III
IP Channel

The understanding of the loss characteristics of the IP channel is important for its simulation and construction of a channel coding scheme capable to overcome associated problems. This chapter will cover the modeling of the IP channel as a *Packet Erasure Channel* (PEC) and the erasure protection schemes most commonly employed for Transport Streams over IP.

III.1 IP as a Packet Erasure Channel

The IP channel can be modeled as a *Discrete Memoryless Channel* (DMC) with input $\mathbf{x}$ and output $\mathbf{y}$. It is said *Discrete*, because the alphabet for the input variables is finite and *Memoryless*, because output of the channel is not dependant on the values transmitted in previous time intervals.

A *Binary Erasure Channel* (BEC) is a DMC that serves as a model for the IP channel. The BEC channel input $\mathbf{X}$ can assume 0 or 1, while its output $\mathbf{Y}$ can assume one of the values 0, 1 or e, where e means *erasure*. The channel erasure probability is represented by P_e. Given these parameters, the following probabilities can be used to describe the BEC channel:

$$\begin{aligned} P(Y=0|X=0) &= 1-P_e \\ P(Y=e|X=0) &= P_e \\ P(Y=1|X=0) &= 0 \\ P(Y=e|X=1) &= P_e \\ P(Y=0|X=1) &= 0 \\ P(Y=1|X=1) &= 1-P_e \end{aligned}$$

A BEC with erasure probability P_e has capacity $C = 1-P_e$. The Capacity is expressed in terms of *per channel use* and is different from the Bandwidth B, specified in the standards commonly referenced to during system design, which

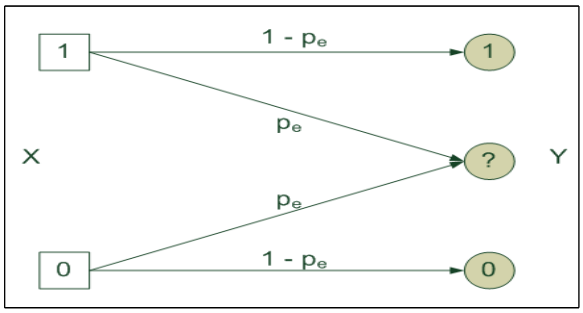

Figure III.1: Binary Erasure Channel

represents the amount of channel uses per time interval. The application being transmitted will use the available rate, which can be expressed in terms of the available Bandwidth and the Capacity: $R = C * B$.

Since the atomic units or symbols for channel encoding are not ones and zero solely and the end-to-end IP path is rarely uniform in terms of loss pattern, the "pure single" BEC channel is not a realistic approach for the scenario considered herein. As in [10], three aspects for a more realistic modeling of BEC channels can be considered:

- cascaded BEC channels;
- channels with input given by vectors of bits, i.e. packets;
- channels with feedback.

The *cascade* approach considers that the packets travel through links defined by different erasure probabilities P_e and that these are independent from each other. Considering that the individual channel erasure probabilities are given by δ, the end-to-end capacity C_ε is given by the product of the individual capacities and finally the end-to-end loss probability δ_ε is obtained from C_ε:

$$\begin{aligned} P_e(Y = e|X_i) &= \delta_i \quad , \quad i \in 1, 2, ..., L \\ C_\varepsilon &= \Pi_{i=1}^{L}(1 - \delta_i) \\ \delta_\varepsilon &= 1 - \Pi_{i=1}^{L}(1 - \delta_i) \end{aligned}$$

It can be noted that the capacity of an end-to-end route composed by several links is bounded by the capacity of the "worst" link in the route. The

link with minimum capacity provides information on the performance upper bound for the overall route. Likewise, the total rate R_t is bounded by the minimum rate throughout the route.

$$\begin{aligned} C_\varepsilon \leq C_{\min} &= \min_i(C_i) \\ R_t \leq \min_i(R_i) &= \min_i(B_i C_i) \end{aligned}$$

When the amount of transmission errors or information lost along the communication's path trespasses the thresholds supported by the lower level protocols, a packet loss at transport layer is declared, i.e. an RTP packet is dropped. In this case, all bits in that packet are discarded. It can be concluded that all bits within the same packet are fully dependent on each other, since either all bits are received successfully or all bits are not received at all. Hence, the IP channel can be viewed as a Packet Erasure channel (PEC) or it can also be referred to as an M-ary Erasure Channel. In this approach the input $\mathbf{X}$ is a vector of random variables, where each of its elements is a binary random variable. The output $\mathbf{Y}$ can result in "erasure" or all possible input vectors. Since the conditional probabilities are independent of the input vector, the PEC will have the same capacity expressed in terms of erasure probability as the BEC. The Capacity of the PEC is expressed in Packets per channel use instead of bits per channel use as in the BEC case.

