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

Keyur Parikh and Junius Kim
GatesAir
Mason Ohio

Abstract – *The use of wide area IP networks to transport broadcast audio provides a cost effective and flexible option for broadcasters. However, IP networks possess impairments that have to be overcome before one realizes the same level of reliability of traditional circuit switching networks. One of the most difficult type of network impairment to overcome is packet loss, especially when transporting real-time audio. In real-time applications usage of reliable transport TCP is not suitable due to either delay or incompatibility with multicasting. As a consequence, mitigation techniques such as FEC, interleaving, and redundant streaming are used in conjunction with RTP over UDP. However, packet losses can follow different patterns depending on the network and quantifying these patterns using standard modeling techniques is important in selecting an effective packet loss mitigation method. In this paper, we will provide a comprehensive look at the packet loss impairments including a discussion on modeling methods and analytic tools used to quantify network losses. We then look at performance of various mitigation techniques against different packet loss models emphasizing the importance of modeling.*

NETWORK CHALLENGES

There are several challenges associated with transporting audio over IP networks, among these are: network jitter, duplicate and out-of-order packets, network failures, and packet loss. Let's examine each of these in detail along with mitigation techniques that can be deployed within the architecture of an audio over IP system.

Network Jitter

Network jitter is defined as a variance in end-to-end one way delay time of packets. It is also referred to as Packet Delay Variance (PDV). Network jitter can be caused by transmission system factors such as congestion on the router and switches. If not handled properly, it can cause missing packets to occur if the receiver's jitter buffer is unable to handle packets that arrive too late or too early. Proper sizing and configuration of a receive jitter buffer, either statically or dynamically based on the measured jitter is used to absorb network PDV.

Duplicate and Out-of-order Packets

Duplicate packets at the receiver can be caused by inappropriate link level retransmission or switching problems, while out-of-order packet generally point to a layer 3 routing event. In either case, if these are not handled properly at the receiver, audio distortion will occur. By using Real-time Transport Protocol (RTP) which provides for packet sequence numbers, duplicate packets can be discarded and the out-of-order packets can be re-sequenced prior to play-out.

Packet Loss

IP packet losses can occur without a complete failure of a network. These losses occur for many reasons, such as routing changes, degradation of links, congestion, etc. The patterns of these losses can vary based on type of network connection. For a managed, guaranteed bandwidth type connection where congestion should not be an issue, we generally see random isolated losses. For a "best effort" type service, packet loss patterns can vary widely from random to heavy burst losses. What makes mitigation of packet losses a difficult challenge is the effectiveness of the mitigation technique depend on the types of packet loss pattern and therefore packet loss modeling becomes a critical step in selecting the appropriate mitigation technique. Furthermore, the packet loss rate and pattern on a network can vary over time and therefore the mitigation technique should dynamically adapt to these conditions in order to maintain effectiveness.

Although audio packet loss concealment techniques such as replaying previous packet or energy substitution can be applied, the audio quality is degraded when the packet loss rate increases beyond a "soft" threshold. As the packet loss rate increases or packet loss occurs in bursts, the effectiveness of the concealment starts to deteriorate and packet loss mitigation techniques must be used along with concealment to maintain high audio quality.

Another critical constraint in real-time audio broadcasting, is keeping the end-to-end audio transport delay within specification. While delay on the order of tens of seconds maybe acceptable for internet audio streaming, real-time radio broadcasting applications typically require delays orders of magnitude less. In addition to the delay constraint, in many cases, network paths are either unidirectional or multicasting is deployed. This makes usage of re-transmission protocols such as Transmission Control Protocol (TCP) unsuitable. For these reasons, the usage of RTP over User Datagram Protocol (UDP) as the transport layer has been standardized for transport of real-time media over IP networks. This began with Voice over Internet Protocol (VoIP) applications and it is now standardized by European Broadcasting Union (EBU) with the N/ACIP interoperability standard for audio and by Society of Motion

Picture and Television Engineers (SMPTE) with the 2022 standard for video.

