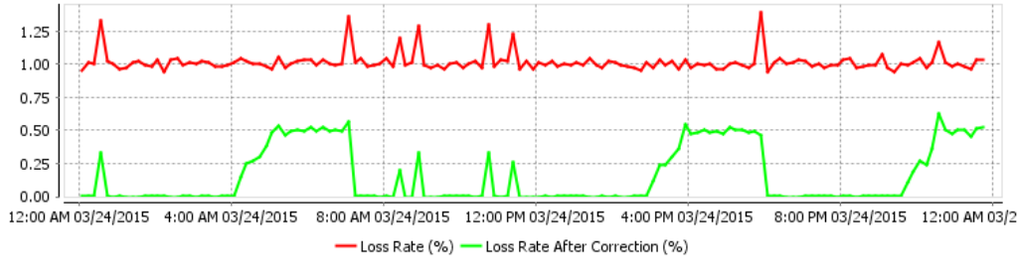
Network Packet Stats

Isolated Losses: 215504.00
Burst Losses: 3599.00

Burst Stats

Max Burst: 793
Avg Burst: 139.12
Min Burst: 25
Avg Burst Density: 76.09

Loss Rate vs Loss Rate After Correction (600 second intervals)

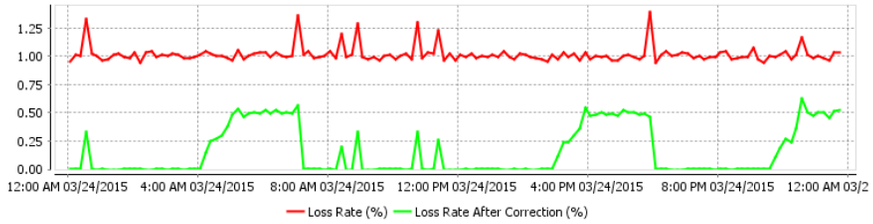


Report Generation

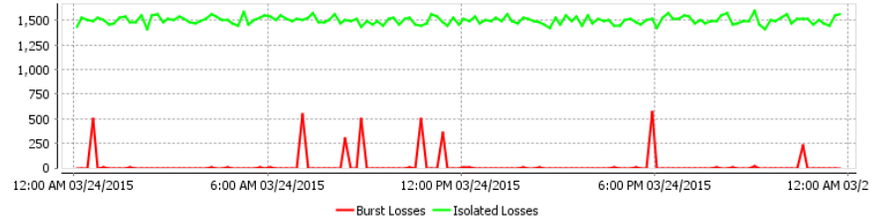
Burst Stats

Max Burst: 793
Avg Burst: 139.12
Min Burst: 25
Avg Burst Density: 76.09

Loss Rate vs Loss Rate After Correction (600 second intervals)



Burst Losses vs Isolated Losses (600 second intervals)

