Raport Badawczy

Research Report

RB/16/2007

Double ring with redundant nodes – a model of highly reliable ring network

J. Malinowski

Instytut Badań Systemowych
Polska Akademia Nauk

Systems Research Institute
Polish Academy of Sciences

POLSKA AKADEMIA NAUK

Instytut Badań Systemowych

ul. Newelska 6

01-447 Warszawa

tel.: (+48) (22) 3810100

fax: (+48) (22) 3810105

Kierownik Pracowni zgłaszający pracę:
Prof. dr hab. inż. Olgierd Hryniewicz

Warszawa 2007

DOUBLE RING WITH REDUNDANT NODES – A MODEL OF HIGHLY RELIABLE RING NETWORK

Jacek Malinowski

Abstract

A concept of a computer network having the structure of a double-ring with redundant nodes is presented. The network is built of cyclically connected modules, each one consisting of two nodes (concentrators). One of the nodes is redundant and continues to operate after the other node fails (hot redundancy). Each node is directly connected to both nodes of the preceding and the succeeding modules while each station (computer) is connected to both nodes of one module. A module is assumed to be operable if one of its nodes is functioning. Redundant nodes ensure high reliability of the network.

A communication protocol adjusted to the network's specific structure is developed. It is based on the token-passing mechanism. A token is a particular sequence of bits circulating in the network, being passed between each two successive functioning stations. The source station can send data only if it receives an unoccupied token; data are then attached to the token and sent. The destination station reads the data but does not free the token which is only released by the source station. The network is assumed to be operable if data sent by any functioning station return to it after transiting all other functioning stations.

With the use of mathematical methods (probability theory, Markov chain theory) an algorithm computing the network's reliability, i.e. the probability that the network is operable expressed in terms of its components' reliabilities, is constructed. The double-ring network model has been solely developed by the author. It is demonstrated that in the reliability aspect the proposed solution surpasses standard techniques like Token Ring or FDDI.

Keywords: Ring network, node redundancy, communication protocol, token passing, network reliability, Markov chain

Notation

G	The graph modeling the considered network
V	The set of G's nodes; $V=\{v_1,...,v_n\}$
$\oplus$	The "cyclical" addition operation; $i \oplus 1 = i + 1$ for $1 \le i \le n-1$, $n \oplus 1 = 1$
$\ominus$	The "cyclical" subtraction operation; $i \ominus 1 = i - 1$ for $2 \le i \le n$, $1 \ominus 1 = n$
$p_V(i)$	The probability of the event "the node v_i is functioning"
$p_E(i,j)$	The probability of the event "the link connecting v_i to v_j is functioning"
R	The network's reliability, i.e. the probability of the event "data can be exchanged between every two operable end stations"

1. Introduction

In this paper the question of ring networks reliability is considered. The aim of the author is to propose a solution which combines the advantages of ring topology and token-passing media access method with high reliability. A model of a double-ring network is constructed wherein every end station is connected to a pair of concentrators one of which is redundant and continues to operate after the other concentrator fails (hot redundancy). Subsequently, the rules of the communication protocol controlling data transmission in the network are formulated. It is then demonstrated that the proposed solution surpasses the standard techniques in the reliability aspect.

Nowadays most local area networks (LANs) are built according to Ethernet standard which historically used bus topology, but its contemporary variant – switched Ethernet – uses star, extended star, or star-mesh topology. However, there is still room for ring networks

which use protocols based on the token-passing mechanism (unlike Ethernet which is based on CSMA/CD protocol). Such networks have one essential advantage – the transmission time can be predicted with high accuracy. This feature makes ring networks especially applicable e.g. for real-time control systems where it is important that the control signal arrive to its destination before the state of the controlled process changes.

In the simplest case a ring network has the single-ring structure. Such a network is composed of n cyclically connected nodes, i.e. the node v_i is directly linked to the nodes $v_{i\oplus 1}$ and $v_{i_{\ominus 1}}$, where $\oplus$ and $\ominus$ respectively denote cyclical addition and cyclical subtraction. Data can only be transmitted "clockwise", i.e. v_i can directly send data only to $v_{i\oplus 1}$, but not to $v_{i_{\ominus 1}}$. Therefore, if v_i sends data to v_j, then they must pass through all links and nodes located between v_i and v_j.

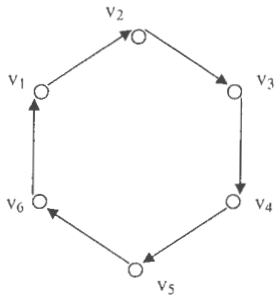

Fig. 1. A single-ring network with 6 nodes

In a single-ring network the nodes can be either end-stations or concentrators to which end-stations are connected. In the latter case the source station sends data to its local concentrator, then they are forwarded between the successive functioning stations until received by the destination station. As there are no direct links between stations, data

forwarded between two stations must always pass through a concentrator. The use of concentrators allows to bypass failed or offline stations which would otherwise cause the network's malfunction. Such mode of operation is proper to Token Ring networks (see [2]).

Usually, it is assumed that a single-ring network is operable if and only if all its nodes and links are functioning. Otherwise, data transmission is possible only if the failed elements are **not** located between the source and the destination nodes. Besides, there is more important justification of that assumption. Most protocols implemented in ring networks are based on the token-passing mechanism. A token is a particular sequence of bits circulating in a network, being passed between successive stations. Only the station which possesses an unoccupied token can transmit data. Data to be sent are attached to the token which thus becomes occupied. Next, the token and data are passed (by means of concentrators) between successive functioning stations until they reach the destination station. The destination station reads the data, but does not free the token which is sent back to the source station, and released therein upon its return. This mechanism permits the destination station to inform the source station that the data have been received. Clearly, if data reception acknowledgments are used, then the functioning of all the nodes and links is necessary to ensure the network's operability. The functioning of only the links located between the source and the destination stations is not sufficient.

