SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2013; **6**:942–954
Published online 12 October 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.638

RESEARCH ARTICLE

Cipher feedback mode under go-back-N and selective-reject protocols in error channels

Xiannuan Liang[1], Yang Xiao[1]*, Suat Ozdemir[2], Athanasios V. Vasilakos[3] and Hongmei Deng[4]

[1] Department of Computer Science, The University of Alabama, 101 Houser Hall, Tuscaloosa, AL 35487-0290, U.S.A.
[2] Computer Engineering Department, Gazi University Maltepe, Ankara TR-06570, Turkey
[3] Department of Computer and Telecommunications Engineering, University of Western Macedonia, Greece
[4] Intelligent Automation, Inc., 15400 Calhoun Dr. Suite 400, Rockville, MD 20855, U.S.A.

ABSTRACT

To produce ciphertexts, two modes of encryption are applied—block ciphers, which encrypt a fixed size block of plaintext at a time, and stream ciphers, which encrypt stream data, one or more bits at a time. As one of stream ciphers, the cipher feedback (CFB) mode is implemented by a block cipher via multiple stages, and in each stage, 1 bit or a number of bits of plaintext are encrypted at a time. Throughout this paper, the study will focus upon the error performance of the stream-based CFB under two sliding-window protocols, go-back-N and selective-reject, in an error channel in terms of throughput. We model the performance of the CFB in terms of application-level throughput and derive the number of stages needed to achieve the optimal throughput, under a given error rate in an error channel. Copyright © 2012 John Wiley & Sons, Ltd.

KEYWORDS
cipher feedback mode; flow control; sliding-window; error channel

***Correspondence**
Yang Xiao, Department of Computer Science, The University of Alabama, 101 Houser Hall, Tuscaloosa, AL 35487-0290, U.S.A.
E-mail: yangxiao@ieee.org

1. INTRODUCTION

Throughout the work, there is a collective study of the performance of a stream cipher mode called cipher feedback (CFB) mode [1,2] with the link control mechanisms' sliding-window protocols [3] including go-back-N ARQ (automatic repeat-request) and selective-reject ARQ. Stream ciphers are used to encrypt one or more bits/bytes at a time and normally generate a keystream XORed with the plaintext to generate the ciphertext. To decrypt the ciphertext, the plaintext is recovered at the receiver by generating the same keystream.

There have been many stream ciphers in wireless networks (e.g., IEEE 802.11 [4] and voice encryption in wireless telephones [5,6]). Telnet adopts CFB [7,2]. Potentially, CFB can be applied in wireless networks (e.g., in Telnet over wireless networks or voice encryption in wireless telephones/messaging).

In [8,7], with CFB and under the stop-and-wait link protocol [3], the authors provided an error analysis for the CFB in a wireless error channel and analytically model the throughput as well as the probability that a portion or absolutely the complete ciphertext may not be successfully decrypted by the CFB. However, stop-and-wait is the simplest of the three common protocols used for flow and error control at the link level. The other common protocols are go-back-N and selective-reject [3].

Throughout this work, we focus on studying the performance and impact of the CFB under the sliding-window protocols go-back-N and selective-reject. According to the authors' knowledge, there is no work on the CFB with go-back-N and selective-reject in the literature. The work is the first attempt at studying the CFB under the sliding-window protocols. Coupled with the CFB, the performance analyses of go-back-N and selective-reject are much more complicated than those of the simple stop-and-wait protocol used in [8,7]. Now, we focus on solving this problem: under go-back-N and selective-reject, given a bit error rate in an error channel and the number of bits encrypted each time, how many stages are needed to obtain the optimal throughput? The results presented in this paper should help to select values for the parameters of the CFB when used with sliding-window protocols in error channels. First, the channel throughput is evaluated as a function of the channel parameters of bit error rate, the CFB parameters, and the specific protocol used (go-back-N or selective-reject). The problem of maximizing the channel throughput with respect to the CFB parameters is then analyzed, and the results are supported by performance evaluation. Note that an early short version of this paper was presented in a conference [9]. There are also some related papers in [10–51].

The rest of the paper is organized as follows: In Section 2, we briefly introduce sliding-window protocols including both go-back-N and selective-reject. In Section 3, we introduce the

CFB. In Section 4, we provide a throughput analysis of go-back-N and selective-reject. In Section 5, we provide an optimality analysis of go-back-N and an optimality analysis of selective-reject. In Section 6, we evaluate the performance; we conclude this paper in Section 7.

2. BRIEF INTRODUCTION TO SLIDING-WINDOW PROTOCOLS

Three techniques that are commonly used for flow and error control at the link level are stop-and-wait, go-back-N, and selective-reject. The final two techniques are special cases of the sliding-window techniques.

2.1. Stop-and-wait

Stop-and-wait flow control [3] is simplest form of flow control. In stop-and-wait, a source station transmits a frame once. After reception, the destination station sends back an acknowledgment frame for the frame it has just received, thus indicating that it is ready to accept another frame. Before the source station receives the acknowledgment frame, it must wait to send the next frame.

The problem with stop-and-wait is that if the bit length of the link is greater than the frame length, then serious inefficiencies will occur, where the bit length of the link is defined as the time it takes one bit to travel from the beginning of the link to the end, that is, propagation delay, and the frame length is the time it takes to transmit a frame, that is, transmission time.

2.2. Sliding-window

Allowing two or more frames to be transmitted at a time may greatly reduce inefficiency.

Consider two stations, a source and a destination, which are connected with a full-duplex link [3]. The destination allocates buffer space for n frames and, thus, may accept n frames. The source is allowed to send up to n frames without waiting for an acknowledgment frame (ACK). The scheme can be used to acknowledge multiple frames. For example, the destination could receive frames denoted as 1, 2, and 3, but would not send an ACK until frame 3 has arrived. By returning an ACK with the sequence number of frame 4, the destination acknowledges frames 1, 2, and 3 at one time by indicating that it is ready to receive frame 4. The source maintains a list of sequence numbers that it is allowed to send, and the destination gets a queue of sequence numbers that it is ready to receive. Each of these lists can be considered to be a window of frames, and the operation is called therefore as sliding-window flow control.

Go-back-N ARQ [3] is the most commonly used form of error control based on sliding-window flow control. In go-back-N ARQ, a source may sequentially send a series of frames numbered modulo some maximum value. The number of outstanding, unacknowledged frames depends on the window size. If no errors occur, the destination will acknowledge incoming frames as usual. If the destination detects any error in a frame, it will send a negative ACK and get rid of that frame and all future incoming frames until the frame in error is correctly received. After receiving a negative ACK, the source will retransmit the frame in error as well as all succeeding frames that were transmitted in the interim.

