Packet Loss Due to Encryption in Space Data Systems

Hyuck M. Kwon, Member, IEEE

Abstract—This paper analyzes the probabilities of data packet loss for both an encrypted channel in self-synchronous cipher feedback mode and a nonencrypted channel, in the space data systems. Simulation results show reasonable agreement with analytical results. When channel bit error probability is $10^{-7}$ and the total number of packets per frame is 3, the analytical model gives 0.39% packet loss while the simulation gives 0.22% packet loss due to encryption. Although the analysis is performed for the space data systems, the resulting derived equations with minor change will be useful in many packet communication applications.

I. INTRODUCTION

The Consultative Committee for Space Data Systems (CCSDS)—a worldwide cooperative effort of national space agencies—began to develop a comprehensive set of standards in the mid 1980's [1]-[4]. The standards cover techniques for data handling, classification, and transmission. Data encryption is required to provide privacy and security in many communications channels, as it is in the space data systems.

The performance analysis of the encrypted CCSDS links is a timely subject. Data packets are more likely to be lost in an encrypted communication system than in a nonencrypted system. This paper analyzes the probabilities of data packet loss for both an encrypted channel and a nonencrypted channel. Section II describes the system models, and Section III provides the analysis. The details are analyzed in the Appendices A and B. Section IV presents the numerical results, and Section V concludes the paper.

II. SYSTEM MODELS

Fig. 1 shows a simplifies block diagram of the Ku-band single access return link (KSAR) with self-synchronous cipher-feedback data encryption in a typical spacecraft communication link. Source data from digital audio, control and monitor subsystem (CMS) core data, and selected digital video are encrypted by the Data Encryption Standard (DES) encryptor in self-synchronous cipher feedback mode (Fig. 2; described later).

A frame formatter then forms a 10112 bit transfer frame (T-frame). The T-frame bits are binary phase-shift keying (BPSK) modulated and transmitted, and white Gaussian noise is shown added to the transmitted signal. Fig. 1 also includes Reed-Solomon (RS) coding with interleaver depth 5, which may or may not be employed. At the receiver, the signal is BPSK demodulated. The BPSK demodulated signal is deinterleaved, decoded (if coding is employed), and decrypted. It is assumed that the coded channel symbols are memoryless because the interleaver and deinterleaver are employed. The burst error effects on the packet transmission are not included in this paper.
Fig. 2 shows the DES encryptor in a self-synchronous cipher feedback mode. \(P_n\) denotes the \(n\)th character, which consists of \(m\) bits of plain text (i.e., from the digital audio, video, or CMS core data), \(K_n\) denotes the \(n\)th keystream character, which consists of \(m\) bits from the DES, and \(C_n\) denotes the ciphertext character (consisting of \(m\) bits) obtained by the binary modulo addition of \(K_n\) and \(P_n\). In a self-synchronous stream cipher, each key character \(K_n\) is derived from a fixed number \(M\) of the preceding ciphertext characters \(C_{n-1}, C_{n-2}, \ldots, C_{n-M}\) by feeding back to the input of the shift register. Initialization is provided by a known input, \(I_0\). The memory depth \(M\) is the number of stages in the shift register generator divided by the number of bits in the feedback ciphertext character. In this paper, \(M\) is equal to one because a 64 stage shift register generator is employed and feedback ciphertext character size \(m\) is chosen to be 64 bits. At each iteration, the output of the shift register is used as input to the DES algorithm [5]–[7]. The low-order output from a fixed number of the preceding ciphertext characters \(M\) is correct but the current received cipher character \(C_n\) is in error, a decrypted plaintext character \(P_{n+1}\) is the event where the \(i\)th packet application process ID \(Y_i\) or \(Z_i\) is the event where the \(i\)th packet application process ID of the 11 encrypted bits is incorrect.

If the critical bits are incorrect due to channel bit error or encryption propagation error, most information of a T-frame can be lost. A reasonable model for packet loss analysis is described as follows. If event \(W\) or \(X\) happen, all packets in a T-frame are lost. If event \(Y_i\) happens, two cases are considered. Case 1 is where all packets in a T-frame are lost and represents a pessimistic case, and Case 2 is where the previous packets are correct if events \(Y_1, \ldots, Y_i\) did not happen, but the current packet as well as the succeeding packets are lost. If event \(Z_i\) happens, only the \(i\)th packet in a T-frame is lost.