$$\begin{aligned} X &= \{X_1, X_2, ..., X_n\} \\ Y &= \{Y_1, Y_2, ..., Y_n, e\} \\ P[Y = e|X] &= \delta \\ P[Y = X|X] &= 1 - \delta \end{aligned}$$

III.2 Overcoming Packet Drops and Jitter

As seen in the previous section, the IP channel can be modeled as a *Packet Erasure Channel*, susceptible to service affecting issues. The most commonly employed method to mitigate the packet losses and assure packet delivery, is the well known *Automatic Repeat Request*(ARQ) Protocol, which consists in the retransmission of the dropped content as per receivers' requests. An overview of this method is presented in the next sub-section. A reference for ARQ is found in [11].

The bandwidth wastefulness inherent to simple retransmission network protocols, when facing significant rates of packet drops, motivates the deployment of erasure correction techniques, specially for latency critical applications, such as transport of real-time multimedia. There are schemes available, which are defined by RFC's and recommendations. A commonly employed scheme will be presented in the second part of this section and the same will be used in the simulations presented in the next chapter.

(a) Automatic Repeat Request (ARQ)

Automatic-Repeat-Request protocols can be divided in *pure ARQ* techniques, where the transmitter keeps re-sending the packets, upon receiver requests and *Hybrid ARQ*, where both retransmission and channel coding are employed.

In ARQ schemes, the receiver makes use of acknowledgement (`ACK`) or non-acknowledgement (`NACK`) messages to inform to the transmitter if a particular packet has been properly received, or else, if packet re-transmission is needed.

Stop-and-Wait is the first and most basic pure ARQ technique — the transmitter only sends the next packet upon reception of an `ACK` of the most recently transmitted packet and, otherwise, upon reception of a `NACK`, the packet is retransmitted until successful reception is declared. A mandatory, idle time is accumulated while waiting for the receiver's feedback. The transmitter wastes much time in idle state, making this scheme highly inefficient.

The evolution of *Stop-and-Wait* protocol is known as *Go-back-N*. The transmitter does not have to wait for an `ACK` message before proceeding with the packets transmission, what reduces the time intervals spent on idle state. Packets are continuously transmitted and only upon reception of a `NACK` message for a particular packet, the transmitter will go back and retransmit all packets from that point on.

Further improvement can be obtained with *Selective-Repeat* `ARQ` scheme. It is similar to its antecessor, in the sense that the transmitter does not have to wait for the arrival of `ACK` messages, before proceeding with transmission of the packet sequence. Moreover, only those packets contemplated with `NACK` messages are subject to retransmission. This scheme requires a buffer in the receiver large enough to store all transmitted packets that follow the unacknowledged packet.

Improved variations can be built, which are a combination of Selective-

Repeat and Go-back-N protocols. An example of a simple combination is a protocol, which works under Selective-Repeat mode until a pre-defined amount of retransmissions μ for any given packet, without receiving an `ACK`. At this point, the protocol enters a Go-back-N mode, where it remains until an `ACK` is received, when it switches back to Selective-Repeat.

Finally, retransmission based protocols which also make use of channel coding, have been proposed. These schemes, known as Hybrid-ARQ, can be classified in two types. Type-I Hybrid ARQ transmits packets carrying data that are FEC encoded. If at the receiving end, the packet cannot be successfully decoded, it is discarded by the receiver and a retransmission request is sent.

Type II Hybrid ARQ schemes also transmit FEC encoded packets. However, in the event that a failure is declared, additional parity symbols only, instead of the entire packet, are transmitted. A description of such schemes can be found in [10].

(b) Channel Coding for Video over IP

This sub-section reviews the erasure protection schemes most commonly employed for protection of real-time multi-media over IP. These will provide comparison parameters in the simulations presented in Chapter IV.

The RFC2733 [4] defines a payload format for the RTP packet in order for it to support generic erasure correction of real time media, such as MPEG-2 Transport Streams. It mentions Reed-Solomon and Hamming, but does not define any specific parameters, such as which code dimension to use or rate.