Let R_1 denote the reliability of a single-ring network. It is clear that

$$R_1 = \prod_{i=1}^{n} p_V(i)\, p_E(i, i \oplus 1) \tag{1}$$

The reliability of a ring network can be increased by means of using special devices called Dual Access Concentrators (DAC), and connecting them with double links. In consequence, thus constructed network has the double-ring structure; the primary ring is used

for usual data transmission, the secondary ring – only in case of a concentrator or a link failure. In such case both rings are automatically connected and the network continues to operate. The above described solution is implemented in FDDI networks (see [5]). Figure 2 illustrates the closure of a double-ring in an FDDI network built on four DAC devices.

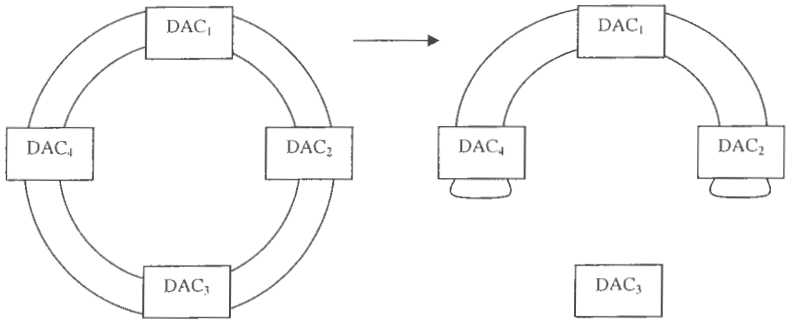

Fig. 2. Double ring closure in an FDDI network

Assuming that DACs are the only failure prone components, a double-ring network, in the reliability aspect, is a 2-out-of-n:F system (see [4]). Hence

$$R_2 = p_V(2) \cdot \ldots \cdot p_V(n) + \sum_{i=2}^{n} q_V(i) \prod_{j \neq i} p_V(j) \tag{2}$$

where R_2 denotes the reliability of a double-ring network.

More information about ring networks reliability can be found in [1], which also contains a short review of literature on the subject. If someone is interested in the reliability of computer networks in general, then [3] is a good reference.

The reliability of ring networks can be further increased by implementing a model, developed by the author of this paper, called the double-ring with redundant nodes. A network

constructed according to this model has the structure of a directed graph with 2n nodes and 4n arcs, $V=\{v_1,...,v_{2n}\}$ being the set of vertices. If i is an odd number, $1 \le i \le 2n$, then v_i is directly connected to $v_{i\oplus 2}$ and $v_{i\oplus 3}$; if i is even, then v_i is directly connected to $v_{i\oplus 1}$ and $v_{i\oplus 2}$. Figure 3 is an illustration of thus structured network for n = 8.

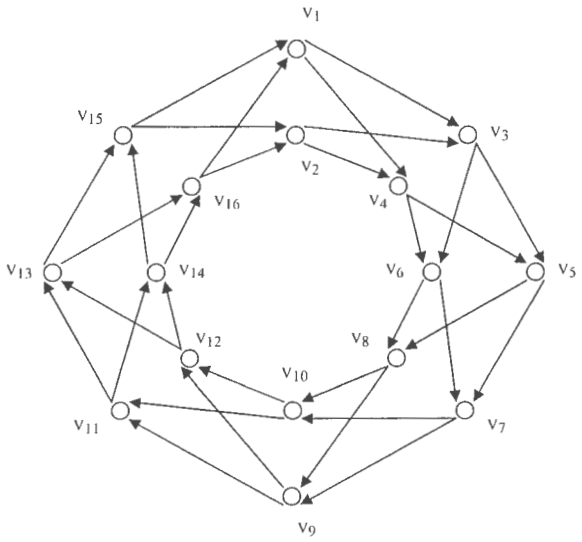

Fig. 3. A double ring with redundant nodes composed of 8 modules

A double ring with redundant nodes can be viewed as a set of n modules; every module is composed of two nodes one of which is redundant, i.e. it continues to operate after the other node has failed, and performs the failed node's functions (hot redundancy). Each node can directly send data to both nodes of the subsequent module, but the nodes of one module cannot directly exchange data – such possibility would significantly complicate the communication protocol controlling data transmission in the network.

The above presented model is particularly applicable for networks whose nodes are concentrators to which end stations are connected. Each station is connected to both concentrators of one module. When a station sends a data frame, its two identical copies are sent to both concentrators of the station's local module. The concentrator which receives data either delivers them to the next functioning station connected to that concentrator, or forwards the data to both concentrators of the next module (the sending station is the last functioning one connected to the concentrator). Failed stations are bypassed, therefore they are irrelevant to the network's operation. Obviously, each data frame is duplicated when it is sent from a station/concentrator to both concentrators of the local/subsequent module, because in either case it must be sent through both links connected to the device's output ports. Frame duplication, directly related to nodes' redundancy, could pose a problem, but is duly handled by the communication protocol described in the next section.

