안전한 전송을 위한 MRNS (Mixed Radix Number System) 네트워크에서의 비밀 다중 경로의 설계

김 성 열† · 정 일 용††

요 약

경로보안은 데이타의 전송을 위해 선택된 경로의 비밀성에 관한 것이다. 만일 경로의 일부분이라도 알려진다면 이 경로를 통해 전달된 데이타가 유출될 확률은 크다. 이런 이유때문에 데이타의 전송경로는 보호되어야 하며 이를 위해 우리는 한 개의 중간노드를 비밀리 선택하여 기존의 최단 거리를 이용하여 데이타를 전송하는 방법을 선택하지 않고 이 중간 노드를 이용하여 데이타를 전송한다.

더 나아가 우리가 여러 개의 비밀경로를 이용한다면 한 개의 경로에 모든 데이타를 보내는 대신에 각 경로에 partial 데이타를 보낼 수 있기 때문에 데이타의 보안은 좀 더 강해진다. 이러한 아이디어를 실현하기 위해 데이타는 정보분산 방법을 이용하여 여러개의 partial 데이타로 나누어진다. 본 논문에서는 위에서 제시한 아이디어를 MRNS 네트워크상에서 구현한다.

The Design of Secret Multi-Paths on MRNS(Mixed Radix Number System) Network for Secure Transmission

Seong Yeol Kim† · Il Yong Chung††

ABSTRACT

Routing security is the confidentiality of a route taken by the data transmitted over communication networks. If the route is detected by an adversary, the probability is high that the data are lost or the data can be intercepted by the adversary. Therefore, the route must be protected. To accomplish this, we select an intermediate node secretly and transmit the data using this intermediate node, instead of sending the data to a destination node using the shortest direct path.

Furthermore, if we use a number of secret routes from a starting node to a destination node, data security is much stronger since we can transmit partial data rather than entire data along a secret route. Finally, the idea above is implemented on MRNS Network.

1. Introduction

When we transmit the data in a distributed network, we must consider routing security[1]. Routing security is the security of the route taken by the data transmitted over the network. If the route is detected by the adversary, the probability is high that the data are lost or the data can be intercepted by the adversary.

※본 논문은 1995년도 조선대학교 학술연구비의 지원을 받아 연구되었음

† 준 회 원:조선대학교 전자계산학과 박사과정
†† 종신회원:조선대학교 전자계산학과 조교수

논문접수:1995년 9월 23일, 심사완료:1996년 1월 12일

Therefore, the route must be protected. To accomplish this, we select an intermediate node secretly and transmit the data using this intermediate node, instead of sending the data to the destination node using the shortest direct path. The above route consisting of two paths-the first path from the source node to the intermediate node and the second path from that intermediate node to the destination node, is called a secret route. Furthermore, if we use a number of secret routes from the starting node to the destination node, data security is much stronger since we can transmit partial data rather than the entire data along a secret route. To employ the above idea, the data is dispersed into n packets by the DAF(Dispersal Algorithm using the FFT algorithm)[2]. Then, each packet is transmitted simultaneously to the destination along its own secret route in the n-dimensional MRNS network. For this routing, we must find these n secret routes from the starting node to the destination node. Also, all the packets should arrive at the destination in the minimum possible time. Therefore, each secret route should be disjoint from all other secret routes.

Finding a set of disjoint paths in a general network is a computationally difficult problem[3]. However, researchers have proved that there exist sets of disjoint paths in specific kinds of networks. From these proofs, they have designed combinatorial algorithms for finding a set of disjoint paths. Unfortunately, these combinatorial algorithms require much time for obtaining these paths. Some approaches have been tried to reduce the time complexity for these algorithms. Rabin[4] has applied an error-correcting code method to the parallel routing algorithms for the hypercube network. Rabin's algorithm employs an (n x n) Hadamard matrix, every two different rows of which differ in exactly n/2 positions. This algorithm is central to the current studies in Routing security and we continue his work below.