The Pro-MPEG FEC Code of Practice 3.2($CoP3.2$) [20] is highly available in systems transmitting Transport Streams over IP networks. It makes use of the payload format specified by the RFC2733 and moreover, it defines how the input symbols have to be arranged with respect to dimension and interleaving of the channel encoder's input block. It also defines a second dimension for the channel coding scheme in order to cope with erasure patterns not addressed by the previous RFC.

The arrangement of the original stream into the code's input block, as defined in the first scheme presented in the CoP.3.2 is shown in figure III.2. The Bytes of the incoming RTP packets are arranged as the lines of a matrix and the channel code is applied vertically, providing interleaving by a factor L. The resulting overhead can be transmitted through a separate UDP port, in order for non FEC-compatible receivers to be able to receive the content as well.

This scheme is useful for recovery from burst losses (by burst loss it is meant that a group of neighboring RTP packets is lost). However, if some

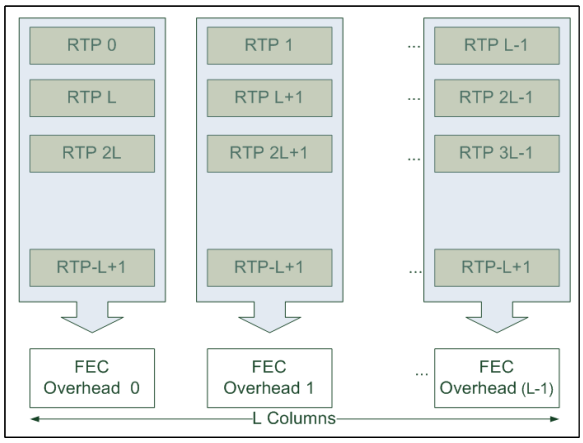

Figure III.2: Previous FEC scheme

punctual losses occur across the same column (punctual loss meaning that a single RTP packet, in between correctly received neighboring RTP packets, has been erased) in addition to the burst losses, the decoding process might fail.

An alternate scheme presented in CoP3.2 specifies a second dimension for the FEC code, applied across the lines of the input matrix, as depicted in figure III.3. The second dimension of the code is intended to cope with individual packet drops. According to the specification, the second dimension of the coding scheme is transmitted through a third separate UDP port (considering that the payload and the overhead resulting from the first dimension already occupy two separate ports). The composition of the source blocks for each code dimension is shown in figure III.3.

The channel decoder makes use of particular fields of the header of each RTP packet. A complete description of such packets is given in [1]. The main header items that the receiver needs to observe for recovering each column include the Sequence Number (SN), the RTP Packet Offset (L) and the Packet Numbering field (NA). All these fields are explained in the reference provided.

The specification also makes reference to TSP sizes. All equipment must handle 188-bytes TSPs, whereas 204-byte TSPs are optional. From 1-7 TSPs should be included in each RTP packet. It is important to consider the network's *Maximum Transfer Unit* (MTU), since the IP don't fragment bit is set for RTP streaming. By default, IP networks have an MTU of 1,500 bytes. According to the standard, equipment should support RTP packets containing 1, 4 and 7 TSPs as a minimum requirement. The RTP Payload Type, as specified in [1], has to be equal to 96, which corresponds to the first available

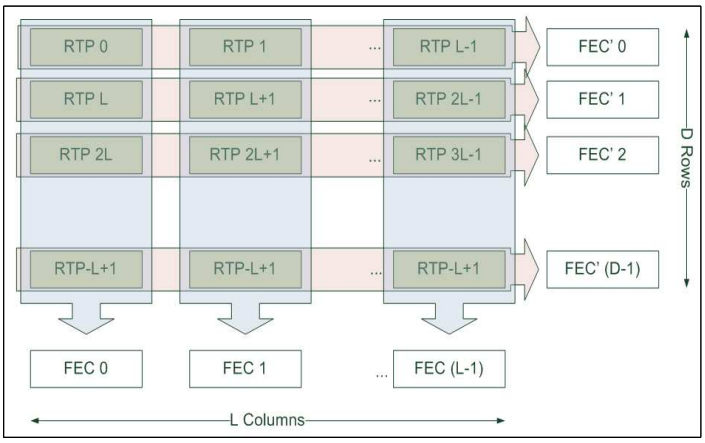

Figure III.3: Coding scheme defined in CoP 3.2

dynamic identification.

The recommendation also makes reference to the codes' dimensions. The values for L and D, indicated in figure III.3 are bounded as follows:

$$L \cdot D \leq 100$$
$$1 \leq L \leq 20$$
$$4 \leq D \leq 20$$

Where L and D are quantified in units of RTP packets.