Optimal Information-Dispersal for Fault-Tolerant Communication Over a Burst-Error Channel

Shiuh-Pyng Shieh, Yea-Ching Tsai, and Yu-Lun Huang

***Abstract*—The (m, n) wireless information dispersal scheme (WIDS) is useful for fault-tolerant parallel wireless communications, where it can be used to tolerate up to $n - m$ path (sub-channel) failures. This paper constructs a performance model of (m, n) WIDS used in wireless communications, and proposes an algorithm to find the optimal set of (m, n) with the highest reliability. This algorithm reduces the complexity of finding the candidate set of (m, n) from $O(N^2)$ to $O(N)$; N is the maximum number of available sub-channels.**

***Index Terms*—Fault tolerance, security, threshold scheme, wireless communications.**

ACRONYMS[1]

IDS	information-dispersal scheme
WIDS	Wireless IDS

NOTATION

n	the degree of information dispersal
η_2	greatest-integer-lower-bound of $n/2$
η_u	greatest-integer-lower-bound of n/u
η^*	greatest-integer-lower-bound of $(N \cdot a)/2$
m	[see (m, n)-WIDS]
n/m	ratio of information expansion; $n/m \geq 1$
(m, n)-WIDS	a WIDS which breaks a data block into n pieces and transmits them in parallel over n wireless channels such that 'any m pieces received' suffice for reconstructing the data block; $1 \leq m \leq n$
N	maximum number of available communication sub-channels
u	upper bound of the information expansion ratio, n
P_s	$\Pr\{$a sub-channel can deliver the correct information piece$\}; 0 < P_s < 1$
$R(m, n)$	$\text{binfc}(m; \sqrt[n]{P_s}, n); \Pr\{$the transmitted data block can be correctly constructed using the $(m, n) - \text{WIDS}\}$
$P_s^*[(i, j), (k, l)]$	critical probability: the P_s such that $R(i, j) = R(k, l)$
P_s^*	$P_s^*[(i, j), (k, l)]$
S_i	piece #i of (m, n)-WIDS, $1 \leq i \leq n$
$F_{u,N}$	(m, n)-WIDS; for all $m, n, u \in N, 1 \leq n/m \leq u, n \leq N$: feasible WIDS set
TR	tolerable error

DEFINITIONS

dispersal degree:	the number of sub-channels used to transmit the data.
information expansion ratio	the ratio expanded when transmitting a message M. For example, if one makes n copies of a message M and transmits these copies over n channels, then the expansion ratio of the message M is n.

I. INTRODUCTION

IN THE PAST decade, wireless communications technology emerged rapidly. Wireless networks allow people to communicate with each other anytime and anywhere. With the rapid development of communication networks, the need for reliable-transmission increases. The probability of successful transmission in a wire-line environment is very high nowadays. But in wireless environments, the probability of transmission failure can increase because of bad weather, terrain, weak transmission power, etc. When a data-set is transmitted incorrectly, then it needs to be retransmitted. Retransmission can be very expensive and unacceptable for real-time applications. To support more reliable transmission quality in such environments, some schemes are needed to increase the probability of successful transmission.

We have already used IDS to increase the reliability of a network service provided by a cluster of servers [9]. This paper proposes and analyzes the WIDS to support fault-tolerant, parallel wireless communications. In an (m, n) WIDS, the sender transforms a message M into n pieces, $S_i (1 \leq i \leq n)$, and transmits them over parallel wireless channels such that any m pieces collected at the receiver suffice for reconstructing the message M. In parallel wireless communications, fixed assignment protocols partition a wireless communication link into channels in time, frequency, or code domain. These pieces of data-packets can be transmitted in parallel over n channels, and can still be reconstructed by the receiver even if up to $n - m$ packets fail.

This paper proposes the WIDS to support fault-tolerant, parallel wireless communications, and gives the algorithm to find

Manuscript received December 30, 1998; revised October 8, 2001 and March 23, 2003. This work was supported in part by the Ministry of Education, and National Science Council, Taiwan, and the Lee & MTI Center, National Chiao Tung University. Responsible Editor: W. H. Sanders.

The authors are with the Department of Computer Science and Information Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan-ROC (e-mail: SSP@csie.nctu.edu.tw; YCTsai@csie.nctu.edu.tw; YLHuang@csie.nctu.edu.tw).

Digital Object Identifier 10.1109/TR.2003.820498

[1]The singular and plural of an acronym are always spelled the same.

the optimal set of (m, n) WIDS which gives the highest communication reliability. This algorithm greatly reduces the complexity of finding the candidate set of (m, n) from $O(N^2)$ to $O(N)$.

Section II introduces the WIDS used in the fault-tolerant parallel wireless communications. Related research on wireless communications is also reviewed. Section III discusses and analyzes the success probability of parallel transmission using WIDS. Then it presents some theorems for the WIDS model used in parallel wireless communications. These theorems help develop the schemes that find the (m, n) with the optimal performance. Section IV proposes some methods of getting the optimal (m, n) WIDS set to achieve better reliability. Section V discusses some properties of (m, n) WIDS for fault tolerance.

II. Information Dispersal Scheme

In a wireless communication environment, there are many factors that can cause a data-transmission error. These include bad weather and outside noise. Although error-correcting codes [3], [8] can be used to control error in the transmission, the probability of a channel failure still can not be negligible, especially in bad transmission conditions. An intuitive solution [10] to this problem is to send a message along a path, request a confirmation, and retransmit it along a different path in case of failure. However, re-transmission is time-consuming and expensive, thus it is undesirable for communications. WIDS can be used to increase the probability of successful transmission.

IDS [6] was first proposed as a method of breaking a file F into n packets of length L/m , where $m < n$, such that m of them suffice to reconstruct the original file F. Let $F = (b_1, b_2, \ldots, b_L)$ be a string of characters; n_0, m_0 be 3 integers with $m_0 \le n_0$. For simplicity, assume that L is a multiple of m_0. Find a $n_0 \times m_0$ matrix A such that all its $m_0 \times m_0$ submatrices are inevitable. Break F into strings of length m_0:

$$\begin{aligned} F &= (b_1, b_2, \ldots, b_{m_0})(b_{m_0+1}, \ldots, b_{2m_0}) \ldots \\ &\quad \times (b_{L-m_0+1}, \ldots, b_L) \\ &= S_1, S_2, \ldots, S_{L/m_0}. \end{aligned}$$

The splitting operation transforms F into n_0 pieces by

$$\begin{bmatrix} F_1 \\ F_2 \\ \vdots \\ F_{n_0} \end{bmatrix} = A \begin{bmatrix} b_1 & b_{m_0+1} & \cdots & b_{L-m_0+1} \\ b_2 & b_{m_0+2} & \cdots & b_{L-m_0+2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m_0} & b_{2m_0} & \cdots & b_L \end{bmatrix}$$

Obviously, $|F_i = L/m_0$ is independent of n_0, where L is the length of F. The total number of characters produced by WIDS is $(n_0/m_0)^* \cdot L$. Then the information expansion ratio of WIDS is n_0/m_0. The computation complexity is $O(m_0^2)$.

Since then, WIDS has been applied to fault-tolerant parallel communications in several types of networks, such as hyper-cube and Omega networks [1], [2], [4]. These methods can prevent paths or channels from failing. If n pieces are transmitted over n vertex-disjoint paths or channels, it can tolerate up to $n - m$ packet failures. However, there is little research to date discussing the relations among the 3 important factors which influence communication reliability:

- information dispersal degree,
- information expansion ratio,
- $\Pr\{\text{successful transmission of each packet}\}$.

Also there is no efficient way to determine the optimal set of (m, n) WIDS with the highest communication reliability when applying WIDS in wireless communications.

Reference [7] defines a burst-error channel using a Markov model; and describes the throughput analysis method of a hybrid automatic repeat request (ARQ) under the burst-error channel using the 3-state Markov model. The applicable range of the burst-error channel has been clarified for the hybrid ARQ using burst-error correction codes—convolutional coding.

After the sequence of analysis step in this paper, the P_c of a burst-error correction code is:

$$P_c = \sum_{i=1}^{M_b} B(i) \sum_{i=M_g}^{\infty} G(i);$$

$B(i) \equiv$ occurrence probability of each burst length i,
$G(i) \equiv$ $\Pr\{1$ error bit occurrence after silent section length $i\}$,
$M_b \equiv$ burst length,
$M_g \equiv$ guard length, as described in (11).
$B(i)$ and $G(i)$ are found from the bit error rate of the channel, which depends on the noise condition of the environment.

Let:
$N_B \equiv$ the average silence length,
$N_G \equiv$ the average burst length.

If the transmitted data is large, the average burst number of a packet is $N/(N_B + N_G)$ when the packet consisting of N bits. So, the error correction probability of the packet of N bits is: $P_c^{N/(N_B+N_G)}$.

$N \equiv$ size of the data, in bits.

When applying (m, n) WIDS in a system with a fixed code rate R, a message, M, will be transformed into n pieces. Each piece of the packet is framed with a fixed size $(|M|/m)$. Thus, the packet size of data is $(|M|/m)^* \cdot (1/R)$. The packet size is influenced by m. If the packet size of $(1, 1)$ WIDS is L, then the packet size of (m, n) WIDS is L/m. In wireless communications, the error probability can be influenced by the packet size.

Because these n pieces of message M are transmitted simultaneously over n adjacent subchannels, assume that these data packets are transmitted in the same environment: the bit error-rate of each subchannel is the same. The same bit error-rate derives the same $B(i)$ and $G(i)$ and thus results in the same P_c for every parallel subchannel.

Let the original packet size be L, and let the success probability of transmitting a message M be P_s. When using the $(1, n)$ WIDS to transmit the message M, the success probability becomes P_s. When using the $(2, n)$ WIDS to transmit this message over the burst-error subchannels, the packet size becomes $L/2$, independent of n. Thus, the success probability of each data packet becomes $\sqrt{P_s}$. Similarly, when using the (m, n) WIDS to transmit this message over the burst-error wireless subchannels, the probability of the successful transmission of each packet becomes $\sqrt[m]{P_s}$.

This result can be applied to the WIDS used in parallel wireless communication. Section III discusses some useful theorems of (m, n) WIDS used in a wireless environment. These theorems can help to find the optimal set of (m, n) WIDS.

III. Fundamental Theorems

This section describes the fundamental theorems of the proposed (m, n)-WIDS in the following *Assumption*.

- All communication sub-channels have the same success probability of transmitting a data packet.