We have two methods for designing n secret paths from the starting node to the intermediate nodes. One of them is to select the intermediate nodes secretly, and then to find the disjoint paths from the starting node to the intermediate nodes. The other is to make the disjoint paths secretly and then to randomly select the nodes on these paths as the intermediate nodes. Since these paths are made secretly and the nodes on these paths are selected randomly, each node in this network is chosen secretly. Rabin's algorithm follows the first method. Valiant's algorithm[5], which involves finding one secret path, may be adopted to yield an example of the second method. Our method, as yet unexplained, is designed based on the second method.

We propose an alternative algebraic method for secret routing on the MRNS(Mixed Radix Number System) network[6]. For the first part of the secret routes from the source node to intermediate nodes, our method is to transform a set of vertex-disjoint paths into disjoint sets and then to investigate these disjoint sets. Later, these sets with some constraints are used to construct a special class of matrices, where each set is used as an element of a matrix. We construct a special latin square called as HCLS (Hamiltonian Circuit Latin Square)[7](see Appendix), which belongs to the MMGSP(Modified Matrix for Generating Secret Paths)(see Appendix), from which the first part of the secret routes are designed. For the second part of the secret routes from these intermediate nodes to the destination node, the PLS(Partial Latin Square)[8](see Appendix) is employed. The reader is referred to [8] for extensive discussion of latin squares and their applications.

This paper is organized of the following three sections. Section 2 describes what MRNS network is. Section 3 gives an application of this matrix to the secret routing algorithm for the MRNS network. Finally, concluding remarks appear in Section 4.

2. Description of the MRNS Network

The MRNS network is constructed from the mixed radix number system(MRNS). The routing algorithms

of the MRNS network are similar to those of the hypercube network[9]-[12]. Each algorithm is composed of two phases. The first phase is to transmit the packet to a randomly chosen intermediate node through the secret route. The second phase is to send the packet from this intermediate node to the destination node along the secret path. This section provides the definition of the MRNS, gives a description of the MRNS network, and presents two routing algorithms of the MRNS network.

2.1 A Mixed Radix Number System(MRNS)

Let N be the total number of nodes of the MRNS network and let N be represented as a product of m_i's, $m_i \rangle 1$ for $0\ i\ n-1$.

$$N = m_{n-1} * m_{n-2} * \cdots * m_1 * m_0$$

Then, each node u between 0 and $N-1$ can be represented as an n-tuple $(u_{n-1}\, u_{n-2} \cdots u_1\, u_0)$ for $0 \le u_i \le (m_i-1)$. Associated with each u_i is a weight w_i, such that

$$u = \sum_{i=0}^{n-1} u_i * w_i \text{ and } w_i = \prod_{j=0}^{i-1} = m_{i-1} * m_{i-2} \cdots m_0,\ w_0 = 1$$

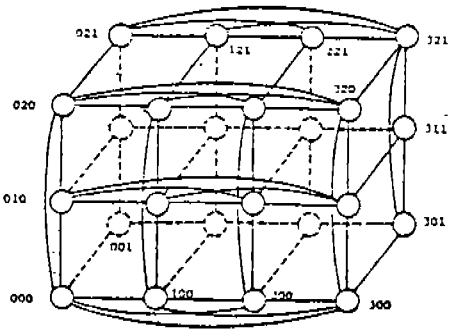
Example 1: For N=24, mi and wi can be computed as follows.

$24 = 4 * 3 * 2$.

$m_0 = 2,\ m_1 = 3,\ m_2 = 4$

$w_0 = 1,\ w_1 = 2,\ w_2 = 6$.