2. The communication protocol controlling data transmission in a DRRN network.

2.1. The protocol's general rules

1. A station can transmit data only if it possesses an unoccupied token – a special frame that moves around the ring in one direction, being forwarded between each two successive functioning stations.
2. When data is transmitted, the token becomes occupied by the source station. The destination station reads the data but does not free the token which is only released on return to the source station. Thus, periodically, each station has opportunity to transmit data. However, one station cannot take possession of a token for indefinitely long time.
3. The first token is generated by Active Monitor – a station chosen in the process called Active Monitor election (see the next chapter). Active Monitor has three more functions – updating the token, generating a new token in place of the lost one, and releasing the token which the source station failed to release.
4. The header of a token frame contains the Identification (ID) field consisting of the address of origin (the generating Active Monitor's address), and the time stamp (Active Monitor's local time when the token was generated). Also, the header contains the Last Passed Station (LPS) field in which every station writes its own address before passing the token to the next station.
5. The maximum time in which a frame returns to the transmitting station is specified by the MFCT (Maximum Frame Circulation Time) parameter. Clearly, the value of MFCT depends on the network equipment's processing speed and the links' throughput. The MFCT parameter should be configurable so that it can be adjusted to the network's size.

6. Each station maintains Wait Timer – a clock measuring the time since the transmission of the last frame. Wait Timer is zeroed when a frame is sent or forwarded. It is not zeroed when a frame is dropped.

Note: The rules 5 and 6 apply not only to token but also to ballot frames used for Active Monitor election.

7. A token is updated each time it passes through Active Monitor. This can be done by updating the time stamp in the token's header.
8. If a token gets lost – this happens when a station receives a token but fails to forward it, then Active Monitor generates a new token. Active Monitor regards the token as lost when its Wait Timer has exceeded the MFCT value.
9. If the source station fails before releasing the occupied token, then Active Monitor releases the token which has bypassed the source station and continues to circulate.
10. If a station receives two successive tokens with the same ID (Active Monitor failed to update the token) or the station's Wait Timer has exceeded the MFCT value (the token was lost but Active Monitor failed to generate a new one) then the station starts the Active Monitor Election process. In case of two successive tokens with the same ID the second one is dropped.

Note: Each station must remember the ID of the last sent or forwarded token so that it can be compared to the ID of the next received token. The same requirement holds for ballot frames. Both events described in rule 10 indicate that Active Monitor has failed to perform its functions, hence a new one has to be elected.

2.2. Active Monitor election rules

1. If no Active Monitor has been previously elected (the network is starting to operate) or if Active Monitor has failed, then each station whose Wait Timer exceeds the MFCT value sends a ballot frame – a special frame used solely for the purpose of Active Monitor election.
2. A ballot frame is identified by the address of origin (the sending station's address) and the time stamp (the station's local time when the frame is sent).
3. If a station **not** participating in the current election (one which has **not** sent a ballot frame) receives a ballot frame before its Wait Timer has reached the MFCT value, then it forwards the frame.
4. If a station participating in the current election (one which has sent a ballot frame) receives another ballot frame with the address of origin smaller than its own address, then it forwards the frame. Otherwise, i.e. if the received ballot frame's address of origin is greater than the station's own address, then the frame is dropped.
5. The station which receives its own ballot frame becomes the Active Monitor. It drops that frame, then generates and sends a token. The Active Monitor election process is thus completed.

Note: It follows from the rules 4 and 5 that of all stations participating in the election process the one with the smallest address becomes Active Monitor.

6. If a station receives, for the second time, a ballot frame which is not its own, then it drops that frame.

Note: The event described in the rule 6 occurs when the potential Active Monitor fails before its own ballot frame returns. In such case, another station must drop that frame, otherwise it would circulate endlessly.

7. If a ballot frame sent by potential Active Monitor gets lost – this happens when another station receives the frame but fails to forward it, then a new ballot frame will be sent by each station whose Wait Timer has expired.

Note: Classical token passing mechanism operates in the following way. A station which had received the token and sent a data frame holds the token until the data frame circles the entire ring (data and token are separate frames). Data are then removed by the transmitting station which releases the token and passes it to the subsequent station. In a DRRN network separate token and data frames would be more difficult to handle due to frame duplication, therefore token and data are sent as one frame.

The rules formulated in sections 2.1 and 2.2 are applicable for both single-ring and double-ring networks. However, data transmission in double-ring networks is a more complicated process, therefore it requires some additional principles of control which are formulated in the next chapter.

2.3. The protocol's features directly related to the specific structure of DRRN.

Avoiding uncontrolled frame duplication.

The network is constructed in such a way that each frame is duplicated every time it leaves a device (a station or a concentrator). One copy of the frame is sent to each of both concentrators directly connected to the device's outputs. On the other hand, each device receives two copies of every frame, one from each of both concentrators directly connected to the device's inputs.

Note: As all pieces of equipment of the same type operate with equal speed, theoretically both copies of a duplicated frame should arrive at each device simultaneously, but in practice one copy is always a little ahead of the other.

Thus it is clear that, without appropriate measures, each frame after successful transition through k devices would have 2^k copies. Hence, the communication protocol must prevent the uncontrolled frame duplication. This is achieved by means of applying the following rule:

Rule 1. If two consecutively received frames of the same type have equal IDs, then the second frame is dropped.

The rule 1 generalizes the rule 10 of "General rules" and the rule 6 of "Active Monitor election rules". However, in the single-ring case the IDs of two consecutively received frames can only be equal due to the active monitor failure (token frames) or the potential Active Monitor failure (ballot frames). In the double-ring case repeated frames occur not only randomly, due to equipment failure, but mainly as a planned effect of the duplication

mechanism. For example, if two identical token frames arrive almost simultaneously (i.e. the time between their arrivals is much smaller than MFCT), then they are two copies of a duplicated token frame received from two different concentrators. If the time between the arrivals of two identical token frames is close to MFCT, then the second frame is a copy of the not updated token (Active Monitor's failure). Most probably, the duplicate of the not updated token will be immediately received (if it is not lost) through the other input. Obviously, all repeated frames are dropped, according to the rule 1.