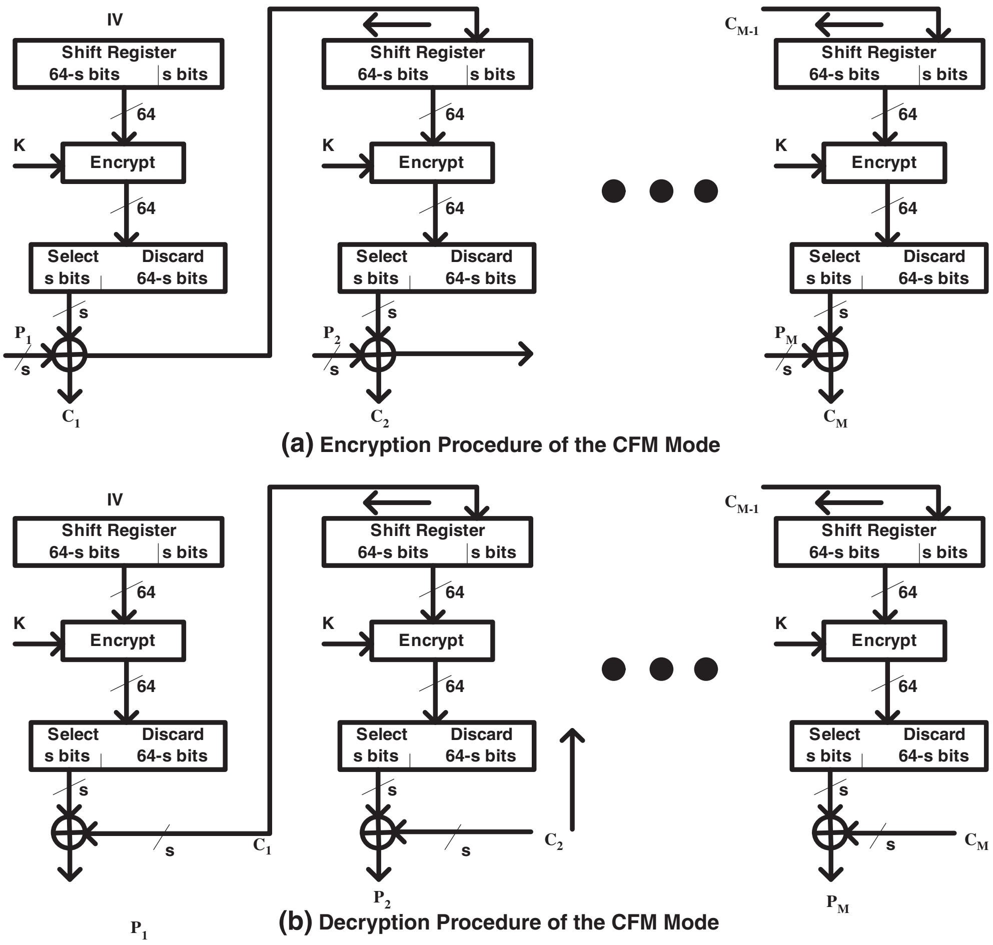
In selective-reject [3], if an error occurs, the source only retransmits the frames that either receives a negative ACK, or those in the case of time out. Selective-reject appears to be more efficient than go-back-N in terms of minimizing the number of retransmissions, but the destination must maintain a buffer large enough to save frames until the frame in error arrives and is reinserted in the proper sequence. The source also requires more complex logic to handle the cases in which a frame is sent out of sequence. In other words, go-back-N is simpler than selective-reject. Because of such complications, selective-reject is much less widely used than go-back-N.

3. CIPHER FEEDBACK MODE

The CFB mode [8,7,52,1] is one mechanism used by a block cipher to implement a stream cipher. A stream cipher is one that encrypts a stream of data, such as voice, video, or Telnet traffic, one bit/byte at a time. The autokeyed Vigenere cipher and the Vernam cipher are two examples of stream ciphers. CFB was originally derived from block ciphers, such as the Data Encryption Standard (DES) [8,7,52,1,53,2]. However, CFB is not limited to the DES and can be used with the Advanced Encryption Standard, Triple DES, Skipjack, and so on. In the CFB mode, a plaintext (P) is divided into M units $P = P_1||P_2||P_3||...||P_M$ and each unit has s bits ($s = 1, 2, ..., 64$). The corresponding ciphertext is denoted as $C = C_1||C_2||C_3||...|| C_M$. For $j = 1, ..., M$, the encryption is done by $C_j = F(\mathrm{DES}_K(H_j)) \oplus P_j$ and $H_1 = \mathrm{IV}$, where $H_j = L\text{-Shift}(H_{j-1}, s)\ C_{j-1}$, IV is an initialization vector of length L ($L = 64$), F denotes the function of obtaining the (left) most significant s bits, $\mathrm{DES}_K()$ denotes the encryption of the DES using the key K, and L-Shift(H, s) denotes the function of left shifting H with s shifts such that the (left) most significant s bits are discarded. For $j = 1, ..., M$, the decryption is done by $P_j = F(\mathrm{DES}_K(H_j)) \oplus C_j$. The following subsections give more details about CFB encryption and decryption.

3.1. Encryption

In the CFB mode, a plaintext (P) is divided into M units $P = P_1||P_2||P_3||...||P_M$, and each unit has s bits ($s = 1, 2, ..., 64$), as shown in Figure 1a. In other words, s bits of data are encrypted at a time. An IV of length L ($L = 64$ in Figure 1) is used as the initial input block of the DES encryption for P_1, and the (left) most significant s bits of the output block of the DES encryption are XORed with the s-bit plaintext unit P_1 to produce the cipher text C_1. Let F denote the



(a) Encryption Procedure of the CFM Mode

(b) Decryption Procedure of the CFM Mode

Figure 1. The cipher feedback mode (CFM).

function of obtaining the (left) most significant s bits, and let K denote the key of DES. We have $C_1 = F(\text{DES}_K(\text{IV})) \oplus P_1$.

Generally, the initial input block is IV, and then the input block, referred to as the shift register, changes each time. The input block H_j ($j = 1, \ldots, M$) is encrypted with DES, and an output block is produced. The (left) most significant s bits of the output block of the DES encryption are XORed with the s-bit plaintext unit Pj. For $j = 1, \ldots, M$, we have

$$C_j = F\left(\text{DES}\left(H_j\right)\right) \oplus P_j \tag{1}$$

$$H_1 = \text{IV} \tag{2}$$

In Equation (1), we notice that the unused $64 - s$ bits of the DES output block are discarded. The next input block is created by discarding the (left) most significant s bits of the previous input block, shifting the remaining bits $64 - s$ positions to the left, and then inserting the s bits of cipher text just produced in the encryption operation. Let L-Shift(H, s) denote the function of left shifting H with s shifts such that the (left) most significant s bits are discarded. For $j = 2, \ldots, M$, we have

$$H_j = L\text{-Shift}\left(H_{j-1}, s\right) \oplus C_{j-1} \tag{3}$$

This process continues until the entire plain text message (P) has been encrypted.

3.2. Decryption

Decryption is shown in Figure 1b, in which s bits of data are decrypted at a time. The initial input block is the same as the encryption listed in Equations (2) and (3). The DES encryption is still used to encrypt the input block H_j ($j = 1$, ,M) to generate the output block. The (left) most significant s bits of the output bock of the DES encryption are XORed with the s-bit ciphertext unit C_j to produce the plaintext block P_j. Therefore, for $j = 1, \ldots, M$, we have

$$P_j = F\left(\text{DES}_K\left(H_j\right)\right) \oplus C_j \tag{4}$$

We can easily prove Equation (4) as follows.

$$F\left(\text{DES}_K\left(H_j\right)\right) \oplus C_j = F\left(\text{DES}_K\left(H_j\right)\right) \oplus \left[F\left(\text{DES}_K\left(H_j\right)\right) \oplus P_j\right] = P_j$$

In Equation (4), we notice that the unused $64-s$ bits of the DES output block are discarded. The subsequent input block is created by discarding the (left) most significant s bits of the previous input block, shifting the remaining bits $64-s$ positions to the left, and then inserting the s bits of cipher text just produced in the encryption operation.This process continues until the entire cipher text message $(C = C_1||C_2||C_3||...||C_M)$ has been decrypted.

3.3. Discussion

With encryption and decryption of the CFB mode, we may notice that the CFB mode is an implementation of a stream cipher with a block cipher. A stream cipher is useful for stream data.

Note that in both encryption and decryption of the CFB mode in Figure 1, the DES encryption is used, but not the DES decryption. In fact, the DES is used to encrypt the input block so that different s-bit outputs are produced.

4. THROUGHPUT STUDY OF SLIDING-WINDOW PROTOCOLS

In this part, we will study both the normalized link-level throughput and the normalized application-level throughput of transmissions under sliding-window protocols.

4.1. Application scenarios

For sliding-window flow and error control protocol, it is natural to assume that there is a full-duplex channel (path) with one source and one destination. The full-duplex channel can be a multiple-hop path if the connection between the source and the destination has an end-to-end flow and error control; the examples of multiple-hop path are TCP channels and paths over frame relay or Asynchronous Transfer Mode (ATM) networks for transmissions with no flow control in upper layer (such as User Datagram Protocol (UDP) transmission). The full-duplex channel can also be a one-hop path if the connection is over a network using a hop-by-hop flow control such as X.25 and some kinds of LANs. Application scenarios over sliding-window flow control include UDP transmission over X.25, ATM or frame relay networks, TCP transmissions, and more.

