(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 037 653 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Claims EN 4

(48) Corrigendum issued on:
13.03.2013 Bulletin 2013/11

(45) Date of publication and mention of the grant of the patent:
17.10.2012 Bulletin 2012/42

(21) Application number: **08014004.9**

(22) Date of filing: **05.08.2008**

(51) Int Cl.:
H04L 29/06 *(2006.01)* ***H04L 12/56*** *(0000.00)*

(54) **Method for data transmission in communication system**

Verfahren zur Datenübertragung in einem Kommunikationssystem

Procédé de transmission de données dans un système de communication

(84) Designated Contracting States:
DE FR GB

(30) Priority: **27.08.2007 JP 2007220046**

(43) Date of publication of application:
18.03.2009 Bulletin 2009/12

(60) Divisional application:
10075347.4 / 2 302 859

(73) Proprietor: **MITSUBISHI ELECTRIC CORPORATION**
Chiyoda-ku
Tokyo 100-8310 (JP)

(72) Inventor: **Kawahigashi, Haruko**
Tokyo 100-8310 (JP)

(74) Representative: **Pfenning, Meinig & Partner GbR**
Patent- und Rechtsanwälte
Theresienhöhe 13
80339 München (DE)

(56) References cited:
US-A1- 2006 282 677

- **LUISA LIMA ET AL: "Random Linear Network Coding: A free cipher?" INFORMATION THEORY, 2007. ISIT 2007. IEEE INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 24 June 2007 (2007-06-24), pages 546-550, XP031282139 ISBN: 978-1-4244-1397-3**
- **JIANLONG TAN ET AL: "Secure Network Coding with a Cost Criterion" MODELING AND OPTIMIZATION IN MOBILE, AD HOC AND WIRELESS NETWORKS, 200 6 4TH INTERNATIONAL SYMPOSIUM ON BOSTON, MA, USA 03-06 APRIL 2006, PISCATAWAY, NJ, USA, IEEE, 3 April 2006 (2006-04-03), pages 1-6, XP010933027 ISBN: 978-0-7803-9549-7**
- **NING CAI ET AL: "A Security Condition for Multi-Source Linear Network Coding" INFORMATION THEORY, 2007. ISIT 2007. IEEE INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 24 June 2007 (2007-06-24), pages 561-565, XP031282141 ISBN: 978-1-4244-1397-3**
- **S-Y R LI ET AL: "Linear Network Coding" IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE, US, vol. 49, no. 2, 1 February 2003 (2003-02-01), pages 371-381, XP011221038 ISSN: 0018-9448**

Printed by Jouve, 75001 PARIS (FR)

(Cont. next page)

- RALF KOETTER AND MURIEL MÉDARD: "An Algebraic Approach to Network Coding" IEEE / ACM TRANSACTIONS ON NETWORKING, IEEE / ACM, NEW YORK, NY, US, vol. 11, no. 5, 1 October 2003 (2003-10-01), pages 782-795, XP007908088 ISSN: 1063-6692
- HARUKO KAWAHIGASHI ET AL: "Security Aspects of the Linear Network Coding" MILITARY COMMUNICATIONS CONFERENCE, 2007. MILCOM 2007. IEEE, IEEE, PISCATAWAY, NJ, USA, 29 October 2007 (2007-10-29), pages 1-7, XP031232511 ISBN: 978-1-4244-1512-0

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a method of data transmission in a communication system.

2. Description of the Related Art

[0002] A conventional network that performs packet communication includes communication devices called nodes that are interconnected by links. Information is transmitted in the network from a source node to a destination node through communication paths that include relay nodes. A relay node only sorts the packets based on the data in the packets and redirects them towards the corresponding destination nodes. In other words, a relay node does not perform any process on user data in a packet.

[0003] In addition to sorting the packets, data encoding can be performed at each relay node by using a network coding technology to efficiently transmit the data over the network. For a more complete description of the network coding technology, reference may be had to, e.g., nonpatent literature as follows:

R. Ahlswede et al., "Network information flow", IEEE trans. on Information Theory, Vol. 46, No. 4, July 2000, pp. 1204-1216;
Yamamoto Miki, "Network coding", Journal of Institute of Electronics, Information and Communication Engineers (IEICE), Vol. 90, No. 2, February 2007, pp. 111-116; and
S-Y. R. Li et al., "Linear network coding", Vol. 49, No. 2, February 2003, pp. 371-381.

[0004] Main advantage of the network coding, apart from allowing efficient use of communication resources such as a bandwidth, is that it provides better data confidentiality. Concretely, in the network coding technology, encoding process is performed on the data in each packet at each relay node, so that even if an outsider succeeds in tapping the data during transmission, it is difficult to break the data code thereby maintaining the data security.

[0005] However, quantitative evaluation of the security level is not performed in the abovementioned network coding technology. Thus, it is difficult to determine the security level of data encoding thereby failing to ensure that the data security is maintained at all the time.

[0006] The publication of Luísa Lima, Muriel Médard, João Barros, "Random Linear Network Coding: A free cipher?", Proc. of the IEEE International Symposium on Information Theory, Nice, France, June 2007, pp. 546-550 discloses a measure for the security of networks, wherein the number of symbols an intermediate node has to guess in order to decode one of the transmitted symbols is utilized. A calculation of that measure is likely to consume too many resources and to increase the complexity of the security mechanisms.

SUMMARY OF THE INVENTION

[0007] It is an object of the present invention to at least partially solve the problems in the conventional technology.

[0008] According to an aspect of the present invention, there is provided a method of transmitting data in a communication system, the communication system including a source node that generates the data and a plurality of general nodes, each bering a destination node for the data or a relay node for relaying the data, the source node being linked with each of the general nodes by at least one independent path, the data being encoded by using an encoding matrix at the source node and the relay node. The method including determining a general node from among the general nodes that has maximum number of independent paths up to the source node; setting a size of a set formed by elements of the encoding matrix; calculating a tap-proof index (also known as wire-tap robustness index, i.e., WTR index) that indicates security level against tapping of the data flowing in the communication system based on the maximum number of independent paths and the size of the set; and controlling the tap-proof index.

[0009] According to another aspect, which is regarded as useful but not within the scope of this invention, there is provided a method of transmitting data in a communication system, the communication system including a source node that generates the data and a plurality of general nodes, each being a destination node for the data or a relay node for relaying the data, the source node being linked with each of the general nodes by at least one independent path, the independent path including at least one communication link, the data being encoded at the source node and the relay node. The method including determining a general node from among the general nodes that has maximum number of independent paths up to the source node; calculating an encoding vector corresponding to each of the communication links; encoding data passing through a communication link by multiplying an encoding vector corresponding to the

communication link to the data passing through the communication; obtaining a subspace of each of the encoding vectors; selecting encoding vectors of less than or equal to a second maximum number of independent paths from among the encoding vectors, the second maximum number of independent paths being one less than the maximum number of independent paths; first-calculating, when number of the encoding vectors selected at the selecting is less than the second maximum number of independent paths, a vector subspace that is formed by the encoding vectors selected at the selecting and a vector, the vector belonging to a group of vectors that have number of dimensions equal to the maximum number of independent paths with only one of components being 1 and all other components being 0; second-calculating, when the number of the encoding vectors selected at the selecting is equal to the second maximum number of independent paths, a vector subspace formed by only the encoding vectors selected at the selecting; deselecting the vector subspace calculated at any one of the first-calculating and the second-calculating when the vector subspace includes the subspace obtained at the obtaining; repeating the selecting, the first-calculating, the second-calculating, and the deselecting if there is a vector in the group yet to be processed at the first-calculating and an encoding vector yet to be selected at the selecting; and assigning an encoding vector, the vector subspace of which is not deselected at the deselecting, to the communication link.

[0010] According to still another aspect of the present invention, there is provided a communication system including a source node that generates the data and a plurality of general nodes, each being a destination node for the data or a relay node for relaying the data, the source node being linked with each of the general nodes by at least one independent path, the data being encoded by using an encoding matrix at the source node and the relay node. Any one node from among the source node and the general nodes includes a determining unit that determines a general node from among the general nodes that has maximum number of independent paths up to the source node; a setting unit that sets a size of a set formed by elements of the encoding matrix; a calculating unit that calculates a tap-proof index that indicates security level against tapping of the data flowing in the communication system based on the maximum number of independent paths and the size of the set; and a controlling unit that controls the tap-proof index.