PACKET LOSS MODELS

Packet loss patterns fall into one of two major model categories: random or burst loss. In the random loss model, each packet has an equal probability of getting lost. In other words consecutive packet to packet loss probabilities are uncorrelated. In the burst loss model consecutive packet to packet loss probabilities are correlated and losses tend to occur in bursts.

Most real world network losses can be modeled with burst loss model which can be simulated using a four-state Markov model as shown in Figure 1.

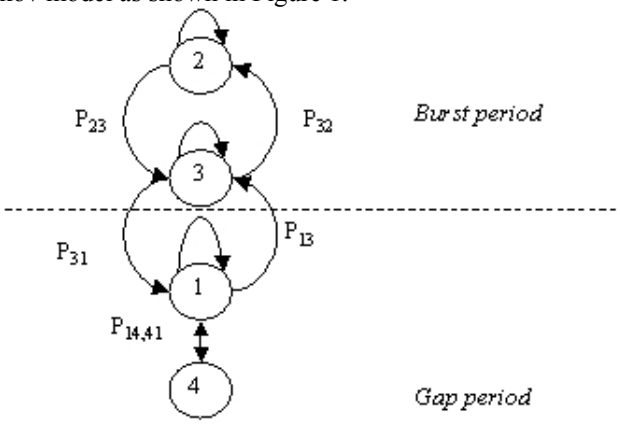

FIG 1 FOUR-STATE MARKOV MODEL

The four-state Markov model is a combination of two 2-state Markov sub-models that represent a burst period in 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 [1] [3].
Where:

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

For example, using the loss pattern:
0000011001010101101100000000000000000000000001000000000 where 1 represents a lost packet and 0 is a good received packet, correlates to the state pattern:
1111133223232323323311111111111111111111111114111111111

Besides providing an accurate representation of real world type network losses, what makes the four-state Markov model attractive is the algorithm model's burst statistics are specified in an Internet Engineering Task Force (IETF) standard RFC 3611 [5]. This allows cross platform interoperability between routers using this model to emulate packet loss and network edge devices using the model to quantify packet loss. This helps re-create real world network patterns within the lab environment by using the model parameters calculated by the edge devices and using emulation routers to re-create the loss pattern.

In the burst loss model, losses are divided into two periods, the burst period and gap period, as shown in Figure 1. The burst period is where majority of the losses occur. While the gap period is when isolated losses occur. The parameters used to characterize a burst loss model are: burst density, gap density, burst length, and gap length. The algorithm for calculating these parameters is explained in more detail in RFC 3611 [5]. The burst density indicates the probability of losing a packet within the burst loss period, while gap density is an indication of the loss probability within the gap period – or quiet period. Burst length and the gap length indicate the duration of each period in terms of packets or time. Of these four parameters, the burst density is the most important in regards to error mitigation as it indicates the degree of randomness of the overall loss. Lower burst density implies the losses are spread out and appear more random. For example, to represent 100% random loss, the burst density would be 0% and the gap density would be the overall network loss rate. To represent a burst loss only type network environment, the gap density would be 0%. As the burst density increases, the probability of multiple consecutive packet losses increases within the burst length.

The technique to effectively mitigate an average packet loss rate of 1% with burst density of 80% compared to same average packet loss rate with same burst length, but with burst density of 10% are different. The 10% burst density loss appears more random and techniques such FEC can be very effective, while a burst density of 80% requires more than just FEC to bring the effective packet loss rate to an acceptable level. Therefore it is important to not only quantify the overall network loss rate but also quantify the pattern of losses using burst loss modeling so an accurate picture of the severity of the losses can be obtained. This provides valuable input into selecting the most effective packet loss mitigation setting.

PACKET LOSS ANALYSIS

Quantification of the network characteristics in an audio over IP (AoIP) application requires usage of an analysis tool. Figure 2 shows how such a tool functions. The analyzer examines stream statistics at both the ingress and the egress points of the AoIP stream processing. Ingress analysis looks at the characteristics of the network performance and the egress shows the performance of the stream after whatever packet recovery processes have been completed by the streaming processing block. For example, recovery processes such as FEC, redundant streaming, and packet interleaving can be implemented to recover lost packets. After the AoIP stream processing, the packet loss rate is the Effective Packet Loss (EPL) or the packet loss rate that goes into the audio decoder.