It is assumed, for worst case, that the block of bits representing event \(X\), the block of bits representing event \(Y_i\), and the block of bits representing event \(Z_i\) each belongs to a different ciphertext character. For example, under the above case 1 consideration, if the block of bits representing event \(Y_i\) and the block of bits representing event \(Z_i\) fall in the same ciphertext character, then a maximum of \(N_p\) packets may be lost due to events \(Y_i\) or \(Z_i\). However, if the block of bits representing event \(Y_i\) and the block of bits representing event \(Z_i\) fall in different ciphertext characters from each other, then a maximum of \(N_p + 1\) packets may be lost due to events \(Y_i\) or \(Z_i\). As noted previously, ciphertext character size is chosen to be 64. The size of the ciphertext character is larger than that of any block representing a critical event. In a practical case, the block of bits representing an event, e.g., \(Y_i\), may fall on a boundary of a ciphertext character. However, it can be shown...
that the number of packets lost due to the event $Y_i$ does not depend on whether the block of bits representing the event $Y_i$ falls on a boundary of a ciphertext character or not.

In addition, it is assumed that the ciphertext character $C_n$ carrying the block of bits representing an event, e.g., $Y_i$, and the ciphertext character $C_m$ carrying the block of bits representing another event, e.g., $Z_j$, are not neighbors, i.e., the difference between indexes $n$ and $m$ is greater than 1. This assumption and the assumption in the preceding paragraph assure that all events, $X$, $Y_i$, and $Z_j$, $i = 1, 2, \ldots, N_p$ are independent. These assumptions are removed, and R-S coding with interleaver depth 5 was used, in the simulation [8]. The simulation yields results somewhat better than analysis results because the assumptions for the analysis are the worst case. It is also assumed that frames are synchronized; and furthermore that data is encrypted frame by frame, with encryption initialization for each frame.

III. ANALYSIS

A. Probability of Packet Loss in a T-Frame: Case 1

Case 1 is the worse case where all packets in a T-frame are lost when events $Y_i$ (the $i$th packet length information of the 16 encrypted bits is incorrect), $W$, or $X$ happen for any $i = 1, \ldots, N_p$. In this paper, the notation $Y_i \cap Y_j$ is defined to mean that both event $Y_i$ and $Y_j$ occur, and hence that both the $i$th and the $j$th packet length information is incorrect, and $Y_i \cup Y_j$ to mean either the $i$th or the $j$th packet length information is incorrect or both are incorrect. Let event $Y$ be the union of $Y_i$, $i = 1, \ldots, N_p$. Then the probability of the event $Y$ is

$$\Pr\left(Y = \bigcup_{i=1}^{N_p} Y_i\right) = \sum_{k=1}^{N_p} (-1)^{k+1} \binom{N_p}{k} \Pr^k(Y_i)$$  \hspace{1cm} (1)$$

because events $Y_i$ are identical and independent. $\binom{N_p}{k}$ is the binomial coefficient $N_p!/(k!(N_p - k)!))$. $Pr(Y_i)$ is the probability that the $i$th packet length information of the 16 encrypted bits is incorrect, which can be written as \(1 - (1 - P_b)^{64} + (1 - P_b)^{64}(1 - (1 - P_b)^{16})\), $i = 1, 2, \ldots, N_p$ where $P_b$ is the coded or uncoded channel bit error probability. The detailed derivation of $Pr(Y_i)$ is shown in the following:

Suppose the 16 bit packet length information was received in the current ciphertext character $C_n$ as shown in Fig. 4. The decrypted plaintext character $P_n$ is a binary addition of the current decryption key $K_n$ and the current received ciphertext character $C_n$, which can be written as $P_n = C_n \oplus K_n = C_n \oplus f_D(C_n-1)$ where $\oplus$ is a binary addition and $f_D$ is the DES decryption key function. If the previous received ciphertext character $C_n-1$ is in error, the current decryption key $K_n$ is in error, which causes the decrypted plaintext character $P_n$ to be in error. The event $Y_i$ happens if the current decryption key $K_n$ is in error or if the current decryption key $K_n$ is correct but the 16 bit block in the current received ciphertext $C_n$ is in error. Thus the probability of event $Y_i$ can be written as $Pr(C_n-1 = f_D^{-1}(K_n) \text{ is in error})$ plus $Pr(K_n \text{ is correct}) \times Pr(\text{the 16 bit block in } C_n, \text{ is in error})$.