[0011] In another useful embodiment, which is not within the scope of this invention, there is provided a communication system including a source node that generates the data and a plurality of general nodes, each being a destination node for the data or a relay node for relaying the data, the source node being linked with each of the general nodes by at least one independent path, the independent path including at least one communication link, the data being encoded at the source node and the relay node. Any one node from among the source node and the general nodes including a determining unit that determines a general node from among the general nodes that has maximum number of independent paths up to the source node; an encoding-vector calculating unit that calculates an encoding vector corresponding to each of the communication links; an encoding unit that encodes data passing through a communication link by multiplying an encoding vector corresponding to the communication link to the data passing through the communication; a subspace calculating unit that calculates a subspace of each of the encoding vectors; a selecting unit that selects encoding vectors of less than or equal to a second maximum number of independent paths from among the encoding vectors, the second maximum number of independent paths being one less than the maximum number of independent paths; a first selected-subspace calculating unit that calculates, when number of the encoding vectors selected by the selecting unit is less than the second maximum number of independent paths, a vector subspace that is formed by the encoding vectors selected by the selecting unit and a vector, the vector belonging to a group of vectors that have number of dimensions equal to the maximum number of independent paths with only one of components being 1 and all other components being 0; a second selected-subspace calculating unit that calculates, when the number of the encoding vectors selected by the selecting unit is equal to the second maximum number of independent paths, a vector subspace formed by only the encoding vectors selected by the selecting unit; a deselecting unit that deselects the vector subspace calculated by any one of the first selected-subspace calculating unit and the second selected-subspace calculating unit when the vector subspace includes the subspace calculated by the subspace calculating unit, wherein the selecting unit, the first selected-subspace calculating unit, the second selected-subspace calculating unit, and the deselecting unit repeat their operations if there is a vector in the group yet to be processed by the first selected-subspace calculating unit and an encoding vector yet to be selected by the selecting unit; and an assigning unit that assigns an encoding vector, the vector subspace of which is not deselected by the deselecting unit, to the communication link.

[0012] The above and other objects, features, advantages and technical and industrial significance of this invention will be better understood by reading the following detailed description of presently preferred embodiments of the invention, when considered in connection with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013]

Fig. 1 is an exemplary schematic diagram of a communication system according to a first embodiment of the present invention;

Fig. 2 is an exemplary schematic diagram of a communication system that is out of the scope of the first embodiment;
Fig. 3 is another exemplary schematic diagram of a communication system according to the first embodiment;
Fig. 4 is a schematic diagram of data transmitted from a source node shown in Fig. 3;
Fig. 5 is an exemplary diagram depicting a plurality of links originating from the source node;
Fig. 6 is an exemplary schematic diagram of links inbound to a general node and links emerging from the general node;
Fig. 7 is a flowchart of an exemplary procedure of determining whether data encoding is tap-proof;
Fig. 8 is an exemplary schematic diagram of a communication system considered to be tapped by another tapping approach;
Fig. 9 is a diagram of an exemplary encoding vector;
Fig. 10 is an exemplary schematic diagram of a communication system in which an encoding method according to a second embodiment, which is not within the scope of this invention, is implemented;
Figs. 11A and 11B are flowcharts of an exemplary procedure of selecting encoding vectors corresponding to one of a plurality of links shown in Fig. 10; and
Fig. 12 is a flowchart of an exemplary procedure of selecting the encoding vectors corresponding to all the links of all nodes shown in Fig. 10.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Exemplary embodiments of the present invention are described in detail below with reference to the accompanying drawings. The present invention is not limited to these exemplary embodiments.

[0015] Fig. 1 is an exemplary schematic diagram of a communication system 10 according to a first embodiment of the present invention. The communication system 10 includes a plurality of communication devices called nodes from 1-1 to 1-8. Each of the nodes 1-1 to 1-8 is linked by a link L having a predetermined communication direction shown by arrow marks in Fig. 1. For example, a link L1 links the node 1-3 to the node 1-4 such that the node 1-3 can transmit data to the node 1-4 but not vice versa.

[0016] A communication system shown in Fig. 2 is out of the scope of the first embodiment; because, it includes a recursive communication path. That is, a link L emerging from a node 1-1 eventually returns to the node 1-1.

[0017] Fig. 3 is another exemplary schematic diagram of a communication system 20 according to the first embodiment. The first embodiment is described in detail below with reference to Fig. 3. The communication system 20 includes a source node 2 for transmitting information and general nodes from 1-1 to 1-12. A general node functions as a relay node for relaying the information or a destination node for receiving the information. The source node 2 is linked to each of the general nodes 1-1 to 1-12 by one or more independent paths. Each independent path linking a source node to a destination node includes exclusive links L. For example, if the general node 1-3 is the destination node, three independent paths exist between the source node 2 and the destination node: a path RT1 through the relay nodes 1-1 and 1-2, a path RT2 through the relay node 1-4, and a path RT3 through the relay nodes 1-7 and 1-6.

[0018] The number of independent paths inbound to each of the general nodes 1-1 to 1-12 is counted, and the general node having the maximum number, d, of inbound independent paths is determined. For example, in the communication system 20, the source node 2 is linked to the general node 1-9 by four independent paths, which is more than in case of any other general nodes 1-1 to 1-8 and 1-10 to 1-12. Therefore, for the communication system 20 the value of d is four (d=4).

[0019] Given below is the description of how data is transmitted in the communication system 20. First, scalar quantization is performed to obtain a set of scalars that form components of a vector. An integer 'Z' is divided by a prime number 'p' to obtain a finite set of remainders 'K' on which all four arithmetic operations can be performed. The size of the set K (i.e., the number of remainders in the set K) is considered to be 'k'. Naturally, the value of k is equal to that of p. The set K can be expressed as follows:

$$K=\{x \mid x=\mathrm{mod}(Z,p)\}=\{0,1,2,\ldots,p-1\} \quad (1)$$

[0020] To simplify the description, the value of p is set to 2. A d-dimensional vector is generated from the elements of the set K and is considered to be the unit of encoding. In other words, the data is transmitted by digitizing and encoding (encrypting) in the form of d-dimensional vectors having the elements of the set K as their components.

[0021] Fig. 4 is a schematic diagram of data transmitted from the source node 2 toward a destination node. The data is digitized into d-dimensional vectors such as vectors 3-1, 3-2, 3-3, ... Elements 'KG' of the set K form components of the vectors 3-1, 3-2, 3-3, ... Hereinafter, a d-dimensional vector such as any one of the vectors 3-1, 3-2, 3-3, ... is referred to as a d-dimensional vector 3. As described above, because the value of p is set to 2, the elements KG are 0 and 1. The data in the source node 2 is divided in d-dimensional vectors and transmitted in the order of the vector 3-1, the

vector 3-2, the vector 3-3, and so on. The data corresponding to each of the vectors 3-1, 3-2, 3-3, ..., i.e., the components of each of the vectors 3-1, 3-2, 3-3, ... are transmitted through the corresponding d number of independent paths.

[0022] Given below is the description of how the source node 2 encodes data before transmitting the data to another node. Fig. 5 is an exemplary diagram depicting 's' number of the links L originating from the source node 2. First, data in the form of a d-dimensional vector VS1 formed by arbitrary remainders in the set K is multiplied by a matrix MS1 having s number of columns and d number of rows to obtain a data vector VSD1. The data vector VSD1 is transmitted to each of the links L corresponding to the d number of independent paths. That is, the data vector VSD1 is transmitted as the d-dimensional vector 3 in an encoded form. Equation (2) is an example of the data vector VSD1 when p=2, d=3, and s=4.

$$VSD1 = MS1 \cdot VS1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (2)$$

[0023] The order of the matrix MS1 used in Equation (2) is exemplary and not limited to that is actually shown. The matrix MS1 can be any matrix formed by the elements in the set K and having s number of columns and d number of rows.

[0024] Given below is the description of how a general node 1-n (n is a natural number representing node number). Fig. 6 is an exemplary schematic diagram depicting 'm' number of links L inbound to the general node 1-n and 's' number of links L emerging from the general node 1-n. In this example, the general node 1-n receives data transmitted through each of the m number of links L. The data transmitted to the general node 1-n from the source node 2 and through the links L is in the form of the elements of the set K. The data transmitted to the general node 1-n can be expressed as a one dimensional vector VT2. The one dimensional vector VT2 can be converted to a data vector VD2 by multiplying by a matrix MT having s number of columns and one row. The data vector VD2 is transmitted through the links L emerging from the general node 1-n to subsequent nodes. Equation (3) is an example of the data vector VD2 when p=2, 1=4, and s=2.

$$VTD2 = MT2 \cdot VT2 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (3)$$

[0025] The order of the matrix MT used in Equation (3) is exemplary and not limited to that actually shown. The matrix MT can be any matrix formed by the elements in the set K and having s number of columns and d number of rows. As described above, because it is assumed that a recursive communication path is out of the scope of the first embodiment, the data to be transmitted through each of the links L can be determined by repeating the encoding procedures.