  In a (m, n) WIDS, the probability of successful transmission of each packet is $\sqrt[m]{P_s}$. Thus, the sum of the probabilities in the following cases calculate the communication reliability $R(m, n)$:
- a receiver receives any m pieces from the n sub-channels and reconstructs M:

$$C_m^n \cdot (\sqrt[m]{P_s})^m \cdot (1 - \sqrt[m]{P_s})^{n-m};$$
$$C_m^n \rightarrow \text{ any } m \text{ from } n$$
$$(\sqrt[m]{P_s})^m \rightarrow m \text{ successes}$$
$$(1 - \sqrt[m]{P_s})^{n-m} \rightarrow n - m \text{ failures}$$

- a receiver receives any $m+1$ pieces from the n sub-channels and reconstructs M:

$$C_{m+1}^n \cdot (\sqrt[m]{P_s})^{m+1} \cdot (1 - \sqrt[m]{P_s})^{n-(m+1)}$$

- a receiver receives n pieces from the n sub-channels and reconstructs M:

$$C_n^n \cdot (\sqrt[m]{P_s})^n \cdot (1 - \sqrt[m]{P_s})^{n-n};$$
$$C_{m+1}^n \rightarrow \text{any } m+1 \text{ from } n$$
$$(\sqrt[m]{P_s})^n \rightarrow n \text{ successes}$$
$$(1 - \sqrt[m]{P_s})^{n-(m+1)} \rightarrow n - (m+1) \text{ failures}$$
$$R(m,n) = C_m^n \cdot (\sqrt[m]{P_s})^m \cdot \left(1 - \sqrt[m]{P_s}\right)^{n-m} + C_{m+1}^n \cdot (\sqrt[m]{P_s})^{m+1} \cdot (1 - \sqrt[m]{P_s})^{n-m-1} + \cdots + C_n^n \cdot (\sqrt[m]{P_s})^n \cdot (1 - \sqrt[m]{P_s})^{n-n};$$
$$= \sum_{i=m}^{n} C_i^n \cdot (\sqrt[m]{P_s})^i \cdot (1 - \sqrt[m]{P_s})^{n-i}.$$

Theorem 3.1: $R(m, n)$ is strictly increasing for $0 < P_s < 1$. (See Appendix A for the proof)

Theorem 3.1 suggests that $R(m, n)$, for fixed m & n, is proportional to P_s: the $R(m, n)$ increases as the P_s of individual sub-channel increases.

Theorem 3.2: If $0 < P_s < 1$, then $R(m, n) < R(m, n + k)$ for $k > 0$.

(See Appendix B for the proof) Theorem 3.2 suggests that the communication reliability of (m, n) WIDS is lower than that of $(m, n + k)$ WIDS: if more pieces of the message are sent, but the same number is needed to be received in order to recover the message, then the communication reliability is improved.

Fig. 1 shows the distribution of reliability curves. When $P_s \rightarrow 1$, then $R(m, n) \rightarrow 1$. Similarly, when $P_s \rightarrow 0$, then $R(m, n) \rightarrow 0$. The following theorems (3.3)–(3.8) the optimal (m, n) among $R(1, n), R(2, n), \ldots, R(n, n)$.

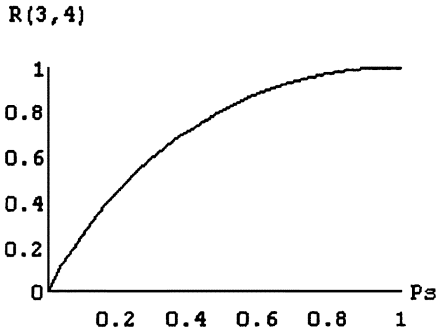

Fig. 1. The communication reliability curve for a (3, 4) WIDS.

Theorem 3.3: If $0 < P_s < 1$, then $R(m, n) > R(m + 1, n)$ when $P_s \rightarrow 1$. (See Appendix C for the proof.)

Theorem 3.3 implies that any WIDS which needs fewer message pieces to reconstruct the original message, has higher reliability, while the message dispersal degree n is fixed and $P_s \rightarrow 1$. Hence, corollary 1 is true.

Corollary 1: $R(1, n)$ is the optimal of $R(i, n)$ when $P_s \rightarrow 1$, for $1 \leq i \leq n$.

Theorem 3.4: $R(\eta_2)$ is the optimal of $R(i, n)$ when $P_s \rightarrow 0+$ for $1 \leq i \leq n$. (See Appendix D for the proof.)

By Theorem 3.4, η_2 is a critical number, while the success probability of communication channels is very low. Theorems 3.5–3.7 show that the curves of $R(\eta_2, n), \ldots, R(n, n)$ do not have intersections.

Theorem 3.5: Let $f(p) = ((1 - \sqrt[b-1]{p})^{a+1})/((1 - \sqrt[b]{p})^a)$ where $a, b \in N - \{1\}$.

$N - \{1\} \rightarrow$ the set of integers from 0 to N, but not including the integer: 1. Then there exists one $P_j \in (0, 1)$, such that $f(p)$ increases in $(0, P_j)$ and decreases in $(P_j, 1)$.

(See Appendix E for the proof.)

Theorem 3.6: If $m \geq \eta_2$ then $R(m, n) > R(m + 1, n)$.

(See Appendix F for the proof.)

Theorem 3.7: If $2 \leq m \leq \eta_2$ then there exists exactly one critical probability, P_s^*, such that

$$R(m,n) > R(m-1,n) \quad \text{when } 0 < P_s < P_s^*,$$
$$R(m,n) = R(m-1,n) \quad \text{when } P_s = P_s^*,$$
$$R(m,n) < R(m-1,n) \quad \text{when } P_s^* < P_s < 1.$$

(See Appendix G for the proof.)

As in Theorem 3.7, every pair of WIDS has, at most, 1 critical probability. Define $P_s^*[(i, j), (k, l)]$ as the critical probability of 2 different WIDS, (i, j) WIDS and (k, l) WIDS, that satisfies the following 3 conditions:

1) $R(i, j) > R(k, l)$ if $0 < P_s < P_s^*[(i, j), (k, l)]$,
2) $R(i, j) = R(k, l)$ if $P_s = P_s^*[(i, j), (k, l)]$,
3) $R(i, j) < R(k, l)$ if $P_s^*[(i, j), (k, l)] < P_s < 1$.

Thus these Theorems (3.5)–(3.7) indicate that for any 2 WIDS in the WIDS class, a WIDS can have better reliability in a range of P_s, but worse reliability in the other range. That is, a particular WIDS does not always give better reliability than another. This suggests that a designer must determine the range of P_s first, and then choose the right WIDS in the class.

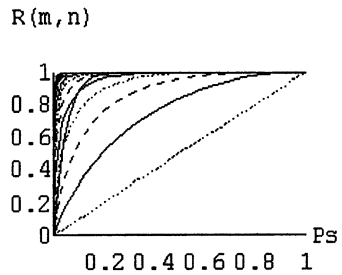

Fig. 2. The curves of communication reliability for $(m, 20)$ WIDS, where $1 \leq m \leq n$.

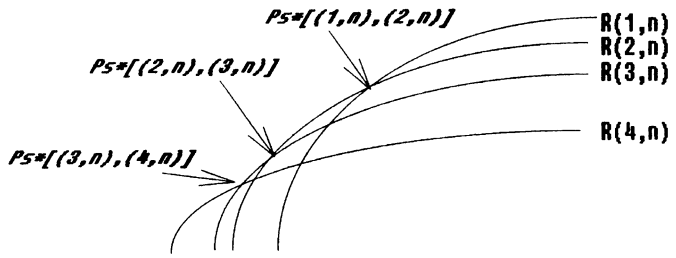

Fig. 3. The relationships between the $R(1,n), R(2,n), R(3,n)$, and $R(4,n)$.

Theorem 3.8 proves the intersections of $P_s^*[(m-i,n),(m-i-1,n)]$ have decreasing order when i increases for fixed n. Based on this and previous Theorems 3.5–3.7, it is possible to find the optimal WIDS with low complexity.

Theorem 3.8: For fixed $n \geq 6$, if $2 \leq m \leq \eta_2$, then

$$P_s^*[(m-1,n),(m,n)] > P_s^*[(m,n),(m+1,n)].$$

(See Appendix H for the proof.)

Theorem 3.1 proves that $R(m,n)$ is an increasing function from 0 to 1. Fig. 2 is the graph of all (m,n) WIDS curves for $n = 20$.

In Fig. 2, some $R(m,20)$ functions rapidly increase to 1 when P_s approaches 0.1. The transmission reliability is greatly improved when P_s is very small. The performance of WIDS approaches 1 when P_s is greater than some value, such as 0.1 in this example. The simulation results show that the greater n is, the faster $R(m,n)$ approaches 1. When choosing the optimal (m,n) combination, this phenomenon suggests that there will be no difference in choosing those $R(m,n)$ which approach 1; this is discussed in Section V.

IV. Optimal Information Dispersal Scheme

Section IV-A provides a method for determining the optimal WIDS with highest communication reliability when the fixed n sub-channels are all used in the parallel communication. The optimal m value depends on what region, $P_s^*[(i,n),(i+1,n)], P_s$ belongs to. Algorithm 4.1 reduces the complexity of finding the optimal (m,n) WIDS which have optimal communication reliability from $O(n)$ to $O(1)$.

Then, Section IV-B considers the case of the WIDS used to support fault-tolerant communication when the maximum available sub-channels, N, is given. The optimal WIDS uses a total of N sub-channels when the problem of 'information expansion ratio' is ignored. Section IV-C considers the information expansion ratio. A method is proposed to determine the candidate WIDS set of the optimal (m,n) WIDS when an upper-bound of information expansion ratio (u) and the number of available sub-channels (N) are given. This method can reduce the number of elements in candidate WIDS set from $O(N^2)$ to $O(N)$.

A. Determining Optimal m With Fixed n for (m,n) WIDS

This section proposes a method to determine the optimal WIDS with the highest communication reliability over n sub-channels. Theorem 3.6 shows that when $m \geq \eta_2$, the (m,n) WIDS has higher communication reliability than $(m+1,n)$ WIDS. Theorem 3.7 shows that if $P_s > P_s^*[(i,n),(i+1,n)]$, then $R(i,n)$ is better than $R(i+1,n)$; otherwise, $R(i+1,n)$ is better than $R(i,n)$. Thus, the optimal WIDS for the two ranges:

$$P_s > P_s^*[(i,n),(i+1,n)], \quad \text{and } P_s < P_s^*[(i,n),(i+1,n)]$$

are different. Theorem 3.8 shows that the intersections $P_s^*[(i,n),(i+1,n)]$ of (m,n) WIDS are in decreasing sequence:

$$P_s^*[(1,n),(2,n)] > P_s^*[(2,n),(3,n)] > \cdots > P_s^*[\eta_2 - n),(\eta_2,n)].$$

Theorems 3.7 and 3.8, provide the relationship between $R(1,n), R(2,n), \ldots, R(\eta_2,n)$ as shown in Fig. 3.

In the region $P_s^*[(1,n),(2,n)] < P_s < 1$, by Theorem 3.7, $R(1,n) > R(2,n)$. By Theorem 3.8,

$$P_s^*[(2,n),(3,n)] < P_s^*[(1,n),(2,n)].$$

Thus in this region, $R(2,n) < R(1,n)$. Similarly, the $P_s^*[(3,n),(4,n)]$ (if it exists) is smaller than $P_s^*[(1,n),(2,n)]$; thus $R(3,n) < R(1,n)$, and so on. Therefore, when $P_s \to 1-$, it is clear that $R(1,n) > R(2,n) > \cdots > R(n,n)$ in this region. If the information expansion ratio problem is not considered, then $R(1,n)$ is optimal in this region. If $(1,n)$ WIDS do not satisfy the information expansion ratio, then choose $R(2,n), R(3,n), \ldots, R(n,n)$ respectively, until the selected (m,n) WIDS satisfies the information expansion ratio.

Corollary 2: If $P_s^*[(1,n),(2,n)] < P_s < 1$, then the optimal value of m is 1. If $(1,n)$ WIDS do not satisfy the information expansion ratio, then choose $R(2,n), R(3,n), \ldots, R(n,n)$ respectively, until the selected (m,n) WIDS satisfies the information expansion ratio.