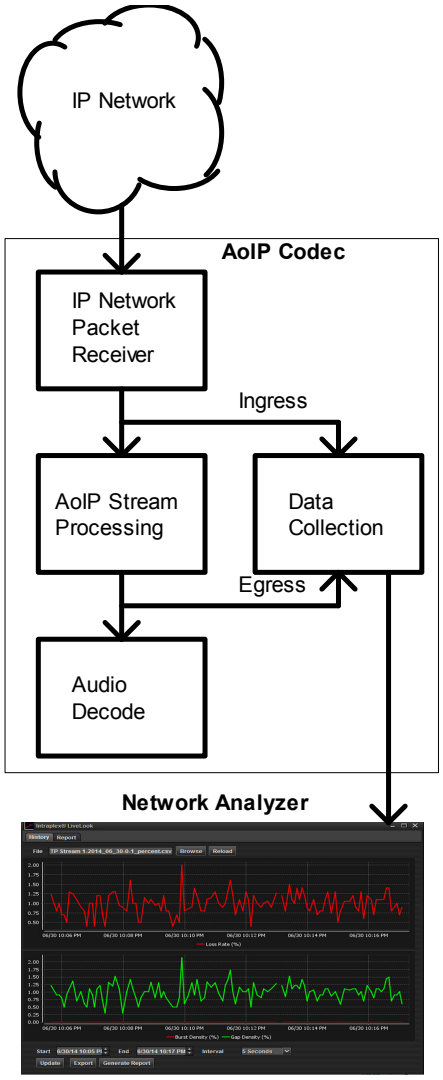

FIG 2 AOIP ANALYSIS TOOL

Packet losses can be recorded using an AoIP codec with built-in network statistics gathering and packet loss data collection. This data can be remotely retrieved from the codec by a host computer with a network analytics tool such as Intraplex LiveLook which provides graphical analysis and logging of performance data both pre and post stream processing. In addition this tool has algorithms to automate packet analysis by analyzing performance data and recommending the best packet error protection methods to use on the codec. The collected data can be graphed into sets of traces showing packet loss rate, gap density, and burst density over time.

The AoIP stream processing ingress point statistics are analyzed using the four-state Markov model and follows the algorithms detailed in RFC 3611 [5]. RFC 3611 defines a performance reporting standard called RTP Control Protocol Extended Reports (RTCP XR), which includes a set of burst packet metrics. In RFC 3611, a burst is defined as the maximum sequence of starting and ending with a lost packet, not including the gap duration. RFC 3611 burst metrics include the burst density (the fraction of packets in bursts), gap density (the fraction of packets in the gaps between bursts), burst duration (the mean duration of bursts in seconds), and gap duration (the mean duration of gaps in seconds).

The burst analysis can be used by the analyzer tool's report generation function to recommend the best error recovery technique to use. By including analysis at pre and post AoIP stream processing, the analyzer provides valuable metrics on the performance of the stream's error protection thus enabling users to adjust the packet recovery process settings such in a more informed manner vs. a trial and error type process.

Packet loss patterns of a network often vary over time. These changes can be permanent or it can be temporary or periodic. For unmanaged networks, congestion can be experienced during certain hours of the day. For managed networks, where the bandwidth is guaranteed, changes in the network path can cause an overall change in the packet loss rate. Performance analysis needs to account for time variance so long term logging of data and saving to files by the analyzer tool is a valuable function.

PACKET LOSS SIMULATION

The Linux module netem [2] provides network emulation functionality for testing protocols by emulating the properties of wide area networks. The current version of netem emulates variable delay, loss, duplication, and re-ordering. netem is part of the standard Linux kernel 2.6.7 and later.

A Linux based router with netem was used to emulate the network cloud in an AoIP application. The graph in Figure 3 shows the analysis tool with the router configured for a 1% random network packet loss. The figure shows for random loss, the gap density tracks the overall packet loss rate. At the same time the burst density is zero, implying all the losses are counted in the gap state. Using the methods in RFC 3611, the analysis tool is able to accurately represent the packet loss characteristic as being random.