[0026] Such encoding process is performed in all the general node 1-n that exist between the source node 2 and the destination node. As a result, encoded data reaches the destination node. In this process of encoding, it is necessary to protect the encoding parameters, i.e., the matrices MS1 and MT, so that an unauthorized person can not tap them. Even if an unauthorized person is successful in tapping encoded data in any of the links, the original data remains protected until the encoding parameters remain undetected. Thus, from the security point of view, it is necessary to prevent the encoding parameters from getting detected or at least prolong the amount of time at which the data code may be broken.

[0027] To achieve that object, first, the security (safety) level against tapping is determined by defining a tap-proof index that represents the average number of times for which a tapping procedure needs to be repeated to tap the entire encoding method, i.e., the matrices MS1 and MT. Such a tap-proof index F(k,d) can be expressed by Equation (4):

$$F(k,d) = \sum_{j=1}^{d} \frac{k^j}{k^j - 1} \qquad (4)$$

[0028] If the value of the tap-proof index F(k,d) is higher than a predetermined threshold, the encoding is considered to be sufficiently tap-proof. On the other hand, if the value of the tap-proof index F(k,d) is lower than a predetermined threshold, the encoding is considered to be vulnerable to tapping. Fig. 7 is a flowchart of an exemplary procedure for determining whether the encoding is tap-proof. First, the size of the set K, i.e., the value of p is determined (step S11). Then, the maximum number d by which the source node 2 is linked to the general node 1-n is counted (step S12). The tap-proof index is obtained by Equation (4) by using the values of p and d (step S13). It is then determined whether the tap-proof index is higher than a predetermined threshold (step S14). If the tap-proof index is higher than the predetermined threshold (YES at step S14), the encoding is considered to be sufficiently tap-proof (step S15). On the other hand, if the tap-proof index is lower than the predetermined threshold (NO at step S14), the encoding is considered to be vulnerable to tapping (step S16).

[0029] Thus, with this procedure it can be determined whether the encoding, i.e., the set K is tap-proof. A tap-proof coding (also known as wire-tap robust coding, i.e., WTRC) can be achieved by appropriately adjusting the size of the set K, e.g., in the source node 2 or the general node 1-n.

[0030] The set K can be then notified to all the general nodes (in this case, the source node 2 and the general node 1-n) such that tap-proof coding can be performed at each general node. Alternatively, an external computing device can also be used to determine whether the encoding is tap-proof. When an external computing device is used, the size of the set K can be adjusted based on the determination of the external computing device and then used when encoding the data at each general node.

[0031] Sometimes it may not be possible to adjust the size of the set K due to some restrictions. In that case, other parameters in the communication system can be adjusted such that the security level of the transmitted data improves.

[0032] Meanwhile, Equation (4) is used under the assumption that all the data transmitted by each of the links L is tapped. However, Equation (4) can also be used in the following case. Fig. 8 is an exemplary schematic diagram of a communication system 30 in case a tapping approach other than the abovementioned tapping is adopted. The dotted lines shown in Fig. 8 indicate that the links between the corresponding general nodes are abbreviated for simplification.

[0033] In the communication system 30, the data in the form of a d-dimensional vector transmitted from the source node 2 is tapped along with the elements of the set K transmitted through a link LT. Moreover, it is also assumed that the relation between the d-dimensional vector and elements of the set K can be obtained by repetitive tapping for a number of times. To handle such a case, Equation (4) can be used to calculate the average number of times for which the repetitive tapping is required. In other words, Equation (4) can be used to protect the encoding not only when the matrices MS1 and MT are assumed to be tapped but also when the d-dimensional vector and the elements of the set K are assumed to be tapped.

[0034] As described above, data encoding is performed in each node of the communication systems 10, 20, 30. A source node in the communication system is linked to all general nodes by one or more independent paths. The number of independent paths by which the source node is linked to each of the general nodes is counted and the general node having the maximum number of inbound independent paths is determined. A tap-proof index is calculated based on the maximum number of independent paths and the size of a set of elements formed by data transmitted in the communication system. The security level against tapping of the data is determined based on whether the value of the tap-proof index is higher than a predetermined threshold. A tap-proof data can be transmitted by appropriately adjusting the size of the set of elements such that the value of the tap-proof index is higher than the predetermined threshold.

[0035] In the communication systems 10, 20, 30, the security level against tapping is evaluated based on the tap-proof index. However, depending on the values of the elements in the matrices used in the encoding, there is a possibility of original data being transmitted without encoding. Although adopting the encoding method makes it difficult to tap the entire data or the encoding parameters, it is undesirable that the original data gets transmitted. For example, it is dangerous to transmit a portion of a credit-card number without encrypting. To take care of this issue, another encoding method that prevents transmission of original data over a network is described below as a second embodiment, which is not part of this invention. The structure of a communication system according to the second embodiment is identical to that according to the first embodiment.

[0036] In the encoding method according to the first embodiment, the data in the form of a d-dimensional vector is multiplied by the matrix MT. The matrix MT can be assumed to be formed by d-dimensional row vectors corresponding to each of the links L emerging from a particular node and the column vectors equal to the number of links L. In case of the source node 2, it can be assumed that for each of the links L transmitting the data (elements of the set K), a d-dimensional row vector is multiplied to the d-dimensional vector VS1, which is the data in the source node 2. A d-dimensional row vector under this assumption is referred to as an encoding vector ECVT. Fig. 9 is a diagram of an

exemplary encoding vector ECVT when the maximum number of independent paths, i.e. the value of d is equal to four (d=4). According to the second embodiment, **which is not part of this invention**, it is assumed that the encoding vector ECVT is separately determined for each of the links L. The object is to propose an appropriate way of determining the elements of the encoding vector ECVT such that transmission of raw data over the network is prevented.

[0037] Fig. 10 is an exemplary schematic diagram of a communication system 40 in which the encoding method according to the second embodiment, **which is not part of this invention**, is implemented. The communication system 40 includes a plurality of nodes from 1-1 to 1-6. Each of the nodes 1-1 to 1-6 is linked by a link L having a communication direction from a node with a lower reference numeral towards a node with a higher reference numeral (in this case, the reference numeral 1-1 is lower than the reference numeral 1-2, the reference numeral 1-2 is lower than the reference numeral 1-3, and so on). Such a numbering is possible because, alike in the first embodiment, the communication system shown in Fig. 2 that includes a recursive communication path is out of the scope of the second embodiment. The encoding vector ECVT is determined in the order of the nodes with lower reference numerals.

[0038] The encoding vector ECVT corresponding to a link L emerging from, e.g., the general node 1-n (n is a natural number representing node number) is determined as given below. First, consider a liner combination V of, e.g., two encoding vectors ECVT. The linear combination V is a plane including the two encoding vectors ECVT. Reference may be had to "Linear network coding" (Vol. 49, No. 2, February 2003, pp. 371-381) by S-Y. R. Li et al., which is incorporated herein by reference and in which it is described that selecting a general vector from the linear combination V gives the best result.

[0039] According to the second embodiment, additional conditions are set while selecting the general vector to prevent the transmission of original data over the network. First, an ej-vector is determined in which only j-th component of d-th dimension has the value 1 and all other components have the value 0 (zero). The number of links L inbound to the general node 1-n is considered to be 't'. The subspace formed by the encoding vectors ECVT corresponding to the t number of links L is referred to as a subspace V. From among the encoding vectors ECVT corresponding to the links L emerging from the nodes with lower reference numerals than the general node 1-n, the encoding vectors ECVT less than the maximum number of independent paths are selected (i.e., the number of selected encoding vectors ECVT$\leq$(d-1)). When the number of selected encoding vectors ECVT is not equal to (d-1), one ej-vector is selected. The subspace formed by the t number of the encoding vectors ECVT and the one ej-vector is referred to as a subspace W. If the subspace W includes the subspace V, the subspace W is not considered for further procedure. When the number of selected encoding vectors ECVT is equal to (d-1), the subspace formed only by the selected encoding vectors ECVT is referred to as a subspace W. In that case also, if the subspace W includes the subspace V, the subspace W is not considered for further procedure. Irrespective of the selected encoding vectors ECVT and the ej-vector, the elements of the subspace V, which is not included in the subspace W, are assigned to be the encoding vector of the links L emerging from the general node 1-n.

