(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 March 2020 (12.03.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/048611 A1

(51) International Patent Classification:
H04J 3/14 (2006.01) *H04L 12/707* (2013.01)
H04J 3/16 (2006.01) *H04L 12/24* (2006.01)
H04L 12/703 (2013.01)

(21) International Application Number:
PCT/EP2018/074147

(22) International Filing Date:
07 September 2018 (07.09.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building Bantian Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventor; and

(71) Applicant *(for US only)*: **GKATZIKIS, Lazaros** [GR/FR]; c/o Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(72) Inventors: **ZHAO, Min**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **LEGUAY, Jeremie**; Huawei Technologies Duesseldorf GmbH Riesstr.25, 80992 Munich (DE). **YAN, Kerong**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **XIA, Bin**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(74) Agent: **KREUZ, Georg**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

(54) Title: DEVICE, METHOD AND NETWORK SYSTEM FOR PROVIDING FAILURE DEPENDENT PROTECTION AND RECOVERING THE AFFECTED SERVICES

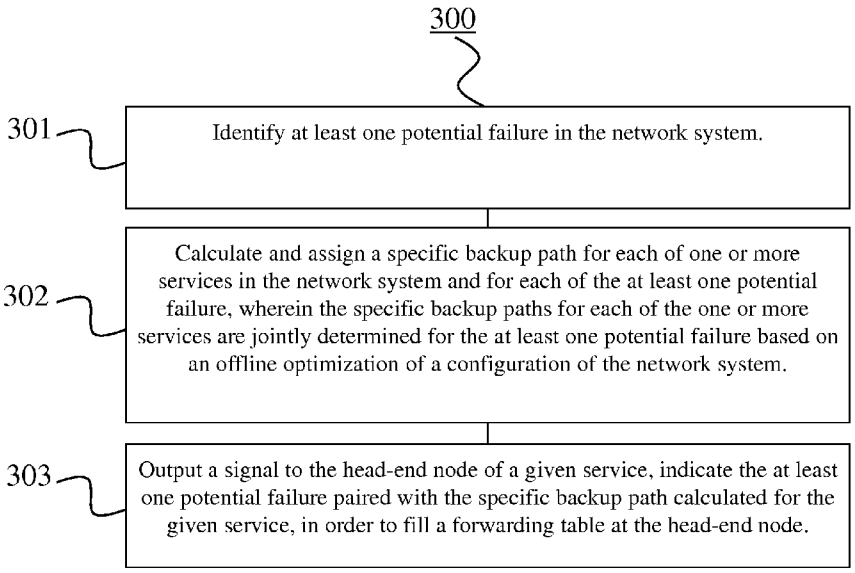

FIG. 3

(57) Abstract: The present invention is related to the field of failure-dependent protection in a network system. In particular, the present invention provides a device for providing failure dependent protection in a network system comprising a plurality of nodes. The device is configured to identify at least one potential failure in the network system; calculate and assign a specific backup path for each of one or more services in the network system and for each of the at least one potential failure, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system; and output a signal to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table at the head-end node.

WO 2020/048611 A1

[Continued on next page]

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

DEVICE, METHOD AND NETWORK SYSTEM FOR PROVIDING FAILURE DEPENDENT PROTECTION AND RECOVERING THE AFFECTED SERVICES

TECHNICAL FIELD

The present invention relates generally to the field of failure-dependent protection in a network system. More particularly, the present invention relates to a device, a method, and a network system for providing failure dependent protection and recovering the failing services in the network system.

BACKGROUND

Failure resilience is a crucial feature of all types of network systems. For example, in Optical Transport Networks (OTN), failures may be caused by various factors such as fiber cuts, amplifier dysfunctions, failures of electronic components, etc. In order to protect against such failures, various recovery schemes have been proposed.

Conventional devices and methods are based on two main types of recovery schemes including restoration and protection. The restoration (a.k.a. dynamic rerouting) is a reactive approach. The protection is a proactive approach, and hence the necessary resources for recovery have to be reserved in advance.

Furthermore, in the conventional devices and methods, which work based on the restoration, once a failure occurs, the rerouting of the affected services is calculated on-the-fly, and based on the current network state, by the head-end nodes or by the network controller. The network controller may be the Path Computation Element (PCE) in the Generalized Multiprotocol Label Switching (GMPLS) networks or the transport software defined network (T-SDN) (T-SDN) controller in the Automatically Switched Optical Networks (ASON). Restoration is a best-effort process, and hence a successful recovery cannot be guaranteed. In addition, restoration may be a slow process since it requires on-the-fly path calculation.

Moreover, the conventional devices and methods, which support protection, enable fast and guaranteed recovery, and they come in two different varieties including a link protection and a path protection scheme.

In the link protection, the end nodes of the failing link detect the failure, and may further detour the affected traffic from the failed link to another path. In the path protection, any failure occurring along the path of a service causes the head-end node to move the traffic to a pre-computed new route called backup path. Moreover, since the backup paths are established in advance, recovery is fast, however, the backup paths should be carefully designed so that the overall network resource reservation is minimized. The path protection is the most efficient of the conventional schemes.