Then, $u = (u_2\, u_1\, u_0),\ 0 \le u_0\ 1,\ 0 \le u_1 \le 2,\ 0 \le u_2\ 3$ for any u in the rang $0\text{-}23.0_{10} = (000),\ 23_{10} = (321)$ in this mixed number system. Any node can be described in this system between (000) and (321). Node (000) is directly connected to nodes (001), (010), (020), (100), (200) and (300) as shown in Fig. 1. For the sake of clarity, connection is not completed in this figure shown by dotted lines.



(Fig. 1) 4*3*2 MIRNS Network

2.2 Structure of the MRNS Network

Each node $u = (u_{n-1}\, u_{n-2} \cdots u_i \cdots u_1)$ is connected to nodes $(u_{n-1}\, u_{n-2} \cdots u'_i \cdots u_1)$ for all $1 \le i \le n$, where u'_i can be any integer from $\{0, 1, \cdots, m_i-1\}$ except u_i itself. Given n-dimensions with m_i number of nodes in the i^{th} dimension, the following facts are described.

(1) The total number of links per node is $l = \sum_{i=0}^{n-1} (m_i-1)$.

(2) The total number of links in the MRNS network is $N/2 * l$ where N is the total number of nodes.

(3) Each dimension is constructed as a complete graph. This means that for the i^{th} dimension, the total number of vertices is mi and the total number of links is $m_i * (m_i-1)/2$. Then, the link(p, q) is represented as (i, j), where $j = \sum_{k=0}^{p-1} (m_i-k-1) + (q-p)$, $p \langle q,\ p, q \in Z_{m_i}$.

(4) The n-dimensional MRNS is a connected graph of diameter n.

Now, we examine the flexibility of designing the MRNS network. Given N nodes(N ≠ prime number), more than one kind of MRNS network can be designed based on considerations such as the dynamic security, the volume of data to be transmitted, and the cost of the hardware. If the network is more secure and has a large volume of data, then the network can be constructed with more links. However, the cost for constructing the network is a primary consideration, so the network should be designed with

as few links as possible.

Example 2: Given 24 nodes, four kinds of MRNS networks, NK_1, NK_2, NK_3, and NK_4 can be designed.

$NK_1 = Z_2 \times Z_{12}$
$NK_2 = Z_3 \times Z_8$
$NK_3 = Z_4 \times Z_6$
$NK_4 = Z_2 \times Z_3 \times Z_4$

From 2. 2-(2), the total number of links are 144, 108, 96, 72 for NK_1, NK_2, NK_3, NK_4, respectively.

3. The Design of A Secret Routing Algorithm on the MRNS Network

The routing algorithms of the MRNS network are similar to those of the hypercube network. For the MRNS network, the number of channels is determined by the modular number for each dimension, while the modular number of each dimension in the hypercube network is always 2. Considering the structure of the MRNS network, the following two propositions are described and proven in [13].

Proposition 1: Let A and B be any two nodes in the MRNS network and assume that $H(A, B)[12] < n$. Then there are H(A, B) parallel paths of length H(A, B) between the nodes A and B.

Proposition 2: Let A and B be any two nodes of an n-dimensional MRNS network and assume that $H(A, B) < n$. Then there are ℓ parallel paths between A and B, where $\ell = \sum_{i=0}^{n-1} (m_i - 1)$. The length of each path is at most $H(A, B) + 2$.

For the design of secret routing algorithm, we describe the special matrices called the HCLS (Hamiltonian Circuit Latin Square).

Definition 1: The HCLS is constructed as follows: Given distinct n points, a Hamiltonian circuit $a_0\ a_1 \cdots a_{n-2}\ a_{n-1}\ a_0$ is randomly selected. On the circuit each row of the matrix obtained from the Hamiltonian path, starting at any position $a_j (0 \le j \le n-1)$, under the condition that no two rows begin at the same position. If a Hamiltonian path is ak $a_{k+1}, \ldots, a_{k-1}$, then the row obtained from it is $[a_k\ a_{k+1} \cdots a_{k-1}]$

Given an n-dimensional MRNS network, the following routing algorithm describes how to construct ℓ secret routes. The structure of each dimension is described as a complete graph of given nodes. The ℓ secret paths of the MRNS network are more secure than those of the hypercube network, since the choice of the link at each dimension in the MRNS network is flexible.