Note: If a concentrator has the functionality allowing it to drop identical frames received from two preceding concentrators, then the number of identical frames received by the leftmost connected station (assuming clockwise transmission) is reduced from 4 to 2. Obviously, a station cannot send two identical frames to one concentrator, hence concentrators need not analyze frames received from directly connected stations.

Handling of a delayed token frame.

Apart from duplicate copies, the second phenomenon that can occur in double-ring networks, but cannot occur in single-ring ones, is the so-called delayed token. Theoretically, it is possible that the second copy of a duplicated token frame arrives at a device later than the first copy of the next duplicated token frame. The frame which arrived later is called a delayed token because its Time Stamp is older than that of the earlier arrived frame. Hence, if two consecutive token frames arriving at a device's inputs have the same address of origin while the second frame's Time Stamp is older than the first frame's Time Stamp, then the second frame is a delayed token. The example given below should help to understand this somewhat confusing definition.

Let us consider an example module with two end stations attached, illustrated in Figure 4. The concentrators are denoted by C_1 and C_2, the stations – by A and B.

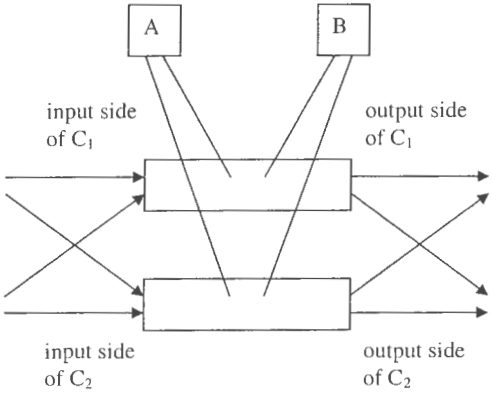

Fig. 4. An example module

It is assumed that for some reason the concentrator C_2 was temporarily slower than C_1. In consequence, the following events (listed in chronological order) occurred:

- A sends (duplicated) data frame F_1 with the time stamp T_1
- The first copy of F_1 is forwarded to B by C_1
- A sends (duplicated) data frame F_2 with the time stamp T_2, $T_2 > T_1$
- The first copy of F_2 is forwarded to B by C_1
- The second copy of F_1 is forwarded to B by C_2

Obviously, the second copy of F_1 arrives at B later than the first copy of F_2. However, the time stamp of the second copy of F_1 is older than the time stamp of the first copy of F_2, therefore the second copy of F_1 is a delayed token.

Clearly, a delayed token is (in most cases) a repeated frame, therefore it must be dropped. Hence, the following rule holds:

Rule 2. If two consecutively received token frames have the same address of origin, and the Time Stamp of the second frame is older than the Time Stamp of the first one, then the second frame is dropped.

Note: If a delayed token is the only copy of a duplicated token frame, because the other copy was lost due to equipment failure, then the information contained in the delayed token will not reach the destination station. In such case the higher layers of the protocol stack (TCP or application layer) should have this information sent again. For better understanding let us again refer to Fig. 4 and assume that the following events (listed in chronological order) occurred:

- A sends (duplicated) data frame F_1 with the time stamp T_1
- For some reason, C_1 fails to forward the first copy of F_1 to B
- A sends (duplicated) data frame F_2 with the time stamp T_2, $T_2 > T_1$
- The first copy of F_2 is forwarded to B by C_1
- The second copy of F_1 is forwarded to B by C_2

Obviously, the second copy of F_1 will be the only one received by B. Being a delayed token it will be dropped by B, hence the information contained in F_1 will not reach the destination station.

Unpaired shortcut detection

The unpaired shortcut occurs when a station is not attached to one of the concentrators of the same module (Fig. 5), or a concentrator's port is failed and does not open the shortcut between its neighboring ports even though a station is connected to that port (Fig. 6).

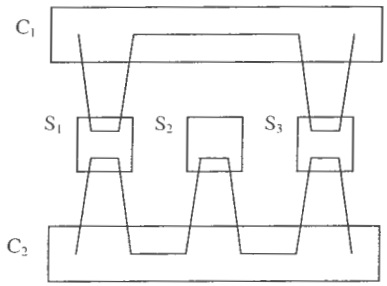

Fig. 5. Unpaired shortcut – station S_2 not attached to C_1

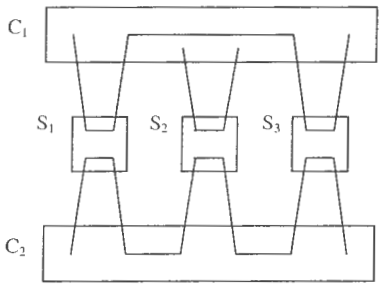

Fig. 6. Unpaired shortcut – C_1 does not open the shortcut between S_1 and S_3

The unpaired shortcut can be easily detected. To explain how, let us refer to one of the above figures. When S1 sends a duplicated token frame, S3 will receive one copy of it

directly from S1, and the other copy directly from S2. As a result, S3 will receive two consecutive frames with different addresses in their LPS fields. The only reason of such situation can be the unpaired shortcut located before S3.

Note: A station can compare the LPS fields of each two consecutively received frames if, apart from remembering the ID field, it also remembers the LPS field of the last received frame.

The unpaired shortcut obviously has negative effect on the network's reliability. Besides, its occurrence violates the order in which a frame should pass through successive stations. In the depicted situation one copy of a frame sent from S1 will reach S3 before the other copy leaves S2. In consequence, the copy received by S3 from S2 will be dropped, because it has the same ID as the copy received from S1, but arrives at S3 later (see Rule 1). Thus S2 is not able to communicate with other stations. This reasoning leads to the formulation of the following rule:

Rule 3. If a station receives two consecutive frames with different addresses in their LPS fields then it stops forwarding frames and issues appropriate warning message about the unpaired shortcut occurrence, i. e. displays it on the station's monitor or sends the message by means of wireless communication to the network's surveillance center.