However, the conventional protection schemes, e.g., in ASON or MPLS networks, which rely on pre-planned recovery paths, have a disadvantage of only considering the failure-independent paths, and consequently, any failure affecting the working path may cause traffic to move to a new backup path, which usually does not share any critical resources with the original path.

Additionally, an important aspect of protection is Shared Risk Groups (SRG). The SRG is a concept used in optical, Multiprotocol Label Switching (MPLS) or Internet Protocol (IP) networks to indicate, which network elements (e.g., nodes, links, etc.) may suffer from a common failure. The most commonly used SRG is related to the links, and is called Shared Risk Link Groups (SRLG). For example, all IP links transported by a single optical fiber may belong to the same SRLG, since they all may be down, for example, in the case of a fiber cut.

Next, three conventional protection based methods and their characteristics are discussed. A conventional protection method namely 1+1 is known, in which two signals are simultaneously sent over two SRG-disjoint paths. This ensures immediate recovery, since neither failure detection nor any reconfiguration is needed. However, the 1+1 protection method has the disadvantage that it significantly incurs a larger resource reservation (e.g., increases the cost of protection), since it actually doubles the traffic in the network system.

A second conventional protection method, namely 1:1 (or shared backups), is also known. The 1:1 method is a failure-independent protection scheme that uses shared backup paths. The 1:1 protection method reserves bandwidth for backup paths in such a way that if two paths do not fail together, they can possibly share the same backup reservation. The 1:1 protection method ensures a fast recovery, since only the intermediate switches need to be reconfigured. However, the 1:1 protection method has the disadvantage that it supports only partial resource sharing, since the reaction is the same to any failure in the network system.

Furthermore, a third conventional protection method, namely Failure-Dependent (FD) recovery, is also known. In this method a different backup path is selected for each possible SRG failure.

The FD recovery is more economical than the 1+1 and 1:1 methods, since it achieves the reuse of primary and backup resources. Moreover, the FD recovery has the characteristics that it enables re-using of released resources of primary paths (Stub release). Moreover, the backup paths do not have to be SRG-disjoint to the primary paths, and it further enables more sharing opportunities. From the above discussed benefits, it becomes evident that the failure-dependent (FD) recovery is a better option than 1+1 and 1:1 in terms of resource efficiency.

However, the FD recovery method has the disadvantage that it is a slow method, since SRG failure detection and backup establishment is a time-consuming process.

For example, when an SRG failure occurs, the conventional FD recovery schemes apply the following sequence of processes:

1. SRG failure detection and notification to the central network controller;
2. Calculation of failure-dependent backups by the central network controller (an optional process, since paths may be pre-computed and centrally stored on the control plane ((e.g., PCE)); and
3. Establishment of FD backup paths by the central network controller.

Shared Mesh Protection (SMP) is a specific method of implementing the FD protection without the intervention of a central controller. A detailed description including the

necessary signalling and the modules involved to support the SMP functionality can be found, for example, in the related ITU-T Standard documents of "G. 808.3 Generic protection switching-Shared mesh protection", and "G.873.3 optical transport network-Shared mesh protection".

The conventional existing failure-dependent protection mechanisms suffer from slow recovery, since they heavily rely on a centralized control plane (e.g., PCE). To overcome the slow recovery, the Shared Mesh Protection (SMP) scheme has been proposed as a solution that totally avoids interacting with the control plane.

In the ITU-T Standard document with the reference of "G. 808.3 Generic protection switching-Shared mesh protection", a traditional SMP system is described that uses pre-computed protection paths that are pre-configured into the network elements. These protection paths can be activated when necessary via data plane protocol operations.

Furthermore, the conventional SMP systems use multiple shared backups (e.g., P1, P1', P2) for each working service (W1). Using multiple shared backups for each working service may introduce contention for resources among different services, and priorities among services may be defined. For example, if P1 is available, then W1 switches to P1, otherwise W1 switches to P1'. However, if P2 is of higher priority, it will interrupt P1, thus W1 switches to P2.

As a consequence, the conventional SMP system supports multiple backups per each service, and hence enables the creation of efficient protection mechanisms. However, since it is a distributed recovery scheme, it introduces contention for resources, and consequently it delays the recovery process. Likewise, the backup of each service to be used is independently selected by the head-end node of the service. Thus, the exact configuration of the network system after a failure and the incurred delay are non-deterministic. For that reason, if the backup paths are not carefully designed, SMP could eventually lead to recovery failure. In addition, a monitoring mechanism is needed that constantly monitors the availability of backup resources. Thus, the conventional SMP systems have an additional disadvantage that they require an extensive signalling to monitor all the network resources.

Moreover, the conventional method based on the SRLG Failure-dependent reaction, have a disadvantage that the recovery is slow.

Further, conventional devices and methods are also known which are based on the local protection and provide a relatively fast recovery. However, they have a disadvantage of inefficient resource utilization and no end to end (e2e) delay is guaranteed.

Although, there exist techniques for providing a protection scheme and recovering a failing service, for example, providing a failure-independent path, providing backup paths that do not share any critical resources with the original path, and providing multiple backups paths per each service, etc., it is generally desirable to improve devices, methods and systems for providing a failure dependent protection and recovering a failing system.