SR_MRNS Algorithm

cobegin

1) Split Px into ℓ packets $P_{x0}, P_{x1}, \cdots, P_{x(\ell-1)}$, P_x is the data at node x.
2) Randomly choose a sequence from the n! permutations of $\langle 0, 1, 2, \cdots, n-1 \rangle$.
3) Design an (n x n) HCLS, and construct the (n x (n−1)) matrix by randomly choosing (n−1) columns of the HCLS.
4) Design an (ℓ x (n−1)) matrix by randomly choose a set k1 of links from the set of all possible links the current node is connected to, $|k_i| = (n-1)$ and select k_2 for the length of each path, $k_2 \in \{1, 2, \cdots, n-1\}$.
5) Using the (ℓ x (n−1)) matrix described and k_2, construct pairwise vertex-disjoint paths $D_0, D_1, \cdots, D_{\ell-1}$ from x to $R_0, R_1, \cdots R_{\ell-1}$, respectively, each length is at most (n−1).
6) Construct a set of different bit positions of R_i and $\pi(x)$ for the i^{th} packet, $0 \le i \le \ell - 1$.
7) Randomly choose a sequence from the n! permutations of $\langle 0, 1, 2, \cdots, n-1 \rangle$ and design an (n x n) HCLS.
8) From Steps 6) and 7), we design the (ℓ x (n +1)) matrix PLS(see Definition 4 in Appendix), and then make dynamical edge-disjoint paths E_0,

$E_1, \cdots, E_{\ell-1}$ from R_0, R_1, $R_{\ell-1}$, respectively, to the destination node $\pi(x)$. Each path E_i has length $\leq n+1$.

9) Attach the i^{th} routing path E_i to (P_{xi}, D_i)

coend.

The Algorithm presented above describes how to construct ℓ parallel routes for the n-dimensional MRNS network, where $\ell = \sum_{i=0}^{n-1} (m_i - 1)$. Unlike other algorithms, this algorithm uses the HCLS to make partitions, each consisting of secret paths. Paths belonging to the same partition utilize the same dimensions at fixed times for the packets, if necessary. Since the source node has ℓ channels, the data is dispersed into ℓ packets and all packets of the data are transmitted to the neighboring nodes. These ℓ channels are determined by two factors-the dimension that the HCLS assigns to each partition, and the link of each dimension that each partition assigns to the packet. By considering the structure of each dimension in the MRNS network, Proposition 1 and Proposition 2, the second part of the route is determined. To construct disjoint paths in each partition, we use the property of the MMGSP. But it is hard to check that each element(which represents a link) in the MMGSP is distinct from all other elements. Instead of examining all the elements, we just look at the element in the first and last columns. For the first phase of the route, suppose that all the elements in the first column are distinct. Then, the paths represented by the rows of the matrix, will be disjoint, even if the elements in all columns other than the first are the same. For the second phase of the route, if two elements in the last column are the same, change one of the elements in the first column(in the same row as one of the elements in the last column), and compensate for this by adding an extra step at the end of that path.

The following example will provide a better understanding of the Algorithm described above.

Example 3: Let x=(0000) and $\pi(x)=(1100)$, and let m_i $(0 \leq i \leq 2)$ be 3. The MRNS network is Z_3 x Z_3 x Z_3 x Z_3. The total number of nodes $N=3^4$, and the total number of links ℓ per node is 8. Then, SR_MRNS Algorithm is executed as follows:

(1) Following the first step of the Algorithm, the data at node x is dispersed into ℓ packets using the DAF.