[0040] Figs. 11A and 11B are flowcharts of an exemplary procedure of selecting the encoding vectors ECVT corresponding to one of the links L. First, the subspace V formed by the encoding vectors ECVT corresponding to the t number of links L inbound to the general node 1-n is obtained (step S21). A set X of must-be-avoided subspace from among the subspace V is then put into an empty set (step S22). From among the encoding vectors ECVT corresponding to links L emerging from the nodes with lower reference numerals than the general node 1-n, the encoding vectors ECVT less than (d-1) are selected (step S23). When the step S23 is repeated after returning from step S33 described below, the encoding vectors ECVT are selected from among the encoding vectors ECVT selected at the previous time at step S23.

[0041] It is then determined whether the number of selected encoding vectors ECVT is equal to (d-1) (step S24). If the number of selected encoding vectors ECVT is equal to (d-1) (YES at step S24), the system control proceeds to step S30. If the number of selected encoding vectors ECVT is not equal to (d-1) (NO at step S24), one ej-vector is selected (step S25). When the step S25 is repeated, the ej-vector is selected from among the ej-vectors not selected at the previous time at step S25.

[0042] The subspace W formed by the selected encoding vectors ECVT and the selected ej-vector is obtained (step S26). It is then determined whether the subspace W includes the subspace V (step S27). If the subspace W includes the subspace V (YES at step S27), the system control proceeds to step S29. If the subspace W does not include the subspace V (NO at step S27), the system control proceeds to step S28. The subspace W is added to the set X (step S28).

[0043] It is determined whether there is any ej-vector that has yet to be selected at step S25 (step S29). If there is a yet to be selected ej-vector (YES at step S29), the system control returns to step S25. If all the ej-vectors are selected (NO at step S29), the system control proceeds to step S30. The subspace W formed only by the selected encoding vectors ECVT at step S23 is obtained (step S30). It is then determined whether the subspace W includes the subspace V (step S31). If the subspace W includes the subspace V (YES at step S31), the system control proceeds to step S33. If the subspace W does not include the subspace V (NO at step S31), the subspace W is added to the set X (step S32).

[0044] It is then determined whether the selected encoding vectors ECVT are still less than (d-1) (step S33). If the selected encoding vectors ECVT are still less than (d-1) (YES at step S33), the system control returns to step S23. If no more encoding vectors ECVT can be selected (NO at step S33), an encoding vector ECVT is selected from the

subspace V, which is not included in the subspace W in the set X, and assigned to be the encoding vector ECVT of the corresponding link L emerging from the general node 1-n (step S34).

[0045] The abovementioned procedure can be performed with respect to each of the links L emerging from the general node 1-n. Fig. 12 is a flowchart of a procedure of selecting the encoding vectors ECVT corresponding to all the links L of all the nodes (the source node 2 and the general nodes such as the general node 1-n) in the communication system 40. First, a node is selected from among the nodes on which encoding-vector processing is yet to be performed (step S41). From among the links L emerging from the selected node, one link L is selected on which encoding-vector processing is to be performed (step S42). The encoding vectors ECVT are selected corresponding to the selected link L by following the steps described in the abovementioned flowchart with reference to Figs. 11b and 11B (step S43). It is then determined whether all the links L emerging from the selected node are selected for encoding-vector processing (step S44). If all the links L are not yet selected for encoding-vector processing (NO at step S44), the procedure returns to step S42. If all the links L are already selected for encoding-vector processing (YES at step S44), it is determined whether there is any node on which encoding-vector processing is yet to be performed (step S45).

[0046] If there is a node on which encoding-vector processing is yet to be performed (YES at step S45), the system control returns to step S42. If encoding-vector processing is already performed on all the nodes (NO at step S46), the procedure ends.

[0047] As described above, encoding vectors are determined for each of the links emerging from each of the nodes. Alternatively, encoding vectors can be determined for each of the links emerging from a particular node and then notified to the other nodes. Moreover, an external computing device can also be used to determine the encoding vectors and set as the encoding vectors for each of the nodes.

[0048] If the subspace W includes the subspace V, the subspace W is not considered for further operations. Thus, the encoding vector ECVT is selected from the subspace V not included in the subspace W. As a result, in addition to the advantages according to the first embodiment, un-encoded raw data is prevented from being transmitted over the network thereby improving the data confidentiality and data security.

[0049] According to one aspect of the present invention, data encoding is performed in each node of a communication system. A source node in the communication system is linked to all general nodes by one or more independent paths. The number of independent paths by which the source node is linked to each of the general nodes is counted and the general node having the maximum number of inbound independent paths is determined. A tap-proof index indicating security level against tapping of data is calculated based on the maximum number of independent paths and the size of a set of elements formed by the data transmitted in the communication system. The tap-proof index is set to be higher than a predetermined threshold thereby improving the security level of data transmission in the communication system.

[0050] Although the invention has been described with respect to specific embodiments for a complete and clear disclosure, the appended claims are not to be thus limited but are to be construed as embodying all modifications and alternative constructions that may occur to one skilled in the art that fairly fall within the basic teaching herein set forth.

Claims

1. A method of transmitting data in a communication system **(10, 20, 30)**, the communication system **(10, 20, 30)** including a source node **(2)** that generates the data and a plurality of general nodes **(1-1 to 1-12)**, each being a destination node for the data or a relay node for relaying the data, the source node **(2)** being linked with each of the general nodes **(1-1 to 1-12)** by at least one independent path **(RT1 to RT3)**, the data being encoded by using an encoding matrix at the source node **(2)** and the relay node, the method comprising:

   determining a general node from among the general nodes **(1-1 to 1-12)** that has maximum number of independent paths up to the source node **(2)** ;
   setting a size of a set formed by elements of the encoding matrix;
   calculating a tap-proof index that indicates security level against tapping of the data flowing in the communication system **(10, 20, 30)** based on the maximum number of independent paths and the size of the set; and
   controlling the tap-proof index.

2. The method according to claim 1, wherein the controlling includes determining whether the tap-proof index is higher than a threshold, and when the tap-proof index is lower than the threshold, resetting the size of the set such that the tap-proof index becomes higher than the threshold.

3. A communication system **(10, 20, 30)** including a source node **(2)** that generates the data and a plurality of general nodes **(1-1 to 1-12),** each being a destination node for the data or a relay node for relaying the data, the source node **(2)** being linked with each of the general nodes **(1-1 to 1-12)** by at least one independent path **(RT1 to RT3)**,

the data being encoded by using an encoding matrix at the source node **(2)** and the relay node, any one node from among the source node **(2)** and the general nodes **(1-1 to 1-12)** comprising:

a determining unit that determines a general node from among the general nodes **(1-1 to 1-12)** that has maximum number of independent paths up to the source node **(2)** ;
a setting unit that sets a size of a set formed by elements of the encoding matrix;
a calculating unit that calculates a tap-proof index that indicates security level against tapping of the data flowing in the communication system **(10)** based on the maximum number of independent paths and the size of the set; and
a controlling unit that controls the tap-proof index.

4. The communication system **(10, 20, 30)** according to claim **3**, wherein the controlling unit determines whether the tap-proof index is higher than a threshold, and when the tap-proof index is lower than the threshold, resets the size of the set such that the tap-proof index becomes higher than the threshold.

Patentansprüche

1. Verfahren zum Übertragen von Daten in einem Kommunikationssystem (10, 20, 30), wobei das Kommunikationssystem (10, 20, 30) einen Quellknoten (2) umfasst, der die Daten erzeugt, sowie eine Vielzahl von allgemeinen Knoten (1-1 bis 1-12), von denen jeder ein Zielknoten für die Daten oder ein Vermittlungsknoten zum Vermitteln der Daten ist, wobei der Quellknoten (2) mit jedem der allgemeinen Knoten (1-1 bis 1-12) durch mindestens einen unabhängigen Pfad (RT1 bis RT3) verbunden ist, wobei die Daten kodiert werden unter Verwendung einer Kodiermatrix am Quellknoten (2) und dem Vermittlungsknoten, wobei das Verfahren umfasst:

Bestimmung eines generellen Knotens aus den generellen Knoten (1-1 bis 1-12), der eine größte Anzahl an unabhängigen Pfaden aufwärts zu dem Quellknoten (2) besitzt;
Festsetzen einer Größe eines Sets, das durch die Elemente der kodierenden Matrix gebildet wird;
Berechnung eines Abhörsicherungs-Index, der ein Sicherheitsniveau gegen Abhören der Daten anzeigt, die in dem Kommunikationssystem (10, 20, 30) fließen, auf der Grundlage der maximalen Anzahl von unabhängigen Pfaden und der Größe des Sets; und
Steuerung des Abhörsicherungs-Index.