Note: All the rules listed in Section 2 may not conform to the Token Ring or FDDI specifications according to IEEE 802.5 or ANSI standards. They have been developed solely by the author of this paper with the aim to construct a protocol best suited for the double ring topology presented in the introduction.

3. Reliability analysis of a DRRN network.

The whole network is considered to be operable if data sent from any functioning station return to it after passing through all intermediate functioning devices. Note that data received by a functioning concentrator are received and forwarded by all functioning stations connected to that concentrator. Let A_i be the event described as follows: "data sent from the module μ_i return to it after passing through all other modules". Thus, the network's operability is equivalent to the occurrence of the event $A_1 \cap \ldots \cap A_n$. In consequence, the network's reliability is given by the probability $Pr(A_1 \cap \ldots \cap A_n)$. We have:

$$(3) \qquad Pr(A_1 \cap \ldots \cap A_n) = Pr(A_i)$$

for any $i \in \{1,\ldots, n\}$. The proof of (3) is very simple. Indeed, let $A_{i,j}$ be the event described as follows: "data sent from the module μ_i are received by μ_j. For $i \neq j$ the equalities

$$(4) \qquad A_i = A_{i,j} \cap A_{j,i} = A_{j,i} \cap A_{i,j} = A_j$$

hold, thus the equality

$$(5) \qquad A_1 \cap \ldots \cap A_n = A_i$$

holds for any $i \in \{1,\ldots, n\}$, which implies (3). In view of (3), the network's reliability is given by $Pr(A_i)$ for any $i \in \{1,\ldots, n\}$, thus it is given by $P(A_1)$.

Now let us proceed to the construction of the algorithm finding $P(A_1)$. First, the events V_i, W_i, $1 \leq i \leq 2n$, are defined in the following way:

V_i – the node v_i is operable

W_i – data sent from the module μ_1 is received by v_i

Next, the random variables X_i, Y_i, $1 \le i \le n$, with values in the set $\{0, 1, 2, 3\}$ are defined as follows:

$$X_i = \begin{cases} 0 \Leftrightarrow \textit{the event } V_{2i-1}^C \cap V_{2i}^C \textit{ occurs} \\ 1 \Leftrightarrow \textit{the event } V_{2i-1} \cap V_{2i}^C \textit{ occurs} \\ 2 \Leftrightarrow \textit{the event } V_{2i-1}^C \cap V_{2i} \textit{ occurs} \\ 3 \Leftrightarrow \textit{the event } V_{2i-1} \cap V_{2i} \textit{ occurs} \end{cases}$$

$$Y_i = \begin{cases} 0 \Leftrightarrow \textit{the event } W_{2i-1}^C \cap W_{2i}^C \textit{ occurs} \\ 1 \Leftrightarrow \textit{the event } W_{2i-1} \cap W_{2i}^C \textit{ occurs} \\ 2 \Leftrightarrow \textit{the event } W_{2i-1}^C \cap W_{2i} \textit{ occurs} \\ 3 \Leftrightarrow \textit{the event } W_{2i-1} \cap W_{2i} \textit{ occurs} \end{cases}$$

where the superscript C denotes the complement of a set. The network's construction principles imply that if $2 \le i \le n$ holds, then for fixed values of X_1, Y_2,..., Y_i the value of $Y_{i \oplus 1}$ depends on Y_i alone, which is expressed by the following formula:

$$(6) \qquad \Pr(Y_{i\oplus 1} = y_{i\oplus 1} \mid Y_i = y_i, \ldots, Y_2 = y_2, X_1 = x_1) = P(Y_{i\oplus 1} = y_{i\oplus 1} \mid Y_i = y_i)$$

Thus, the sequence $\{X_1, Y_2,..., Y_n, Y_{n\oplus 1}\} = \{X_1, Y_2,..., Y_n, Y_1\}$ is a Markov chain. The equality (6) yields the following lemma:

Lemma 1

If $2 \leq i \leq n$ holds, and a and c are arbitrary numbers belonging to the set {1, 2, 3}, then we have:

$$\Pr(Y_{i\oplus 1} = a \mid X_1 = c) = \sum_{b=1}^{3} \Pr(Y_{i\oplus 1} = a \mid Y_i = b) \Pr(Y_i = b \mid X_1 = c) \tag{7}$$

Proof:

For $2 \leq i \leq n$ the following equalities hold:

$$\begin{aligned} &\Pr(Y_{i\oplus 1} = a,\ X_1 = c) = \sum_{b=1}^{3} \Pr(Y_{i\oplus 1} = a,\ Y_i = b,\ X_1 = c) = \\ &= \sum_{b=1}^{3} \Pr(Y_{i\oplus 1} = a \mid Y_i = b,\ X_1 = c) \Pr(Y_i = b \mid X_1 = c) \Pr(X_1 = c) = \\ &= \sum_{b=1}^{3} \Pr(Y_{i\oplus 1} = a \mid Y_i = b) \Pr(Y_i = b \mid X_1 = c) \Pr(X_1 = c) \end{aligned} \tag{8}$$

The last equality in (8) is a consequence of the Markov's property applied to the conditional probability $\Pr(Y_{i\oplus 1} = a \mid Y_i = b, X_1 = c)$. Dividing the left-hand and the right-hand sides of (8) by $\Pr(X_1 = c)$ we obtain (7). Thus the proof is completed.