The probability of packet loss in a T-frame can be expressed as the average number of packets lost in a T-frame divided by the total number of packets in a T-frame; detailed derivations of the probability of packet loss are provided in Appendix A. The probability of packet loss can be written as

$$Pr(\text{Packet Loss}) = Pr(W) + Pr(X) + Pr(Y) + Pr(Z_1)$$

$$- Pr(W) Pr(X)$$

$$- Pr(W) Pr(Y) - Pr(X) Pr(Y)$$

$$- Pr(W) Pr(Z_1) + Pr(X) Pr(Z_1)$$

$$- Pr(Y) Pr(Z_1) + Pr(W) Pr(Y) Pr(Z_1)$$

$$+ Pr(X) Pr(Y) Pr(Z_1) - Pr(W)$$

$$Pr(X) Pr(Y) Pr(Z_1)$$

$$Pr(\text{Packet Loss}) \approx Pr(W) + Pr(X) + N_p Pr(Y_i)$$

$$+ Pr(Z_1)$$

$$\approx (2N_{\text{SRG}} + N_W + N_X + N_{Z_1})$$

$$+ (N_{\text{SRG}} + N_Y) N_p P_b$$

$$= (156 + 80N_p) P_b$$  \hspace{1cm} (3)$$

where $N_{\text{SRG}}$ is the number of stages in the shift register generators which are used for the encryption and decryption keys, $N_W$ is the number of bits in the VCDU channel ID
field, \( N_X \) is the number of bits in the MPDU first header pointer, \( N_Z \) is the number of bits in the \( i \)th packet application process ID, and \( N_Y \) is the number of bits in the \( i \)th packet length information. Notice that the approximated probability of packet loss is a linear function of bit error probability \( P_b \), and also a linear function of the number of packets \( N_p \) in a T-frame. This is reasonable because the packet length field or application process ID of different packets have the same chance to be incorrect.

**B. Probability of Packet Loss in a T-Frame: Case 2**

In this case, if events \( Y_1 \) through \( Y_{N_p-1} \) do not happen and event \( Y_i \) happens, \( (N_p - i + 1) \) packets in a T-frame (i.e., the current packet as well as the succeeding packets) are lost. If \( W \) or \( X \) happen, all packets in a T-frame are lost. If \( Z_i \) happens, the \( i \)th packet is lost.

The probability of packet loss in a T-frame can be expressed as the average number of packets lost in a T-frame divided by total number of packets in a T-frame; detailed derivations of the probability of packet loss are provided in Appendix B. The probability of packet loss can be written as

\[
\Pr(\text{Packet Loss}) = \Pr(W \cup X) + \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
+ \frac{1}{N_p} \sum_{k=1}^{N_p} \sum_{j=\max(1, k-i+1)}^{N_p-j} j \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot \Pr(Z_1) \text{(or)} \Pr(Y_1) \left(\frac{N_p}{k}\right) \\
\cdot \Pr(W \cup X) \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
+ \frac{1}{N_p} \Pr(W \cup X) \sum_{i=1}^{N_p} \sum_{k=\max(1, k-i+1)}^{N_p-j} j \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot \Pr(Z_1) \text{(or)} \Pr(Y_1) \left(\frac{N_p}{k}\right) \\
\cdot \Pr(W \cup X) \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
\cdot \Pr(W \cup X) \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
\cdot \Pr(Z_1) \text{(or)} \Pr(Y_1) \left(\frac{N_p}{k}\right) \\
\cdot \Pr(W \cup X) \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
\cdot \Pr(W \cup X) \sum_{i=1}^{N_p} \left(1 - \frac{i - 1}{N_p}\right) \\
\cdot (1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \\
\cdot \Pr(Z_1) \text{(or)} \Pr(Y_1) \left(\frac{N_p}{k}\right)
\]

(4)

where \( \Pr(W \cup X) \) is equal to \( \Pr(W) + \Pr(X) - \Pr(W) \times \Pr(X) \).