SUMMARY

In view of the above-mentioned problems and disadvantages, the present invention aims to improve the conventional devices, methods and systems. The present invention has the objective to provide a device, a method and a system for providing a failure dependent protection for rapid recovery of a failing system.

The objective of the present invention is achieved by the solution provided in the enclosed independent claims. Advantageous implementations of the present invention are further defined in the dependent claims.

In particular, the present invention proposes a device for providing a failure dependent protection in a network system, and a fast recovery with a minimum resource reservation may be obtained.

A first aspect of the present invention provides a device for providing failure dependent protection in a network system comprising a plurality of nodes, the device being configured to identify at least one potential failure in the network system; calculate and assign a specific backup path for each of one or more services in the network system and for each of the at least one potential failure, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an

offline optimization of a configuration of the network system; and output a signal to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table at the head-end node.

The first aspect of the present invention has the advantages that it enables design and establishment of the failure-dependent resilient networks. Moreover, the offline calculation of failure-dependent protection may minimize the overall resource reservation, since the reaction to each failure is carefully designed in an offline manner. In addition, prefetching failure-dependent specific backup paths at network nodes enables a faster failure recovery. Therefore, an immediate recovery from network failures may be guaranteed.

In an implementation form of the first aspect, the device is further configured to react to link failures, and upon detection of a link failure caused by Shared Risk Link Groups, provide a notification signal to the head-end node indicating the failing link.

This is beneficial, since a failure can be more quickly detected. Moreover, the notification signal may be provided, and the network may recover rapidly from the link failure.

In a further implementation form of the first aspect, the link failure is detected based on a high order optical channel data unit, ODU, tandem connection monitoring, TCM, of adjacent nodes.

This is beneficial, since the failing link can be detected, and the performance of the network system can be monitored. Moreover, since the backup path for the failing link is calculated and pre-fetched, the network system and all the affected services may recover rapidly.

In a further implementation form of the first aspect, the working paths of the services and the specific backup paths are jointly determined such that the overall network cost is minimized with respect to a predefined criterion.

By means of jointly calculating (i.e., determining) the working paths of the services and the specific backup paths, for example, for one or more services, a reservation of the resources can be implemented. Such a reservation of the required resources may enable

overall network cost to be minimized. Therefore, a faster and deterministic recovery with a minimum cost can be achieved. In addition, prefetching centrally-designed failure-dependent (FD) backup paths at the nodes of the network system ensures a fast and guaranteed recovery at minimum cost.

In a further implementation form the first aspect, the working paths of the services and the specific backup paths are jointly determined based on maximizing sharing of resources in the network system.

This is beneficial, since the working paths of the services and the specific backup paths can be jointly determined and the sharing of resources may be maximized. Moreover, it enables more sharing opportunities, for example, due to re-using of released resources of primary paths.

In a further implementation form of the first aspect, the device is further configured to calculate a network configuration and output an additional signal S1 for filling the forwarding table to each of the plurality of nodes (A, B, C, D, E, F) before recovery of the network system from the detected failure, wherein the additional signal comprises a new specific backup path being calculated for a subsequent potential failure.

This is beneficial, since multiple consecutive failures in the network system may be protected, and the network system may be able to recover from the sequential failures. For example, initially when there is no failure, the offline calculation of reaction to potential failures (i.e. optimization of the configuration of the network system) can be performed along with prefetching the specific backup paths via signal S1, as discussed before. Then, when the failure is detected, the network system may reconfigure to a new network configuration. Afterward, the device may perform the offline calculation once again in order to protect the second potential failure, etc.

In a further implementation form of the first aspect, the potential failure comprises at least one of a node failure, a link failure, and a shared risk link group failure.

This is beneficial, since multiple failures including different types of failures may be protected.

In a further implementation form of the first aspect, the device is based on an optical network device.

The device may be based on an optical network, and the signal may be encoded onto light to transmit information among the plurality of nodes of the network system. For example, the output signal may be a notification message including the potential failure paired with corresponding specific backup path, etc.

In a further implementation form of the first aspect, the failure notification signal (S2) is based on an in-band signal.

This is beneficial, since the failure can be quickly detected and the network system may be able to recover from the detected failure, for example, in a fast and deterministic way.

A second of the present invention provides a method for providing a failure dependent protection in a network system comprising a plurality of nodes, the method comprises the steps of identifying at least one potential failure in the network system; calculating and assigning a specific backup path for each of one or more services in the network system and for each of the at least one potential failure, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system; and outputting a signal to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table at the head-end node.

In an implementation form of the second aspect, the method further comprises reacting to link failures, and upon detection of a link failure caused by Shared Risk Link Groups, providing a notification signal to the head-end node indicating the failing link.

In an implementation form of the second aspect, the method further comprises detecting the link failure based on a high order optical channel data unit, ODU, tandem connection monitoring, TCM, of adjacent nodes.

In a further implementation form of the second aspect, the working paths of the services and the specific backup paths are jointly determined such that the overall network cost is minimized with respect to a predefined criterion.