If $P_s^*[(2,n),(3,n)] < P_s < P_s^*[(1,n),(2,n)]$, then $R(2,n) > R(3,n)$ and $R(2,n) > R(1,n)$ from Theorem 3.7. By Theorem 3.8, $P_s^*[(3,n),(4,n)] < P_s^*[(2,n),(3,n)]$; thus $R(4,n) < R(3,n) < R(2,n)$; and so forth. Thus, the optimal communication reliability is $R(2,n)$ in this region. If the information expansion ratio is not tolerable, then choose $R(3,n), R(2,n), \ldots, R(n,n)$ instead of previous choice, until the information expansion ratio is satisfied.

Corollary 3: If $P_s^*[(2,n),(3,n)] < P_s < P_s^*[(1,n),(2,n)]$, then the optimal value of m is 2. If $(2,n)$ WIDS does not satisfy the information expansion ratio, then choose $R(3,n), R(4,n), \ldots, R(n,n)$ respectively, until the selected (m,n) WIDS satisfies the information expansion ratio.

Similarly, when $P_s^*[(I+1,n),(i+2,n)] < P_s < P_s^*[(i,n),(i+1,n)]$, then the optimal WIDS is $R(i+1,n)$. If

TABLE I
THE INTERSECTIONS: $P_s^*[i,j] \equiv P_s^*[(i,j),(i+1,j)]$ FOR $j = 4 - 84$

j	$P_s^*[1,j]$	$P_s^*[2,j]$	$P_s^*[3,j]$	$P_s^*[4,j]$	$P_s^*[5,j]$
4	0.271837				
5	0.579696				
6	0.768788	0.022815			
7	0.874048	0.132044			
8	0.931467	0.294322	0.001058		
9	>0.95	0.457744	0.016607		
10	>0.96	0.597068	0.065319	3.2471*-5	
11	>0.93	0.706502	0.147927	0.0013733	
12	>0.90	0.788786	0.251678	0.0096283	1.1519*-5

j	$P_s^*[2,j]$	$P_s^*[3,j]$	$P_s^*[4,j]$	$P_s^*[5,j]$	$P_s^*[6,j]$	$P_s^*[7,j$
13	>0.85	0.361982	0.0324719	$8.2062^* - 5$		
14	>0.875	0.468065	0.0741481	0.0010300	$1.6455^* - 5$	
15	>0.875	0.563811	0.133610	0.0052147	$3.2609^* - 5$	
16	>0.875	0.646666	0.216248	0.0161839	$8.4637^* - 5$	$1.9121^* - 5$

j	$P_s^*[3,j]$	$P_s^*[4,j]$	$P_s^*[5,j]$	$P_s^*[6,j]$	$P_s^*[7,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$
17	> 0.7	0.286239	0.037125	$6.4493* - 4$	$3.1882^* - 4$		
18	> 0.7	0.368209	0.069620	0.0027409	$5.5832^* - 6$	$< 10^* - 14$	
19	> 0.7	0.448005	0.113332	0.0080738	$6.4052^* - 5$	$4.450^* - 9$	
20	> 0.7	0.558350	0.166442	0.0185811	$3.7310^* - 4$	$1.091^* - 8$	$9.413^* - 11$
21	> 0.7	0.66091	0.226317	0.0358782	$1.4181^* - 3$	$5.251^* - 6$	$1.164^* - 10$

j	$P_s^*[4,j]$	$P_s^*[6,j]$	$P_s^*[7,j]$	$P_s^*[8,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$	
22	> 0.5	0.290135	0.060860	$4.0303^* - 3$	$4.1486^* - 5$	$1.408^* - 11$	$< 10^* - 14$
23	> 0.5	0.355296	0.093581	$9.2965^* - 3$	$2.0641^* - 4$	$3.638^* - 7$	$1.003^* - 11$
24	> 0.5	0.418394	0.133343	0.0183573	$7.2479^* - 4$	$3.9637^* - 6$	$5.622^* - 10$ $< 10^* - 14$

j	$P_s^*[5,j]$	$P_s^*[6,j]$	$P_s^*[7,j]$	$P_s^*[8,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$
25	> 0.5	0.178925	0.032180	$2.0126^* - 3$	$2.5416^* - 5$	$2.1420^* - 8$	$5.398^* - 14$	
26	> 0.5	0.228823	0.051391	$4.6505^* - 3$	$1.1119^* - 4$	$3.2689^* - 7$	$9.323^* - 10$	$< 10^* - 14$
27	> 0.5	0.283291	0.076197	$9.3471^* - 3$	$3.7051^* - 4$	$2.691^* - 6$	$9.11^* - 9$	$< 10^* - 14$

j	$P_s^*[6,j]$	$P_s^*[7,j]$	$P_s^*[8,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j$
28	> 0.3	0.10683	0.016830	$1.0053^* - 3$	$1.4652^* - 5$	$2.328^* - 8$	$9.31^* - 10$	$< 10^* - 14$	
29	> 0.3	0.1414	0.027741	$2.3261^* - 3$	$5.8875^* - 5$	$2.49^* - 7$	$5.22^* - 11$	$< 10^* - 14$	
30	> 0.3	0.1803	0.033333	$4.7428^* - 3$	$1.8805^* - 4$	$1.686^* - 6$	$1.3968^* - 9$	$1.62^* - 14$	$< 10^* - 14$

j	$P_s^*[7,j]$	$P_s^*[8,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$
31	> 0.2	0.06153	$8.7319^* - 3$	$5.002^* - 4$	$8.1797^* - 6$	$2.0356^* - 8$	$2.158^* - 12$	$< 10^* - 14$		
32	> 0.2	0.08469	0.0147868	$1.163^* - 3$	$5.0806^* - 5$	$1.7144^* - 7$	$8.312^* - 11$	$< 10^* - 14$	$< 10^* - 14$	
33	> 0.2	0.112	0.0233628	$2.400^* - 3$	$9.5173^* - 5$	$1.0046^* - 6$	$3.299^* - 10$	$8.04^* - 14$	$< 10^* - 14$	
34	> 0.2	0.131	0.034829	$4.503^* - 3$	$2.5098^* - 4$	$4.465^* - 6$	$1.555^* - 8$	$4.22^* - 12$	$< 10^* - 14$	$< 10^* - 14$

j	$P_s^*[8,j]$	$P_s^*[9,j]$	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$
35	> 0.1	0.0494	$7.804^* - 3$	$5.818^* - 4$	$1.598^* - 5$	$1.101^* - 7$	$9.744^* - 11$	$< 10^* - 14$	
36	> 0.1	0.067	0.012650	$1.212^* - 3$	$4.803^* - 5$	$5.780^* - 7$	$1.270^* - 9$	$1.94^* - 14$	$< 10^* - 14$

j	$P_s^*[9,j]$	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[(14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$
37	> 0.06	0.01937	$2.311^* - 3$	$1.254^* - 4$	$2.398^* - 6$	$1.806^* - 8$	$5.782^* - 11$	$< 10^* - 14$		
38	> 0.06	0.0282	$4.087^* - 3$	$2.909^* - 4$	$8.238^* - 6$	$6.726^* - 8$	$9.394^* - 11$	$< 10^* - 14$		
39	> 0.06	0.0395	$6.776^* - 3$	$6.115^* - 4$	$2.426^* - 5$	$3.242^* - 7$	$9.711^* - 10$	$3.15^* - 13$	$< 10^* - 14$	
40	> 0.06	0.053	0.010633	$1.182^* - 3$	$6.268^* - 5$	$1.272^* - 6$	$7.22^* - 9$	$6.34^* - 12$	$< 10^* - 14$	
41	> 0.06	0.06	0.0159	$6.213^* - 3$	$1.455^* - 4$	$4.225^* - 6$	$3.976^* - 8$	$7.92^* - 11$	$1.57^* - 14$	$< 10^* - 14$

j	$P_s^*[10,j]$	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$
42	> 0.06	0.0228	$3.598^* - 3$	$3.081^* - 4$	$1.222^* - 5$	$1.784^* - 7$	$6.86^* - 10$	$3.92^* - 13$	$< 10^* - 14$	
43	> 0.05	0.031	$5.769^* - 3$	$6.027^* - 4$	$3.133^* - 5$	$6.69^* - 7$	$4.449^* - 9$	$5.93^* - 12$	$< 10^* - 14$	
44	> 0.05	> 0.03	$8.828^* - 3$	$1.101^* - 3$	7.276*-5	$2.16^* - 6$	$2.285^* - 8$	$6.06^* - 11$	$2.25^* - 14$	$< 10^* - 14$

the information expansion ratio is not satisfied, then choose the second consideration $R(i+2,n), R(i+3,n), \ldots, R(n,n)$, respectively, until the information expansion ratio is satisfied.

Corollary 4: In the region $P_s^*[(I+1,n),(i+2,n)] < P_s < P_s^*[(i,n),(i+1,n)]$, the optimal value of m is $i+1$. If $(i+1,n)$ WIDS do not satisfy the information expansion ratio, then choose $R(i+1,n), R(i+2,n), \ldots, R(n,n)$ respectively, until the selected (m,n) WIDS satisfies the information expansion ratio.

By Theorem 3.6, the smallest intersection of (m,n) WIDS for fixed n is $P_s^*[(\eta_2,n),(\eta_2+1,n)]$. When P_s is in the region $(0, P_s^*[(\eta_2,n),(\eta_2+1,n)])$, the optimal m is η_2.

When giving n sub-channels, and success probability P_s for transmitting the original message using $(1,1)$ WIDS, choose the

TABLE I *(Continued)*
THE INTERSECTIONS: $P_s^*[i,j] \equiv P_s^*[(i,j),(i+1,j)]$ FOR $j = 4 - 84$

j	$P_s^*[11,j]$	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$
45	> 0.03	0.01296	$1.897^* - 3$	$1.550^* - 4$	6.139*-6	$9.62^* - 8$	$4.563^* - 10$	$4.08^* - 13$	$< 10^* - 14$
46	> 0.03	0.018	$3.101^* - 3$	$3.066^* - 4$	$1.566^* - 5$	$3.494^* - 7$	$2.684^* - 9$	$4.94^* - 12$	$< 10^* - 14$

j	$P_s^*[12,j]$	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$
47	> 0.02	$4.84^* - 3$	$5.680^* - 4$	$3.638^* - 5$	$1.1^* - 6$	$1.286^* - 8$	$4.32^* - 11$	$2.62^* - 14$	$< 10^* - 14$
48	> 0.02	$7.2^{*-}3$	$9.939^* - 4$	$7.796^* - 5$	$3.086^* - 6$	$5.192^* - 8$	$2.907^* - 10$	$3.72^* - 13$	$< 10^* - 14$

j	$P_s^*[13,j]$	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$
49	> 0.01	$1.65^* - 3$	$1.556^* - 4$	$7.827^* - 6$	$1.813^* - 7$	$1.575^* - 9$	$3.788^* - 12$	$< 10^* - 14$	
50	> 0.01	$2.63^* - 3$	$2.919^* - 4$	$1.819^* - 5$	$5.594^* - 7$	$7.119^* - 9$	$2.916^* - 11$	$2.63^* - 14$	$< 10^* - 14$
51	> 0.01	$4.40^* - 3$	$5.183^* - 4$	$3.918^* - 5$	$1.550^* - 6$	$2.758^* - 8$	$1.782^* - 10$	$2.08^* - 13$	$< 10^* - 14$