For small bit error probability \( P_b \leq 10^{-5} \) and for total number of packets in a T-frame \( N_p \leq 50 \), all higher order terms of \( P_b \) greater than or equal to 2 in (4) are insignificant and (4) can be greatly simplified. Thus, the probability of packet loss can be well approximated as

\[
\Pr(\text{Packet Loss}) \\
\approx \Pr(W) + \Pr(X) + \frac{N_p + 1}{2} \Pr(Y_1) + \Pr(Z_1) \\
\approx \left\{ 2N_{SRG} + N_W + N_X + N_Z + \frac{N_p + 1}{2} \right\} P_b \\
= \left( 156 + 80N_p + 1 \right) P_b.
\]

(5)

Notice that the approximated probability of packet loss in Case 2 is equal to that of Case 1 if \( N_p \) is replaced by \( (N_p + 1)/2 \). This is reasonable since the average number of packets lost in Case 2 due to events \( Y_1, \ldots, Y_{N_p} \), is approximately equal to \( N_p/2 \).

If the channel is nonencrypted, error propagation does not happen. Thus, the probability of packet loss for a nonencrypted channel is the same as equation (2) and (4) for Cases 1 and 2, respectively, except \( \Pr(W), \Pr(X), \Pr(Y_i), \text{ and } \Pr(Z_i) \) are given by \( 1 - (1 - P_b)^6 \), \( 1 - (1 - P_b)^9 \), \( 1 - (1 - P_b)^{11} \), and \( 1 - (1 - P_b)^{13} \), respectively. The probability of packet loss for Case 1 can be approximated as

\[
\Pr(\text{Packet Loss}) \approx \Pr(W) + \Pr(X) + N_p \Pr(Y_1) \\
+ \Pr(Z_1) \\
\approx \left\{ N_W + N_X + N_{Z_1} + N_{Y_1}N_p \right\} P_b \\
= \left( 28 + 16N_p \right) P_b.
\]

(6)

The approximated probability of packet loss for a nonencrypted channel is also a linear function of channel bit error probability \( P_b \), and of the number of packets \( N_p \) in a T-frame. The probability of packet loss for Case 2 is (6) with \( N_p \) replaced by \( (N_p + 1)/2 \) for the same reason stated in the encrypted channel analysis.

\[
\Pr(\text{Packet Loss}) \approx \Pr(W) + \Pr(X) + N_p \Pr(Y_1) + \Pr(Z_1) \\
\approx \left\{ N_W + N_X + N_{Z_1} + N_{Y_1} \frac{N_p + 1}{2} \right\} P_b \\
= \left( 28 + 16N_p + 1 \right) P_b.
\]

(7)

**IV. NUMERICAL RESULTS**

The channel bit error probability is assumed to be \( 10^{-5} \) in this paper. If the channel bit error probability is changed to \( 10^{-6} \) or \( 10^{-7} \), and so on, the probability of packet loss is changed to \( 10^{-1} \) (or \( 10^{-2} \) and so on) times the probability of packet loss in this paper because the approximated results are close to exact ones and the approximated probability of packet loss is a linear function of the channel bit error probability as shown in (3), (5), (6), and (7).

Fig. 5 shows the probability of packet loss versus total number of packets \( N_p \), for an encrypted channel. Fig. 6 shows the probability of packet loss versus total number of packets \( N_p \), for a nonencrypted channel. It is observed that the probability of packet loss is a linear function of the total
number of packets in a $T$-frame. For large $N_p \geq 10$, the probability of packet loss in Case 1 (all packets are lost if the $i$th packet length information is incorrect, i.e., event $Y_i$) is almost twice that of Case 2 (the current as well as succeeding packets are lost if event $Y_i$ happens but $Y_1$ through $Y_{i-1}$ do not happen), which is expected. For small $N_p$, this is not true. If the total number of packets is 1, the probability of packet loss is the same for both cases. This is obvious because there is no distinction between Case 1 and Case 2 strategies for $N_p - 1$.