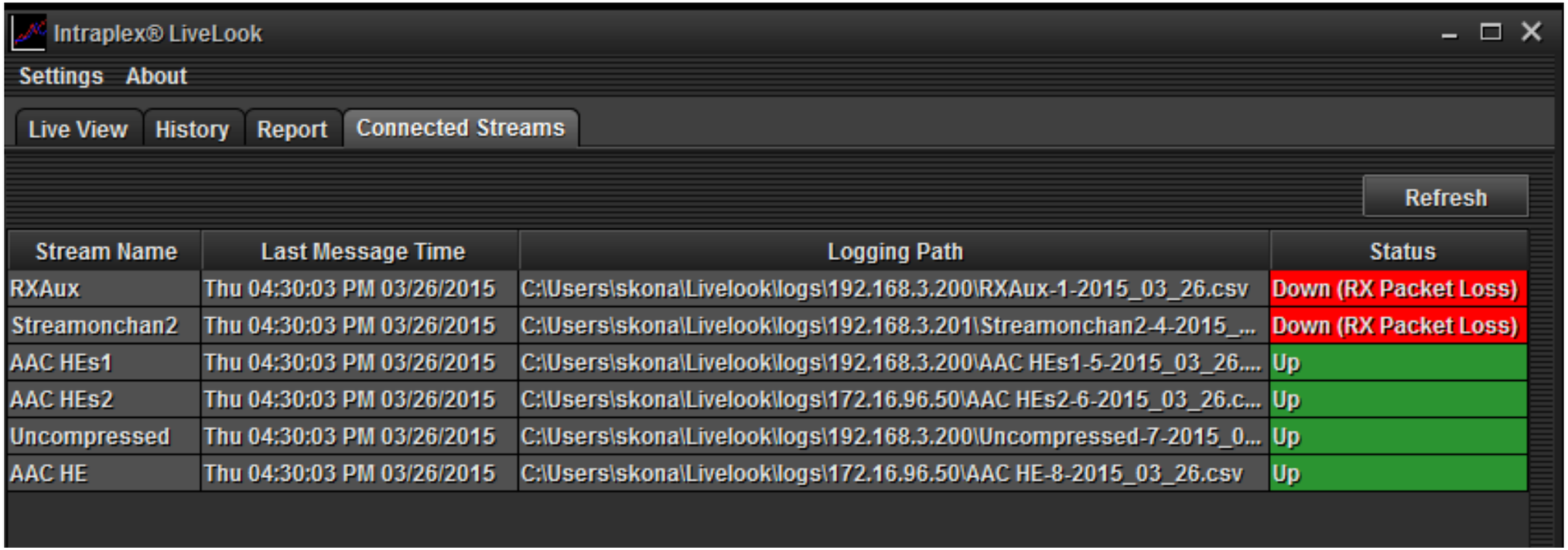


Recommendations

Stream Splicing with Time Diversity of 500 ms is recommended for this Network

Time Diversity Required for .5%: 500 ms
Time Diversity Required for .1%: 500 ms
Time Diversity Required for .05%: 500 ms

Stream Selection