2. Verfahren nach Anspruch 1, wobei die Steuerung umfasst die Bestimmung, ob der Abhörsicherungs-Index höher ist als ein Schwellwert, und wenn der Abhörsicherungs-Index niedriger ist als der Schwellwert Zurücksetzen der Größe des Sets derart, dass der Abhörsicherungs-Index höher wird als der Schwellwert.

3. Kommunikationssystem (10, 20, 30) umfassend einen Quellknoten (2), der die Daten erzeugt, und eine Vielzahl von allgemeinen Knoten (1-1 bis 1-12), von denen jeder ein Zielknoten für die Daten oder ein Vermittlungsknoten zum Vermitteln der Daten ist, wobei der Quellknoten (2) mit jedem der allgemeinen Knoten (1-1 bis 1-12) durch mindestens einen unabhängigen Pfad (RT1 bis RT3) verbunden ist, wobei die Daten codiert werden unter Verwendung einer Kodiermatrix an dem Quellknoten (2) und dem Vermittlungsknoten, wobei jeder Knoten der Quellknoten (2) und der allgemeinen Knoten (1-1 bis 1-12) umfasst:

eine Bestimmungseinheit, die einen allgemeinen Knoten aus den allgemeinen Knoten (1-1 bis 1-12) bestimmt, der eine maximale Anzahl an unabhängigen Pfaden aufwärts zu dem Quellknoten (2) besitzt;
eine Einstelleinheit, die eine Größe eines Sets festsetzt, dass durch Elemente der Codiermatrix gebildet wird;
eine Berechnungseinheit, die einen Abhörsicherungs-Index berechnet, der ein Sicherheitsniveau gegenüber Abhören der Daten, die in dem Kommunikationssystem (10) fließen, anzeigt, basierend auf der maximalen Anzahl an unabhängigen Pfaden und der Größe des Sets; und
eine Steuereinheit, die den Abhörsicherungs-Index steuert.

4. Kommunikationssystem (10, 20, 30) nach Anspruch 3, wobei die Steuereinheit bestimmt, ob der Abhörsicherungs-Index höher ist als ein Schwellwert und wenn der Abhörsicherungs-Index niedriger ist als der Schwellwert, die Größe des Sets derart zurücksetzt, dass der Abhörsicherungs-Index größer wird als der Schwellwert.

Revendications

1. Procédé de transmission de données dans un système de communication (10, 20, 30), le système de communication (10, 20, 30) comprenant un noeud source (2) qui génère les données et une pluralité de noeuds généraux (1-1 à 1-12), chacun étant un noeud de destination pour les données ou un noeud de relais pour relayer les données, le noeud source (2) étant lié à chacun des noeuds généraux (1-1 à 1-12) par au moins un trajet indépendant (RT1 à RT3), les données étant codées en utilisant une matrice codée au noeud source (2) et le noeud de relais, le procédé comprenant :

   la détermination d'un noeud général parmi les noeuds généraux (1-1 à 1-12) qui a un nombre maximal de trajets indépendants jusqu'au noeud source (2) ;
   la détermination d'une taille d'un ensemble formé par les éléments de la matrice de codage ;
   le calcul d'un indice anti-dérivation qui indique le niveau de sécurité contre la dérivation des données dans le système de communication (10, 20, 30) sur la base du nombre maximal de trajets indépendants et de la taille de l'ensemble ; et
   la régulation de l'indice anti-dérivation.

2. Procédé selon la revendication 1, dans lequel la commande comprend la détermination du fait que l'indice anti-dérivation est ou non supérieur à un seuil, et lorsque l'indice anti-dérivation est inférieur au seuil, la réinitialisation de la taille de l'ensemble, de sorte que l'indice anti-dérivation devienne supérieur au seuil.

3. Système de communication (10, 20, 30) comprenant un noeud source (2) qui génère les données et une pluralité de noeuds généraux (1-1 à 1-12), chacun étant un noeud de destination pour les données ou un noeud de relais pour relayer les données, le noeud source (2) étant lié à chacun des noeuds généraux (1-1 à 1-12) par au moins un trajet indépendant (RT1 à RT3), les données étant codées en utilisant une matrice de codage au noeud source (2) et au noeud de relais, un noeud quelconque parmi le noeud source (2) et les noeuds généraux (1-1 à 1-12) comprenant :

   une unité de détermination qui détermine un noeud général parmi les noeuds généraux (1-1 à 1-12) qui a un nombre maximal de trajets indépendants jusqu'au noeud source (2) ;
   une unité de définition qui définit une taille d'un ensemble formé par les éléments de la matrice de codage ;
   une unité de calcul qui calcule un indice anti-dérivation qui indique le niveau de sécurité contre la dérivation des données circulant dans le système de communication (10) sur la base du nombre maximal de trajets indépendants et de la taille de l'ensemble ; et
   une unité de commande qui régule l'indice anti-dérivation.

4. Système de communication (10, 20, 30) selon la revendication 3, dans lequel l'unité de commande détermine si l'indice anti-dérivation est supérieur à un seuil, et lorsque l'indice anti-dérivation est inférieur au seuil, réinitialise la taille de l'ensemble de sorte que l'indice anti-dérivation devient supérieur au seuil.