FIG 3 MODEL FOR 1% RANDOM PACKET LOSS

FIG 4 MODEL FOR 1% BURST PACKET LOSS

Figure 4 shows a router configured for a burst packet loss model. The router generates a 1% average packet loss rate with 80% burst density, 16 packet burst size and 0% losses in the gap state (no isolated losses, only burst losses). The analysis tool is able show the losses being burst type and to accurately measure the loss characteristics.

PACKET LOSS MITIGATION METHODS

Having looked at network packet loss patterns let's review several packet loss mitigation techniques along with their effectiveness for various patterns of losses.

Single RTP Stream with FEC

In this mitigation model, a single RTP stream with FEC is sent from an audio encoder to a decoder over the Wide Area Network (WAN) as shown below.

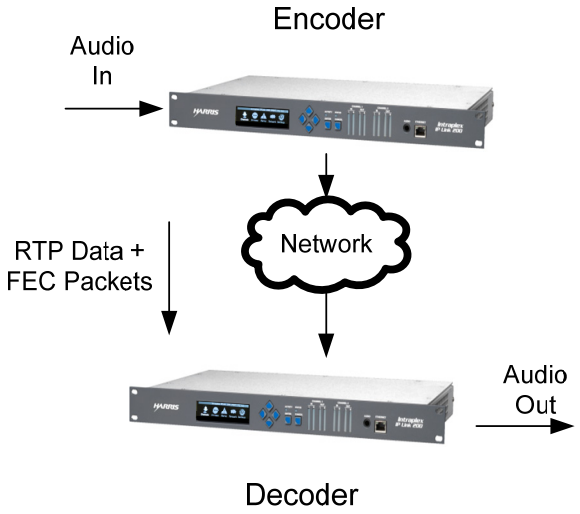

FIG 5 FEC PROTECTED RTP STREAM

RTP FEC has been around for several years and its use has been specified in several RFCs such as RFC 2733 [4] and RFC 5109 [6]. In Figure 5, data flow starts at the encoder, which ingests PCM audio samples and generates an encoded audio frame. The encoded frame is then packetized with RTP to generate a stream of audio packets. Concurrently, FEC packets are then generated from a matrix of audio packets. Both RTP and FEC packets are streamed to a receiver or audio decoder, where they are de-jittered using a receive jitter buffer. The decoder will periodically pull the next packet to be decoded from the receive jitter buffer for play-out. If a packet is missing, then the corresponding FEC and audio packets are used to re-create the missing packet. If a missing packet cannot be created, then the decoder's concealment technique will fill in the time gap for the missing packet. FEC uses additional network bandwidth to reduce the packet loss rate. However, the effectiveness of how well the FEC works depends on several factors such as the type of FEC being utilized as well as the packet loss model.

RTP Level FEC and its Effectiveness

FEC packets are generated by arranging the RTP data packets into a two dimensional matrix of N rows and M columns and then XORing the RTP packets (including RTP header) in each row or column. Single dimension FEC generally creates only column FEC packets, while two dimensional FEC creates both column and row FEC packets. Table 1 shows the rows and columns with the RTP packets represented sequentially as 1, 2, 3, all the way to 16 for the 4x4 matrix. On the recovery side, a lost packet can be recovered by XORing the FEC packet with the rest of the column or row data packet. The recovery algorithm works over the full matrix of data and FEC packets to recover packet in an iterative manner. The bandwidth overhead for FEC packets is the ratio of the FEC packets to data packets in the matrix. As an example, Table 1 shows a 4x4 two-dimensional matrix which has 8 FEC packets to every 16 data packets; hence 50% additional bandwidth is required for the stream.

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

TABLE 1 4X4 TWO-DIMENSIONAL FEC MATRIX

The correction capability of FEC is dependent on a number of factors such as the amount of FEC packets, the size of the matrix, and matrix dimensions. A larger matrix size provides better protection for burst loss. However, the delay at the receiver is also higher since N x M data packets need to be buffered at the FEC generator. The column FEC packets provide burst packet loss protection up to the number of columns in the matrix. The row FEC packets provide random packet loss protection. In theory FEC can be used to effectively recover most types of packet losses. In practice, due to the delay requirements of real-time audio streaming as well as computational burden, there are constraints to the sizes of the matrices used.