Mitigation of Packet Loss

- Mitigation methods
  - Forward Error Correction (FEC)
  - Interleaving
  - Redundant streaming
  - Network diversity
- Mitigation of random packet loss
- Mitigation of burst packet loss

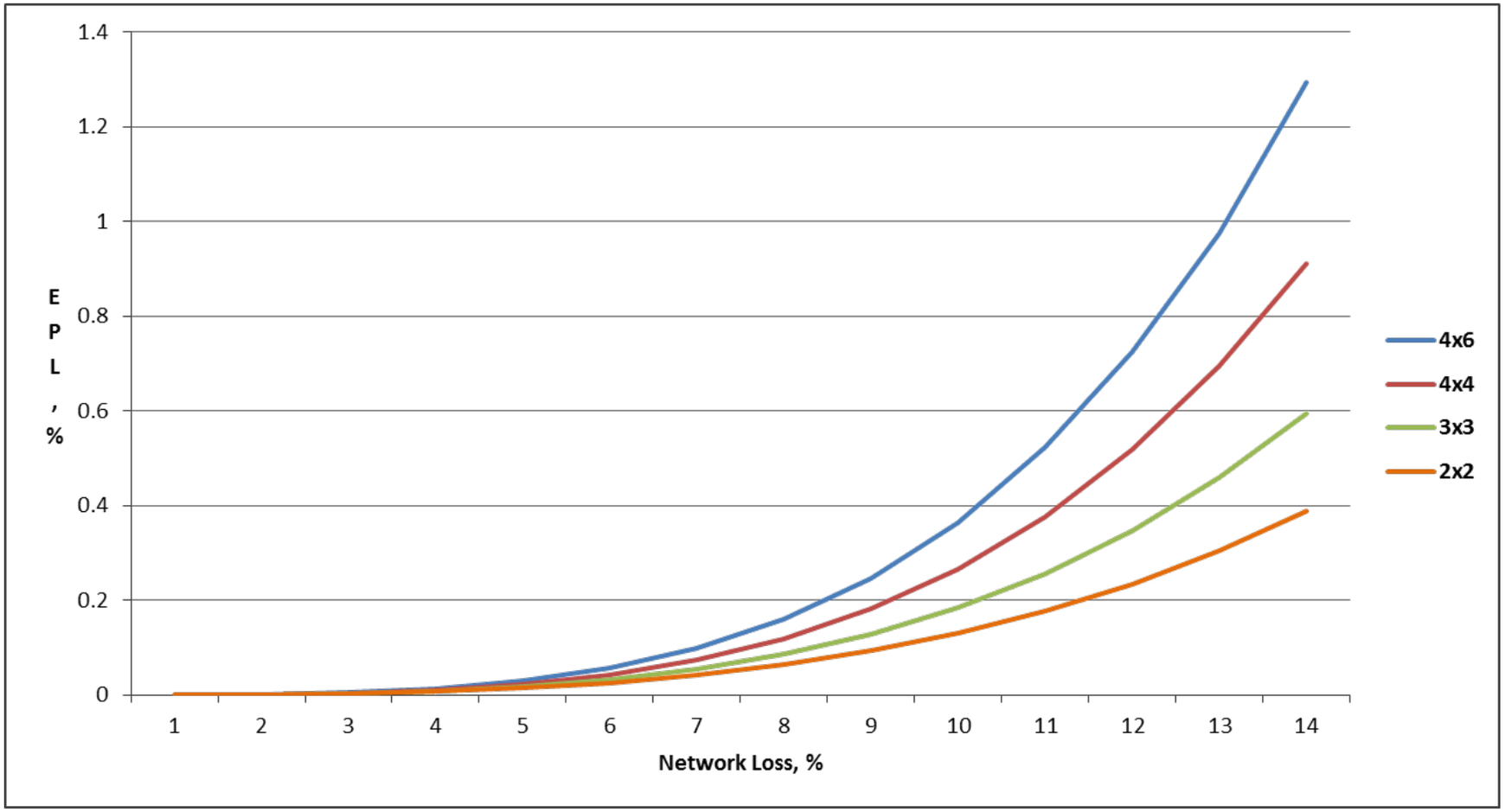
RTP Forward Error Correction (FEC)