FIG.1

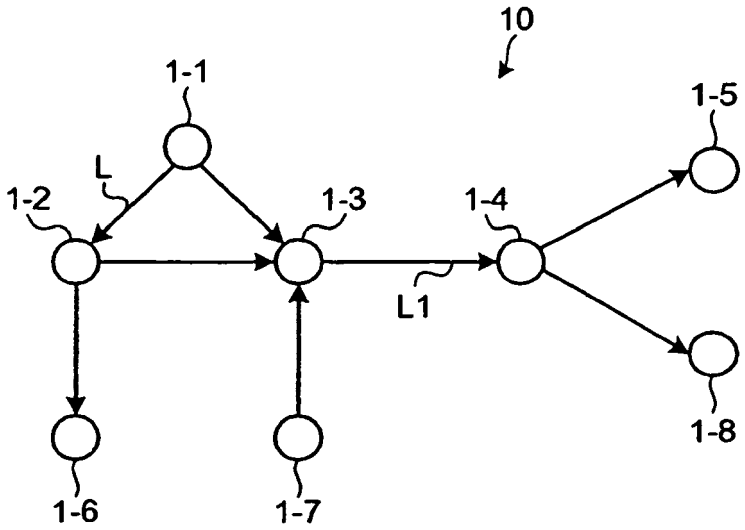


FIG.2

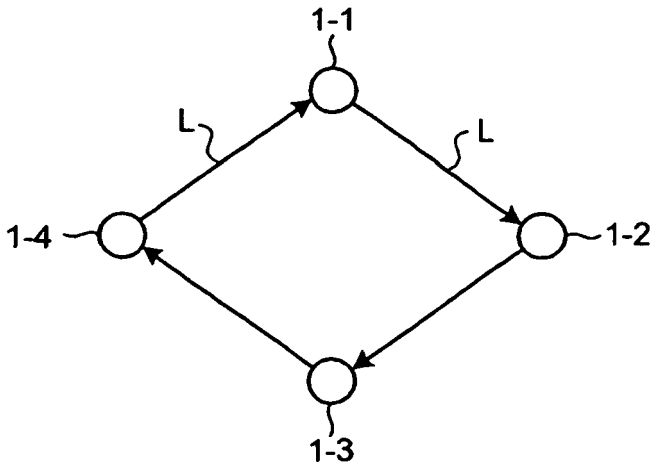


FIG.3

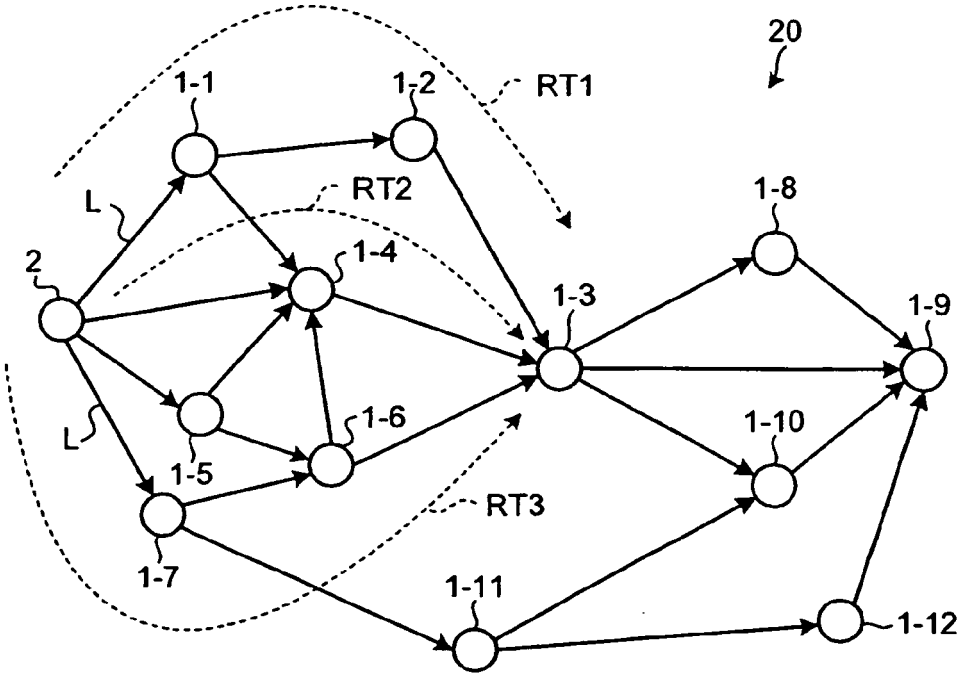

20
1-1
1-2
RT1
RT2
L
2
1-4
1-8
1-3
1-9
L
1-6
1-10
1-5
RT3
1-7
1-11
1-12

FIG.4

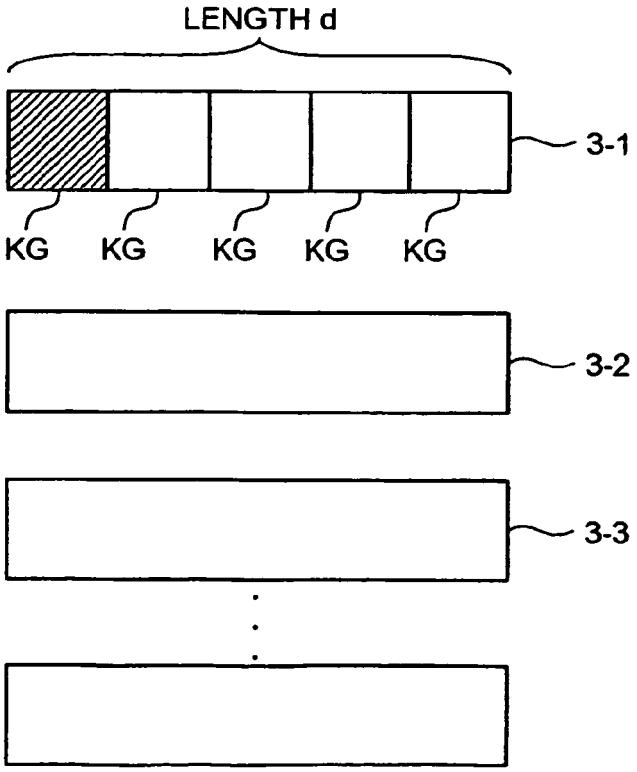

LENGTH d
3-1
KG
KG
KG
KG
KG
3-2
3-3

FIG.5

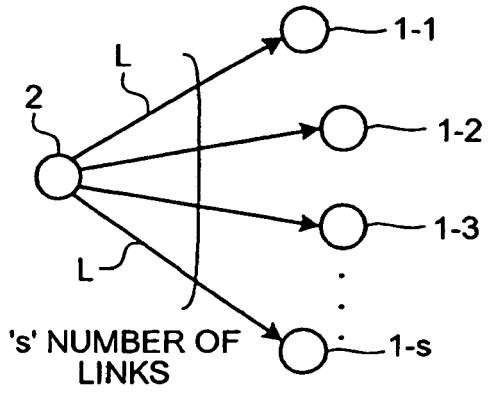

1-1
L
2
1-2
1-3
L
's' NUMBER OF LINKS
1-s

FIG.6

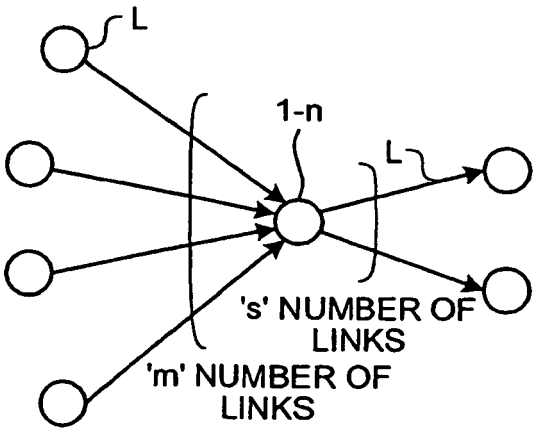

L
1-n
L
's' NUMBER OF LINKS
'm' NUMBER OF LINKS

FIG.7

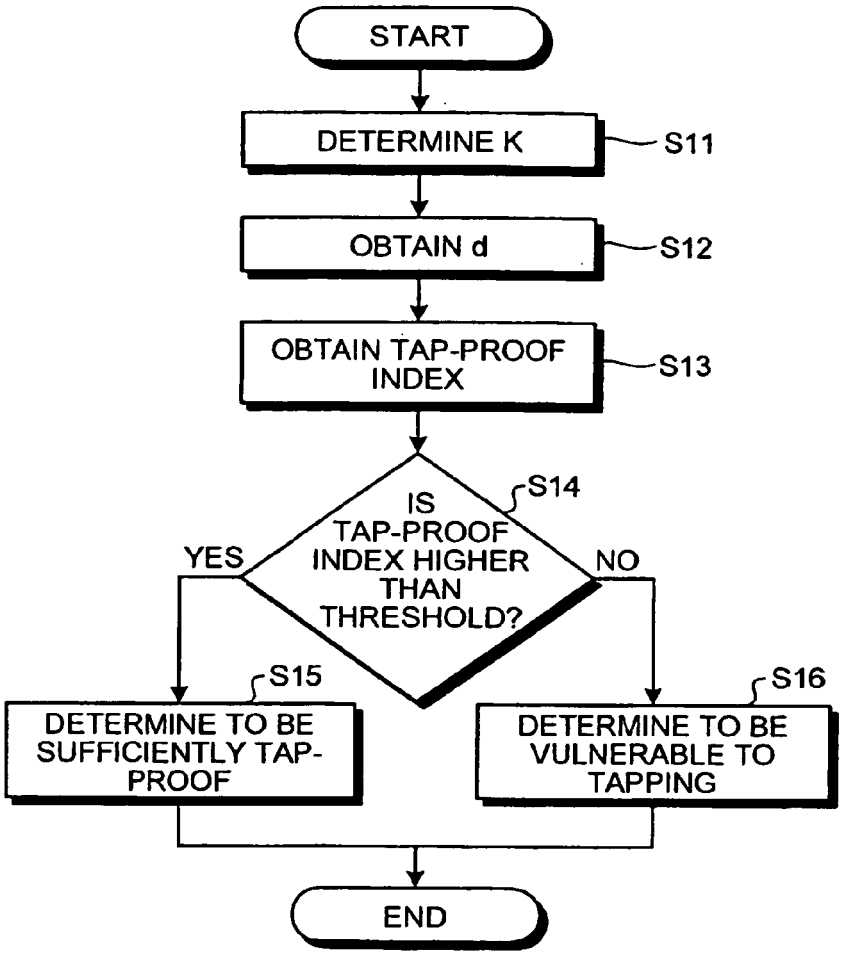

START
DETERMINE K
S11
OBTAIN d
S12
OBTAIN TAP-PROOF INDEX
S13
IS TAP-PROOF INDEX HIGHER THAN THRESHOLD?
S14
YES
NO
S15
DETERMINE TO BE SUFFICIENTLY TAP-PROOF
S16
DETERMINE TO BE VULNERABLE TO TAPPING
END