Before we study the performance of CFB under the sliding-window protocols, we need to first define or denote the quantities and variables involved in Sections 4 and 5. Besides that, we also put the notations of the quantities and variables in Table I. Let T and G denote normalized link-level throughput [3] and normalized application-level throughput (goodput) [54], respectively. Let P denote the probability that an error occurs when a frame is transmitted. Let α denote the ratio of the propagation delay to the transmission time of a frame, that is, $\alpha = T_{prop}/T_{trans}$, where T_{trans} is the transmission time and T_{prop} is propagation delay. Let T_{data} denote the transmission time of the

Table I. Notations.

T	Link-level throughput
G	Application-level throughput
T_r	The time from the beginning of the transmission of a frame to the reception of the acknowledgment
T_{trans}	The transmission time of a frame
T_{prop}	Propagation delay
T_{data}	The transmission time of the application-level data in a frame
T_{t_ack}	The transmission time of an acknowledgment
α	T_{prop}/T_{trans}
β	T_{t_ack}/T_{trans}
P	The probability that there is an error occurring in the transmission of a frame (error either in the frame itself or in the acknowledgment)
s	The volume in bits of cipher text outputted at the end of each stage of a CFB encryption
M	The number of stages in a CFB encryption
M_{opt}	The number of stage(s) for encryption/decryption which leads to the optimal application-level throughput without considering the capacity of application-level data in a frame
$\bar{M}_{opt}$	The optimal number of stages for encryption/decryption in consideration of the capacity of application-level data in frame
R	The transmission rate in bits per second
H	The frame/packet overhead in bits including header (Medium Access Control header, IP header, TCP/UDP header) and trailer
L_{ACK}	The length of the acknowledgment frame/packet in bits
T_p	The transmission time for the physical header
R_{BER}	The channel bit error rate
W	The number of frames in a window
$I(e)$	The indication function, which returns 1 if e is true and 0 if it is not

DOI: 10.1002/sec

application-level data in a frame. Let W denote the window size, that is, the maximum number of frames that can be buffered. When the source transmits a frame, it takes time for the source to receive an acknowledgment (ACK) from the destination. Let T_r denote the time from the beginning of the transmission of the frame to the reception of the acknowledgment. Let $I(e)$ denote the indication function, which returns 1 if e is true and 0 if it is not. Note that from the definitions of normalized throughput (link level) in [3] and normalized goodput in [54], the following expression holds:

$$G = \frac{T_{data}}{T_{trans}} \cdot T,$$

4.2. Error-free sliding-window flow control

The link-level throughput for a sliding-window flow control under an error-free channel was given as follows [3]:

$$T = I(W \geq 2\alpha + 1) + WI(W < 2\alpha + 1)/(2\alpha + 1) \tag{5}$$

However, in [3], the author ignored transmission time of an ACK by assuming $T_r = T_{trans} + 2T_{prop}$. We want to consider ACKs as follows. Let T_{t_ack} denote the transmission time for the ACK. We have $T_r = T_{trans} + 2T_{prop}\ T_{t\_ack}$. Let $\beta = T_{t\_ack}/T_{trans}$ denote the ratio of the transmission time of an ACK to the transmission time of a frame. Thus, if we do not ignore the transmission time of the ACK, the expression of the throughput without error is

$$\begin{aligned} T &= I\left(W \geq \frac{T_{trans} + 2T_{prop} + T_{t\_ack}}{T_{trans}}\right) \\ &\quad + \frac{WT_{trans}}{T_{trans} + 2T_{prop} + T_{t\_ack}} I\left(W < \frac{T_{trans} + 2T_{prop} + T_{t\_ack}}{T_{trans}}\right) \\ &= I(W \geq 1 + 2\alpha + \beta) + \frac{W}{(1 + 2\alpha + \beta)} I(W < 1 + 2\alpha + \beta) \end{aligned} \tag{6}$$

4.3. Sliding-window flow control with error

During the transmission of frames, an error occurs if there is either a damaged frame or a damaged ACK. In [3], the author deducted expressions of the normalized throughput in the cases go-back-N and selective-reject under the possibility of those errors. In the following, we will revise those throughput expressions from [3] in consideration of the transmission time of an acknowledgment, which was ignored in the throughput deduction in [3]. Note that the results in [3] are about link-level throughput and is based on the assumption that the propagation delay is stable and has nothing to do with the frame size. This assumption is true in a one-hop channel. In a multiple-hop channel such as ATM channel, it is realistic that the propagation delay is assumed to be stable and have nothing to do with the frame size because of high data transmission rate and small data payload in a frame. Generally speaking, in a multiple-hop channel such as TCP, applying that assumption is a way to make the study less complicated and more tractable. In the study throughout this paper, we hold that assumption.

4.3.1. Go-back-N

From [3], with go-back-N, we obtain the following expression:

$$\begin{aligned} T &= \frac{1 - P}{1 - P + (2\alpha + 1)P} I(W \geq 2\alpha + 1) \\ &\quad + \frac{W}{(2\alpha + 1)} \cdot \frac{(1 - P)}{(1 - P + WP)} I(W < 2\alpha + 1) \end{aligned} \tag{7}$$

However, in Equation (7), the author ignores the transmission time of an acknowledgment. Considering the transmission time of an acknowledgment, the aforementioned expression can be modified as follows:

$$\begin{aligned} T &= \frac{1 - P}{1 - P + (T_r P)/T_{trans}} I\left(W \geq \frac{T_{\mathrm{r}}}{T_{trans}}\right) \\ &\quad + \frac{W}{T_r/T_{trans}} \cdot \frac{(1 - P)}{(1 - P + WP)} I\left(W < \frac{T_r}{T_{trans}}\right) \end{aligned} \tag{8}$$

Note that the normalized throughput T in Equation (8) is not an application-level throughput but link-level throughput. To convert the normalized throughput to normalize application-level throughput (goodput) G, we have the following expression:

$$\begin{aligned} G &= \frac{T_{data}}{T_{trans}} \cdot T = \frac{T_{data}}{T_{trans}} \cdot \frac{1 - P}{1 - P + (T_r P)/T_{trans}} I\left(W \geq \frac{T_r}{T_{trans}}\right) \\ &\quad + \frac{T_{data} W}{T_r} \cdot \frac{(1 - P)}{(1 - P + WP)} I\left(W < \frac{T_r}{T_{trans}}\right) \end{aligned} \tag{9}$$

4.3.2. Selective-reject

From [3], with selective-reject, we obtain the following expression:

$$T = (1 - P)I(W \geq 2\alpha + 1) + \frac{W(1 - P)}{2\alpha + 1} I(W < 2\alpha + 1) \tag{10}$$

Similar to the discussion of go-back-N, if we do not ignore the transmission time of acknowledgments, the aforementioned expression should be modified to

$$T = (1 - P)I\left(W \geq \frac{T_r}{T_{trans}}\right) + \frac{T_{trans} W(1 - P)}{T_r} I\left(W < \frac{T_r}{T_{trans}}\right) \tag{11}$$

Similar to the case in go-back-N, the normalized goodput G has the following expression:

$$G=\frac{T_{data}}{T_{trans}}\cdot T=\frac{T_{data}}{T_{trans}}\cdot(1-P)I\left(W\geq\frac{T_r}{T_{trans}}\right)+\frac{T_{data}W(1-P)}{T_r}I\left(W<\frac{T_r}{T_{trans}}\right)\tag{12}$$

Expressions (9) and (12) are two segment functions with the value of depending on whether $W<\frac{T_r}{T_{trans}}$ or not.