(2) Steps (2) and (3) of the Algorithm requires the design of a (4 x 4) HCLS, which is described as follows: According to Definition 1, the Hamiltonian circuit $(2 \rightarrow 1 \rightarrow 3 \rightarrow 0 \rightarrow 2)$ is randomly selected among 4! Hamiltonian circuit. Then, the first, second, third and fourth rows are obtained from four hamiltonian paths, starting at the first, second, third and fourth positions, respectively. Using the HCLS designed, construct the matrix by randomly selecting three columns of the HCLS.

the HCLS (4 x 3) matrix

$$\begin{bmatrix} 2 & 1 & 3 & 0 \\ 1 & 3 & 0 & 2 \\ 3 & 0 & 2 & 1 \\ 0 & 2 & 1 & 3 \end{bmatrix} \qquad \begin{bmatrix} 2 & 1 & 3 \\ 1 & 3 & 0 \\ 3 & 0 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

In Step (4), construct the (8 x 3) rectangular matrix by choosing {1, 2, 1}, {2, 2, 2}, {1, 1, 2}, {2, 2, 1}, {1, 2, 2}, {2, 2, 1}, {1, 1, 2}, {2, 2, 1} for a set of eight links and choose 1, 2, 3, 2, 3, 2, 2, 1 for the lengths of eight paths, respectively.

(8 x 3) matrix

$$\begin{bmatrix} (2,1) & (1,2) & (3,1) \\ (2,2) & (1,1) & (3,2) \\ (1,1) & (3,1) & (0,2) \\ (1,2) & (3,2) & (0,1) \\ (3,1) & (0,2) & (2,2) \\ (3,2) & (0,1) & (2,1) \\ (0,1) & (2,1) & (1,2) \\ (0,2) & (2,2) & (1,1) \end{bmatrix}$$

(3) According to Step (5), construct pairwise vertex-disjoint paths $D_0, D_1, \cdots, D_7$ from x to R_0, R_1, R_7, respectively.

D_0 : (0000) (0100) : ((2, 1))
D_1 : (0000) (0200) (0210) : ((2, 2) (1, 1))
D_2 : (0000) (0010) (1010) (1012) : ((1, 1) (3, 1) (0, 2))
D_3 : (0000) (0020) (2020) : ((1, 2) (3, 2))
D_4 : (0000) (1000) (1002) (1202) : ((3, 1) (0, 2) (2, 2))
D_5 : (0000) (2000) (2001) : ((3, 2) (0, 1))
D_6 : (0000) (0001) (0101) : ((0, 1) (2, 1))
D_7 : (0000) (0002) : ((0,2))

For synchronization, we add $((n-1)-|D_i|)$ s's to the end of P_{xi}, $0 \le i \le 7$.

D_1 : ((2, 1) s s)
D_0 : ((2, 2) (1, 1) s)
D_3 : ((1, 1) (3, 1) (0, 2))
D_4 : ((1, 2) (3, 2) s)
D_5 : ((3, 1) (0, 2) (2, 2))
D_6 : ((3, 2) (0, 1) s)
D_7 : ((0, 1) (2, 1) s)
D_8 : ((0, 2) s s)

(4) In Step (6), the different position sets between R_i and (1100) for the i^{th} packet, $0 \le i \le \ell - 1$ are computed.

E_0 : (0100) → (1100) : diff. position = ((3, 1))
E_1 : (0210) (1100) : diff. positions = ((1, 1), (2, 3), (3, 1))
E_2 : (1012) (1100) : diff. positions = ((0, 2), (1, 2), (2, 1))
E_3 : (2020) (1100) : diff. positions = ((1, 2), (2, 1), (3, 3))
E_4 : (1202) (1100) : diff. positions = ((0, 2), (2, 3))
E_5 : (2001) (1100) : diff. positions = ((0, 1), (2, 1), (3, 3))
E_6 : (0101) (1100) : diff. positions = ((0, 1), (3, 1))
E_7 : (0002) (1100) : diff. positions = ((0, 2), (2, 1), (3, 1))