FIG.8

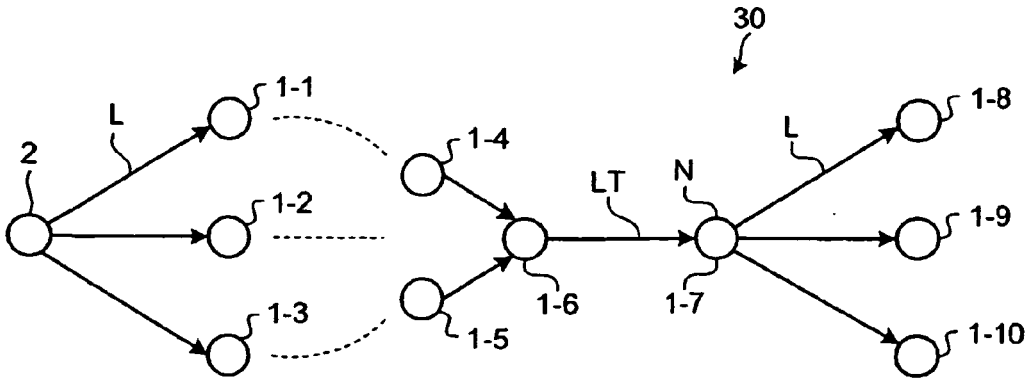

30
2
L
1-1
1-2
1-3
1-4
1-5
1-6
LT
N
1-7
L
1-8
1-9
1-10

FIG.9

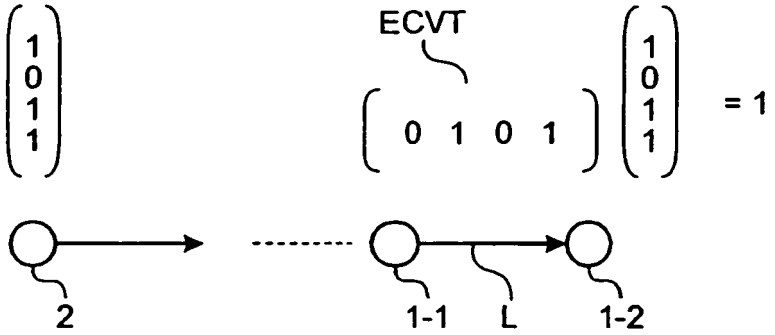


FIG.10

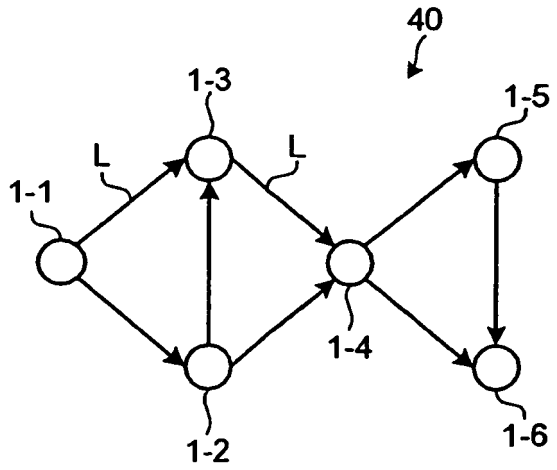


FIG.11A

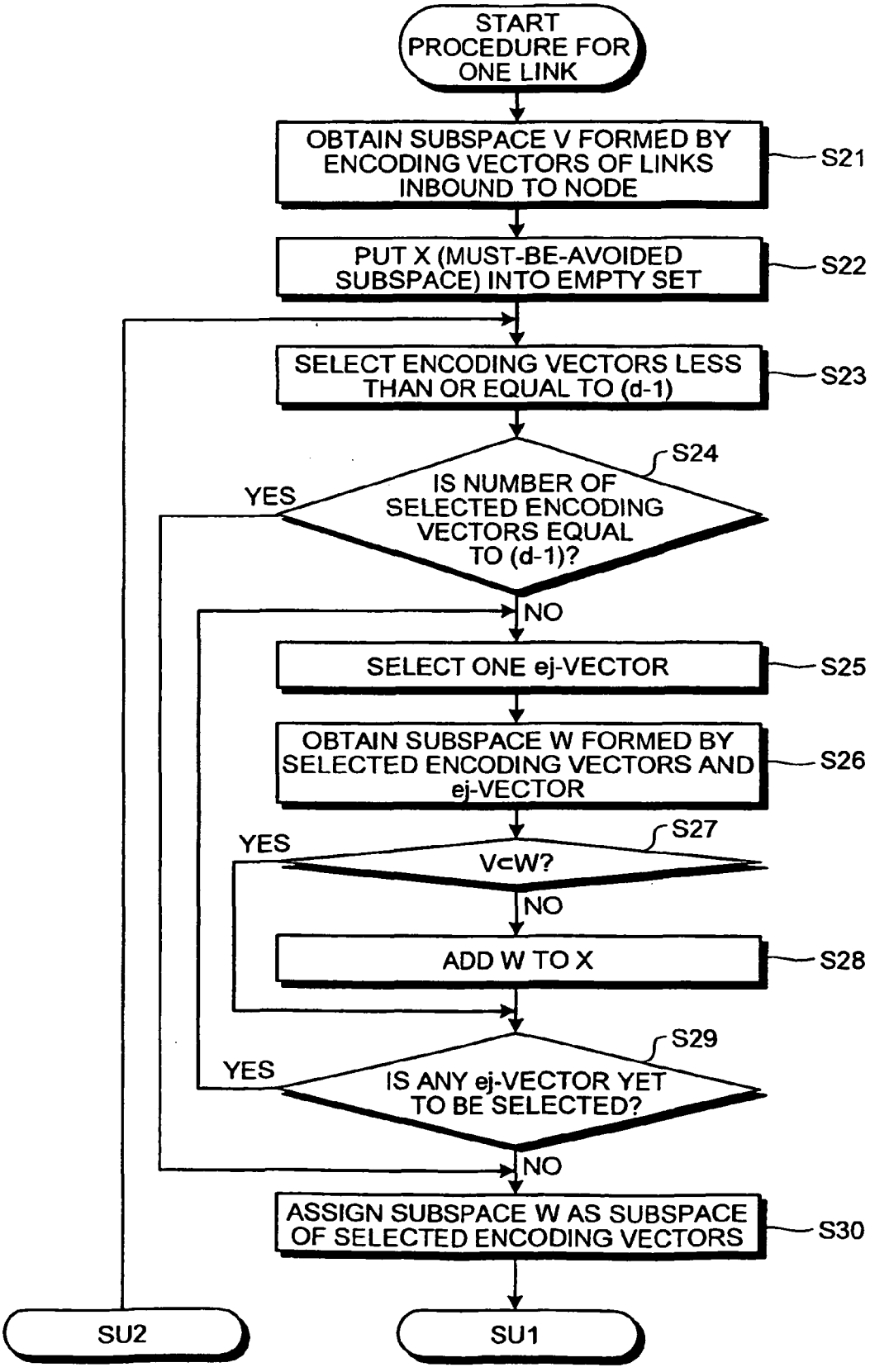

START PROCEDURE FOR ONE LINK
OBTAIN SUBSPACE V FORMED BY ENCODING VECTORS OF LINKS INBOUND TO NODE
S21
PUT X (MUST-BE-AVOIDED SUBSPACE) INTO EMPTY SET
S22
SELECT ENCODING VECTORS LESS THAN OR EQUAL TO (d-1)
S23
S24
IS NUMBER OF SELECTED ENCODING VECTORS EQUAL TO (d-1)?
YES
NO
SELECT ONE ej-VECTOR
S25
OBTAIN SUBSPACE W FORMED BY SELECTED ENCODING VECTORS AND ej-VECTOR
S26
S27
V⊂W?
YES
NO
ADD W TO X
S28
S29
IS ANY ej-VECTOR YET TO BE SELECTED?
YES
NO
ASSIGN SUBSPACE W AS SUBSPACE OF SELECTED ENCODING VECTORS
S30
SU2
SU1