j	$P_s^*[14,j]$	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$
52	> 0.006	$8.76^* - 4$	$7.887^* - 5$	$3.913^* - 6$	$9.368^* - 8$	$5.04^* - 10$	$2.719^* - 12$	$< 10^* - 14$	
53	> 0.008	$1.42^* - 3$	$1.496^* - 4$	$9.908^* - 6$	$2.838^* - 7$	$3.889^* - 9$	$1.88^* - 11$	$2.34^* - 14$	$< 10^* - 14$
54	> 0.008	$2.20^* - 3$	$2.691^* - 4$	$1.968^* - 5$	$7.783^* - 7$	$1.45^* - 8$	$1.06^* - 10$	$2.36^* - 13$	$< 10^* - 14$
55	> 0.008	0.003	$4.615^* - 4$	$3.992^* - 5$	$1.956^* - 6$	$4.820^* - 8$	$5.10^* - 10$	$1.85^* - 12$	$< 10^* - 14$

j	$P_s^*[15,j]$	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$
56	> 0.004	0.0007	$7.648^* - 5$	$4.549^* - 6$	$1.437^* - 7$	$2.104^* - 9$	$1.177^* - 11$	$1.93^* - 14$	$< 10^* - 14$
57	> 0.004	> 0.001	$1.392^{-}4$	$9.789^* - 6$	$3.906^* - 7$	$7.602^* - 9$	$6.243^* - 11$	$1.71^* - 13$	$< 10^* - 14$

j	$P_s^*[16,j]$	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$
58	> 0.001	$2.49^* - 4$	$2.018^* - 5$	$9.778^* - 7$	$2.473^* - 8$	$2.83^* - 10$	$1.215^* - 12$	$< 10^* - 14$	
59	> 0.001	$4.03^* - 4$	$3.901^* - 5$	$2.275^* - 6$	$7.270^* - 8$	$1.12^* - 9$	$7.19^* - 12$	$1.42^* - 14$	$< 10^* - 14$
60	> 0.001	$6.4^* - 4$	$7.178^* - 5$	$4.95^* - 6$	$1.959^* - 7$				
	$3.974^* - 9$	$3.578^* - 11$	$1.17^* - 13$	$< 10^* - 14$					

j	$P_s^*[17,j]$	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$
61	$> 6 * -4$	$1.26^* - 4$	$1.019^* - 5$	$4.888^* - 7$	$1.286^* - 8$	$1.55^* - 10$	$7.69^* - 13$	$< 10^* - 14$	
62	$> 6 * -4$	$2.13^* - 4$	$1.986^* - 5$	$1.137^* - 6$	$3.673^* - 8$	$5.98^* - 10$	$4.248^* - 12$	$1.07^* - 14$	$< 10^* - 14$
63	$> 2^* - 4$	$3.47^* - 4$	$3.691^* - 5$	$2.4894^* - 6$	$9.82^* - 8$	$2.06^* - 9$	$2.02^* - 11$	$7.79^* - 14$	$< 10^* - 14$
64	$> 2^* - 4$	$5.4^* - 4$	$6.56^* - 5$	$5.141^* - 6$	$2.443^* - 7$	$6.456^* - 9$	$8.46^* - 11$	$4.74^* - 13$	$< 10^* - 14$
65	$> 2^* - 4$	$8^* - 4$	$1.12^* - 4$	$1.01^* - 5$	$5.687^* - 7$	$1.853^* - 8$	$3.162^* - 10$	$2.47^* - 12$	$< 10^* - 14$

j	$P_s^*[18,j]$	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$
66	$> 1^* - 3$	$1.85^* - 4$	$1.894^* - 5$	$1.247^* - 6$	$4.927^* - 8$	$1.067^* - 9$	$1.128^* - 11$	$5^* - 14$	$< 10^* - 14$
67	$> 1^* - 3$	$2.9^* - 4$	$3.405^* - 5$	$2.591^* - 6$	$1.221^* - 7$	$3.288^* - 9$	$4.57^* - 11$	$2.86^* - 13$	$< 10^*14$

j	$P_s^*[19,j]$	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$
68	$> 1 * -3$	$4^* - 4$	$5.89^* - 5$	$5.127^* - 6$	$3.844^* - 7$	$9.34^* - 9$	$1.66^* - 10$	$1.42^* - 12$	$< 10^*14$
69	$> 6^* - 4$	$9^* - 5$	$9.679^* - 6$	$6.254^* - 7$	$2.469^* - 8$	$5.50^* - 10$	$6.221^* - 12$	$3.12^* - 14$	$< 10^* - 14$

j	$P_s^*[20,j]$	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$	$P_s^*[28,j]$
70	$> 1^* - 4$	$1.76^* - 5$	$1.305^* - 6$	$6.107^* - 8$	$1.672^* - 9$	$1.44^* - 11$	$1.688^* - 13$	$< 10^* - 14$	
71	$> 1^* - 4$	$3.08^* - 5$	$2.599^* - 6$	$1.442^* - 7$	$4.710^* - 9$	$8.78^* - 11$	$8.024^* - 13$	$< 10^* - 14$	
72	$> 2^* - 4$	$5.2^* - 5$	$4.956^* - 6$	$3.135^* - 7$	$1.237^* - 8$	$2.83^* - 10$	$3.4^* - 13$	$1.90^* - 14$	$< 10^* - 14$
73	$> 2^* - 4$	$8.51^* - 5$	$9.078^* - 6$	$6.57^* - 7$	$3.053^* - 8$	$8.49^* - 10$	$1.297^* - 11$	$9.81^* - 14$	$< 10^* - 14$

j	$P_s^*[21,j]$	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$	$P_s^*[28,j]$	$P_s^*[29,j]$
74	$> 1^* - 4$	$1.60^* - 5$	$1.316^* - 6$	$7.110^* - 8$	$2.371^* - 9$	$4.52^* - 11$	$4.485^* - 13$	$< 10^* - 14$	
75	$> 6^* - 4$	$2.74^* - 5$	$2.528^* - 6$	$1.571^* - 7$	$6.20^* - 9$	$1.45^* - 11$	$1.842^* - 12$	$1.1^* - 14$	$< 10^* - 14$
76	$> 2^* - 4$	$4.5^* - 5$	$4.670^* - 6$	$3.308^* - 7$	$1.526^* - 8$	$4.31^* - 10$	$6.87^* - 12$	$5.62^* - 14$	$< 10^* - 14$
77	$> 2^* - 4$	$7^* - 5$	$8.324^* - 6$	$6.663^* - 7$	$3.555^* - 8$	$1.193^* - 9$	$2.349^* - 11$	$2.48^* - 13$	$< 10^* - 14$

j	$P_s^*[22,j]$	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$	$P_s^*[28,j]$	$P_s^*[29,j]$	$P_s^*[30,j]$
78	$> 4^* - 4$	$1.43^* - 5$	$1.288^* - 6$	$7.873^* - 8$	$3.106^* - 9$	$7.42^* - 11$	$9.914^* - 13$	$< 10^* - 14$	
79	$> 3^* - 4$	$2.39^* - 5$	$2.397^* - 6$	$1.664^* - 7$	$7.631^* - 9$	$2.18^* - 10$	$3.617^* - 12$	$3.18^* - 14$	$< 10^* - 14$
80	$> 3^* - 4$	$3.9^* - 5$	$4.311^* - 6$	$3.368^* - 7$	$1.777^* - 8$	$6.00^* - 10$	$1.215^* - 11$	$1.36^* - 13$	$< 10^* - 14$

j	$P_s^*[23,j]$	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$	$P_s^*(8,j)]$	$P_s^*[29,j]$	$P_s^*[30,j]$	$P_s^*[31,j]$
81	$> 4^* - 4$	$7.5^* - 6$	$6.554^* - 7$	$3.944^* - 8$	$1.55^* - 9$	$3.79^* - 11$	$5.303^* - 13$	$< 10^* - 14$	
82	$> 3^* - 4$	$1^* - 5$	$1.229^* - 6$	$8.366^* - 8$	$3.815^* - 9$	$1.10^* - 10$	$1.896^* - 12$	$1.78^* - 14$	$< 10^* - 14$

j	$P_s^*[24,j]$	$P_s^*[25,j]$	$P_s^*[26,j]$	$P_s^*[27,j]$	$P_s^*[28,j]$	$P_s^*[29,j]$	$P_s^*[30,j]$	$P_s^*[31,j]$
83	$> 2^* - 5$	$2.22^* - 6$	$1.701^* - 7$	$8.889^* - 9$	$3.02^* - 10$	$6.27^* - 12$	$7.412^* - 14$	$< 10^* - 14$
84	$> 2^* - 4$	$3.91^* - 6$	$3.331^* - 7$	$1.975^* - 8$	$7.79^* - 10$	$1.93^* - 11$	$2.8^* - 13$	$< 10^* - 14$

optimal m by finding the region to which P_s belongs. Algorithm 4.1 shows how to find the optimal m.

Algorithm 4.1: Finding Optimal m for (m, n) WIDS
Input: n: the number of sub-channels

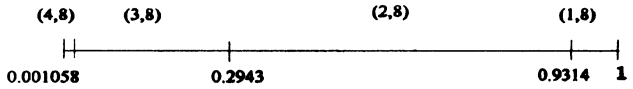

Fig. 4. The optimal (m, n) WIDS for $n = 8$.

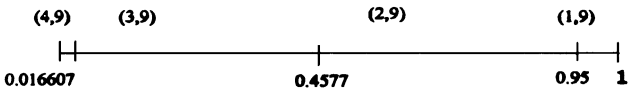

Fig. 5. The optimal (m, n) WIDS for $n = 9$.

Output: m: the optimal value of m, such that (m, n) WIDS can achieve the optimal communication reliability

1. Estimate P_s when transmitting the message using (1, 1) WIDS. (That is, the traditional way to transmit the data.)

2a. After estimating the P_s, look in Table I for $j = n$ to determine the region to which P_s belongs.

2b. Search for the optimal m value as follows.

· case 1: If $P_s > P_s^*[(1, n), (2, n)]$, then the optimal m is 1.

· case 2: If P_s is in the region: $[P_s^*((m' - 1, n), (m', n)), P_s^*((m', n), (m' + 1, n))]$, then the optimal m is m'.

· case 3 If P_s is smaller than the smallest intersection: $(0, P_s^*[(\eta_2, n), \eta_2 + 1, n)])$, then the optimal m is η_2.

3. If the optimal m cannot satisfy the information expansion ratio requirement, then choose $(m + 1, n)$ WIDS, $(m + 2, n)$ WIDS, $\ldots, (n, n)$ WIDS instead of (m, n) WIDS respectively, until the information expansion ratio is satisfied.

4. Output m.

B. Determining Optimal m With an Upper-Bound of n

Section IV-A considers the cases of the Information Dispersal Scheme used to support fault-tolerant parallel communication with n available sub-channels. This section considers the (m, n) WIDS performance when a different number of sub-channels n_1 and n_2 are used. Some principles are provided to help users determine the optimal WIDS with highest communication reliability. The problem of the information expansion ratio is not considered in this section.

Appendix I lists the intersections for $4 \leq n \leq 84$. This is the range of n where WIDS is used. Observing these intersections, shows that $P_s^*[(m, n), (m+1, n)]$ is always smaller than $P_s^*[(m, n+1), (m+1, n+1)]$ if $P_s^*[(m, n+1), (m+1, n+1)]$ exists. This phenomenon is described in the following *Assumption*: $P_s^*[(m, n), (m+1, n)] < P_s^*[(m, n+1), (m+1, n+1)]$, if both of them exist.

As mentioned in Section IV-A, every region of P_s has its optimal (m, n) WIDS. Divide an axis line into many regions by the intersections, $P_s^*[(i, j), (i + 1, j)]$, and indicate the optimal (m, n) WIDS in every divided region. For example, indicate the optimal (m, n) WIDS for $n = 8$ as shown in Figs. 4 and 5.