To shorten the notation, let us define:

$$\pi_{a,b}^{(1)} = \Pr(Y_2 = a \mid X_1 = b) \tag{9}$$

(10) $$\pi_{a,b}^{(i)} = \Pr(Y_{i\oplus 1} = a \mid Y_i = b), \quad 2 \le i \le n$$

and

(11) $$\varphi^{(1)}(b) = \begin{bmatrix} \Pr(X_1 = 1 \mid X_1 = b) \\ \Pr(X_1 = 2 \mid X_1 = b) \\ \Pr(X_1 = 3 \mid X_1 = b) \end{bmatrix}$$

(12) $$\varphi^{(i+1)}(b) = \begin{bmatrix} \Pr(Y_{i\oplus 1} = 1 \mid X_1 = b) \\ \Pr(Y_{i\oplus 1} = 2 \mid X_1 = b) \\ \Pr(Y_{i\oplus 1} = 3 \mid X_1 = b) \end{bmatrix}, \quad 1 \le i \le n$$

where a and b belong to $\{1, 2, 3\}$. Note that $\varphi^{(1)}(1) = (1, 0, 0)$, $\varphi^{(1)}(2) = (0, 1, 0)$, $\varphi^{(1)}(3) = (0, 0, 1)$. Lemma 1, in connection with the definitions (9) – (12), yields the following matrix equations:

(13) $$\varphi^{(i+1)}(b) = \Pi^{(i)} \varphi^{(i)}(b), \quad 1 \le i \le n, \quad b \in \{1,2,3\}$$

where

(14) $$\Pi^{(i)} = \begin{bmatrix} \pi_{1,1}^{(i)} & \pi_{1,2}^{(i)} & \pi_{1,3}^{(i)} \\ \pi_{2,1}^{(i)} & \pi_{2,2}^{(i)} & \pi_{2,3}^{(i)} \\ \pi_{3,1}^{(i)} & \pi_{3,2}^{(i)} & \pi_{1,1}^{(i)} \end{bmatrix}$$

Let us now specify the events whose occurrence is necessary and sufficient for the event A_1 to occur. The events in question are $\{X_1 = 1\} \vee \{X_1 = 2\} \vee \{X_1 = 3\}$ and $\{Y_{n\oplus 1} = 1\} \vee \{Y_{n\oplus 1} = 2\} \vee \{Y_{n\oplus 1} = 3\}$, i.e. „at least one of the nodes v_1 and v_2 is operable" and „data sent from the module μ_1 returns to μ_1". Thus the following equalities hold:

$$
\begin{aligned}
\Pr(A_1) &= \Pr\Big(\bigcup_{b=1}^{3}\{X_1 = b\} \cap \bigcup_{a=1}^{3}\{Y_{n\oplus 1} = a\}\Big) = \\
&= \sum_{b=1}^{3}\sum_{a=1}^{3}\Pr(Y_{n\oplus 1} = a,\ X_1 = b) = \\
&= \sum_{b=1}^{3}\left[\sum_{a=1}^{3}\Pr(Y_{n\oplus 1} = a \mid X_1 = b)\right]\Pr(X_1 = b) = \\
&= \sum_{b=1}^{3}\left[\sum_{a=1}^{3}\varphi_a^{(n+1)}(b)\right]\Pr(X_1 = b)
\end{aligned}
\tag{15}
$$

where $\varphi_a^{(n+1)}(b)$ denotes the a-th coordinate of the vector $\varphi^{(n+1)}(b)$. The formulas (13) and (15) constitute the mathematical basis of the following algorithm computing $P(A_1)$:

Algorithm 1

$\Pr(A_1) \leftarrow 0$;

for each b in [1, 2, 3] do {

$\psi \leftarrow \varphi^{(1)}(b)$;

for each i in [1,..., n] do

$\psi \leftarrow \Pi^{(i)} \times \psi$;

$\Pr(A_1) \leftarrow \Pr(A_1) + (\psi_1 + \psi_2 + \psi_3)\cdot\Pr(X_1 = b)$; ## ψ_1, ψ_2, ψ_3 are the coordinates of ψ

}

As the internal "for" loop has n cycles, the algorithm's numerical complexity is equal to O(n).

In order to use Algorithm 1 we still need formulas defining the elements of the matrix $\Pi^{(i)}$, $1 \le i \le n$. Here are the formulas for $\Pi^{(1)}$:

$$
\begin{aligned}
&\pi^{(1)}_{1,1} = p_E(1,3)q_E(1,4) \\
&\pi^{(1)}_{1,2} = p_E(2,3)q_E(2,4) \\
&\pi^{(1)}_{1,3} = [1 - q_E(1,3)q_E(2,3)] \cdot q_E(1,4) \cdot q_E(2,4)
\end{aligned} \tag{16}
$$

$$
\begin{aligned}
&\pi^{(1)}_{2,1} = q_E(1,3)p_E(1,4), \\
&\pi^{(1)}_{2,2} = q_E(2,3)p_E(2,4), \\
&\pi^{(1)}_{2,3} = q_E(1,3) \cdot q_E(2,3) \cdot [1 - q_E(1,4)q_E(2,4)]
\end{aligned} \tag{17}
$$

$$
\begin{aligned}
&\pi^{(1)}_{3,1} = p_E(1,3)p_E(1,4) \\
&\pi^{(1)}_{3,2} = p_E(2,3)p_E(2,4) \\
&\pi^{(1)}_{3,3} = [1 - q_E(1,3)q_E(2,3)] \cdot [1 - q_E(1,4)q_E(2,4)]
\end{aligned} \tag{18}
$$

The proofs of all the above equalities are similar, therefore it is sufficient to prove one of them only. Let us consider the situation presented in Fig 7. It illustrates the occurrence of the event $\{Y_2 = 2\}$ on condition that the event $\{X_1 = 3\}$ has taken place. It is clear that the event $\{Y_2 = 2\}$ occurs if and only if at least one of the links (v_1, v_4) and (v_2, v_4) is operable, and both of the links (v_1, v_3) and (v_2, v_3) are failed. In consequence, the last of the equalities in (17) holds. The remaining equalities in (16) – (18) are proved analogously.