(5) In Step 7, select a sequence (0 3 1 2) and construct (4 x 4) HCLS.

$$\begin{bmatrix} 0 & 3 & 1 & 2 \\ 3 & 1 & 2 & 0 \\ 1 & 2 & 0 & 3 \\ 2 & 0 & 3 & 1 \end{bmatrix}$$

(6) Design the (8 x 5) rectangular matrix, which belongs to the MMGSP(Modified Matrix for Generating Secret Paths) defined in Appendix.

$$\begin{bmatrix} s & (3,1) & s & s & s \\ (0,1) & (3,1) & (1,1) & (2,3) & (0,1) \\ s & (1,2) & (2,1) & (0,2) & s \\ (3,3) & (1,2) & (2,1) & s & s \\ s & (2,3) & (0,2) & s & s \\ s & (2,1) & (0,1) & (3,3) & s \\ s & (0,1) & (3,1) & s & s \\ (2,1) & (0,2) & (3,1) & s & s \end{bmatrix}$$

(7) Attach the i^{th} routing path E_i to (P_{xi}, D_i).

(P_{x0}, (2, 1) s s s (3, 1) s s s)
(P_{x1}, (2, 2) (1, 1) s (0, 1) (3, 1) (1, 1) (2, 3) (0, 1))
(P_{x2}, (1, 1) (3, 1) (0, 2) s (1, 2) (2, 1) (0, 2) s)
(P_{x3}, (1, 2) (3, 2) s (3, 3) (1, 2) (2, 1) s s)
(P_{x4}, (3, 1) (0, 2) s s (2, 3) (0, 2) s s)
(P_{x5}, (3, 2) (0, 1) s s (2, 1) (0, 1) (3, 3) s)
(P_{x6}, (0, 1) (2, 1) s s (0, 1) (3, 1) s s)
(P_{x7}, (0, 2) s s (2, 1) (0, 2) (3, 1) s s)

4. Conclusion

This paper presents parallel communication and a secret routing algorithm in the MRNS(Mixed Radix Number System) network. Two topics are involved in this paper-parallelism and data security. For the aspect of parallelism, we construct a set of vertex-disjoint paths in the MRNS network employing the special matrices. Our algorithm for constructing n parallel paths in the n-dimensional MRNS network requires only O(n) for the time complexity, while other algorithms, such as Rabin's Routing Algorithm, need more than O(n). For the aspect of data security, this paper introduces the topic of Routing security. Routing security is the security of the route taken by the data transmitted over the network. If the route is detected by the adversary, the probability is high that the data will be intercepted. In order to receive the

data safely at the destination node, the route must be protected. To accomplish this, we select the intermediate nodes secretly and transmit the data via these intermediate nodes to the destination node.

Important extensions of this research would involve constructing secret routes in other network models, and investigating the entropy of secret routings.

REFERENCES

[1] Seberry, J. and Pirprzyk, J., *An Introduction to Computer Security*. Prentice Hall, Englewood Cliffs, NJ,1989

[2] Chung, I., "The Design of the Dispersal Algorithm Using the FFT Algorithm(DAF) for Reliable and Secure Communications," *Proc. Information Security and Cryptology*, WISC, pp. 167-180, 1992

[3] Knuth, D. E., *The Art of Computer Programming, Vol 1: Fundamental Algorithms*. Addison-Wesley, Reading, MA, 1983

[4] Rabin, M. O., "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance," *J. ACM*, vol. 36, no. 2, pp. 335-348, Apr. 1989

[5] Valiant, L. G., "A Scheme for Fast Parallel Communication," *SIAM J. Comput.*, vol. 11, no. 2, pp. 350-361, May 1982

[6] Bhuyan, L. N., and Agrawal, D. P., "Generalized Hypercube and Hyperbus Structures for a Computer Network," *IEEE Trans. Comput.*, vol. 33, no. 4, pp. 323-333, Apr. 1984