- FEC packets are generated from a matrix of RTP data packets
- Both data and FEC packets are sent to the receiver
- FEC attempts recovery of lost data packets at the receiver
- Unrecovered packets are considered lost and concealment is applied
- Effectiveness of recovery depends on the packet loss model

FEC Matrix

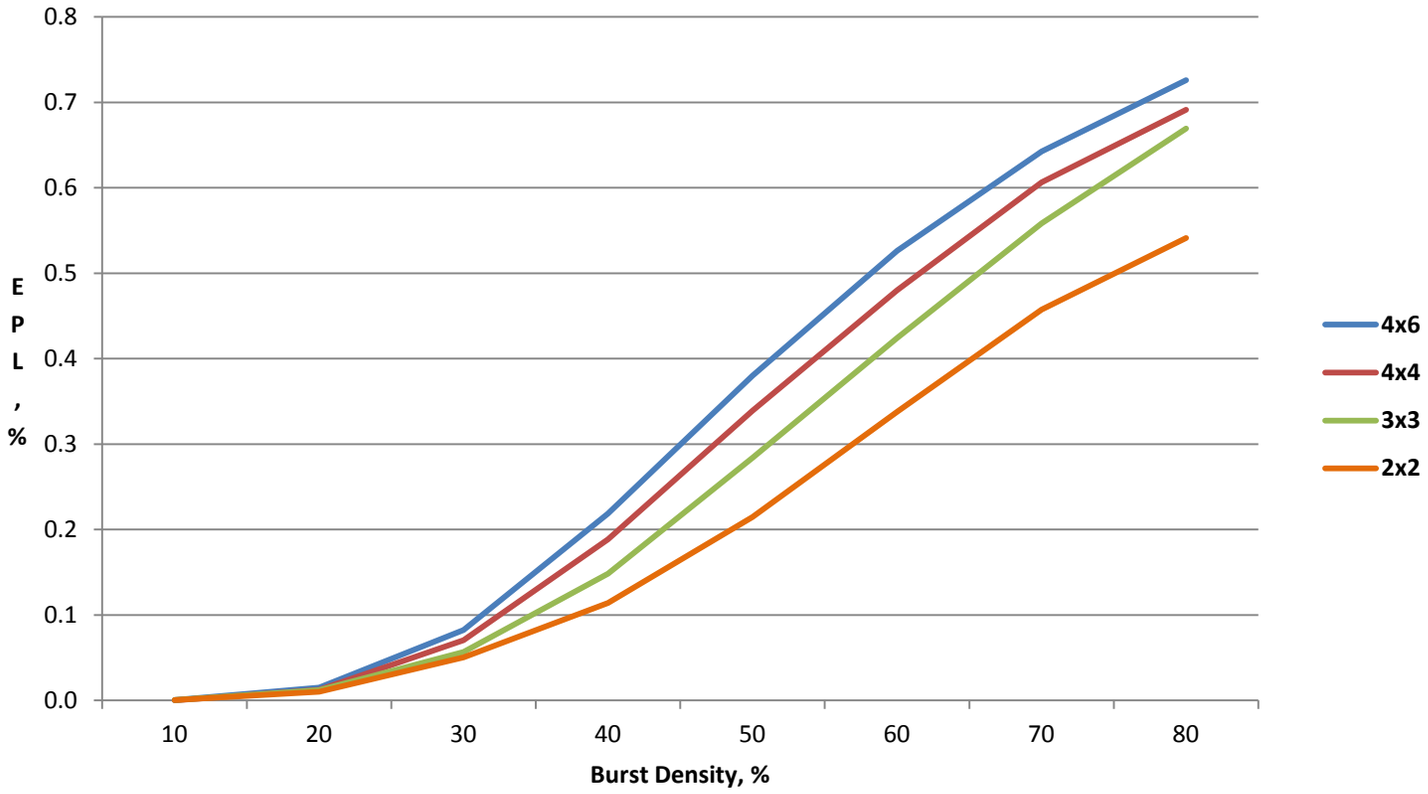
	Col 1	Col 2	Col 3	Col 4	FEC(x)
Row 1	1	2	3	4	XOR(1,2,3,4)
Row 2	5	6	7	8	XOR(5,6,7,8)
Row 3	9	10	11	12	XOR(9, 10,11,12)
Row 4	13	14	15	16	XOR(13, 14,15,16)
FEC(x)	XOR(1,5,9,13)	XOR(2,6, 10,14)	XOR(3,7, 11,15)	XOR(4,8, 12,16)	