5. OPTIMAL STUDY

With CFB encryption/decryption and sliding-window flow and error control, both the data security and efficiency can be supported in data transportation and communication. Data encryption/decryption can be applied in different levels of communication from application level to link level [55]. In this section, we will study the optimal number of stages of CFB encryption under sliding-window protocols and the optimal throughput that can be reached under the assumption that the data encrypted is application-level data; this indicates that our deduction is to maximize the application-level throughput *G*. Actually, if data encryption happens in the lower level and the goal is to maximize throughput on lower level, the deduction process is same as the one in this section with minor changes of the values of the headers. For CFB to maximize the application-level throughput, it is crucial to find out the optimal payload *D* (in bits) of encrypted data in a frame, which leads to maximum throughput. It is natural to consider that the optimal CFB encryption method is to encrypt *D* bits of plain text at one encryption (one encryption can consist of multiple stages) because that will save the effort to segment or combine the encrypted texts to fit the optimal payload *D*. Then, given the volume *s* of the outputted cipher data in each stage of encryption, we know that $D=s\cdot M_{opt}$ where M_{opt} is the optimal number of stages in an encryption, defined as follows.

Let R, H, L_{ACK}, T_p, R_{BER}, and W denote the transmission rate in bps (bits per second), the frame/packet overhead in bits including header (Medium Access Control header, IP header, TCP/UDP header) and trailer, the length of the acknowledgment frame/packet in bits, the transmission time for the physical header, the channel bit error rate, and the number of frames in a window, respectively. Let M, s, and M_{opt} denote the number of stages of encryption/decryption in the CFB mode, the number of bits in the plaintext to be encrypted/decrypted, and the number of stage(s) for encryption/decryption, which lead to the optimal throughput, respectively.

We have

$$1-P=O_1(1-R_{BER})^{sM}\tag{13}$$

$$O_1=(1-R_{BER})^{H+L_{ACK}}\tag{14}$$

$$T_r=sM/R+sO_2/R\tag{15}$$

$$T_{trans}=sM/R+H/R+T_p\tag{16}$$

$$T_{data}=sM/R\tag{17}$$

$$\frac{T_r}{T_{trans}}=\frac{sM/R+sO_2/R}{sM/R+H/R+T_p}=\frac{M+O_2}{M+\left(H+T_pR\right)/s}\tag{18}$$

$$O_2=\frac{H+L_{ACK}+2RT_p+2RT_{prop}}{s}\tag{19}$$

Here, O_1 and O_2 are two intermediate variables that can make the denotations more concise.

Then, by substituting the aforementioned two expressions about *P* and T_r/T_{trans} into Equations (9) and (12), we can obtain the expression of the normalized throughput in selective-reject and that in go-back-N in the following subsections.

5.1. Selective-reject

By substituting Equations (13)–(19) to Equation (12), we can obtain

$$G=\frac{MO_1(1-R_{BER})^{sM}}{M+\left(H+T_pR\right)/s}I\left(W\geq\frac{M+O_2}{M+\left(H+T_pR\right)/s}\right)+\frac{MWO_1(1-R_{BER})^{sM}}{M+O_2}I\left(W<\frac{M+O_2}{M+\left(H+T_pR\right)/s}\right)\tag{20}$$

From Equation (20), if we fix *M*, we should obtain the following expression:

$$G=G_1I\left(M\geq\frac{O_2-W\left(H+T_pR\right)/s}{W-1}\right)+G_2I\left(0<M<\frac{O_2-W\left(H+T_pR\right)/s}{W-1}\right)\tag{21}$$

where

$$G_1=\frac{MO_1(1-R_{BER})^{sM}}{M+\left(H+T_pR\right)/s}$$

and

$$G_2=\frac{MWO_1(1-R_{BER})^{sM}}{M+O_2}$$

Also, when $M=\frac{O_2-W\left(H+T_pR\right)/s}{W-1}$, we have $G_1=G_2$.

From Equation (21), when $M > \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}$,

$$\begin{aligned}
\frac{dG}{dM} &= \frac{dG_1}{dM} \\
&= \frac{O_1\left[(1-R_{\mathrm{BER}})^{sM} + M(1-R_{\mathrm{BER}})^{sM}\ln(1-R_{\mathrm{BER}})^{s}\right]}{\left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)^2} \\
&\quad \times \left(M + \left(H+T_pR\right)/s\right) - \frac{O_1M(1-R_{\mathrm{BER}})^{sM}}{\left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)^2} \\
&= \frac{O_1}{\left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)^2} \\
&\quad \times [\left(\left(H+T_{\mathrm{p}}R\right)/s\right)(1-R_{\mathrm{BER}})^{sM} \\
&\quad + \left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)M(1-R_{\mathrm{BER}})^{sM}\ln(1-R_{\mathrm{BER}})^{s}] \\
&= \frac{O_1(1-R_{\mathrm{BER}})^{sM}}{\left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)^2} \\
&\quad \times \left[\left(H+T_{\mathrm{p}}R\right)/s + \left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)M\ln(1-R_{\mathrm{BER}})^{s}\right]
\end{aligned}$$

and also from Equation (21), when $0 < M < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}$,

$$\begin{aligned}
\frac{dG}{dM} &= \frac{dG_2}{dM} \\
&= \frac{WO_1\left[(1-R_{\mathrm{BER}})^{sM} + M(1-R_{\mathrm{BER}})^{sM}\ln(1-R_{\mathrm{BER}})^{s}\right]}{(M+O_2)^2} \\
&\quad \times (M+O_2) - \frac{WO_1M(1-R_{\mathrm{BER}})^{sM}}{(M+O_2)^2} \\
&= \frac{WO_1}{(M+O_2)^2} \\
&\quad \times \left[O_2(1-R_{\mathrm{BER}})^{sM} + (M+O_2)M(1-R_{\mathrm{BER}})^{sM}\ln(1-R_{\mathrm{BER}})^{s}\right] \\
&= \frac{WO_1(1-R_{\mathrm{BER}})^{sM}\left[O_2 + (M+O_2)M\ln(1-R_{\mathrm{BER}})^{s}\right]}{(M+O_2)^2}
\end{aligned}$$

Define $L_2(M) = (H+T_pR)/s + (M+(H+T_pR)/s)M\ln(1-R_{BER})^s$ and $L_1(M) = O_2 + (M+O_2)M\ln(1-R_{BER})^s$. Then, L_1 and L_2 are both a monotone decreasing function of M when $M > 0$. Note that we know that

$$\frac{dG}{dM} = \begin{cases} \dfrac{dG_1}{dM} = \dfrac{O_1(1-R_{BER})^{sM}L_2(M)}{\left(M+\left(H+T_pR\right)/s\right)^2} & \text{if} \quad M > \dfrac{O_2 - W\left(H+T_pR\right)/s}{W-1} \\ \dfrac{dG_2}{dM} = \dfrac{WO_1(1-R_{BER})^{sM}L_1(M)}{(M+O_2)^2} & \text{if} \quad 0<M < \dfrac{O_2 - W\left(H+T_pR\right)/s}{W-1} \end{cases} \tag{22}$$

From Equation (22), the signs of $\frac{dG_1}{dM}$ and $\frac{dG_2}{dM}$ are the same as those of $L_2(M)$ and $L_1(M)$, respectively. From the discussion of stop-and-wait in [8,7], we know that $M_1 = \frac{-O_2\ln(1-R_{BER})^s - \sqrt{\left[O_2\ln(1-R_{BER})^s\right]^2 - 4O_2\ln(1-R_{BER})^s}}{2\ln(1-R_{BER})^s}$ and $M_2 = \frac{-\left(\left(H+T_pR\right)/s\right)\ln(1-R_{BER})^s - \sqrt{\left[\left(\left(H+T_pR\right)/s\right)\ln(1-R_{BER})^s\right]^2 - 4\left(\left(H+T_pR\right)/s\right)\ln(1-R_{BER})^s}}{2\ln(1-R_{BER})^s}$ are the solutions to the formula $L_1 = 0$ and $L_2 = 0$, respectively. Because of the decreasing quality of $L_1(M)$ and $L_2(M)$, and the fact that $\frac{dG_1}{dM}$ and $\frac{dG_2}{dM}$ have the same signs as L_2 and L_1, respectively, we know that

$$\begin{cases} \dfrac{dG_1}{dM} < 0 \text{ when } \ M > M_2 \\ \dfrac{dG_1}{dM} > 0 \text{ when } \ M > M_2 \\ \dfrac{dG_2}{dM} < 0 \text{ when } \ M > M_1 \\ \dfrac{dG_2}{dM} > 0 \text{ when } \ M < M_1 \end{cases} \tag{23}$$

Note that $f(x) = \frac{-x\ln(1-R_{BER})^s - \sqrt{\left[x\ln(1-R_{BER})^s\right]^2 - 4x\ln(1-R_{BER})^s}}{2\ln(1-R_{BER})^s}$ is a monotone increasing function of $0 < x < +\infty$. Thus, $M_1 > M_2$ because $O_2 > (H+T_pR)/s$.