Fig. 5 also shows the corresponding simulation results, which are in reasonable agreement with analytical results. It is observed that analytical results are somewhat larger than simulation results; for example, for an encrypted channel with $10^{-5}$ channel bit error probability and $N_p = 3$ packets in a $T$-frame, the analytical result is 0.3952% loss while the simulation result is 0.22% packet loss. As mentioned in Section II (System Models), the difference between analysis and simulation is due to the worst case analysis assumption (i.e., the block of bits representing event $X$, the block of bits representing event $Y$, and the block of bits representing event $Z$, each belong to a different ciphertext character).

V. CONCLUSION

A reasonable model for packet loss analysis was constructed. If VCDU's channel ID or MPDU's first header pointer, both being critical fields, are incorrect, all packets in a transfer frame are lost. If the $i$th packet length information, also a critical field, is incorrect but all previous packet length information is correct, two cases are considered: Case 1) all packets in a $T$-frame are lost for the worst case analysis and Case 2) the current as well as succeeding packets are lost but all previous packets are forwarded to the desired destinations.

If the $i$th packet application process ID, another critical field, is incorrect, only the $i$th packet in a $T$-frame is lost. The above critical fields can be in error due to not only the channel bit errors in the critical fields but also errors in the previous ciphertext characters of 64 bits located just before each critical field because of error propagation in self-synchronous cipher feedback mode encryption. In this paper, exact and approximate probabilities of packet loss due to encryption were analytically derived. It is observed that the approximate results are very accurate.

Analytical and simulation results are in reasonable agreement. Analytical results are based on a worst case assumption which yields results somewhat worse than simulation results. When channel bit error probability is $10^{-5}$ and the total number of packets per frame is 3, the analytical result is 0.39% packet loss while the simulation result is 0.22% packet loss. Also, the probability of packet loss for a nonencrypted channel was considered, and it is smaller than that for an encrypted channel. However, the probability of packet loss for a nonencrypted channel becomes significant as the number of packets increases.

APPENDIX A

In this Appendix, the detailed derivation of the probability of packet loss is provided for an encrypted channel in self-synchronous cipher feedback mode. Case 1 concerns packet length information, a critical field, and is the case where all packets in a $T$-frame are lost when the current packet length information is incorrect. The model given in the System Models section for packet loss analysis is used. First, the number of packets lost due to critical field events, $W$, $X$, $Y_i$, and $Z_i$ (defined in the main text), and their combined
events, are calculated, and then the probability of packet loss is represented as the number of packets lost divided by the total number of packets \( N_p \) in a T-frame.

Let event \( Y \) be the union of \( Y_i, \ i = 1, \cdots, N_p \). The probability of the event \( Y \) is given in (1). If event \( \{W \cup X \cup Y\} \) happens, \( N_p \) packets are lost. The average number of packets lost due to event \( \{W \cup X \cup Y\} \) is

\[
\text{# of packets lost due to event } \{W \cup X \cup Y\} = N_p \Pr \{W \cup X \cup Y\}. \quad (A-1)
\]

If event \( Z_i \) happens, the \( i \)th packet in a T-frame is lost whether from one bit error or more than one. Let event \( Z \) be the union of \( Z_i, \ i = 1, \cdots, N_p \). Events \( Z_i \) and \( Z_j \) are not disjoint. Event \( Z \) can be decomposed into disjoint events \( D_k, k = 1, \cdots, N_p \). As an example for \( N_p = 3 \) packets, \( Z = D_1 \cup D_2 \cup D_3 \) with

\[
D_1 = \{(Z_1 \cap Z_2 \cap Z_3) \cup (Z_1 \cap Z_2 \cap \overline{Z_3}) \cup (Z_1 \cap \overline{Z_2} \cap Z_3)\},
\]

\[
D_2 = \{(Z_1 \cap Z_2 \cap \overline{Z_3}) \cup (Z_1 \cap \overline{Z_2} \cap Z_3) \cup (\overline{Z_1} \cap \overline{Z_2} \cap Z_3)\},
\]

\[
\text{and } \quad D_3 = \{(Z_1 \cap Z_2 \cap \overline{Z_3})\}
\]