In a further implementation form of the second aspect, the working paths of the services and the specific backup paths are jointly determined based on maximizing sharing of resources in the network system.

In a further implementation form of the second aspect, the method further comprises calculating a network configuration and outputting an additional signal for filling the forwarding table to each of the plurality of nodes before recovery of the network system from the detected failure, wherein the additional signal comprises a new specific backup path being calculated for a subsequent potential failure.

In a further implementation form of the second aspect, the potential failure comprises at least one of a node failure, a link failure, and a shared risk link group failure.

In a further implementation form of the second aspect, the method is performed in an optical network device.

In a further implementation form of the second aspect, the failure notification signal is based on an in-band signal.

A third aspect of the present invention provides a node for recovering a failing service in a network system comprising a plurality of nodes, the node being configured to maintain a forwarding table for indicating one or more services associated to the node, and a specific backup path for each of the one or more services to be used under a potential failure; obtain a signal from a device, indicating at least one potential failure paired with a specific backup path for a given service, in order to fill the forwarding table, and apply, when a failure is detected in the network system, the specific backup path of the detected failure according to the forwarding table to the given service.

A fourth aspect of the present invention provides a network system, comprising a device for providing a failure dependent protection configured to identify at least one potential

failure in the network system; calculate and assign a specific backup path for each of one or more services in the network system and for each of the at least one potential failure, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system; and output a signal to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table at the head-end node; and the network system further comprising a plurality of nodes for recovering a failing service, the nodes being interconnected by a plurality of links, and each node being configured to maintain a forwarding table for indicating at least one or more services associated to the node, and a specific backup path for each of the one or more services to be used under a potential failure obtain, if being the head-end-node of the given service, the signal from the device, indicating the at least one potential failure paired with the specific backup path for the given service, in order to fill the forwarding table, and apply, when detecting a failure in the network system, the specific backup path of the detected failure according to the forwarding table to the given service.

In an implementation form of the fourth aspect, the system is further configured to react to link failures, and upon detection of a link failure caused by Shared Risk Link Groups, provide a notification signal to the head-end node indicating the failing link.

In an implementation form of the fourth aspect, the system is further configured to detect the link failure based on a high order optical channel data unit, ODU, tandem connection monitoring, TCM, of adjacent nodes.

In a further implementation form of the fourth aspect, the working paths of the services and the specific backup paths are jointly determined such that the overall network cost is minimized with respect to a predefined criterion.

In a further implementation form of the fourth aspect, the working paths of the services and the specific backup paths are jointly determined based on maximizing sharing of resources in the network system.

In a further implementation form of the fourth aspect, the system is further configured to calculate a network configuration and output an additional signal for filling the forwarding table to each of the plurality of nodes before recovery of the network system from the detected failure, wherein the additional signal comprises a new specific backup path being calculated for a subsequent potential failure.

In a further implementation form of the fourth aspect, the potential failure comprises at least one of a node failure, a link failure, and a shared risk link group failure.

A fifth aspect of the present invention provides a computer program comprising program code causing a computer to perform the method according to the second aspect, when being carried out on a computer.

A sixth aspect of the present invention provides a non-transitory computer-readable recording medium that stores therein a computer program product which, when executed by a processor, causes the method according to according to the second aspect to be performed.

It has to be noted that all devices, elements, units and means described in the present application could be implemented in the software or hardware elements or any kind of combination thereof. All steps which are performed by the various entities described in the present application as well as the functionalities described to be performed by the various entities are intended to mean that the respective entity is adapted to or configured to perform the respective steps and functionalities. Even if, in the following description of specific embodiments, a specific functionality or step to be performed by external entities is not reflected in the description of a specific detailed element of that entity which performs that specific step or functionality, it should be clear for a skilled person that these methods and functionalities can be implemented in respective software or hardware elements, or any kind of combination thereof.

BRIEF DESCRIPTION OF DRAWINGS

The above described aspects and implementation forms of the present invention will be explained in the following description of specific embodiments in relation to the enclosed drawings, in which

FIG. 1 shows a schematic view of a device for providing a failure dependent protection in a network system according to an embodiment of the present invention.

FIG. 2 shows a schematic view of a device for providing a failure dependent protection in a network system according to an embodiment of the present invention in more detail.

FIG. 3 shows a schematic view of a method for providing a failure dependent protection in a network system according to an embodiment of the present invention.

FIG. 4 shows a schematic view of a method for network slicing with failure-dependent protection according to an embodiment of the present invention.

FIG. 5 shows a schematic view of a flow chart of an algorithm implemented according to an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

FIG. 1 shows a schematic view of a device 100 for providing a failure dependent protection in a network system 1 according to an embodiment of the present invention.

The device 100 is in particular suited to identify at least one potential failure f1 in the network system 1. The network system 1 comprises a plurality of nodes A, B, C, D, E, and F. The plurality of nodes A, B, C, D, E, and F, are interconnected to each other by a plurality of links.

The device 100 is further configured to calculate and assign a specific backup path p1 for each of one or more services w1 in the network system 1, and for each of the at least one

potential failure f1, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system 1.