[7] Chung, Ilyong, "Application of the Special Latin Squares to the Parallel Routing Algorithm on Hypercube, Parallel Routing Algorithm on Hypercube," *J. Korea Info. Sci.*, vol. 19, no. 5, pp. 569-578, Sep. 1992

[8] Denes, J. and Keedwell, A. D., *Latin Squares and Their Applications*. Academic Press, New York, 1974

[9] Saad, Y., and Schultz, M. H., "Topological Properties of Hypercubes," *IEEE Trans. Comput.*, vol. 37, no. 7, pp. 867-872, July 1988

[10] Ibarra, O. H., and Sohn, S. T., "On Mapping Systolic Algorithm onto the Hypercube," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 1, pp. 48-63, Jan. 1990

[11] Wu, A. Y., "Embedding of Tree Networks into Hypercubes," J. *Parallel Distrib. Comput.*, vol. 2, pp. 238-249, 1985

[12] Johnsson, S. L., and Ho, C. -T., "Optimum Broadcasting and Personalized Communication in Hypercube," *IEEE Trans. Comput.*, vol. 38, no. 9, pp. 1249-1268, Sep. 1989

[13] 최완규, 정일용, "MRNS 네트워크에서 특수한 메트릭스를 응용한 병렬 경로 배정 알고리즘의 설계", 정보처리논문지, 제3권, 제1호, pp. 55-62, 1996. 1.

Appendix

Definition 1: Call the matrix M^1 as the MMGSP (Modified Matrix for Generating Secret Paths), no two entries in this matrix are the same. This matrix thus satisfied the following conditions.

i) $M^1=[U_{i,j}]$, $U_{i,j}\subset\{Z_n+s^m\}$ $\{0\le i\le n-1, 0\le j\le n-2, 0\le m\}$, and where's'
means: "stay at the current node".

ii) $|U_{i,j}|=j+1$

iii) $U_{i,j}\neq U_{k,j}$, if $i\neq k$

iv) $U_{i,j}\subset U_{i,j+1}$

v) $U_{i,j+1}=U_{i,j}+\{s\}$, if $s\in U_{i,j}$

Definition 2: Let F be masking function and M^2 be a $(n\times n)$ latin square, where

$M^2=[u_{i,j}]; u_{i,j}\in Z_n,\ 0\le i,j\le n-1.$

$$F_{r_0,r_1,\ldots,r_{n-1}}(u_{i,j})=\begin{cases} u_{i,j}, \text{ if } u_{i,j}\in r_i,\ r_i\subset Z_n \\ s, \quad \text{otherwise}\end{cases}$$

Definition 3: An $(n \times n)$ array such that in some subset of the n^2 cells of the array each one of the cells is occupied by an integer, from the set $0, 1, 2, \cdots, n-1$, and such that no integer from $0, 1, 2, \cdots, n-1$ occurs in any row or column more than once.

The Partial Latin Square(PLS) is constructed according to Definition 3 employing the masking function specified in Definition 2.

Definition 4: Given the $(n \times n)$ LS M^2 and r_i denoting the set of different bit positions between the ith intermediate node and the destination node, this matrix is transformed into partial latin square by the masking function, then this transformed matrix is called the PLS.

김 성 열

1994년 조선대학교 전자계산학과 졸업(학사)
1996년 조선대학교 대학원 전자계산학과 졸업(석사)
1996년~현재 조선대학교 대학원 전자계산학과 박사과정
관심분야: 정보통신, 분산 시스템, 정보보안, 데이터베이스

정 일 용

1983년 한양대학교 공과대학 졸업(학사)
1987년 미국 City University of New York 전산학과(석사)
1991년 미국 City University of New York 전산학과(박사)
1991년~1994년 한국전자통신연구소 선임연구원
1994년~현재 조선대학교 전자계산학과 조교수
관심분야: 컴퓨터 네트워크, 분산 및 병렬 시스템, 망 보안시스템