Now, compare the performance of (m, n) WIDS and $(m, n+1)$ WIDS with a fixed n and a variant m, and find which one has the better reliability. Fig. 4 indicates optimal (m, n) WIDS for $n = 8$, and Fig. 5 indicates optimal (m, n) WIDS for $n = 9$. It is hard to decide which is better from these figures. Now, compare the performance of (m, n) WIDS and $(m, n + 1)$ WIDS, using 3 cases.

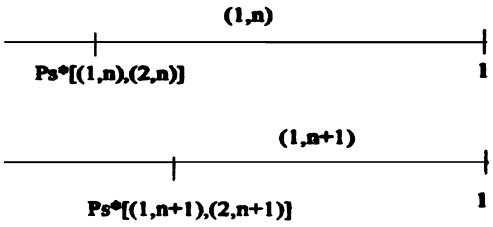

Fig. 6. Indication of optimal (m, n) WIDS when P_s is in $(P_s^*[(1, n), (2, n)], 1)$.

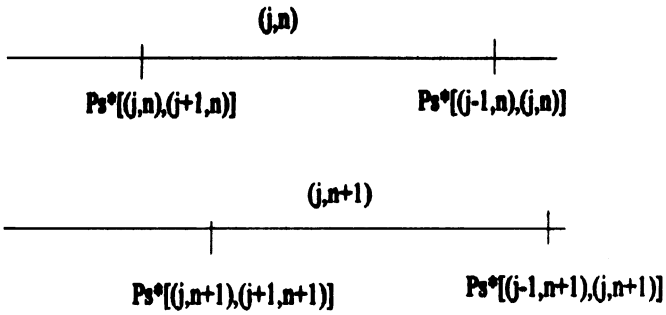

Fig. 7. The indication of (m, n) WIDS, when P_s is between 2 intersections.

- Case 1: P_s is in the region $(P_s^*[(1, n), (2, n)], 1)$,
- Case 2: P_s is between 2 intersections,
- Case 3: P_s belongs to the region $(0, P_s^*[(\eta_2, n), (\eta_2 + 1, n)])$.

The indication is shown in Fig. 6.

Case 1.

Divide this case 1 into 2 cases, A and B

Case 1A: $P_s > P_s^*[(1, n + 1), (2, n + 1)]$; the optimal m values chosen in Section IV-A are both 1 because the sub-channel number is n or $n + 1$. As discussed in Theorem 3.2, $R(m, n + 1)$ has better performance than $R(m, n)$. Thus the optimal m value is $(1, n + 1)$ WIDS.

Case 1B: $P_s^*[(1, n+1), (2, n+1)] < P_s < P_s^*[(1, n), (2, n)]$; the optimal value chosen is 1 when the sub-channel number is n, and is 2 when the sub-channel number is $n + 1$. By using Theorem 3.7, $R(2, n+1) > R(1, n+1)$ when $P_s < P_s^*[(1, n+1), (2, n+1)]$, and $R(2, n+1) > R(1, n+1) > R(1, n)$; thus the optimal (m, n) is $(2, n + 1)$ WIDS.

Case 2.

P_s is between 2 intersections.

By observing the divided regions of $n = 8$ and $n = 9$ in Figs. 4 and 5, the region

$$(P_s^*[(i - 1, 8), (i, 8)], P_s^*[(i, 8), (i + 1, 8)])$$

overlaid with the region

$$(P_s^*[(i - 1, 9), (i, 9)], P_s^*[(i, 9), (i + 1, 9)]).$$

By the assumption in Section IV-B,

$$P_s^*[(m, n), (m + 1, n)] < P_s^*[(m, n + 1), (m + 1, n + 1)].$$

Thus, the indication of optimal (m, n) WIDS of this case is shown Fig. 7.

Consider the region

$$P_s^*[(j, n), (j + 1, n)] < P_s < P_s^*[(j - 1, n), (j, n)];$$

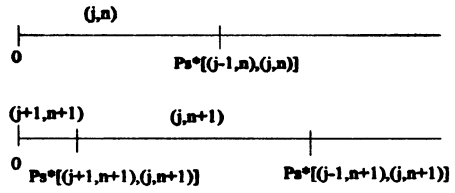

Fig. 8. The indication of optimal (m,n) WIDS when P_s belongs to $(0, P_s^*[(\eta_2,n),(\eta_2+1,n)])$.

divide it into 2 cases, A and B.

Case 2A. $P_s > P_s^*[(j,n+1),(j+1,n+1)]$

The optimal m values chosen in Section I are both j for the sub-channel whether the number is n or $n+1$. As mentioned in Theorem 3.2, $R(j,n+1)$ has better performance than $R(j,n)$. Thus, the optimal m value in this case is $(j,n+1)$ WIDS.

Case 2B. $P_s^*[(j,n),(j+1,n)] < P_s < P_s^*[(j,n+1),(j+1,n+1)]$

The optimal value chosen is j when the sub-channel number is n, and is $j+1$ when the sub-channel number is $n+1$. Using Theorem 3.7,

$$\begin{aligned}&R(j+1,n+1) > R(j,n+1) \text{ when}\\ &P_s < P_s^*[(1,n+1),(2,n+1)], \text{ and}\\ &\text{and } R(j+1,n+1) > R(j,n+1) > R(j,n);\end{aligned}$$

thus the optimal (m,n) value is $(j+1,n+1)$ WIDS.

Case 3.

P_s belongs to the region $(0, P_s^*[(\eta_2,n),(\eta_2+1,n)])$.

When $P_s > P_s^*[(\eta_2,n+1),(\eta_2+1,n)]$, the optimal m chosen in Section II is η_2 when the sub-channel number is n or $n+1$. As discussed in Theorem 3.2, $R(\eta_2,n+1)$ performs better than $R(\eta_2,n)$. Thus the optimal (m,n) value in this case is $(\eta_2,n+1)$ WIDS.

If n is an odd number, there is 1 more intersection of $P_s^*[(\eta_2,n+1),(\eta_2+1,n+1)]$ when the sub-channel number is $n+1$. When P_s belongs to the region

$$(0, P_s^*[(\eta_2,n+1),(\eta_2-1,n+1)]),$$

then $R(\eta_2+1,n+1)$ is better than $R(\eta_2,n)$. And $R(\eta_2,n+1)$ is better than $R(\eta_2,n)$. Thus the optimal (n,m) in this case is $(\eta_2+1,n+1)$ WIDS.

According to this explanation, the performance of $(m,n+1)$ WIDS is better than (m,n) WIDS. Thus, when using total available sub-channels, one gets the highest communication reliability. Algorithm 4.1 shows how to choose m to get the optimal communication reliability; this optimal m depends on what region P_s belongs to.

For example, let $N=8$; then all combinations of (m,n) are:

$(1,1)$ WIDS;

$(1,2)$ WIDS, $(2,2)$WIDS;

$(1,3)$ WIDS, $(2,3)$ WIDS, $(3,3)$ WIDS;

$\ddots$

$(1,8)$ WIDS, $(2,8)$ WIDS, $(3,8)$ WIDS, $(4,8)$ WIDS, $(5,8)$ WIDS, $(6,8)$ WIDS, $(7,8)$ WIDS, $(8,8)$ WIDS.

The optimal (m,n) WIDS is in the set $\{(1,8)$ WIDS, $(2,8)$ WIDS, $(3,8)$ WIDS, $(4,8)$ WIDS$\}$. That is, using total available sub-channels results in the optimal reliability. From Theorem 3.6, $R(4,8) > R(5,8) > R(6,8) > R(7,8) > R(8,8)$; thus $R(5,8), R(6,8), R(7,8), R(8,8)$ are not optimal. The method to find the optimal value of m is described in Section IV-A. This section ignores the problem of information expansion ratio.

C. Optimal WIDS With an Upper Bound on Information Expansion Ratio

This section considers the problem of information expansion ratio. A method is proposed to determine the candidate set of the optimal (m,n) WIDS when an upper-bound of information expansion ratio (u) and the number of available sub-channels (N) are given. This method can reduce the element number of the candidate WIDS set from $O(N^2)$ to $O(N)$.

Section II defines the information expansion ratio to be n/m for (m,n) WIDS. When given an upper-bound of u and the number of available sub-channels N, the candidate WIDS set is defined as:

Definition (Candidate Information Dispersal Scheme Set): A candidate WIDS set, $C_{u\cdot N}$, with u and N, is $\{(m,n)\text{WIDS} \,|\, \text{for all } m,n,u \in N, 1 \le n/m \le u, n \le N, 1 \le m \le n\}$.

The candidate WIDS set can be reduced so that all optimal WIDS are still included in the reduced candidate WIDS set. The reduced candidate WIDS set is a subset of the candidate WIDS set. For any P_s, the optimal WIDS is an element of the reduced $C_{u\cdot N}$.

The candidate WIDS set $C_{u\cdot N}$ can be described as the union of partitions. Each partition consists of all (m,n) WIDS for which m is a constant:

$$\begin{aligned}C_{u\cdot N} &= \{(1,t)\text{WIDS} \,|\, 1 \le t \le u\} \cup \{(2,t)\text{WIDS} \,|\, 2 \le t \le 2u\}\\ &\ddots\\ &\cup \{(k,t)\text{WIDS} \,|\, k \le t \le k\cdot u\}\\ &\cup \{\eta_u,t)\text{WIDS} \,|\, \eta_u+1 \le t \le N\}\\ &\cup \{\eta_u+1,t)\text{WIDS} \,|\, \eta_u+2 \le t \le N\}\\ &\ddots\\ &\cup \{N,N)\text{WIDS}\}, \quad \text{where } k=\eta_u.\end{aligned}$$

By Theorem 3.2, for each partition $\{(i,t)\text{WIDS} \,|\, i \le t \le i\cdot u\}$, $(i,i\cdot u)$ WIDS has the highest communication reliability among them. Similarly, for each partition

$$\{(\eta_u+j,t)\text{WIDS} \,|\, \eta_u+j \le t \le N\},$$

the (η_u+j,N) has the highest communication reliability among them. Thus, $C_{u,N}$ can be reduced to

$$\begin{aligned}&\{(i,i\cdot u)\text{WIDS} \,|\, 1 \le i \le \eta_u\}\\ &\qquad \cup \{(\eta_u+j,N)\text{WIDS} \,|\, 1 \le j \le N-\eta_u\}.\end{aligned}$$

By Theorems 3.6 and 3.7, for the WIDS set

$$\{(\eta_u+j,N)\text{WIDS} \,|\, 1 \le j \le N-\eta_u\},$$

it can be reduced to

$$\{(\eta_u + j, N)\text{WIDS} \,|\, 1 \le j \le N - \eta \quad \text{and} \quad \eta + j \le \eta\}$$

when $2 \le u$. Or it can be reduced to

$$\{(\eta_u + j, N)\text{WIDS} \,|\, j = 1\} \quad \text{when } u \le 2.$$

Therefore, $C_{u,N}$ can be reduced to $\{(i, i \cdot u)\text{WIDS} \,|\, 1 \le i \le \eta_u\} \cup \{(\eta_u + j, N)\text{WIDS} \,|\, 1 \le j \le N - \eta_u \text{and} \eta_u + j \le \eta_2\}$ when $2 \le u$, or $\{(i, i \cdot u)\text{WIDS} \,|\, 1 \le i \le \eta_u\} \cup \{(\eta_u + j, N)\text{WIDS} \,|\, j - 1\}$ when $u \le 2$.