The device 100 may provide a fast and deterministic recovery at minimum cost and/or resource reservation. For example, the device 100 may ensure the resource efficiency by jointly designing all the backup paths (with and/or without the primary paths) that should be used under each possible failure.

The device 100 is further configured to output a signal S1 to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table 101 at the head-end node. The forwarding table 101 may be located in anyone of the device 100, the plurality of nodes A, B, C, D, E, and F, the head-end node, the system 1, etc., without limiting the present invention to the location of the forwarding table 101.

For example, the fast reaction in the network system 1 may be ensured by prefetching the failure-dependent backup paths at the head-end node of the given service, and thus, upon failure detection, a communication with the central network controller may not be required.

Hence, the device 100 is able to provide a failure dependent protection in the network system 1.

FIG. 2 shows a schematic view of a device 100 for providing a failure dependent protection in a network system 1 according to an embodiment of the present invention in more detail.

The device 100 is configured to obtain as an input the resources and services 201 of the network system 1.

The device 100 further comprises a control plane 202, which has a path computation element. For example, the device 100 calculates and assigns a specific backup path p1 for each of one or more services w1 in the network system 1, and for each of the at least one potential failure f1. Moreover, the device 100 performs an offline optimization of a

configuration of the network system 1, and it further jointly determines the specific backup paths for each of the one or more services for the at least one potential failure f1.

For example, the device 100 (e.g., the path computation element of its control plane) centrally implement a planning phase for the calculation and prefetching of the specific backup paths to network nodes. Furthermore, the device 100 and/or its path computation element jointly designs the working and the failure dependent backup paths of all running services according to their requirements and the state of the network so that overall resource reservation is minimized.

The device 100 optionally comprises a storage unit 203, which is configured to store the calculated and assigned the specific backup path p1 for each of the one or more services w1 in the network system 1, and for each of the at least one potential failure f1, which may be pre-fetched to the nodes. The potential failure may be a node failure, a link failure, and a shared risk link group failure, without limiting the present disclosure to a specific failure.

Moreover, each node (i.e. from the plurality of nodes A, B, C, D, E, and F) maintains a forwarding table 101 for indicating one or more services w1 associated to the node, and a specific backup path p1 for each of the one or more services w1 to be used under a potential failure f1. In some embodiments, the forwarding table 101 may be stored in each node, the system, etc., as discussed above.

The device 100 optionally comprises a signal generator 204, which is configured to output a signal S1 to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill the forwarding table at the head-end node.

The head-end node of the given service may obtain the signal S1 from the device 100, indicating the at least one potential failure f1 paired with the specific backup path p1 for the given service w1, and may fill the forwarding table.

The device 100 further optionally comprises a look-up function 205, which is configured to detect a link failure in the network system 1. Moreover, a link failure may be detected in the network system 1, for example, based on a high order optical channel data unit, ODU,

tandem connection monitoring, TCM, of adjacent nodes. For example, the device 100 may further be configured to react to the link failures, and upon detection of a link failure caused by Shared Risk Link Groups, the device 100 (e.g. its signal generator unit 204) may provide a notification signal S2 to the head-end node indicating the failing link.

In some embodiments, the plurality of the nodes in the network system may detect a failure and notify the affected head-end nodes.

The head-end node may further apply the specific backup path of the detected failure according to the forwarding table to the given service.

Hence, the device 100 is able to provide a failure dependent protection in the network system 1 comprising the plurality of nodes A, B, C, D, E, and F, and the plurality of nodes A, B, C, D, E, and F, if being the head-end node, are able to recover the failing service.

FIG. 3 shows a schematic view of a method 300 for providing a failure dependent protection in a network system 1 comprising a plurality of nodes A, B, C, D, E, and F, according to an embodiment of the present invention.

The method 300 comprises a first step of identifying 301 at least one potential failure f1 in the network system 1.

The method 300 comprises a second step of calculating 302 and assigning 302 a specific backup path p1 for each of one or more services w1 in the network system 1 and for each of the at least one potential failure f1, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system 1.

The method 300 comprises a third step of outputting 303 a signal S1 to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table 101 at the head-end node.

FIG. 4 shows a schematic view of a method 400 for network slicing with failure-dependent protection according to an embodiment of the present invention.

In the embodiment of FIG. 4, the present invention is illustrated over Transport SDN for providing Network Slices (NS) with fast recovery in a guaranteed, and minimum resource footprint. Without limiting the present disclosure, the following embodiment is discussed under the OTN network systems.

At step 401, the device 100 obtains the state of the network system as an input.

Initially, the centralized SDN controller is constantly aware of the network status, network resources, and ongoing services.

Moreover, in order to be able to withstand any possible SRLG failure (e.g. any optical failure causing multiple IP Links to fail), the method further comprises a NS planning M.1 which invokes so as to calculate the necessary resource reservations.

The NS planning module (M.1) comprises four steps of 401, 402, 403, and 404.

At step 402, the device 100 jointly designs the primary and the backup paths, for example, by computing the 1+1 solution.

First, the device 100 uses the 1+1 type of solution for all active services. By jointly designing all the primary and backup paths, the device 100 ensures that all the services may be served.

At step 403, the device 100 names the primary and the backup paths towards maximizing disjointness.