FEC Correction Capability for Random Loss



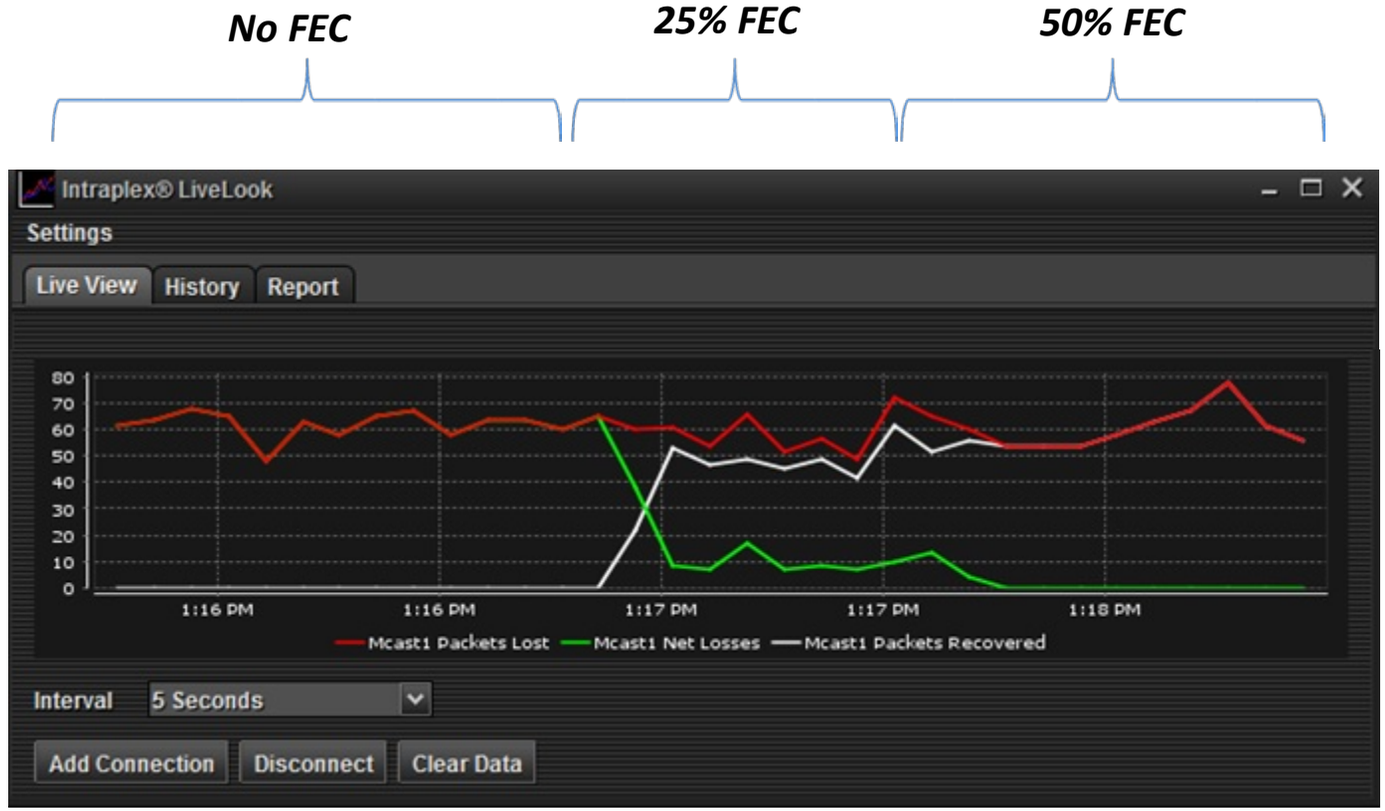
FEC Correction vs. Burst Density

Average Packet Loss = 1%, Burst State Length= 16 packets



FEC Performance for 5% Random Loss

Router Configuration:
5% Random Loss



Packet Interleaving

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Packet sequence before interleaving

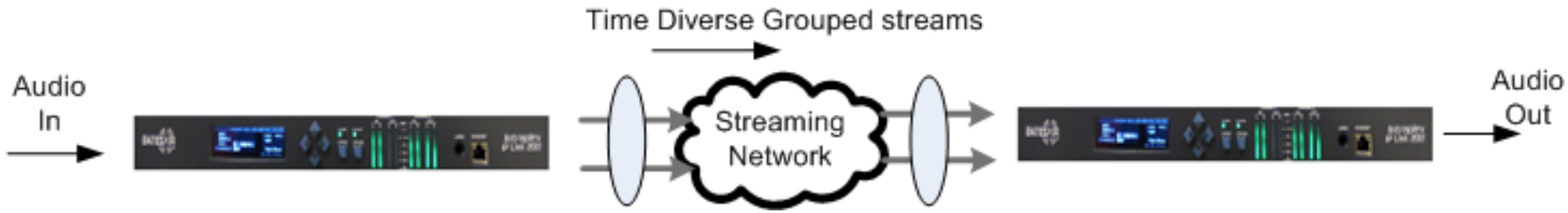
1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

Interleaving matrix

1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Packet sequence after interleaving