The number of the elements in reduced candidate WIDS set is smaller than N. Therefore, the number of the elements in candidate WIDS set can be reduced from $O(N^2)$ to $O(N)$. For example, let $u = 3$ and $N = 11$. n/m should be smaller than 3. The candidate WIDS set is:

$$\begin{aligned} C_{3,11} = {} & \{(1,t)\text{WIDS} \,|\, 1 \le t \le 4\} \\ & \cup \{(2,t)\text{WIDS} \,|\, 2 \le t \le 6\} \\ & \cup \{(3,t)\text{WIDS} \,|\, 3 \le t \le 9\} \\ & \cup \{(4,t)\text{WIDS} \,|\, 4 \le t \le 11\} \\ & \ddots \\ & \cup \{(10,t)\text{WIDS} \,|\, 10 \le t \le 11\} \\ & \cup \{(11,11)\text{WIDS}\} \end{aligned}$$

$C_{3,11}$ can be reduced to be $\{(1,3)$ WIDS$, (2,6)$ WIDS$, (3,9)$ WIDS$, (4,11)$ WIDS, and $(5,11)$ WIDS$\}$. Thus the number of the candidate WIDS sets is reduced from 51 to 5.

There is another example when the case expansion ratio is less than 2.

$$\begin{aligned} & \text{Let} u = 1.5 \text{ and } N = 11, \\ & C_{1.5,11} = \{(1,1)\text{ WIDS}\} \cup \{(2,t)\text{ WIDS} \,|\, 2 \le t \le 3\} \\ & \cup \{(3,t)\text{ WIDS} \,|\, 3 \le t \le 4\} \\ & \ddots \\ & \cup \{(7,t)\text{ WIDS} \,|\, 7 \le t \le 10\} \cup \{(8,t)\text{ WIDS} \,|\, 8 \le t \le 11\} \\ & \ddots \\ & \cup \{(10,t)\text{ WIDS} \,|\, 10 \le t \le 11\} \cup \{(11,11)\text{WIDS}\}. \\ & C_{1.5,11} \text{ can be reduced to be} \\ & \{(1,1)\text{ WIDS}, (2,3)\text{ WIDS}, (3,4)\text{ WIDS}, (4,6)\text{WIDS}, \\ & (5,8)\text{ WIDS}, (6,9)\text{ WIDS}, (7,11)\text{ WIDS}, \text{and} (8,11)\text{ WIDS}\}. \end{aligned}$$

Thus, the number of the candidates in the WIDS set is reduced from 31 to 8.

This paper does not discuss the relations between the 2 elements of the partition $\{(i, i \cdot u)\text{ WIDS} \,|\, 1 \le i \le \eta_u\}$. It is difficult to prove the relationship between $R(i, i \cdot u)$ and $R(i', i' \cdot u)$, because the function $r(P_s) = R(i, i \cdot u) - R(i', i' \cdot u)$ approaches 0 when P_s approaches 1, and both $r'(P_s)$ and $r''(P_s)$ are 0 when $P_s = 1$. It is difficult to claim which one is better. But by the simulation result, $R(i, i \cdot u)$ is better than $R(i - 1, (i-1) \cdot u)$. When $P_s \to 1$, the difference between 1 and $R(i, i \cdot u)$ or $R(i - 1, (i-1) \cdot u)$ is smaller than 10^{-14}. We suggest using $R(i, i \cdot u)$ instead of $R(i - 1, (i-1) \cdot u)$. The partition $\{(i, i \cdot u)\text{ WIDS} \,|\, 1 \le i \le \eta_u\}$ of candidate WIDS set can be reduced to $\{(i, i \cdot u)\text{WIDS} \,|\, i = \eta_u\}$. For example: let $u = 3$ and $N = 11$; then $C_{3,11}$ can be reduced to be $\{(3,9)\text{ WIDS}, (4,11)\text{ WIDS and} (5,11)\text{ WIDS}\}$.

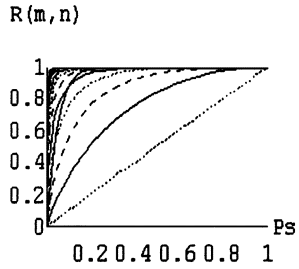

Fig. 9. All curves of communication reliability $(m, 20)$ WIDS, for $1 \le m \le n$.

V. Discussions and Future Work

As in Section III, the transmission reliability is greatly improved when P_s is very small. The WIDS performances approach 1 when P_s is greater than some value, such as 0.1 in Fig. 9.

Now, define TR as the acceptable maximum probability of transmitting a message with the (m, n) WIDS: a (m, n) WIDS is acceptable if

$$1 - R(m, n) < \text{TR}.$$

Also define $Q((m, n))$ as the point (P_s) that the reliability of (m, n) WIDS approaches 1, and $\text{TR} = 10^{-14}$. The list of $Q((m, n))$ when $n = 20$ and $m \le \eta_2$ is:

$$\begin{aligned} & Q((1,20)) = 0.80 \quad Q((2,20)) = 0.688 \\ & Q((3,20)) = 0.667 \quad Q((4,20)) = 0.653 \\ & Q((5,20)) = 0.656 \quad Q((6,20)) = 0.677 \\ & Q((7,20)) = 0.681 \quad Q((8,20)) = 0.685 \\ & Q((9,20)) = 0.712 \quad Q((10,20)) = 0.831 \end{aligned}$$

This phenomenon shows that, if the TR smaller than 10^{-14} can be tolerated, then there is no difference in choosing $(1,20)\text{ WIDS}, (2,20)\text{ WIDS}, \ldots, (10,20)\text{ WIDS}$ when $P_s > 0.83$. If TR is larger, the $Q((m, n))$ becomes smaller; i.e., if larger TR can be tolerated, then smaller P_s will achieve tolerable performance of (m, n) WIDS.

Define $Q10^{-14}[n]$ as the point that all reliability of (m, n) WIDS where $m \le \eta_2 \to 1$ and the difference between 1 and $R(m, n)$ where $m \le \eta_2 < 10^{-14}$. Now, some $Q10^{-14}[n]$ are:

$$\begin{aligned} & Q10^{-14}[10] = 0.99 \quad Q10^{-14}[20] = 0.831 \\ & Q10^{-14}[30] = 0.521 \quad Q10^{-14}[40] = 0.245 \\ & Q10^{-14}[50] = 0.093 \quad Q10^{-14}[60] = 0.029 \\ & Q10^{-14}[70] = 0.0083 \quad Q10^{-14}[80] = 0.001\,91 \end{aligned}$$

The greater n is the smaller $Q10^{-14}[n]$ is; this satisfies Theorem 3.3. When $n = 40$, then $R(m, n) \to 1m$ even though P_s is only 0.245. This means that the (m, n) WIDS improves parallel transmission when $P_s < 0.245$. The more sub-channels that are used, the better the reliability. As

stated before, if TR $= 10^{-14}$ there is no difference between choosing $(1,n)$ WIDS, $(2,n)$ WIDS, $\ldots$, (η_2,n) WIDS when $P_s > Q10^{-14}[n]$. If the user can tolerate the information expansion ratio 2, it will be good enough to choose the (η_2,n) WIDS because the information expansion ratio of (η_2,n) WIDS is the smallest.

For given P_s, there exists one greatest $Q10^{-14}[N \cdot a]$ (the smallest $N \cdot a$) which satisfies $P_s^* > Q10^{-14}[N \cdot a]$. $n = N \cdot a$ can be chosen to get the optimal communication reliability. As mentioned in the previous paragraphs, if TR $= 10^{-14}$, it will make no difference to choose any of $(1, N \cdot a)$ WIDS, $(2, N \cdot a)$ WIDS, $\ldots$, $(\eta^*, N \cdot a)$ WIDS when $P_s > Q10^{-14}[N \cdot a]$. If the user can tolerate the information expansion ratio 2, it will be good enough to choose the $(\eta^*, N \cdot a)$ WIDS because the information expansion ratio of $(\eta^*, N \cdot a)$ WIDS is smallest. Table II (in Appendix I) lists some $Q10^{-14}[n]$.

For example, when $P_s = 0.82$ and $N = 70$, it is obvious that $0.82 > Q10^{-14}[n]$. It seems that (35, 70) WIDS can be the optimal solution because it approaches 1. But $P_s = 0.82$ is also larger than $Q10^{-14}[20], R(10,20) \rightarrow 1$ when $P_s = 0.82$. One can choose the (10, 20) WIDS instead of (35, 70) WIDS—because the computation complexity of (10, 20) WIDS is simpler than that of (35, 70) WIDS.

It is reasonable to use fewer sub-channels to achieve the same performance as using the total sub-channels N, if some small error can be tolerated, such as 10^{-14}. Although a method is not proposed to choose the optimal (m,n) WIDS when some small error can be tolerated, this phenomenon is still described and a method is given to choose the (m,n) WIDS which satisfies the performance requirement. The phenomenon can help choose the optimal (m,n) WIDS when some small error can be tolerated.

This paper proposes the (m,n) WIDS to support the fault-tolerant parallel wireless communication. On the basis that every adjacent sub-channel is in the same environment, the bit error rate of each sub-channel is assumed to be the same. After analyzing the (m,n) WIDS performance, and deriving 8 useful theorems, 3 methods are proposed to determine the optimal (m,n) WIDS with highest reliability in different cases.

1) When given the P_s & n, Algorithm 4.1 can determine the optimal m which (m,n) WIDS will achieve the optimal communication reliability. The optimal value of m depends on what region P_s belongs to. This algorithm reduces the computation complexity from $O(n)$ to $O(1)$.
2) When the information expansion ratio does not have an upper bound, the optimal WIDS uses all N sub-channels.
3) When u & N are given, a method is proposed to reduce the candidate WIDS set for the optimal (m,n) WIDS. This method can reduce the number of elements in the candidate WIDS set from $O(N^2)$ to $O(N)$.

It is reasonable to use fewer sub-channels, instead of all N sub-channels, if the designated performance can be achieved. This phenomenon is described and a method is given to choose the (m,n) WIDS which satisfies the performance requirement. The phenomenon can help choose the optimal (m,n) WIDS for fault tolerance.

APPENDIX

A. Proof of Theorem 3.1

For any m,n, the first order derivation of $R(m,n)$ on P_s is

$$R'(m,n) = C_m^n \cdot (1 - \sqrt[m]{P_s})^{n-m} > 0, \quad \text{for } 0 < P_s < 1.$$

B. Proof of Theorem 3.2

This theorem is proved by mathematical induction.

1) For $k = 1$,

$$R(m,n+1) = R(m,n) + C_{m-1}^n \cdot (\sqrt[m]{P \cdot S})^m \cdot (1 - \sqrt[m]{P \cdot S})^{n-m+1}.$$

Thus, $R(m,n) < R(m,n+1)$.

2) Assume this theorem holds for $k = t$. Now—Let $n' = n + t$ then $R(m,n) < R(m,n+t) = R(m,n') < R(m,n'+1)$. Therefore, $R(m,n) < R(m,n+t+1)$; the theorem also holds for $k = t+1$. By mathematical induction, $R(m,n) < R(m,n+1)$.