In order to minimize the necessary resource reservation, the device 100 names each one of the 1+1 paths as primary or backup such that disjointness, and hence sharing opportunities are maximized.

At step 404, for each service l, the device 100 calculates more efficient link-failure backup $x^{l,f}$ that is SRLG-disjoint to f.

For example, the device 100 derives a failure-dependent backup path for each service, such that the overall reservation is minimized, e.g. using a method as it is generally known to the skilled person.

At step 405, the device 100 reserves the backup resources according to worst SRLG failure, but for each SRLG failure, the device 100 protects against the worst sequence of detected failures according to the following equation (1):

$$\max_{S \in SRLG} \left\{ \sum_{l \in L} d^l \max_{f \in S} x_e^{l,f} \right\} \quad (1)$$

wherein, S corresponds to a specific SRLG failure of the set SRLG, d corresponds to the bandwidth requirement of service l, and f corresponds to any link failure caused by SRLG failure S.

The necessary resources are calculated and reserved according to the worst SRLG failure and according to the worst link failure detection sequence.

At step 406, the device 100 fills failure-dependent look-up tables (M2) via signaling S1.

The calculated primary paths are established and the calculated backup paths are pre-fetched to the network nodes via signaling S1 of the form {failure, path} for each active service. Thus, all the network nodes are configured so that they can react to failures in a distributed manner.

Furthermore, at step 407, a failure may be detected in the network system 1.

At step 408, the nodes detect a failure and notify the affected head-end nodes.

Upon failure, the head-end node receives a notification regarding the failing link. This detection can happen by monitoring the links of the working path links similarly to the OTN SMP approach for protection resources, i.e. via high order ODU TCM monitoring between adjacent nodes

At step 409, the head-end retrieves the corresponding backup entry of the Look-up table. The head-end node establishes the backup path indicated by the look-up table

At step 410, the head-end node initiates the establishment of the backup path for the specific failure.

It may be guaranteed by design that the reserved resources may always be adequate (NS planning is covering the worst case). Thus, the method and/or the device may ensure a fast recovery from a failure at minimum cost, but the slice now may not be protected against a subsequent failure.

Given the new network state (after a failure), the method may further initiate the NS planning module M.1, so as to ensure protection against any subsequent failure. Thus, the method 400 may guarantee protection against multiple failures.

In some embodiments, the module M.1 may be executed periodically, even if no failure has occurred, but some other aspects of the network have changed.

In some embodiments, the steps 402, 403, 404, and 405 may be representative of a first module M1 and the step 406 may be representative of a second module M2, without limiting the present invention to a specific number of steps, modules, etc.

For example, the network recovery may be based on two main phases, an offline phase that calculates the network configuration for each detected failure, and a real-time reaction. Moreover, in M1, the failure-dependent network planning method executed centrally, e.g. at PCE, it jointly designs the working and the FD backup paths of all running services according to their requirements and the state of the network so that overall resource reservation is minimized. Then, in M2 it performs a per service failure-dependent Forwarding table at each network node. Each network node stores a forwarding table indicating for its ongoing services the backup path that should be used under each failure. In addition, the signal the signal S1 is sent from PCE to Network devices to fill the FD look-up tables, for example, for each failure a signal of the form {failure, backup path} is sent to the head-end node of the affected service.

Moreover, in the second phase which is based on the real-time reaction to failure. An immediate recovery based on Table look-up may be performed.

For instance, initially, a standard notification of the head-end about the detected failure affecting the primary/working path is sent. Then, the reaction to detected failure may be applied, and since the reaction to each failure is deterministic and sufficient resources have been reserved, no resource contention exists. Each service eventually switches to the corresponding backup path. Hence, the network system may recover, and once recovery from the failure is completed, it may apply once again the NS planning method M.1, based on the new network state. Thus, a protection against any subsequent failure may be ensured.

FIG. 5 shows a schematic view of a flow chart of an algorithm implemented according to an embodiment of the present invention.

At step 501, the device 100 obtains the network resource and demands, as an input for the offline optimization.

As mentioned before, under any network status change, the device 100, for example, its centralized controller is able to retrieve the network system status, the network system resources, and the active services in the network system. Moreover, due to optical network non-linear impairments, the optical signal can only be transmitted over certain distance before regeneration is needed.

At step 502, the device 100 creates physical reachability graph.

The device 100 creates the physical reachability graph in order to plan failure-dependent backup paths for each service, and further minimize the necessary network resources such as regenerators and wavelengths. For example, the physical reachability graph can be created such that the graph nodes are network nodes, a graph edge is created between two nodes if there is a physical path with available capacity, and the optical signal is reachable without regeneration. A shortest path on the reachability graph is a path with minimal number of regenerators.

At step 503, the device 100 identifies the key physical links and the nodes.

The device 100 may identifies key physical links to reserve resource, and key nodes for regenerator placement in order to, for example, maintain the load balanced over the network during the optimization process.

At step 504, the device 100 loops all failures.

Hence, the device 100 may consider all possible failures during the offline optimization process.

At step 505, the device 100 identifies failed demands.

The device 100 may identify for each failure the affected services.