FIG.11B

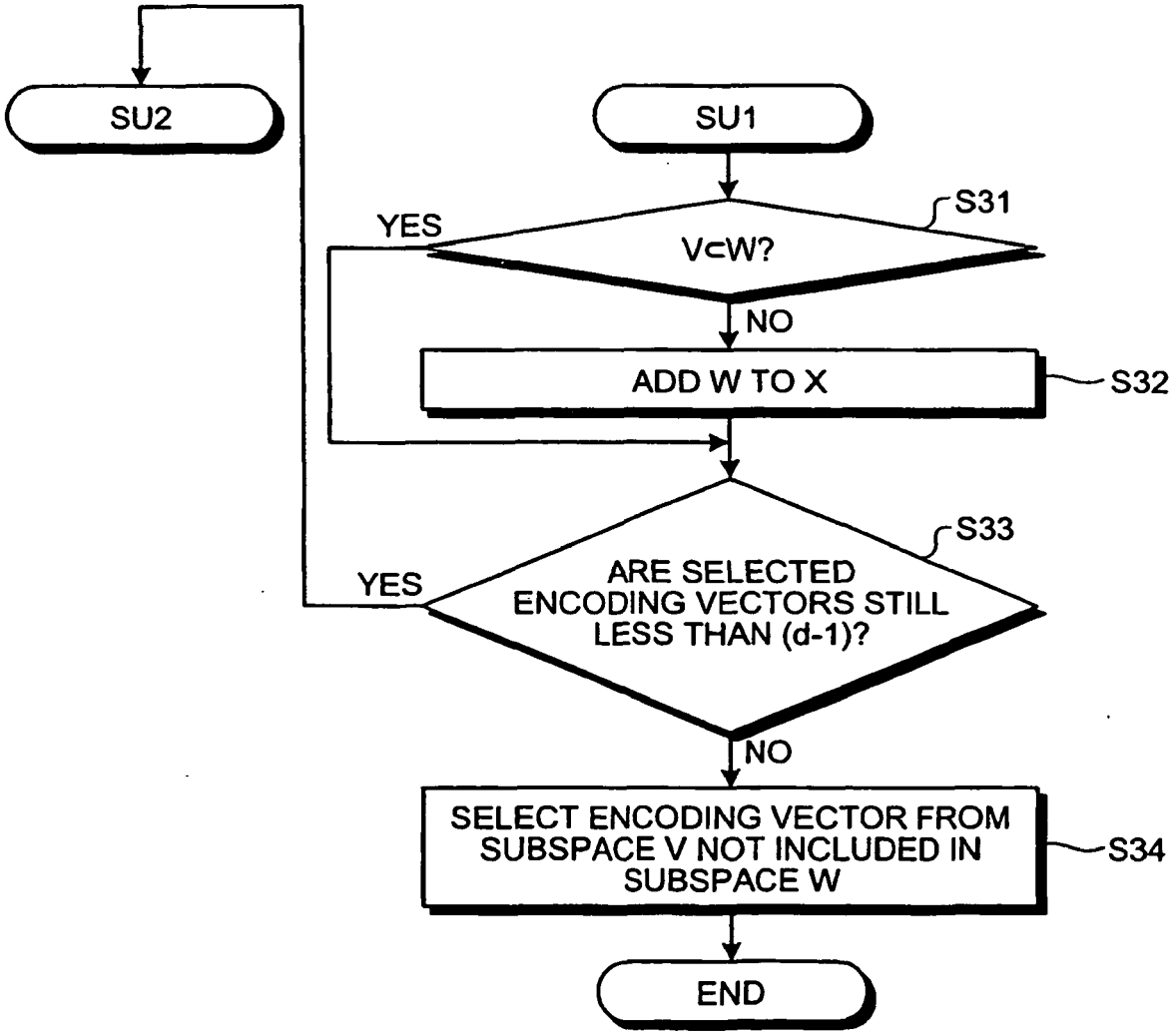
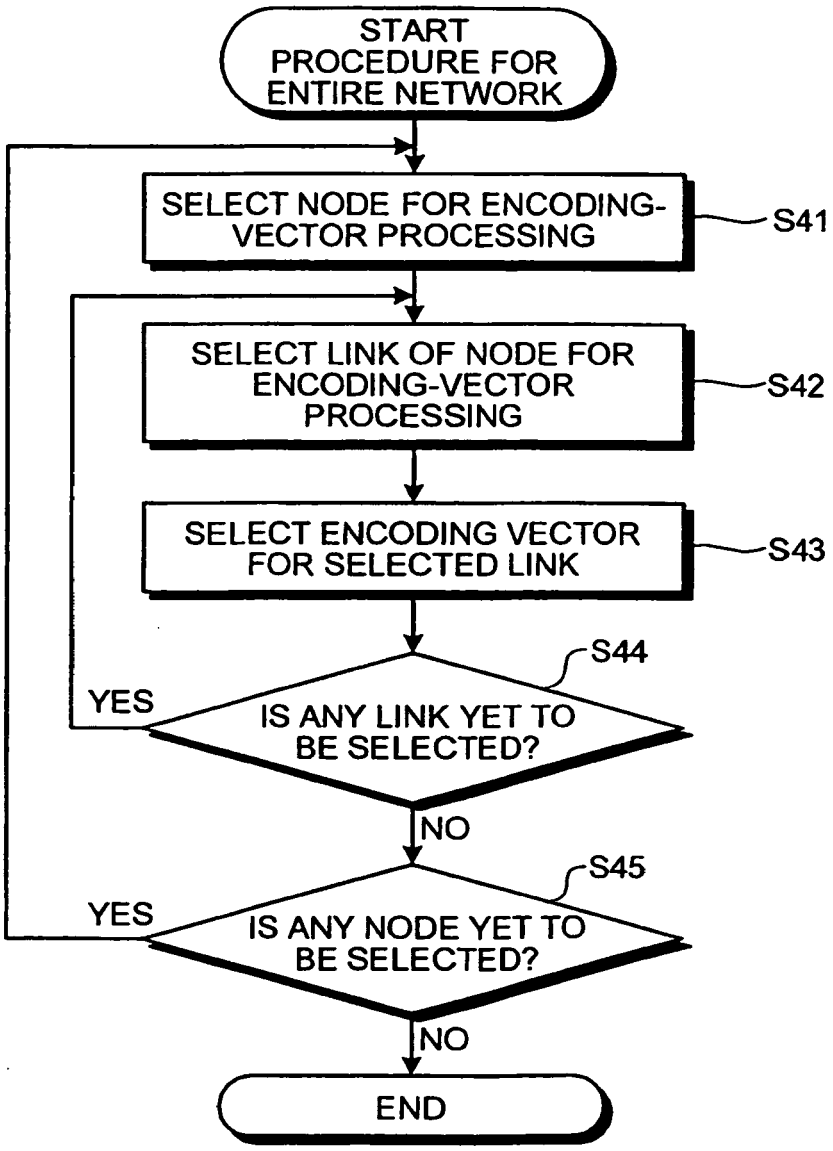

SU2
SU1
S31
YES
V⊂W?
NO
ADD W TO X
S32
S33
YES
ARE SELECTED ENCODING VECTORS STILL LESS THAN (d-1)?
NO
SELECT ENCODING VECTOR FROM SUBSPACE V NOT INCLUDED IN SUBSPACE W
S34
END

FIG.12


START PROCEDURE FOR ENTIRE NETWORK
SELECT NODE FOR ENCODING-VECTOR PROCESSING
S41
SELECT LINK OF NODE FOR ENCODING-VECTOR PROCESSING
S42
SELECT ENCODING VECTOR FOR SELECTED LINK
S43
S44
IS ANY LINK YET TO BE SELECTED?
YES
NO
S45
IS ANY NODE YET TO BE SELECTED?
YES
NO
END

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Non-patent literature cited in the description

- **R. AHLSWEDE et al.** Network information flow. *IEEE trans. on Information Theory,* July 2000, vol. 46 (4), 1204-1216 **[0003]**
- **YAMAMOTO MIKI.** Network coding. *Journal of Institute of Electronics, Information and Communication Engineers,* February 2007, vol. 90 (2), 111-116 **[0003]**
- **S-Y. R. LI et al.** *Linear network coding,* February 2003, vol. 49 (2), 371-381 **[0003]**
- **LUÍSA LIMA ; MURIEL MÉDARD ; JOÃO BARROS.** Random Linear Network Coding: A free cipher?. *Proc. of the IEEE International Symposium on Information Theory,* June 2007, 546-550 **[0006]**
- **S-Y. R. LI.** *Linear network coding,* February 2003, vol. 49 (2), 371-381 **[0038]**