C. Proof of Theorem 3.3

Let $r(P_s) \equiv R(m,n) - R(m+1,n)$.

$$\begin{aligned} r(P_s) &= 1 - \Big[C_0^n \cdot (1 - \sqrt[m]{P_s})^n + C_1^n \cdot \sqrt[m]{P_s}(1 - \sqrt[m]{P_s})^{n-1} \\ &\quad + \cdots + C_{m-1}^n \cdot (\sqrt[m]{P_s})^{m-1} \cdot (1 - \sqrt[m]{P_s})^{n-m+1}\Big] \\ &\quad \times \Big[1 - \Big[C_0^n \cdot (1 - \sqrt[m+1]{P_s})^n + C_1^n \\ &\quad \cdot \sqrt[m+1]{P_s}(1 - \sqrt[m+1]{P_s})^{n-1} \\ &\quad + \cdots + C_m^n \cdot (\sqrt[m+1]{P_s})^m \cdot (1 - \sqrt[m+1]{P_s})^{n-m}\Big]\Big] \end{aligned}$$

It is known that:

$$\lim_{P_s \to 1^-} [\sqrt[m]{P_s}] = \lim_{P_s \to 1^-} [\sqrt[m+1]{P_s}] = 1;$$

$$\lim_{P_s \to 1^-} [(1 - \sqrt[m]{P_s})^k] = \lim_{P_s \to 1^-} [(1 - \sqrt[m+1]{P_s})^k] = 0, \quad \text{for } k \in N.$$

And because

$$(1 - \sqrt[m]{P_s}) > (1 - \sqrt[m+1]{P_s})$$

then

$$\lim_{P_s \to 1} \left[\frac{(1 - \sqrt[m]{P_s})^k}{(1 - \sqrt[m+1]{P_s})^{k'}}\right], \quad \forall k, k' \in N, \quad \text{and} \quad k > k'.$$

$$\lim_{P_s \to 1^-} \left[\frac{r(P_s)}{(1 - \sqrt[m+1]{P_s})^{n-m}}\right] = \lim \left[C_m^n \cdot (\sqrt[m+1]{P_s})^m\right] = C_m^n > 0.$$

Hence $r(P_s) > 0$, i.e., $R(m,n) > R(m+1,n)$ when $P_s \to 1$.

D. Proof of Theorem 3.4

Let $r(P_s) = R(m,n) - R(m+1,n)$, then

$$\begin{aligned} r(P_s) &= \Big[\Big(C_m^n \cdot (\sqrt[m]{P_s}\Big)^m \cdot (1 - \sqrt[m]{P_s})^{n-m} \\ &\quad + \Big(C_{m+1}^n \cdot (\sqrt[m]{P_s}\Big)^{m+1} \cdot (1 - \sqrt[m]{P_s})^{n-m-1} \end{aligned}$$

$$+\ldots+C_n^n\cdot(\sqrt[m]{P_s})^n\Big]$$
$$-\Big[\Big(C_{m+1}^n\cdot(\sqrt[m+1]{P_s}\Big)^{m+1}\cdot(1-\sqrt[m+1]{P_s})^{n-m-1}$$
$$+\Big(C_{m+2}^n\cdot(\sqrt[m+1]{P_s}\Big)^{m+2}\cdot(1-\sqrt[m+1]{P_s})^{n-m-2}$$
$$+\ldots+C_n^n\cdot(\sqrt[m+1]{P_s})^n)\Big].$$

It is known that

$$\lim_{P_s\to 0^+}[\sqrt[m]{P_s}]=\lim_{P_s\to 0^+}[\sqrt[m+1]{P_s}]=0$$

and

$$\lim_{P_s\to 0^+}[(1-\sqrt[m]{P_s})^k]=\lim_{P_s\to 0^+}[(1-\sqrt[m+1]{P_s})^k]=1,\quad \forall k\in N.$$

Thus,

$$\lim_{P_s\to 0^+}\left[\frac{r(P_s)}{(\sqrt[m]{P_s})^m}\right]=\lim_{P_s\to 0^+}\Big[C_m^n(1-\sqrt[m]{P_s})^{n-m}-C_{m+1}^n(1-\sqrt[m+1]{P_s})^{n-m+1}\Big]$$
$$=C_m^n-C_{m+1}^n=\frac{n!\cdot(2m-n+1)}{(m+1)!\cdot(n-m)!}.$$

If $2m-n+1>0$, then $C_m^n-C_{m+1}^n>0$.

Thus,

$$\lim_{P_s\to 0^+}\left[\frac{r(P_s)}{(\sqrt[m]{P_s})^m}\right]>0 \text{ if } \quad n>\eta_2;$$

and $R(\eta_2,n)$ is the optimal of $R(i,n)$ when $P_s\to 0+$, where $1\le i\le n$.

E. Proof of Lemma 3.5

1)

$$\lim_{p\to 1^-}[f(p)]=0,\quad \lim_{p\to 0^+}[f(p)]=1.$$

2)

$$f'(p)=\frac{a}{b}\cdot\left(\frac{1-\sqrt[b-1]{p}}{1-\sqrt[b]{p}}\right)^{a+1}\cdot p^{\frac{1}{b}-1}-\frac{a+1}{b-1}\cdot\left(\frac{1-\sqrt[b-1]{p}}{1-\sqrt[b]{p}}\right)^{a}\cdot p^{\frac{1}{b-1}-1};$$
$$\lim_{p\to 1^-}[f'(p)]=\frac{a}{b}\cdot\left(\frac{b}{b-1}\right)^{a+1}-\frac{a+1}{b-1}\cdot\left(\frac{b}{b-1}\right)^{a}=\left(\frac{b}{b-1}\right)^{a}\cdot\left(\frac{-1}{b-1}\right)<0;$$
$$\lim_{p\to 0^+}\left[\frac{f'(p)}{p^{\frac{1}{b}-1}}\right]=\frac{a}{b}-\left(\frac{a+1}{b-1}\right)\cdot p^{\frac{1}{b\cdot(b-1)}}=\frac{a}{b}>0.$$

Thus, $f(p)$ increases when $p\to 0^+$, and decreases when $p\to 1^-$.

3) Prove that there is only 1 P_j which satisfies $f'(p)=0$. Thus, solve $f'(p)=0$.

$$\frac{1-\sqrt[b-1]{p}}{1-\sqrt[b]{p}}\cdot\frac{1}{\sqrt[b-1]{p^{b\cdot(b-1)}}}=\frac{a+1}{b-1}\cdot\frac{b}{a}\cdot K\equiv\frac{a+1}{b-1}\cdot\frac{b}{a};\quad \text{then } K>1;$$
$$g(p)\equiv\frac{1+\sqrt[b-1]{b}}{1+\sqrt[b]{b}}\cdot\frac{1}{\sqrt[b-1]{p^{b\cdot(b-1)}}}.$$

Because

$$\lim_{p\to 1^-}[g(p)]=\frac{b}{b-1}>0,$$

and

$$\lim_{p\to 0^+}\left[\frac{g(p)}{\sqrt[b-1]{p^{b\cdot(b+1)}}}\right]=\frac{1-\sqrt[b-1]{p}}{1-\sqrt[b]{b}}=1>0.$$

Thus:

$$\lim_{p\to 0^+}[g(p)]\to\infty.$$
$$g'(p)=\frac{p^{-1-\frac{1}{b\cdot(b-1)}}}{b\cdot(b-1)\cdot(\sqrt[b]{p}-1)^2}\cdot[b\cdot\sqrt[b]{p}-b\cdot\sqrt[b-1]{p}+\sqrt[b-1]{p}-1].$$
$$h(p)\equiv b\cdot\sqrt[b]{p}-b\cdot\sqrt[b-1]{p}+\sqrt[b-1]{p}-1.$$

Because $h(0)=-1$ and $h(1)=0$, then

$$h'(p)=p^{\frac{1}{b}-1}-p^{\frac{1}{b-1}-1}=p^{-1}\cdot[\sqrt[b]{p}-\sqrt[b-1]{p}]>0.$$

Thus, $h(p)$ is an increasing function from -1 to 0 when $p\in(0,1)$; and $h(p)<0$ when $0<p<1$. Thus $g'(p)<0$ when $0<p<1$ when $0<p<1$.

Now, look at $g(p)$; it is a decreasing function from ∞ to $(b/b-1)$. Because $K>1$, then $g(p)=K$ has only one solution: $f'(p)=0$ has only one solution when $p=P_j$.

4) Thus, $f(p)$ increases when $0<p<P_j$, and then decreases when $P_i<p<1$.

F. Proof of Theorem 3.6

1) Let $r(P_s)\equiv R(m,n)-R(m+1,n), r(0)=0, r(1)=0$.

2)

$$r'(P_s)=C_m^n\cdot(1-\sqrt[m]{P_s})^{n-m}-C_{m+1}^n\cdot(1-\sqrt[m+1]{P_s})^{n-m-1};$$
$$\lim_{P_s\to 0^+}[r'(P_s)]=C_m^n-C_{m+1}^n\ge 0,$$

because $m\ge\eta_2$.

3) Now, prove that there is only 1 point which satisfies $r'(P_s)=0$.

$$r'(P_s)=C_m^n\cdot(1-\sqrt[m]{P_s})^{n-m}-C_{m+1}^n\cdot(1-\sqrt[m+1]{P_s})^{n-m-1};$$
$$\lim_{P_s\to 0^+}[r'(P_s)]=C_m^n-C_{m+1}^n\ge 0,\quad \text{because } m\ge\eta_2.$$

Let $m+1=b$ and $n-m-1=a$.

By Lemma 3.5, when $K<1$, there is only 1 solution for

$$f(p)=\frac{(1-\sqrt[b-1]{p})^{n+1}}{(1-\sqrt[b]{P})^n}=K.$$

Thus, there is at most 1 point which satisfies $r'(P_s)=0$.

Points 1, 2, and 3, show that the graph of $r(P_s)$ can be plotted. It increases from 0 to 1 local maximum, and then decreases from the local maximum to 0. Thus $r(P_s)$ is positive when $0<P_s<1$. And finally, $R(m,n)>R(m+1,n)$ when $m\ge\eta_2$.

G. Proof of Theorem 3.7

1) Let $r(P_s)=R(m,n)-R(m-1,n)$. It is known that $r(0)=0$ and $r(1)=0$.

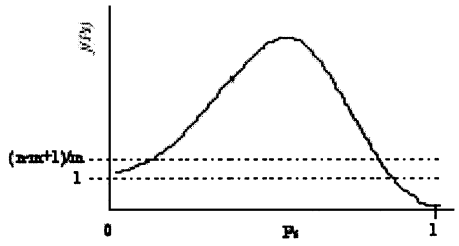

Fig. 10.

2) From Theorem 3.3: $R(m,n) > R(m+1,n)$ and $R(m-1,n) > R(m,n)$, when $P_s \to 1^-$; thus $\lim_{P_s\to 1^-}[r(P_s)] < 0$.
3) From Theorem 3.4:

$$\lim_{P_s\to 0^+}\left[\frac{r(P_s)}{(\sqrt[m]{P_s})^m}\right] = C_m^n - C_{m+1}^n > 0, \quad \text{if } m \le \eta_2.$$

4) Proof that there are at most 2 points which satisfy

$$r'(P_s) = C_m^n \cdot (1-\sqrt[m]{P_s})^{n-m} - C_{m-1}^n \cdot (1-\sqrt[m-1]{P_s})^{n-m-1} = 0.$$

First, show that

$$\lim_{P_s\to 1^-}(r'(P_s)) > 0:$$

$$\lim_{P_s\to 1^-}\left[\frac{r'(P_s)}{1-\sqrt[m]{P_s}}\right]^{n-m} = \lim_{P_s\to 1^-}\left[C_m^n - C_{m-1}^n\cdot\left(\frac{1-\sqrt[m-1]{P_s}}{1-\sqrt[m]{P_s}}\right)^{n-m}\cdot(1-\sqrt[m]{P_s})\right] = C_m^n > 0.$$

Then, show that

$$\lim_{P_s\to 1^+}[r'(P_s)] > 0:$$

$$\lim_{P_s\to 0^+}\left[\frac{r'(P_s)}{\sqrt[m-1]{P_s}}\right] = C_m^n - C_{m-1}^n > 0.$$

Let

$$f(P_s) = \frac{(1-\sqrt[m-1]{P_s})^{n-m+1}}{(1-\sqrt[m]{P_s})^{n-m}} = \frac{C_m^n}{C_{m-1}^n} = \frac{n-m+1}{m};$$

it is known that

$$\frac{n-m+1}{m} > 1 \quad \text{for } m \le \eta_2.$$

Lemma 3.5 shows that there exists a $P_s^* \in (0,1)$ such that $f(P_s)$ increases in $(0,P_s^*)$ and decreases in $(P_s^*,1)$. Also

$$\lim_{P_s\to 1^-}[f(P_s)] = 0, \quad \text{and}$$
$$\lim_{P_s\to 0^+}[f(P_s)] = 1.$$

Thus, there are 2 solutions for

$$f(P_s) = \frac{C_m^n}{C_{m-1}^n} = \frac{n-m+1}{m};$$

and 2 solutions for

$$r'(P_s) = 0.$$

Then, conclude that there are two solutions for $r'(P_s) = 0$, as shown in Fig. 10.