From Equations (21) and (23), and the fact that $M_2 > M_1$,

$$\begin{aligned}
M_{opt} &= M_2 I\left(\frac{O_2 - W\left(H+T_pR\right)/s}{W-1} \leq M_2\right) \\
&\quad + \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} I\left(M_2 < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} \leq M_1\right) \\
&\quad + M_1 I\left(\frac{O_2 - W\left(H+T_pR\right)/s}{W-1} > M_1\right)
\end{aligned}$$

If we consider the case of the limit of the frame size in a link, then the optimal stage applied (denote by $\bar{M}_{opt}$) can be expressed as

$$\bar{M}_{opt} = \min\left\{M_{opt}, P_{\max}/s\right\}$$

where $P_{\max}$ is capacity of application-level data in bits carried in a frame.

5.2. Go-back-N

By substituting Equations (13)–(19) to Equation (9), we can obtain

$$\begin{aligned}
G &= \frac{MO_1(1-R_{BER})^{sM}}{\left(M+\left(H+T_pR\right)/s\right)O_1(1-R_{BER})^{sM} + \left(1 - O_1(1-R_{BER})^{sM}\right)(M+O_2)} \\
&\quad \times I\left(W \geq \frac{M+O_2}{M+\left(H+T_pR\right)/s}\right) \\
&\quad + \frac{MWO_1(1-R_{BER})^{sM}}{(M+O_2)\left(O_1(1-R_{BER})^{sM} + W - WO_1(1-R_{BER})^{sM}\right)} \\
&\quad \times I\left(0 < W < \frac{M+O_2}{M+\left(H+T_pR\right)/s}\right)
\end{aligned} \tag{24}$$

If W is fixed, we can obtain the following expression:

$$\begin{aligned}
G &= F_1 I\left(M \geq \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}\right) \\
&\quad + F_2 I\left(0 < M < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}\right)
\end{aligned} \tag{25}$$

where

$$F_1 = \frac{MO_1(1-R_{BER})^{sM}}{\left(M+\left(H+T_pR\right)/s\right)O_1(1-R_{BER})^{sM}+\left(1-O_1(1-R_{BER})^{sM}\right)(M+O_2)} \tag{26}$$

and

$$F_2 = \frac{MWO_1(1-R_{BER})^{sM}}{(M+O_2)\left(O_1(1-R_{BER})^{sM}+W-WO_1(1-R_{BER})^{sM}\right)} \tag{27}$$

Note that $F_1 = F_2$ when $M = \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}$.

From Equations (25) and (26), when $0 < M < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}$, we obtain

$$\begin{aligned}\frac{dG}{dM} &= \frac{dF_2}{dM}\\ &= \frac{WO_1}{(M+O_2)^2\left[O_1(1-R_{\mathrm{BER}})^{sM}+W-WO_1(1-R_{\mathrm{BER}})^{sM}\right]^2}\\ &\quad\times\left[WM^2\ln(1-R_{\mathrm{BER}})^s+WO_2M\ln(1-R_{\mathrm{BER}})^s\right.\\ &\qquad\left.+O_1O_2(1-W)(1-R_{\mathrm{BER}})^{sM}+O_2W\right]\end{aligned} \tag{28}$$

Define

First, we have

$$\begin{aligned}K'_1(M) &= 2WM\ln(1-R_{BER})^s + WO_2\ln(1-R_{BER})^s\\ &\quad+O_1O_2(1-W)(1-R_{BER})^{sM}\ln(1-R_{BER})^s\\ &= \left[2WM+WO_2\left(1-O_1(1-R_{BER})^{sM}\right)\right.\\ &\quad\left.+O_1O_2(1-R_{BER})^{sM}\right]\ln(1-R_{BER})^s\end{aligned} \tag{30}$$

Then, from $1-O_1(1-R_{BER})^{sM} > 0$ and Equation (30), we can obtain

$$K'_1(M) < 0, 0 < M < \infty, \tag{31}$$

$$\left.\frac{dF_2}{dM}\right|_{M=0} = \frac{WO_1}{(O_2)(O_1+W-WO_1)} > 0, \tag{32}$$

and

$$\begin{aligned}\lim_{M\to\infty}\frac{dF_2}{dM} &= \lim_{M\to+\infty}\frac{WO_1}{(M+O_2)^2\left(O_1(1-R_{\mathrm{BER}})^{sM}+W-WO_1(1-R_{\mathrm{BER}})^{sM}\right)^2}\\ &\quad\times\left[WM^2\ln(1-R_{\mathrm{BER}})^s+WO_2M\ln(1-R_{\mathrm{BER}})^s\right.\\ &\quad\left.+O_1O_2(1-W)(1-R_{\mathrm{BER}})^{sM}+O_2W\right]\\ &= O_1\ln(1-R_{\mathrm{BER}})^s < 0\end{aligned} \tag{33}$$

$$\begin{aligned}K_1(M) = {}& WM^2\ln(1-R_{BER})^2\\ &+WO_2M\ln(1-R_{BER})^2\\ &+O_1O_2(1-W)(1-R_{BER})^{sM}+O_2W\end{aligned} \tag{29}$$

From Equations (28) and (29), the sign of $\frac{dF_2}{dM}$ is the same as $K_1(M)$.

We can further prove as follows that the expression $\frac{dF_2}{dM} = \frac{WO_1\left[WM^2\ln(1-R_{BER})^s+WO_2M\ln(1-R_{BER})^s+O_1O_2(1-W)(1-R_{BER})^{sM}+O_2W\right]}{(M+O_2)^2\left[O_1(1-R_{BER})^{sM}+W-WO_1(1-R_{BER})^{sM}\right]^2} = 0$ has a solution in $0 < M < \infty$.

Then, from Equations (32) and (33), the equation of $\frac{dF_2}{dM} = 0$ must have a solution in $0 < M < \infty$. We denote the solution as S_1. Because the sign of $\frac{dF_2}{dM}$ is the same as that of $K_1(M)$, we then have $K_1(S_1) = 0$. From Equation (31) and the fact that the sign of $\frac{dF_2}{dM}$ is the same as that of $K_1(M)$ and $K_1(S_1) = 0$, we can obtain

$$\frac{dF_2}{dM}\begin{cases} < 0, & \text{when } M > S_1\\ > 0, & \text{when } M < S_1\end{cases} \tag{34}$$

From Equation (34), S_1 is the unique solution of $\frac{dF_2}{dM} = 0$.

When $M > \frac{O_2 - W\left(H+T_pR\right)/s}{W-1}$, we can obtain

$$\begin{aligned}\frac{dG}{dM} = \frac{dF_1}{dM} &= O_1(1-R_{\mathrm{BER}})^{sM}\\ &\quad\times\frac{\left[O_2+\left(\left(H+T_{\mathrm{p}}R\right)/s-O_2\right)O_1(1-R_{\mathrm{BER}})^{sM}+(M+O_2)M\ln(1-R_{\mathrm{BER}})^s\right]}{\left[\left(M+\left(H+T_{\mathrm{p}}R\right)/s\right)O_1(1-R_{\mathrm{BER}})^{sM}+\left(1-O_1(1-R_{\mathrm{BER}})^{sM}\right)(M+O_2)\right]^2}\end{aligned} \tag{35}$$

From Equation (35), it can be deducted that

$$\frac{dF_1}{dM}\bigg|_{M=0} = \frac{O_1\left[(1-O_1)O_2 + \left(\left(H+T_pR\right)/s\right)O_1\right]}{\left[\left(\left(H+T_pR\right)/s\right)O_1 + (1-O_1)O_2\right]^2} > 0 \tag{36}$$

and there exists an M_0 such that for all $M > M_0$, it holds that

$$\frac{dF_1}{dM}|_{M>M_0} < 0 \tag{37}$$

Let $K_2(M) = [O_2 + ((H + T_pR)/s - O_2)O_1(1 - R_{BER})^{sM} + (M + O_2)M\ln(1 - R_{BER})^s]$.