where \( \overline{Z}_i \) is the complement of event \( Z_i \). The \( D_k \) means the \( k \)th subevent of \( Z \), \( D_k \) being the union of \( N_p \times (k!(N_p - k)) ! \) sub-sub-events, and in each sub-sub-event of \( D_k \), the Application Process ID is incorrect in \( k \) packets and the Application Process ID is correct in \((N_p - k) \) packets during a T-frame transmission. In general, \( D_k \) can be represented as (A-2) shown below. The sub-sub-events in \( D_k \) are also disjoint events, and if any sub-sub-event in \( D_k \) happens, \( k \) packets are lost. The probability of \( D_k \) is \( N_p ! / (k!(N_p - k)!)) \Pr_k \{Z_1\}(1 - \Pr \{Z_1\})^{N_p - k} \) because events \( Z_i, \ i = 1, \cdots, N_p \), are identical and independent. Thus, the average number of packets lost due to event \( Z \) can be written as

\[
\text{# of packets lost due to event } Z = \sum_{k=1}^{N_p} k \Pr \{D_k\} = \sum_{i=1}^{N_p} \Pr \{Z_i\} = N_p \Pr \{Z_1\}. \quad (A-3)
\]

Since event \( \{W \cup X \cup Y\} \cap D_k, k = 1, \cdots, N_p, \) is in event \( \{W \cup X \cup Y\} \) of (A-1) and also in event \( D_k \) of equation (A-3), it is counted twice instead of once and hence overcounted.

Thus, from (A-1), (A-3), and (A-4), the average total number of packets lost in a frame is \( N_p \) times \( \{Pr \{W \cup X \cup Y\} + \Pr \{Z_1\} - \Pr \{W \cup X \cup Y\} \Pr \{Z_1\}\} \). Therefore, the probability of packet loss is

\[
\Pr \{\text{packet loss}\} = \Pr \{W \cup X \cup Y\} + \Pr \{Z_1\} - \Pr \{W \cup X \cup Y\} \Pr \{Z_1\}. \quad (A-5)
\]

which becomes (2).

**APPENDIX B**

In this Appendix, the detailed derivation of the probability of packet loss is provided for an encrypted channel in self-synchronous cipher feedback mode. Case 2 concerns an event \( Y_i \) related to the \( i \)th packet length information, i.e., the current packets are forwarded to the desired destinations when the previous packets are lost due to other critical events, i.e., events \( W, X, \) and \( Z_i \) are the same as in Case 1.

If event \( \{W \cup X\} \) happens, \( N_p \) packets are lost. Thus, the average number of packets lost due to event \( \{W \cup X\} \) is

\[
\text{# of packets lost due to event } \{W \cup X\} = N_p \Pr \{W \cup X\}. \quad (B-1)
\]

The average number of packets lost due to event \( Z \) (which is the union of \( Z_i, \ i = 1, \cdots, N_p \)) is shown in (A-3) which is rewritten as

\[
\text{# of packets lost due to event } Z = \sum_{i=1}^{N_p} N_p = N_p \Pr \{Z_1\}. \quad (B-2)
\]

\[
D_k \equiv \left\{ \begin{array}{l}
(Z_1 \cap Z_2 \cap \cdots \cap Z_{k-1} \cap Z_k \cap \overline{Z}_{k+1} \cap \overline{Z}_{k+2} \cdots \cap \overline{Z}_{N_p}) \cup \\
(Z_1 \cap Z_2 \cap \cdots \cap Z_{k-1} \cap Z_k \cap \overline{Z}_{k+1} \cap \overline{Z}_{k+2} \cdots \cap \overline{Z}_{N_p}) \cup \\
\quad \cdots \cup \\
(\overline{Z}_1 \cap \overline{Z}_2 \cap \cdots \cap \overline{Z}_{N_p-k} \cap Z_{N_p-k+1} \cap Z_{N_p-k+2} \cdots \cap \overline{Z}_{N_p}) \end{array} \right\}, \quad k = 1, \cdots, N_p. \quad (A-2)
\]
If previous packet length information is correct but current packet length information is incorrect, i.e., if \( \{Y_1 \cap Y_2 \cap \cdots \cap Y_{i-1} \cap Y_i \} \) happens, \((N_p - i + 1)\) packets are lost. Let \( B_i \) denote event \( \{Y_1 \cap Y_2 \cap \cdots \cap Y_{i-1} \cap Y_i \} \) and let \( B \) denote the union of \( B_i \), \( i = 1, \ldots, N_p \), i.e.,

\[
B_i := \{Y_1 \cap Y_2 \cap \cdots \cap Y_{i-1} \cap Y_i \}
\]

and \( B = \bigcup_{i=1}^{N_p} B_i \). (B-3)