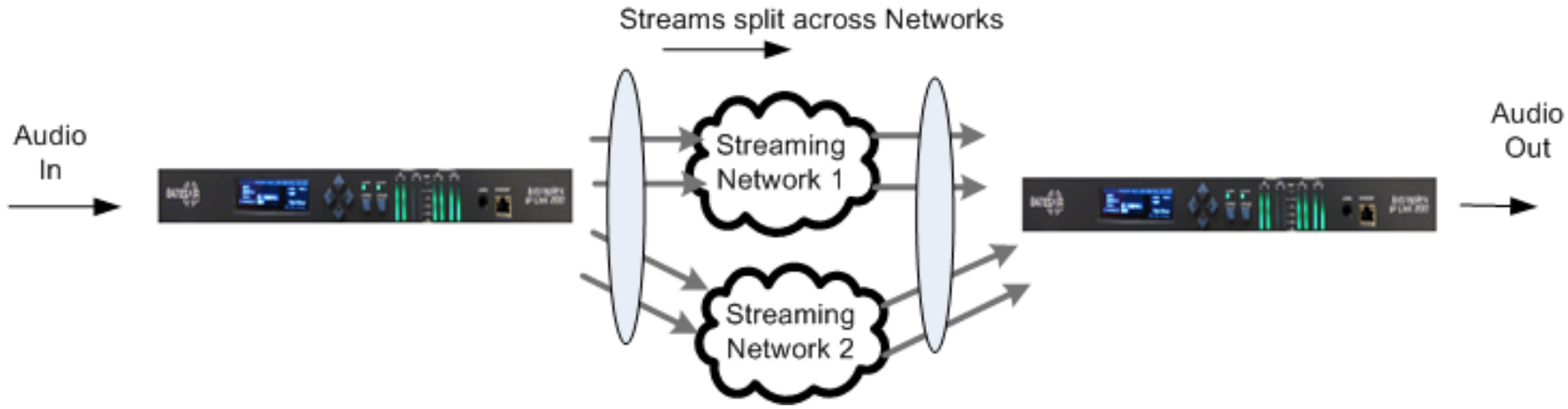
Redundant Streaming



- Two time diverse streams
- Time diversity value is set based on receiver's calculation of burst length

1% Avg PL, 80% Burst Density Network Loss → **Two Time Diverse streams: 400 msec. EPL 0.07**

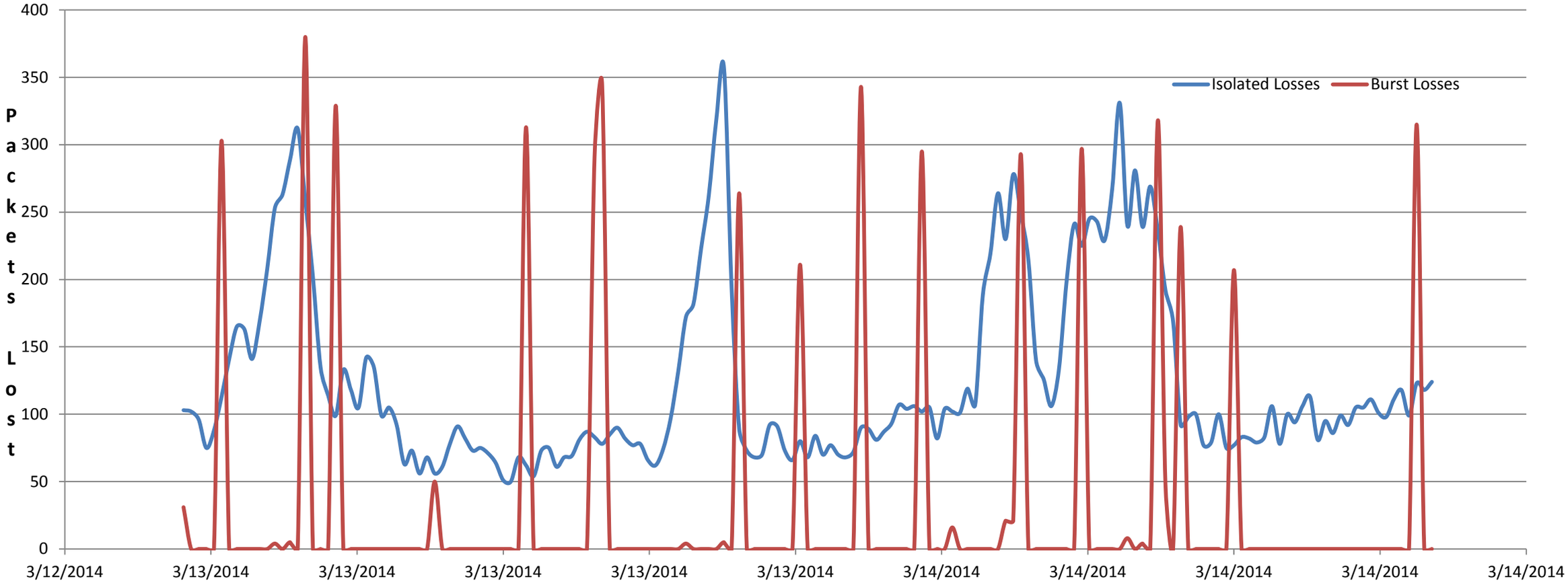
Network Diversity



- Streams of the group are split across multiple diverse networks
- Provides “hitless” protection against failure of any single network
- Provides higher level of packet loss protection due to uncorrelated network paths