Note that $\frac{dF_1}{dM} = \frac{O_1(1-R_{BER})^{sM}K_2(M)}{\left[\left(M+\left(H+T_pR\right)/s\right)O_1(1-R_{BER})^{sM}+\left(1-O_1(1-R_{BER})^{sM}\right)(M+O_2)\right]^2}$ and thus the sign of dF_1/dM is the same as that of $K_2(M)$ for $0 < M < +\infty$. We know that when $0 < M < +\infty$,

$$\begin{aligned} &K'_2(M)\\ &= \ln(1-R_{\mathrm{BER}})^s\\ &\quad\times\left[\left(\left(H = T_{\mathrm{p}}R\right)/s - O_2\right)O_1(1-R_{\mathrm{BER}})^{sM} + O_2 + 2M\right]\\ &= \ln(1-R_{\mathrm{BER}})^s\\ &\quad\times\left[\left(\left(H + T_{\mathrm{p}}R\right)/s\right)O_1(1-R_{\mathrm{BER}})^{sM} + \left(1 - O_1(1-R_{\mathrm{BER}})^{sM}\right)O_2 + 2M\right]\\ &< 0 \end{aligned} \tag{38}$$

From Equations (36)–(38) and the fact that dF_1/dM has the same sign as $K_2(M)$ does, we can know that the formula $\frac{dF_1}{dM} = 0$ must have a unique solution, which is denoted by S_2, and that

$$\frac{dF_1}{dM}\begin{cases} < 0, & \text{when } M > S_2\\ > 0, & \text{when } M < S_2 \end{cases} \tag{39}$$

We now define and introduce a notation $\widetilde{M_Q}(x_1, x_2, \ldots, x_n)$, where Q is a function of variable X. If we consider n values of $X = x_1, x_2, \ldots, x_n$, there must be a subset $S(x_1, x_2, , x_n)$ of these n values in which each element makes $Q(X)$ reach the greatest function value among $Q(x_1), Q(x_2), \ldots, Q(x_n)$. $\widetilde{M_Q}(x_1, x_2, \ldots, x_n)$ denotes the minimum value among $S(x_1, x_2, \ldots, x_n)$.

Then, from Equations (25), (34), and (39), for the function G in Equation (24), we have

$$\begin{aligned} M_{\mathrm{opt}} = {}& S_2 I\left(\frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} \le 0\right)\\ &+\left(\begin{aligned} &\widetilde{M_{\mathrm{G}}}(S_1,S_2)I\left(S_1 < \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} < S_2\right)\\ &+S_2 I\left(S_1 \ge \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} < S_2\right)\\ &+\frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} I\left(S_1 \ge \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} \ge S_2\right)\\ &+S_1 I\left(S_1 < \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} \ge S_2\right) \end{aligned}\right) I\left(\frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} > 0\right) \end{aligned} \tag{40}$$

Equation (40) can be more concisely expressed as

$$\begin{aligned} M_{\mathrm{opt}} = {}& \widetilde{M_G}(S_1,S_2)I\left(S_1 < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} < S_2\right)\\ &+S_1 I\left(S_1 < \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} \ge S_2\right)\\ &+S_2 I\left(S_1 \ge \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} < S_2\right)\\ &+\frac{O_2 - W\left(H+T_pR\right)/s}{W-1} I\left(S_1 \ge \frac{O_2 - W\left(H+T_pR\right)/s}{W-1} \ge S_2\right) \end{aligned} \tag{41}$$

If we consider the case of the limit of the frame size in a link, then the optimal stage applied (denote by $\bar{M_{opt}}$) can be expressed as

$$\begin{aligned} &\bar{M}_{\mathrm{opt}}\\ &= I\left(S_1 < \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} < S_2\right)\\ &\quad\times\left(\begin{aligned} &\min\{S_1, P_{\max}/s\}I\left(S_1 = \widetilde{M_{\mathrm{G}}}(S_1,S_2)\right)\\ &+\left(\begin{aligned} &S_2 I(S_2 \le P_{\max}/s)\\ &+\widetilde{M_{\mathrm{G}}}(S_1, P_{\max}/s)I(S_1 \le P_{\max}/s < S_2)\\ &+(P_{\max}/s)I(S_1 > P_{\max}/s) \end{aligned}\right) I\left(S_2 = \widetilde{M_{\mathrm{G}}}(S_1,,S_2)\right) \end{aligned}\right)\\ &+I\left(S_1 < \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} \ge S_2\right)\min\{S_1, P_{\max}/s\}\\ &+I\left(S_1 \ge \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} < S_2\right)\min\{S_2, P_{\max}/s\}\\ &+I\left(S_1 \ge \frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1} \ge S_2\right)\min\left\{\frac{O_2 - W\left(H+T_{\mathrm{p}}R\right)/s}{W-1}, P_{\max}/s\right\} \end{aligned}$$

where $P_{\max}$ is the capacity of application-level data in bits carried in a frame.

6. PERFORMANCE EVALUATION

In this section, we obtain some numerical results for the performance of CFB under different parameters. Let SR and GBN stand for selective-reject and go-back-N, respectively. In this section, we neither make limit of the maximum size of a frame nor do we make limit of the capacity of the application-level data carried by a frame.

6.1. Optimality of *M*

Figures 2 and 3 use the following parameters: $H = 24 \times 8$, $H + L_{ACK} + 2RT_p + 2RT_{prop} = 16\,800$, $H + T_pR = 42 \times 8$ and $s = 8$. In Figure 2, we fix $R_{BER} = 0.0001$. Figure 2 shows the normalized throughput G with three different W values over the number of stages M in terms of throughput for both selective-reject and go-back-N. As illustrated in Figure 2, an optimal G value exists in both protocols, given a fixed W. With each fixed W, the optimal G in selective-reject is much greater than the one in go-back-N. In both protocols, as W increases, the optimal M value decreases and the optimal G value increases.

In Figure 3, we fix $W = 4$. Figure 3 shows the throughput G over R_{BER} under the optimal M value and other M values in both selective-reject and go-back-N. As illustrated in Figure 3, an optimal M value does provide the best throughput for both protocols. We observe that the optimal throughput is an upper bound, or envelope, of the throughput with other chosen values. Furthermore, as R_{BER} increases, the optimal throughput decreases in both protocols. With the same parameters, the optimal G in selective-reject is much greater than that in go-back-N.

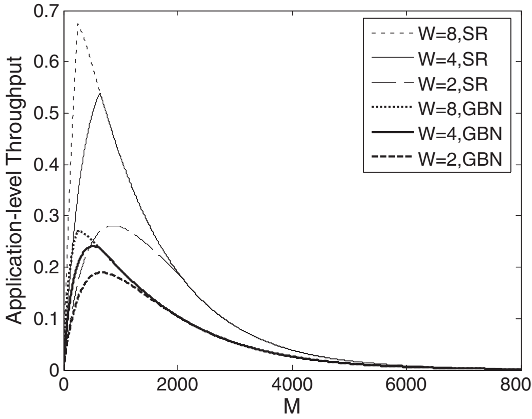


Figure 2. Goodput versus *M*. SR, selective-reject; GBN, go-back-N.