(Notice that events \( B_i \) are disjoint and event \( B \) is the same as the event \( Y \) which is the union of \( Y_i \), \( i = 1, \ldots, N_p \)). Then, the average number of packets lost due to event \( B \) is

\[
\text{# of packets lost due to event } B = \sum_{i=1}^{N_p} (N_p - i + 1) \Pr(B_i)
\]

\[
= \sum_{i=1}^{N_p} (N_p - i + 1)(1 - \Pr(Y_i))^{i-1} \Pr(Y_i)
\]

(B-4)

since events \( Y_i \) are identical and independent.

Since event \( \{W \cup X \cap Z\} \) is in event \( \{W \cup X\} \) of equation (B-1) and also in event \( Z \) of equation (B-2), it is counted twice instead of once and hence overcounted. The average number of packets lost overcounted due to event \( \{W \cup X \cap Z\} \) can be written as

\[
\text{# of packets lost overcounted due to event } \{W \cup X \cap Z\} = \Pr(W \cup X) N_p \Pr(Z_1). \quad \text{(B-5)}
\]

Event \( \{W \cup X \cap B\} \) is likewise overcounted in (B-1) and (B-4). If \( \{W \cup X \cap B_i\} \) happens, \( N_p - i + 1 \) packets are lost. Thus, the average number of packets lost overcounted due to event \( \{W \cup X \cap B\} \) can be written as

\[
\text{# of packets lost overcounted due to event } \{W \cup X \cap B\} = \Pr(W \cup X) \sum_{i=1}^{N_p} (N_p - i + 1) \Pr(B_i)
\]

\[
= \Pr(W \cup X) \sum_{i=1}^{N_p} (N_p - i + 1)(1 - \Pr(Y_i))^{i-1} \Pr(Y_i)
\]

(B-6)

Event \( \{B \cap Z\} \) is overcounted in (B-2) and (B-4). For example, if event \( \{B_1 = Y_1 \cap Y_2 \cap \cdots \cap Y_{i-1} \cap Y_i \cap Z_1 \cap Z_2 \cap \cdots \cap Z_{i-1} \cap Z_{i+1} \cap Z_{i+2} \cap \cdots \cap Z_{N_p}\} \) happens, the overcounted number of packets lost is 1. However, if \( \{B = Y_1 \cap Y_2 \cap \cdots \cap Y_{i-1} \cap Y_i \cap Z_1 \cap Z_2 \cap \cdots \cap Z_{i-1} \cap Z_{i+1} \cap Z_{i+2} \cap \cdots \cap Z_{N_p}\} \) happens, no packets are overcounted as lost since \( B_i \) causes the current and subsequent \((N_p - i + 1)\) packets to be lost while event \( \{Z_1 \cap Z_2 \cap \cdots \cap Z_{i-1} \cap Z_{i+1} \cap Z_{i+2} \cap \cdots \cap Z_{N_p}\} \) causes the previous \(i - 1\) packets to be lost. In general, the average number of lost packets overcounted due to event \( \{B_i \cap D_k\} \) can be written as

\[
\text{# of packets lost overcounted due to event } \{D_k \cap B_i\} = \min(k, N_p - i + 1) \sum_{j=\max(1, k-i+1)}^{i-1} \frac{\binom{N_p - i + 1}{j}}{j} \left(1 - \Pr(Y_1)\right)^{i-j} \Pr(Y_1) \left(1 - \Pr(Z_1)\right)^{N_p - k}, \quad i, k = 1, \ldots, N_p \quad \text{(B-7)}
\]

where binomial coefficient \( \binom{n}{k} \), denoted as “\(N\) choose \(k\),” is equal to \(N! / (k! (N - k)!))\). For example, for \((N_p = 5, \text{events } B_{i=3}, \text{and } D_{k=4})\), the overcount \(j\) in number of packets lost can be from 2 (the maximum of 1 and \((k - i + 1)\)) to 3 (the minimum of \(k\) and \((N_p - i + 1)\)). An overcount \(j = 2\) occurs if any of the following 3 events happens:

1. \(Z_1 \cap Z_2 \cap Z_3 \cap Z_4 \cap Z_5\)
2. \(Z_1 \cap Z_2 \cap Z_3 \cap Z_4 \cap Z_5\)
3. \(Z_1 \cap Z_2 \cap Z_3 \cap Z_4 \cap Z_5\)

where 3 is the result of “\((i - 1 = 2)\)” choose \((k - j = 2)\)” times \((N_p - i + 1 = 3)\) choose \(j = 2\). An overcount \(j = 3\) occurs if either of the following two events happens:

1. \(Z_1 \cap Z_2 \cap Z_3 \cap Z_4 \cap Z_5\)
2. \(Z_1 \cap Z_2 \cap Z_3 \cap Z_4 \cap Z_5\)

where 2 is the result of “\((i - 1 = 2)\)” choose \((k - j = 1)\)” times \((N_p - i + 1 = 3)\) choose \(j = 3\). The \((1 - \Pr(Y_1))^{i-j} \Pr(Y_1)\) in (B-7) is the probability of \(B_i\), and the “\(N_p\) choose \(k\)” times \(\binom{N_p}{k} (1 - \Pr(Z_1))^{N_p - k}\) is the probability of event \(D_k\). Thus, the average overcount due to event \(\{Z \cap B\} \) can be written as

\[
\text{# of packets lost overcounted due to event } \{Z \cap B\} = \sum_{i=1}^{N_p} \sum_{k=1}^{\min(k, N_p - i + 1)} \frac{\binom{N_p - i + 1}{j}}{j} \left(1 - \Pr(Y_1)\right)^{i-j} \Pr(Y_1) \left(1 - \Pr(Z_1)\right)^{N_p - k}, \quad i, k = 1, \ldots, N_p \quad \text{(B-8)}
\]
From equations, (B-1), (B-2), (B-4), (B-5), (B-6), and (B-8), event \( \{(W \cup X) \cap B \cap Z\} \) is counted three times in events \( \{(W \cup X) \cap B\} \), \( \{(W \cup X) \cap Z\} \), and \( \{B \cap Z\} \), and thus ends up not being counted at all. Hence, it still needs to be counted. The average number of packets lost due to event \( \{(W \cup X) \cap B \cap Z\} \) can be written as

\[
\# \text{ of packets lost due to event } \{(W \cup X) \cap B \cap Z\} = \sum_{i=1}^{N_p} \sum_{k=1}^{N_p} \sum_{j=1}^{\min(k, N_p-i+1)} \frac{1}{j} \binom{N_p-i+1}{j} \cdot \Pr(W \cup X)(1 - \Pr(Y_1))^{i-1} \Pr(Y_1) \cdot \binom{N_p}{k} \cdot P_h(Z_1)(1 - \Pr(Z_1))^{N_p-k}.
\]

(B-9)

Therefore, the probability of packet loss, which is obtained from \( \{(B-1) + (B-2) + (B-4) - (B-5) - (B-6) - (B-8) + (B-9)\} \) divided by the total number of packets \( N_p \) in a T-frame, becomes (4).

REFERENCES


Hyuck M. Kwon (S'82-M'84) was born in Korea on May 9, 1953. He received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in computer, information, and control engineering from the University of Michigan, Ann Arbor, MI, in 1984. While at the University of Michigan, he worked as a research assistant at Cooley Electronics Laboratory where he evaluated the performance of digital coding schemes for underwater acoustic multipath channel. From 1985 to 1989, he was with the University of Wisconsin, Milwaukee, WI, as an Assistant Professor in the Electrical Engineering and Computer Science Department. From 1989 to 1993, he was with the Lockheed Engineering and Sciences Company, Houston, TX, as a Principal Engineer, where he was responsible for analysis of the Space Station Freedom and Space Shuttle communication systems, and also responsible for analysis of Lunar-Mars laser communications systems. Since 1993, he has been with the Wichita State University, Wichita, KS, as a faculty member in the Electrical Engineering Department. In addition, he served as a consultant for J. S. Lee Associates, Inc., where, in 1985, he analyzed the performance of spread-spectrum communications systems and, in 1987, was involved in analyzing the narrowband digital FM Radio spread-spectrum communications systems. His current interests include analysis of satellite communication systems, multiple-access communications networks, bandwidth and power-efficient coded modulations, optical-laser communications, and neural networks.