Effectiveness of FEC Matrices for Random Packet Loss

Figure 6 and Table 2 illustrates the correction capability for some combinations of the 2-dimensional FEC matrix when subjected to random packet losses - as illustrated on X-axis on Figure 6. The Effective Packet Loss (EPL) after recovery is shown on the Y-axis.

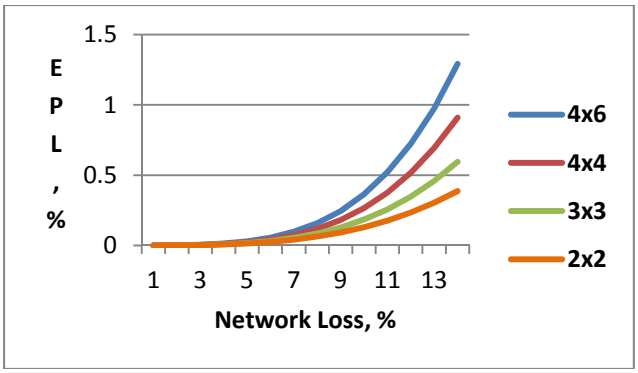

FIG 6 FEC RECOVERY FOR RANDOM PACKET LOSS

FEC Matrix	EPL for 1% Ntwk Loss, (%)	EPL for 5% Ntwk Loss, (%)	EPL for 15% Ntwk Loss, (%)	Ntwk Band-width Over-head, (%)
2x2	1 x 10^{-4}	0.014	0.46	100
3x3	1 x 10^{-4}	0.018	0.75	66
4x4	1 x 10^{-4}	0.023	1.10	50

TABLE 2 FEC RECOVERY FOR RANDOM PACKET LOSS

As we can see from Figure 6 and Table 2, when it comes to random packet losses, FEC matrices are very effective. Even when the network packet loss rate approaches 5%, the EPL rate with all of the FEC schemes can provide good quality audio quality, especially when coupled with loss concealment. The 2x2 matrix gives the best EPL rate, but it also has the highest bandwidth overhead.

Effectiveness of FEC Matrices for Burst Packet Loss

Unfortunately, packet losses in real networks don't tend to exhibit total randomness, so let's examine the performance of FEC matrices when they are subjected to varying degree of burst packet loss.

In the Figure 7, the average packet loss rate is 1%, the burst length is 16 packets and the burst density is varied across the X-axis. The Y-axis provides the corresponding EPL for different schemes tested. The gap density which measures the probability of isolated packet losses was ignored from the simulation without loss of any appreciable resolution.

Looking first at Figure 7, notice as you vary the burst density along the X-axis, going from 0 to 80%, the effectiveness of all FEC scheme start to deteriorate. This is because as burst density increases, the packet loss model becomes less random and there is an increase instance of multiple consecutive packet losses or burst losses. This causes the FEC scheme to become less effective.

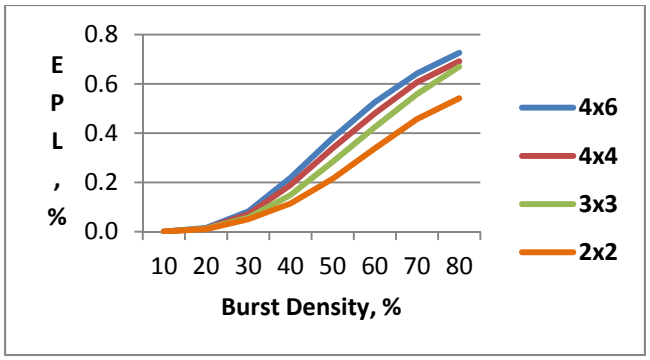

FIG 7 FEC RECOVERY FOR BURST PACKET LOSS

FEC Matrix	EPL for 1% Avg Loss (80% Burst Density), (%)	EPL for 2% Avg Loss (40% Burst Density), (%)	Ntwk Band-width Overhead, (%)
2x2	0.54	0.22	100
4x4	0.69	0.38	50
4x6	0.61	0.40	42