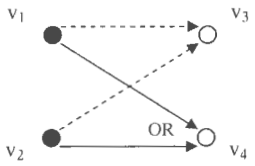

Fig. 7. The occurrence of $\{Y_2 = 2\}$ on condition that $\{X_1 = 3\}$ has occurred

In Fig. 7 the functioning nodes are represented by black circles, whereas the nodes whose states are irrelevant – by gray circles. The functioning links are represented by continuous lines, the failed ones – by dotted lines.

The formulas for $\Pi^{(i)}$, $2 \le i \le n$, are given below:

$$
\begin{aligned}
\pi_{1,1}^{(i)} &= p_V(2i-1)\,p_E(2i-1,2i+1)q_E(2i-1,2i+2)\\
\pi_{1,2}^{(i)} &= p_V(2i)\,p_E(2i,2i+1)q_E(2i,2i+2)\\
\pi_{1,3}^{(i)} &= p_V(2i-1)\,p_V(2i)\times\\
&\quad\times[1-q_E(2i-1,2i+1)q_E(2i,2i+1)]\,q_E(2i-1,2i+2)q_E(2i,2i+2)+\\
&\quad+p_V(2i-1)q_V(2i)\,p_E(2i-1,2i+1)q_E(2i-1,2i+2)\\
&\quad+q_V(2i-1)\,p_V(2i)\,p_E(2i,2i+1)q_E(2i,2i+2)
\end{aligned}
\tag{19}
$$

$$
\begin{aligned}
\pi_{2,1}^{(i)} &= p_V(2i-1)q_E(2i-1,2i+1)\,p_E(2i-1,2i+2)\\
\pi_{2,2}^{(i)} &= p_V(2i)q_E(2i,2i+1)\,p_E(2i,2i+2)\\
\pi_{2,3}^{(i)} &= p_V(2i-1)\,p_V(2i)\times\\
&\quad\times[1-q_E(2i-1,2i+2)q_E(2i,2i+2)]\,q_E(2i-1,2i+1)q_E(2i,2i+1)+\\
&\quad+p_V(2i-1)q_V(2i)q_E(2i-1,2i+1)\,p_E(2i-1,2i+2)\\
&\quad+q_V(2i-1)\,p_V(2i)q_E(2i,2i+1)\,p_E(2i,2i+2)
\end{aligned}
\tag{20}
$$

$$
\begin{aligned}
\pi_{3,1}^{(i)} &= p_V(2i-1)\,p_E(2i-1,2i+1)\,p_E(2i-1,2i+2)\\
\pi_{3,2}^{(i)} &= p_V(2i)\,p_E(2i,2i+1)\,p_E(2i,2i+2)\\
\pi_{3,3}^{(i)} &= p_V(2i-1)\,p_V(2i)\times\\
&\qquad \times[1-q_E(2i-1,2i+1)q_E(2i,2i+1)]\times\\
&\qquad \times[1-q_E(2i-1,2i+2)q_E(2i,2i+2)]+\\
&\quad + p_V(2i-1)q_V(2i)\,p_E(2i-1,2i+1)\,p_E(2i-1,2i+2)\\
&\quad + q_V(2i-1)\,p_V(2i)\,p_E(2i,2i+1)\,p_E(2i,2i+2)
\end{aligned}
\tag{21}
$$

Similarly as in the previous case (i = 1), the proof of only one equality will be presented, as the proofs of the remaining ones are similar. Let us consider the situation presented in Fig. 8. It illustrates the occurrence of the event $\{Y_{i\oplus 1} = 1\}$ on condition that the event $\{Y_i = 3\}$ has taken place, $2 \le i \le n$. The meaning of the graphical symbols is the same as in Fig. 7; additionally, failed nodes are represented by empty circles while missing lines represent links whose states are irrelevant. Three mutually exclusive cases have to be considered: (1) both v_{2i-1} and v_{2i} are functioning, (2) v_{2i-1} is functioning, v_{2i} is failed, (3) v_{2i-1} is failed, v_{2i} is functioning. In the first case the considered event occurs if and only if at least one of the links (v_{2i-1}, v_{2i+1}) and (v_{2i}, v_{2i+1}) is functioning, while both of the links (v_{2i-1}, v_{2i+2}) and (v_{2i}, v_{2i+2}) are failed. In the second case (v_{2i-1}, v_{2i+1}) must be functioning, (v_{2i-1}, v_{2i+2}) must be failed, whereas the states of (v_{2i}, v_{2i+1}) and (v_{2i}, v_{2i+2}) are irrelevant. Finally, in the third case (v_{2i}, v_{2i+1}) must be functioning, (v_{2i}, v_{2i+2}) must be failed, whereas the states of (v_{2i-1}, v_{2i+1}) and (v_{2i-1}, v_{2i+2}) are irrelevant. In consequence, the last of the equalities in (19) holds. The remaining equalities in (19) – (21) are proved analogously.