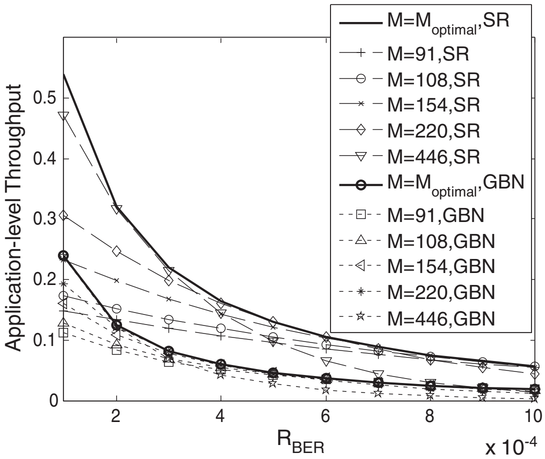


Figure 3. Goodput versus R_{BER}. BER, bit error rate; SR, selective-reject; GBN, go-back-N.

Figure 4 uses the same parameter values as Figure 2, except that it lets R_{BER} vary from 0.0001 to 0.001. Figure 4 shows the optimal M value with three different values of W over R_{BER} in both go-back-N as well as the selective-reject. As illustrated in Figure 4, in both protocols, given a fixed W, the optimal M value decreases as the R_{BER} increases. Furthermore, as W increases, the optimal M value decreases corresponding to any fixed value of R_{BER} that we consider.

6.2. Effect of *s*

Figures 5–7 have the following parameters: $H = 24 \times 8$, $H + L_{ACK} + 2RT_p + 2RT_{prop} = 16\,800$, $H + T_pR = 42 \times 8$ and $R_{\mathrm{BER}} = 0.0001$.

We fix $W = 4$ in Figures 5 and 6. They show the throughput G over s under the optimal M value and other M values in selective-reject and go-back-N, respectively. As illustrated in both figures, an optimal M value does

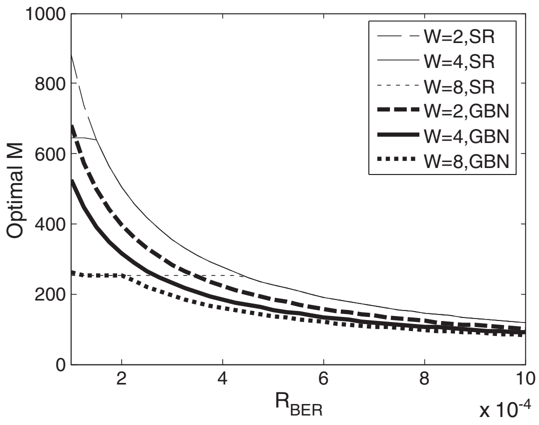


Figure 4. Optimal *M* versus R_{BER}. BER, bit error rate; SR, selective-reject; GBN, go-back-N.

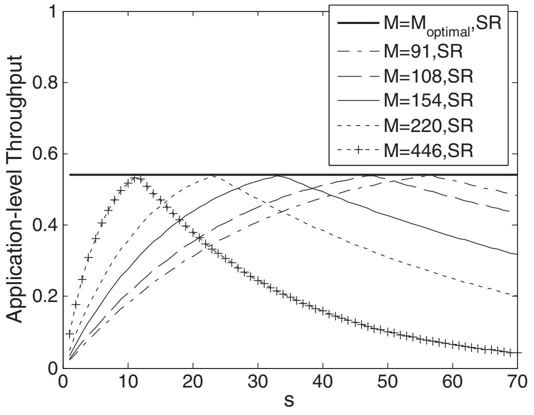


Figure 5. Goodput for selective-reject versus *s*. SR, selective-reject.

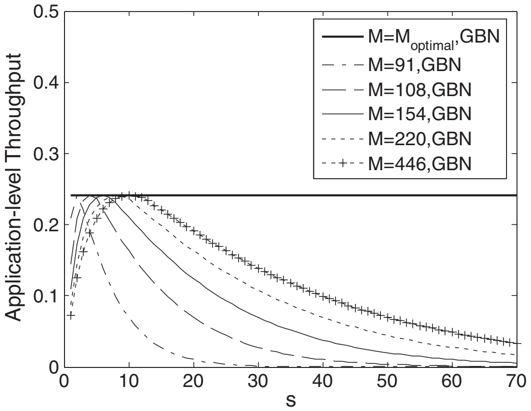


Figure 6. Goodput for go-back-N versus *s*. GBN, go-back-N.

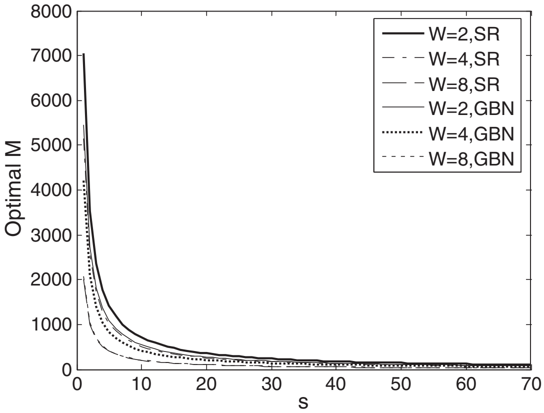


Figure 7. Optimal *M* versus *s*. SR, selective-reject; GBN, go-back-N.

provide the best throughput. We observe that the optimal throughput is an upper bound, or envelope, of the throughput with other chosen values. Furthermore, as *s* increases, the optimal throughput remains constant in both protocols. This is because the product of *s* and *M* can be considered as a variable *sM*, and then, from Equations (20) and (24), in the case of the independent variables excluding a fixed *sM*, we can easily know that Equations (20) and (24) are two functions of *sM*, which only have a maximum point.

Figure 7 shows the optimal *M* value versus *s*, the number of bits to encrypt each time, in both selective-reject and go-back-N. As illustrated in Figure 7, the optimal *M* value decreases as the *s* value increases. Also, as *W* increases, the optimal *M* value decreases corresponding to any fixed value of *s* we consider.

7. CONCLUSIONS

In this paper, we provided an error analysis of the stream-based CFB mode in an error channel under selective-reject and go-back-N protocols. We analytically modeled throughput. We solved the following optimality problem: given a bit error rate and the number of bits to encrypt each time, we wanted to obtain the optimal throughput with the optimal number of stages. We made the following observations: (1) In both protocols, given an R_{BER} and a *W*, an optimal value of *G* exists. Furthermore, as *W* increases, both optimal *M* values decrease, whereas both optimal values of *G* increase. (2) With the same parameters, the optimal throughput in selective-reject is greater than that in go-back-N. In other words, selective-reject performs better than go-back-N. (3) In both protocols, given a *W*, the optimal *M* value decreases as the R_{BER} increases. (4) In both protocols, given a *W* and an *s*, an optimal *M* value exists. The optimal *M* value decreases as the *s* value increases with a fixed *W*. (5) As *W* increases, the optimal *M* value decreases corresponding to any fixed value of *s* we consider.

The proposed work is beneficial for designing the CFB under sliding-window protocols as well as for obtaining designing parameters for the CFB in networks.

ACKNOWLEDGEMENT

This work is supported in part by The U.S. National Science Foundation (NSF), under grants CNS-0716211, CCF-0829827, CNS-0737325, and CNS-1059265.

REFERENCES

1. FIPS Publication 81. *DES Modes of Operation*, U.S. DoC/NIST, December 1980.
2. Ts'o T. RFC 2952: Telnet encryption: DES 64 bit cipher feedback, Request for Comments, Network Working Group, the Internet Society, 2000.
3. Stallings W. *High-speed Networks and Internets: Performance and Quality of Service* (2nd edn). Prentice Hall: New Jersey, 2002.
4. IEEE 802.11-1999. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification, Standard, IEEE, August 1999.
5. Rose G. A stream cipher based on linear feedback over GF(28). *Book Series Lecture Notes in Computer Science* 2006; **1438/1998**:135–146.
6. Hamdy N, El Megeed T, Hamad A, Kamal M. MANAGE1: New Stream Cipher for Data Encryption in CDMA Wireless Networks. The 2006 International Conference on Computer Engineering and Systems, November 2006. ISBN: 1-4244-0271-9.
7. Xiao Y, Chen H, Du X, Guizani M. Stream-based Cipher feedback mode in wireless error channels. *IEEE Transactions on Wireless Communications* 2009; **8**(2):622–626.