TABLE 3 FEC RECOVERY FOR BURST PACKET LOSS

Table 3 shows just knowing the average packet loss rate does not tell the entire story, burst density along with duration are also critical. For instance, looking at 2% average loss rate column, we see the FEC schemes are performing better than the 1% average loss rate column. This is because the 2% average loss rate column has 40% burst density where the losses occur frequently but are more disperse while the 1% average packet loss rate column has 80% burst density, where losses occur less frequently, but when they occur they wipe out most packets in the burst.

So as the burst density and size increase, simply turning on FEC with a reasonable matrix size may not be good enough, the number of FEC columns needs to increase as well. While this can provide an effective mitigation option, it can also increase the system's computational requirement needed to handle the increased depth of packet recovery.

Let's look at some other options to handle burst losses.

Interleaving

Interleaving is often used in digital telecommunications to improve performance of FEC in burst error environments. Using FEC, if consecutive packets are lost, then ability of the FEC code to recover the missing packet maybe exceeded. Interleaving mitigates this problem by shuffling packets across an interleaving period.

As seen in Table 1, XOR type FEC provides interleaving with the length of the interleaving period roughly proportional to the number of columns. We can also explicitly provide interleaving in cases where the FEC interleaving period is shorter than desired. An example of this interleaving with a 4x4 matrix is shown in Figure 8. The disadvantage of interleaving is increased delay since the receiver must wait for all packets in the interleaving period to arrive before starting reconstruction of the original data

stream. In addition, delay is also incurred at the packet transmitter since packets are buffered.

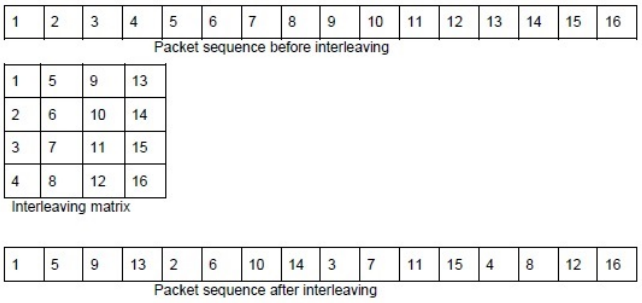

FIG 8 INTERLEAVING

The FEC and interleaving parameters in an AoIP application can be optimized by knowing the network characteristics. For example, if the network loss is random then interleaving is not needed and FEC alone is sufficient to mitigate packet loss. However, if the network loss is burst type, then interleaving should be used in conjunction with FEC and the interleaving period set to be greater than the greatest expected burst duration. Compared to the option of increasing FEC columns, the combination of smaller FEC matrices in conjunction with interleaving has benefit of reduced computational requirements.

Time Diversity for Burst Packet Loss

Another option for packet loss mitigation is using multiple redundant streams. The redundant streams are composed of duplicating the original RTP stream packets and sending each stream in a time diverse manner with respect to one another. For example, if we are sending two streams, the first stream is sent with no delay and the duplicate stream is delayed with respect to the first by some number of packets as determined by the network burst length. This option does increase the bandwidth requirement, but has the least computational requirement and play-out delay.

As the network pipes get bigger and compression algorithm get better, bandwidth utilization is becoming less of issue and therefore, for real-time audio application where play-out delay is important, a practical method to handle burst losses is to utilize redundant streams with time diversity. If there are still residual losses, then FEC can be used in conjunction with time diversity.

Network Diversity

In some cases, a single network may experience burst losses of such long duration that none of the options described earlier may be practical due to excessive delay. For these cases, network diversity (multiple networks) can be used, with each network having its own combination of streams with protection as shown in the Figure 9.

To avoid network service outages, broadcasters are increasingly employing multiple IP network connections. When these connections are used concurrently, identical audio streams may be sent over different network connections for diversity. On the receive side, the system needs to provides means to correlate and assimilate the packets across multiple streams such that packets from any one of these streams at any given time can be used in a "seamless" or "hitless" manner.