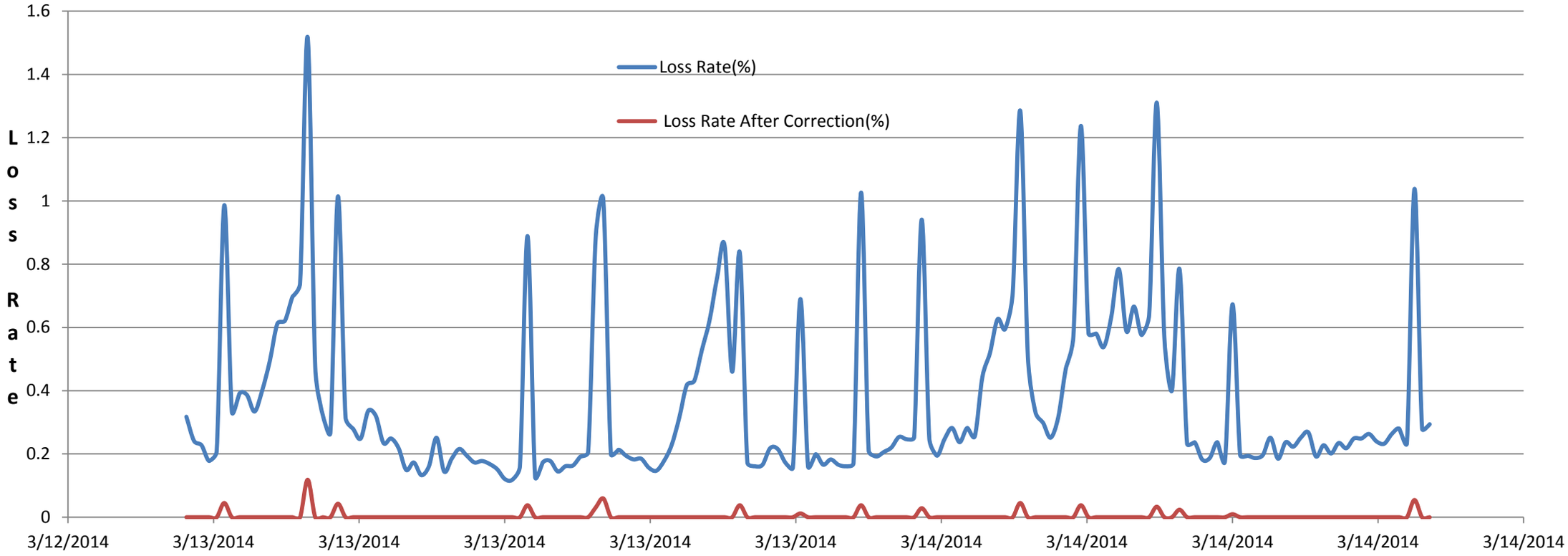
Loss Distribution

Two systems connected via Time Warner at home and Verizon in the lab



AoIP Case Study

- Two streams with time diversity
  - Stream 1 time offset = 0, with 4x4 FEC
  - Stream 2 time offset = 1.25 secs



Summary

- Network impairments: jitter, duplicate, out-of-order, and lost packets
- Real world packet loss tends to occur in bursts
- Packet loss modelling can be used to characterize network behaviour
- Usage of an analytics tool to measure and characterize packet loss in an AoIP application
- Packet loss can be mitigated using FEC, interleaving, stream and network diversity
- Mitigation methods have bandwidth, delay, and network resources trade-offs
- An optimized mitigation strategy can be deployed based upon your network characteristics

Thank You