At step 506, the device 100 finds recovery paths.

For example, for each affected service under a certain failure, the device 100 performs the optimization process, and may find a recovery path with minimal resources required.

At step 507, the device 100 refreshes reachability graph. For instance, once the new recovery paths have consumed some network resources, the original reachability graph may not be valid anymore. Thus, the device 100 may refresh the reachability graph with new network resource status.

At step 508, the device 100 finds cost least recovery paths.

The loop process in step 504 continues and for each failure and each failed service, the device 100. Moreover, the device 100 may always find the least cost recovery path.

At step 509, the device 100 balances the wavelength and regenerators.

Moreover, both of the wavelengths and regenerators are network resources, and they should be used according to operator's objectives. For example, more regenerators could reduce

the wavelengths required; and fewer regenerators may result in more wavelengths being used. Accordingly, the device 100 performs the optimization process and may provide a knob in order to control the balance between these two resources.

At step 510, the device 100 performs a global optimization.

For instance, the required number of regenerators and link wavelengths may strongly depend on the order of consideration of failures and affected services. Moreover, in order to further reduce the network resources required for failure-dependent recovery, the optimization process may include a global adjustment phase to improve the backup resource sharing. The device 100 may further reduce overall network resources reserved or may further increase the number of services recovered under some failures.

Furthermore, after the device 100, for example, its centralized controller finds the specific backup paths for each service under different failures, it will push the recovery paths to the end nodes of each demand through Signal S1 to fill the recovery look-up table.

Moreover, upon a failure detection, the head-end node of the failed service will be notified about the failure, and it will select the correct backup path for the network recovery. Once the recovery process converges, the device 100, e.g., its centralized controller may retrieve the new network status as well as the working demands. The whole process may start again in an iterative procedure in order to fully make use of the available network resources.

The present invention has been described in conjunction with various embodiments as examples as well as implementations. However, other variations can be understood and effected by those persons skilled in the art and practicing the claimed invention, from the studies of the drawings, this disclosure and the independent claims. In the claims as well as in the description the word "comprising" does not exclude other elements or steps and the indefinite article "a" or "an" does not exclude a plurality. A single element or other unit may fulfill the functions of several entities or items recited in the claims. The mere fact that certain measures are recited in the mutual different dependent claims does not indicate that a combination of these measures cannot be used in an advantageous implementation.

Claims

1. A device (100) for providing a failure dependent protection in a network system (1) comprising a plurality of nodes (A, B, C, D, E, F), the device (100) being configured to:

identify at least one potential failure (f1) in the network system (1);

calculate and assign a specific backup path (p1) for each of one or more services (w1) in the network system (1) and for each of the at least one potential failure (f1), wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system (1); and

output a signal (S1) to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table (101) at the head-end node.

2. The device (100) according to claim 1, further configured to react to link failures, and upon detection of a link failure caused by Shared Risk Link Groups, provide a notification signal (S2) to the head-end node indicating the failing link.

3. The device (100) according to claim 2, wherein the link failure is detected based on a high order optical channel data unit, ODU, tandem connection monitoring, TCM, of adjacent nodes.

4. The device (100) according to claim 1, wherein the working paths of the services and the specific backup paths are jointly determined such that the overall network cost is minimized with respect to a predefined criterion.

5. The device (100) according to claim 1, wherein the working paths of the services and the specific backup paths are jointly determined based on maximizing sharing of resources in the network system (1).

6. The device (100) according to anyone of the preceding claims, is further configured to calculate a network configuration and output an additional signal (S1) for filling the forwarding table to each of the plurality of nodes (A, B, C, D, E, F) before

recovery of the network system (1) from the detected failure, wherein the additional signal (S1) comprises a new specific backup path being calculated for a subsequent potential failure.

7. The device (100) according to anyone of the preceding claims, wherein the potential failure comprises at least one of a node failure, a link failure, and a shared risk link group failure.

8. The device (100) according to anyone of the preceding claims, wherein the device (100) is based on an optical network device.

9. The device (100) according to anyone of the preceding claims, wherein the failure notification signal (S2) is based on an in-band signal.

10. A method (300) for providing a failure dependent protection in a network system (1) comprising a plurality of nodes (A, B, C, D, E, F), the method (300) comprises the steps of:

identifying (301) at least one potential failure (f1) in the network system (1);

calculating (302) and assigning (302) a specific backup path (p1) for each of one or more services (w1) in the network system (1) and for each of the at least one potential failure (f1), wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system (1); and

outputting (303) a signal (S1) to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table (101) at the head-end node.

11. A node for recovering a failing service in a network system (1) comprising a plurality of nodes (A, B, C, D, E, F), the node being configured to:

maintain a forwarding table (101) for indicating one or more services (w1) associated to the node, and a specific backup path (p1) for each of the one or more services (w1) to be used under a potential failure (f1);

obtain a signal (S1) from a device (100), indicating at least one potential failure (f1) paired with a specific backup path (p1) for a given service (w1), in order to fill the

forwarding table, and

apply, when a failure is detected in the network system (1), the specific backup path of the detected failure according to the forwarding table to the given service.