Another possible advantage of network diversity is delay. Time diversity incurs a delay equal to or greater than the largest expected burst period. While in network diversity the delay is associated with the highest delay network. For example if you have two networks one with 10 mS delay and the other with 50 mS, you would set your jitter buffer be greater than the delay difference of 50 mS – 10 mS = 40 mS and the delay would be 50 mS.

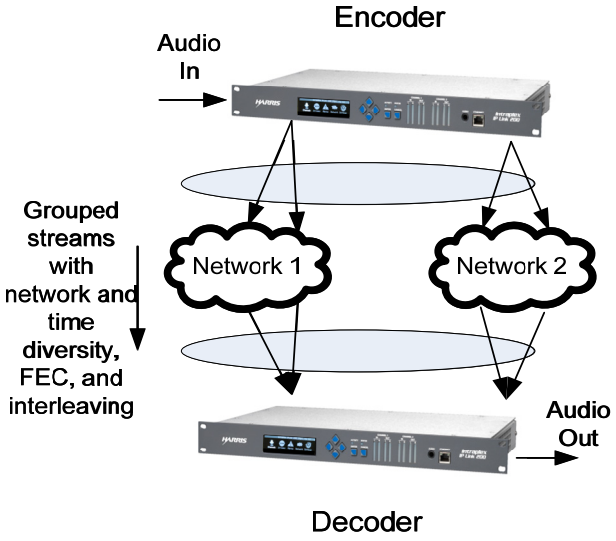

FIG 9 NETWORK DIVERSITY

SUMMARY

Migration from fixed circuit based telecommunication services to IP based connections provides reduction in operational expenses as well flexibility in audio routing. However, the reliability and quality of IP connections may deter users from making this migration. Some packets impairments such as jitter, out-of-order delivery, and duplicate packets can be handled without loss of information, by the receiver using a jitter buffering scheme to re-sequence out-of-order packets and discard duplicate packets. Other packet impairments, such as packet loss, is more difficult problem and requires understanding of the network loss characteristics in order to optimize an effective mitigation technique. Real world networks tend to lose packets in bursts and these loss characteristics can be modeled and loss metrics calculated using IETF standards. In an AoIP application, this requires the use of an analytics tool working in conjunction with your codec. Such a tool can measure and compute network loss metrics. Once these metrics are known, an effective mitigation technique using FEC, interleaving, time or stream diversity can be deployed. These techniques, if utilized in a systematic and intelligent manner can greatly improve the performance of AoIP streaming over impaired IP networks.

REFERENCES

[1] S. Salsano, F. Ludovici, A. Ordone. 2012. Definition of a General and Intuitive Loss Model for Packet Networks and its Implementation in the netem Module in the Linux Kernel.

[2] netem http://www.linuxfoundation.org/collaborate/workgroups/networking/netem

[3] VoIP Troubleshooter http://www.voiptroubleshooter.com/indepth/burstloss.html

[4] RFC 2733, An RTP Payload Format for Generic Forward Error Correction", December 1999

[5] RFC 3611, RTP Control Protocol Extended Reports (RTCP XR)", November 2003

[6] RFC 5109, RTP Payload Format for Generic Forward Error Correction, December 2007

AUTHOR INFORMATION

Keyur Parikh is an Architect and Software Lead with GatesAir in Mason, Ohio. Mr. Parikh has over 23 years of experience in design and development of communication systems for various applications. His current interests include architecture and design of system to reliably transport media over packet based networks. Mr. Parikh holds a BS in electrical engineering with a Master's in communication theory.

Junius Kim is a Hardware Engineer with GatesAir in Mason, Ohio. Mr. Kim was a key member of the GatesAir design team responsible for creating the SynchroCast simulcasting system and IP Link, a next generation AoIP codec. His current interests include the architecture and design of robust packet switched based telecommunication systems. Mr. Kim holds a BS and MS in electrical engineering.

ACKNOWLEDGEMENT

The authors would like to thank Jacob Schreiver and Sudhesh Sudhakaran Nair of GatesAir for their contribution to this research.