Finally, conclude that there is 1 point: $P_s = P_s^*$ ($P_s^* \neq 0$ and $P_s^* \neq 1$) which satisfies

$$r(P_s) = 0,$$
$$r(P_s) > 0 \quad \text{when } 0 < P_s < P_s^*,$$
$$r(P_s) < 0 \quad \text{when } P_s^* < P_s < 1.$$

H. Proof of Theorem 3.8

Let:

$$r_1(P_s) = R(m-1,n) - R(m,n); \quad r_1(P_s) = 0 \quad \text{when } P_s = P_{s_1}^*[(m-1,n),(m,n)].$$
$$r_2(P_s) = R(m,n) - R(m+1,n); \quad r_2(P_s) = 0 \quad \text{when } P_s = P_{s_2}^*[(m,n),(m+1,n)].$$

By Theorem 3.7, if

$$P_s > P_{s_1}^*[(m-1,n),(m,n)], \quad \text{then } R(m-1,n) > R(m,n);$$

otherwise (excluding the critical probability) $R(m-1,n) < R(m,n)$.

Similarly, if

$$P_s > P_{s_2}^*[(m,n),(m+1,n)], \quad \text{then } R(m,n) > R(m+1,n);$$

otherwise (excluding the critical probability) $R(m,n) < R(m+1,n)$.

Consider $P_{s_3}^*[(m-1,n),(m+1,n)]$, which is the probability when $R(m-1,n) = R(m+1,n)$. At the point

$$P_s = P_{s,3}^*[(m-1,n),(m+1,n)], r_1(P_s) = r_2(P_s).$$

Let

$$r_3(P_s) = R(m-1,n) - R(m+1,n) = r_1(P_s) + r_2(P_s).$$

Because $P_{s_3}[(m-1,n),(m+1,n)]$ satisfies

$$r_3(P_{s_3}^*) = r_1(P_{s_3}^*) + r_2(P_{s_3}^*) = 0,$$

the following results are: if $r_1(P_{s_3}^*) < 0$, then $r_2(P_{s_3}^*) > 0$, else, if $r_1(P_{s_3}^*) > 0$, then $r_2(P_{s_3}^*) < 0$.

Thus, $P_{s_3}^*[(m-1,n),(m+1,n)]$ should be between $P_{s,2}^*[(m,n),(m+1,n)]$ and $P_{s,1}^*[(m-1,n),(m,n)]$.

Now, observe $R(m+1,n)$ and $R(m-1,n)$:

$$R(m,n) = C_m^n\cdot(\sqrt[m]{P_s})^m\cdot(1-\sqrt[m]{P_s})^{n-m} + C_{m+1}^n\cdot(\sqrt[m]{P_s})^{m+1}\cdot(1-\sqrt[m]{P_s})^{n-m+1} + \cdots + C_{n-1}^n\cdot(\sqrt[m]{P_s})^{n-1}\cdot(1-\sqrt[m]{P_s}) + C_n^n\cdot(\sqrt[m]{P_s})^n,$$

$$R(m+1,n) = C_{m+1}^n\cdot(\sqrt[m+1]{P_s})^{m+1}\cdot(1-\sqrt[m+1]{P_s})^{n-m-1} + \cdots + C_{n-1}^n\cdot(\sqrt[m+1]{P_s})^{n-1}\cdot(1-\sqrt[m+1]{P_s}) + C_n^n\cdot(\sqrt[m+1]{P_s})^n,$$

$$R(m-1,n) = C_{m-1}^n\cdot(\sqrt[m-1]{P_s})^{m-1}\cdot(1-\sqrt[m-1]{P_s})^{n-m+1} + \cdots + C_{n-1}^n\cdot(\sqrt[m-1]{P_s})^{n-1}\cdot(1-\sqrt[m-1]{P_s}) + C_n^n\cdot(\sqrt[m-1]{P_s})^n.$$

$r_1(P_s)$ has a positive term $C_{m-1}^n\cdot\sqrt[m-1]{P_s}\cdot(1-\sqrt[m-1]{P_s})^{n-m+1}$ but $r_3(P_s)$ has 2 positive terms $C_{m-1}^n\cdot\sqrt[m-1]{P_s}^{m-1}\cdot(1-\sqrt[m-1]{P_s})^{n-m+1}$ and $C_m^n\cdot\sqrt[m]{P_s}^m\cdot(1-\sqrt[m]{P_s})^{n-m}$.

TABLE II
$Q10^{14}$ FOR $n = 10 - 84$

N	ratio = 2	N	ratio = 2
2	0.999999	44	0.170
3	0.999918	45	0.145
4	0.999912	46	0.139
5	0.999576	47	0.121
6	0.999511	48	0.118
7	0.997415	49	0.0974
8	0.997146	50	0.0930
9	0.991069	51	0.0787
10	0.990409	52	0.0781
11	0.978	53	0.0625
12	0.976	54	0.0584
13	0.957	55	0.0478
14	0.955	56	0.0452
15	0.926	57	0.0390
16	0.925	58	0.0366
17	0.885	59	0.0312
18	0.883	60	0.0293
19	0.838	61	0.0245
20	0.831	62	0.0228
21	0.784	63	0.0195
22	0.776	64	0.0179
23	0.726	65	0.0152
24	0.713	66	0.0140
25	0.657	67	0.0107
26	0.647	68	0.0103
27	0.589	69	0.0097
28	0.584	70	0.0069
29	0.525	71	0.0063
30	0.521	72	0.0054
31	0.463	73	0.00537
32	0.458	74	0.00454
33	0.403	75	0.0039
34	0.394	76	0.0033
35	0.351	77	0.00266
36	0.345	78	0.0028
37	0.296	79	0.00199
38	0.296	80	0.00191
39	0.216	81	0.00157
40	0.235	82	0.00141
41	0.215	83	0.00103
42	0.206	84	0.00098
43	0.176		

To make $r_3(P^*_{s,3}) = 0$, then $P^*_{s,3}$ should move toward the advantageous direction: the smaller side. Thus,

$$P^*_{s,3}[(m-1,n),(m+1,n)] < P^*_{s,1}[(m-1,n),(m,n)].$$

Since

$$P^*_{s,3}[(m-1,n),(m+1,n)] \text{falls between } P^*_{s,2}[(m,n),(m+1,n)] \quad \text{and} P^*_{s,1}[(m-1,n),(m,n)],$$

it follows that

$$P^*_{s_2}[(m,n),(m+1,n)] < P^*_{s,3}[(m-1,n),(m+1,n)] < P^*_{s,1}[(m-1,n),(m,n)].$$

I. Tables I and II

The results in Tables I and II are derived using Mathematica (a useful mathematics tool). Mathematica has its limitation in number precision. Because the precision bound of Mathematica is 10^{-14}, the intersection, $P^*_s[(m,n),(m-1,n)]$ is not listed here when $R(m,n) > 1 - 10^{-14}$ (because the estimation can not be obtained using this simulation). In [5], the sub-channels' number used in parallel communication is 84. (Note: There is no intersection when $n = 1, 2, 3$.)

REFERENCES

[1] W. A. Burkhard, K. C. Claffy, and T. J. E. Schwarz, "Performance of balanced disk array schemes," in *Eleventh IEEE Symp. Mass Storage Systems*, 1991, pp. 45–50.

[2] L. Gargono, A. A. Rescigno, and U. Vaccaro, "Fault-tolerant hypercube broadcasting via information dispersal," *Networks*, vol. 23, pp. 271–282, 1993.

[3] R. W. Hamming, *Coding and Information Theory*: Prentice-Hall, 1986.

[4] Y. D. Lyuu, "Fast fault-tolerant parallel communication for de Bruijn and digit-exchange networks using information dispersal," *Networks*, vol. 23, pp. 365–378, 1993.

[5] M. J. de Ridder-de Groote and R. Parsad, "Analysis of new methods for broadcasting digital data to mobile terminals over an FM-channel," *IEEE Trans. Broadcast.*, vol. 40, pp. 29–37, 1994.

[6] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, pp. 335–348, 1989.

[7] T. Sato, M. Kawabe, T. Kato, and A. Fukasawa, "Throughput analysis method for hybrid ARQ schemes over burst error channels," *IEEE Trans. Vehicular Technol.*, vol. 42, pp. 110–118, 1993.

[8] P. Sweeney, *Error Control Coding: An Introduction*: Prentice-Hall, 1991.

[9] H. M. Sun and S. P. Shieh, "Optimal information dispersal for increasing reliability of a distributed service," *IEEE Trans. Rel.*, vol. 46, pp. 462–472, 1998.

[10] L. P. Wilbur, G. C. Henri, and R. A. Nelson, *Satellite Communication Systems Engineering*: Prentice-Hall, 1993.

Shiuh-Pyng Shieh received the M.S. in 1986 and the Ph.D. in 1991 in Electrical and Computer Engineering from the University of Maryland, College Park. He is a Professor and the Chair'n of the Department of Computer Science and Information Engineering, National Chiao Tung University; the Vice Chair'n of the board of Chinese Cryptology and Information Security Association; and director of Cisco Internetworking Technology Lab. From 1988 to 1991, he participated in the design and implementation of the B2 Secure XENIX for IBM, Federal Sector Division, Gaithersburg USA. He is also the designer of SNP (Secure Network Protocols), a very popular security shareware on the Internet. He has consulted in network security and distributed operating systems for many institutes, such as Industrial Technology Research Institute, and National Security Bureau, Taiwan. Dr. Shieh was on the organizing committees of numerous conferences, and is an editor of the *J. Computer Security*, and *J. Information Science and Engineering*. He has received two outstanding research awards, honored by National Chiao Tung University and Executive Yuan of Taiwan. His research interests include internetworking, distributed systems, and network security.

Yea-Ching Tsai received the M.S. in 1996 in Computer Science and Information Engineering from National Chiao Tung University, Taiwan. Her research interests include distributed systems and fault-tolerant schemes. She is a member of the Phi Tau Phi Society.

Yu-Lun Huang received the B.S. in 1995 and the Ph.D. in 2001 in Computer Science and Information Engineering from National Chiao Tung University, Taiwan. She is the Senior Engineer of Ambit Microsystems Corp. Her research interests include electronic commerce, distributed systems, quality of services, and network security. She is a member of the Phi Tau Phi Society.