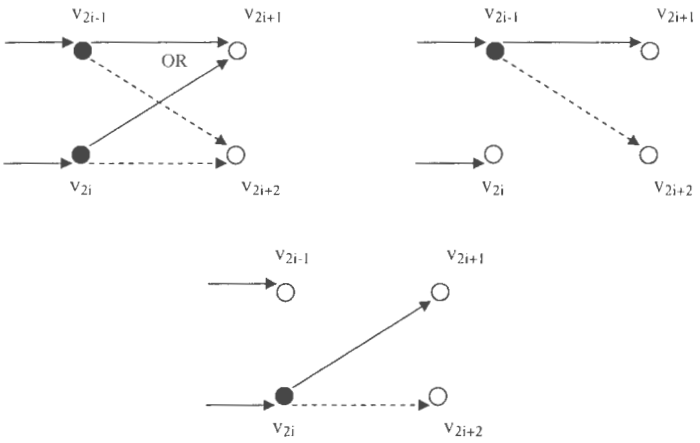

Fig. 8. The occurrence of $\{Y_{i \oplus 1} = 1\}$ on condition that $\{Y_i = 3\}$ has occurred, $2 \leq i \leq n$.

In conclusion, the three types of ring networks discussed in the introduction will be compared with respect to their reliability. For the purpose of that comparison it is assumed that only the nodes of a network are failure prone, while the probability of a link failure is equal to zero. As a result, the computations become considerably simpler, especially in the case of a double ring network with redundant nodes. Such network with infallible links is operable if and only if each module contains at least one functioning concentrator. The probability $\Pr(A_1)$ is then given by the following formula:

$$\Pr(A_1) = \prod_{i=1}^{n} [1 - q_V(2i-1)q_V(2i)] \tag{22}$$

Let $R_3 = \Pr(A_1)$. In the tables below the exemplary values of R_1, R_2, and R_3 for ring networks of different sizes are presented. It is assumed that each network is composed of infallible links and equally reliable nodes, where p_V is the reliability of a node.

Table 1. Exemplary values of R_1, R_2, and R_3 for n = 4

pv	R_1	R_2	R_3
0,2	0,001600	0,027200	0,016796
0,4	0,025600	0,179200	0,167772
0,6	0,129600	0,475200	0,497871
0,8	0,409600	0,819200	0,849347
0,9	0,656100	0,947700	0,960596
0,95	0,814506	0,985981	0,990037
0,99	0,960596	0,999408	0,999600
0,995	0,980150	0,999851	0,999900
0,999	0,996006	0,999994	0,999996
0,9995	0,99800150	0,99999850	0,99999900
0,9999	0,99960006	0,99999994	0,99999996

Table 2. Exemplary values of R_1, R_2, and R_3 for n = 6

pv	R_1	R_2	R_3
0,1	0,000001	0,000055	0,000047
0,2	0,000064	0,001600	0,002177
0,4	0,004096	0,040960	0,068719
0,6	0,046656	0,233280	0,351298
0,8	0,262144	0,655360	0,782758
0,9	0,531441	0,885735	0,941480
0,95	0,735092	0,967226	0,985093
0,99	0,941480	0,998540	0,999400
0,995	0,970373	0,999630	0,999850
0,999	0,994015	0,999985	0,999994
0,9995	0,99700375	0,99999626	0,99999850
0,9999	0,99940015	0,99999985	0,99999994

Table 3. Exemplary values of R_1, R_2, and R_3 for n = 8

pv	R_1	R_2	R_3
0,1	0,000000	0,000001	0,000002
0,2	0,000003	0,000084	0,000282
0,4	0,000655	0,008520	0,028147
0,6	0,016796	0,106376	0,247876
0,8	0,167772	0,503317	0,721390
0,9	0,430467	0,813105	0,922745
0,95	0,663420	0,942755	0,980174
0,99	0,922745	0,997310	0,999200
0,995	0,960693	0,999314	0,999800
0,999	0,992028	0,999972	0,999992
0,9995	0,99600699	0,99999301	0,99999800
0,9999	0,99920028	0,99999972	0,99999992

Table 4. Exemplary values of R_1, R_2, and R_3 for n = 12

pv	R_1	R_2	R_3
0,2	0,000000	0,000000	0,000005
0,4	0,000017	0,000319	0,004722
0,6	0,002177	0,019591	0,123410
0,8	0,068719	0,274878	0,612710
0,9	0,282429	0,659002	0,886385
0,95	0,540360	0,881640	0,970409
0,99	0,886385	0,993825	0,998801
0,995	0,941623	0,998405	0,999700
0,999	0,988066	0,999935	0,999988
0,9995	0,99401647	0,99998355	0,99999700
0,9999	0,99880066	0,99999934	0,99999988

As could be expected, double ring networks are far more reliable than single-ring ones. It is also interesting to see that the application of redundant nodes can decrease the reliability of a double ring network if the nodes have low reliability and the network size is

small (e.g. $p_V \leq 0.4$, $n = 4$ or $p_V \leq 0.1$, $n = 6$). In a more realistic scenario, i.e. if a node's reliability exceeds 0.8, the relative increase of the network's reliability, resulting from nodes redundancy, is proportional to the network's size. More precisely, the value of the quotient $R_3 - R_2 / R_2$ increases with n if p_V is fixed and greater than or equal to 0.9. However, this conclusion is based solely on the analysis of some special cases rather than on a formal proof.

4. Bibliography

[1] C.B. Silio, H.M. Dao, Ring network with a constrained number of consecutively-bypassed stations, IEEE Transactions on Reliability, Vol. 47 (1998), No 1, 35-43.

[2] James T. Carlo, Understanding Token Ring Protocols and Standards, Artech House Publishers, 1998.

[3] Martin L. Shooman, Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design. John Wiley & Sons, 2002.

[4] R.E. Barlow, F. Proschan, Statistical theory of reliability and life testing, Holt, Rinehart and Winston, 1975.

[5] R. Jain, FDDI Handbook: High-Speed Networking using fiber and other media, Addison-Wesley, 1994.