DOI: 10.1002/sec

8. Xiao Y, Guizani M. Optimal stream-based cipher feedback mode in error channel. Proceedings of the IEEE Global Telecommunications Conference (Globecom '05), November 2005, 1660–1664.
9. Liang X, Xiao Y, Vasilakos AV, Deng H, Meng K. CFB under sliding-window protocols in error channels, MILCOM 2010; 1502–1507.
10. Boyer S, Robert J, Otrok H, Rousseau C. An adaptive tit-for-tat strategy for IEEE 802.11 CSMA/CA Protocol. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
11. Kim K, Jeon J, Yoo K. Efficient and secure password authentication schemes for low-power devices. *International Journal of Sensor Networks* 2006; **2**(1/2):77–81.
12. Wong DS, Tian X. E-mail protocols with perfect forward secrecy. *International Journal of Security and Networks* 2012; **7**(1): 1–5.
13. Janies J, Huang C, Johnson NL, Richardson T. SUMP: a secure unicast messaging protocol for wireless ad hoc sensor networks. *International Journal of Sensor Networks* 2007; **2**(5/6):358–367.
14. Vespa L, Chakrovorty R, Weng N. Lightweight testbed for evaluating worm containment systems. *International Journal of Security and Networks* 2012; **7**(1): 6–16.
15. Cam H. Multiple-input turbo code for secure data aggregation and source-channel coding in wireless sensor networks. *International Journal of Sensor Networks* 2007; **2**(5/6):375–385.
16. Kandah F, Singh Y, Zhang W, Wang T. A misleading active routing attack in mobile ad-hoc networks. *International Journal of Security and Networks* 2012; **7**(1): 17–29.
17. Butun I, Wang Y, Lee Y, Sankar R. Intrusion prevention with two level user authentication in heterogeneous wireless sensor networks. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
18. Yao Z, Kim D, Doh Y. PLUS: parameterised localised trust management-based security framework for sensor networks. *International Journal of Sensor Networks* 2008; **3**(4):224–236.
19. Xiao Y. Editorial: security and privacy issues. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
20. Alsubhi K, Alhazmi Y, Bouabdallah N, Boutaba R. Security configuration management in intrusion detection and prevention systems. *International Journal of Security and Networks* 2012; **7**(1): 30–39.
21. Chang CG, Snyder WE, Wang C. Secure target localisation in sensor networks using relaxation labelling. *International Journal of Sensor Networks* 2008; **4** (3):172–184.
22. Kolesnikov V, Lee W. MAC aggregation resilient to DoS attacks. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
23. Xiao Z, Xiao Y. PeerReview re-evaluation for accountability in distributed systems or networks. *International Journal of Security and Networks* 2012; **7**(1): 40–58.
24. Baig ZA. Rapid anomaly detection for smart grid infrastructures through hierarchical pattern matching. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
25. Szczechowiak P, Scott M, Collier M. Securing wireless sensor networks: an identity-based cryptography approach. *International Journal of Sensor Networks* 2010; **8**(3/4):182–192.
26. Neji NB, Bouhoula A. Managing hybrid packet filter's specifications. *International Journal of Security and Networks (IJSN)* 2012; **7**(2).
27. Al-Salloum ZS. Defensive computer worms—an overview. *International Journal of Security and Networks* 2012; **7**(1): 59–70.
28. Krontiris I, Dimitriou T. Scatter—secure code authentication for efficient reprogramming in wireless sensor networks. *International Journal of Sensor Networks* 2011; **10**(1/2):14–24.
29. Chen Z, Chen C, Li Y. Deriving a closed-form expression for worm-scanning strategies. *International Journal of Security and Networks* 2009; **4**(3):135–144.
30. Lee S, Sivalingam KM. An efficient one-time password authentication scheme using a smart card. *International Journal of Security and Networks* 2009; **4** (3):145–152.
31. Watkins L, Beyah R, Corbett C. Using link RTT to passively detect unapproved wireless nodes. *International Journal of Security and Networks* 2009; **4** (3):153–163.
32. Drakakis KE, Panagopoulos AD, Cottis PG. Overview of satellite communication networks security: introduction of EAP. *International Journal of Security and Networks* 2009; **4**(3):164–170.
33. Chakrabarti S, Chandrasekhar S, Singhal M. An escrow-less identity-based group-key agreement protocol for dynamic peer groups. *International Journal of Security and Networks* 2009; **4**(3):171–188.
34. Ehlert S, Rebahi Y, Magedanz T. Intrusion detection system for denial-of-service flooding attacks in SIP communication networks. *International Journal of Security and Networks* 2009; **4**(3):189–200.
35. Berthier R, Cukier M. An evaluation of connection characteristics for separating network attacks. *International Journal of Security and Networks* 2009; **4**(1/2):110–124.
36. Wu B, Wu J, Dong Y. An efficient group key management scheme for mobile ad hoc networks. *International Journal of Security and Networks* 2009; **4**(1/2):125–134.
37. Mayrhofer R, Nyberg K, Kindberg T. Foreword. *International Journal of Security and Networks* 2009; **4**(1/2):1–3.

38. Scannell A, Varshavsky A, LaMarca A, De Lara E. Proximity-based authentication of mobile devices. *International Journal of Security and Networks* 2009; **4**(1/2):4–16.
39. Soriente C, Tsudik G, Uzun E. Secure pairing of interface constrained devices. *International Journal of Security and Networks* 2009; **4**(1/2):17–26.
40. Buhan I, Boom B, Doumen J, Hartel PH, Veldhuis RNJ. Secure pairing with biometrics. *International Journal of Security and Networks* 2009; **4**(1/2):27–42.
41. McCune JM, Perrig A, Reiter MK. Seeing-is-believing: using camera phones for human-verifiable authentication. *International Journal of Security and Networks* 2009; **4**(1/2):43–56.
42. Goodrich MT, Sirivianos M, Solis J, Soriente C, Tsudik G, Uzun E. Using audio in secure device pairing. *International Journal of Security and Networks* 2009; **4**(1/2):57–68.
43. Laur S, Pasini S. User-aided data authentication. *International Journal of Security and Networks* 2009; **4**(1/2):69–86.
44. Suomalainen J, Valkonen J, Asokan N. Standards for security associations in personal networks: a comparative analysis. *International Journal of Security and Networks* 2009; **4**(1/2):87–100.
45. Kuo C, Perrig A, Walker J. Designing user studies for security applications: a case study with wireless network configuration. *International Journal of Security and Networks* 2009; **409**(1/2):101–109.
46. Bai L, Zou X. A proactive secret sharing scheme in matrix projection method. *International Journal of Security and Networks* 2009; **4**(4):201–209.
47. Bettahar H, Alkubeily M, Bouabdallah A. TKS: a transition key management scheme for secure application level multicast. *International Journal of Security and Networks* 2009; **4**(4):210–222.
48. Huang H, Kirchner H, Liu S, Wu W. Handling inheritance violation for secure interoperation of heterogeneous systems. *International Journal of Security and Networks* 2009; **4**(4):223–233.
49. Rekhis S, Boudriga NA. Visibility: a novel concept for characterising provable network digital evidences. *International Journal of Security and Networks* 2009; **4**(4):234–245.
50. Djenouri D, Bouamama M, Mahmoudi O. Black-hole-resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks. *International Journal of Security and Networks* 2009; **4**(4):246–262.
51. Hu F, Dong D, Xiao Y. Attacks and countermeasures in multi-hop Cognitive Radio Networks. *International Journal of Security and Networks* 2009; **4**(4):263–271.
52. FIPS Publication 46-3. Data Encryption Standard (DES), U.S. DoC/NIST, October 25, 1999.
53. FIPS Publication 800-38A. *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, U.S. DoC/NIST, 2001.
54. Qi J, Aissa S, Zhao X. Optimal frame length for keeping normalized goodput with lowest requirement on BER. Proceedings of the 4th International Conference on Innovations in Information Technology, 2007; 715–719.
55. Kurose J, Ross K. *Computer Networking: a Top–Down Approach* (4th edn). Addison Wesley, 2007 Boston, MA.

DOI: 10.1002/sec