12. A network system (1), comprising a device (100) for providing a failure dependent protection configured to:

identify at least one potential failure (f1) in the network system (1);

calculate and assign a specific backup path (p1) for each of one or more services (w1) in the network system (1) and for each of the at least one potential failure (f1), wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system (1); and

output a signal (S1) to the head-end node of a given service, indicating the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table (101) at the head-end node; and

the network system (1) further comprising a plurality of nodes (A, B, C, D, E, F) for recovering a failing service, the nodes being interconnected by a plurality of links, and each node being configured to:

maintain a forwarding table (101) for indicating at least one or more services (w1) associated to the node, and a specific backup path (p1) for each of the one or more services (w1) to be used under a potential failure (f1);

obtain, if being the head-end-node of the given service, the signal (S1) from the device (100), indicating the at least one potential failure (f1) paired with the specific backup path (p1) for the given service (w1), in order to fill the forwarding table, and

apply, when detecting a failure in the network system (1), the specific backup path of the detected failure according to the forwarding table (101) to the given service.

13. A computer program comprising program code causing a computer to perform the method according to claim 10, when being carried out on a computer.

14. A non-transitory computer-readable recording medium that stores therein a computer program product which, when executed by a processor, causes the method according to claim 10 to be performed.

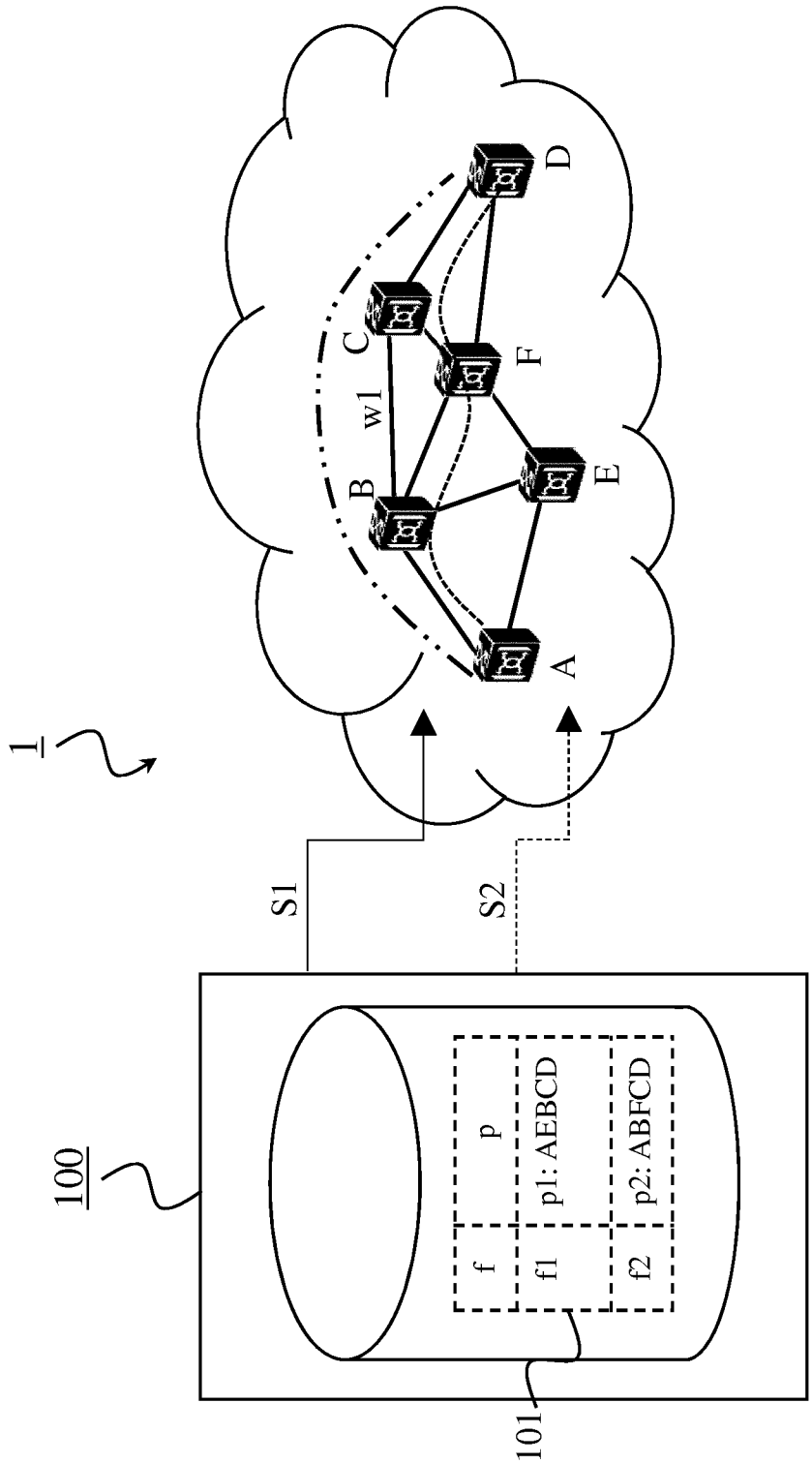

FIG. 1

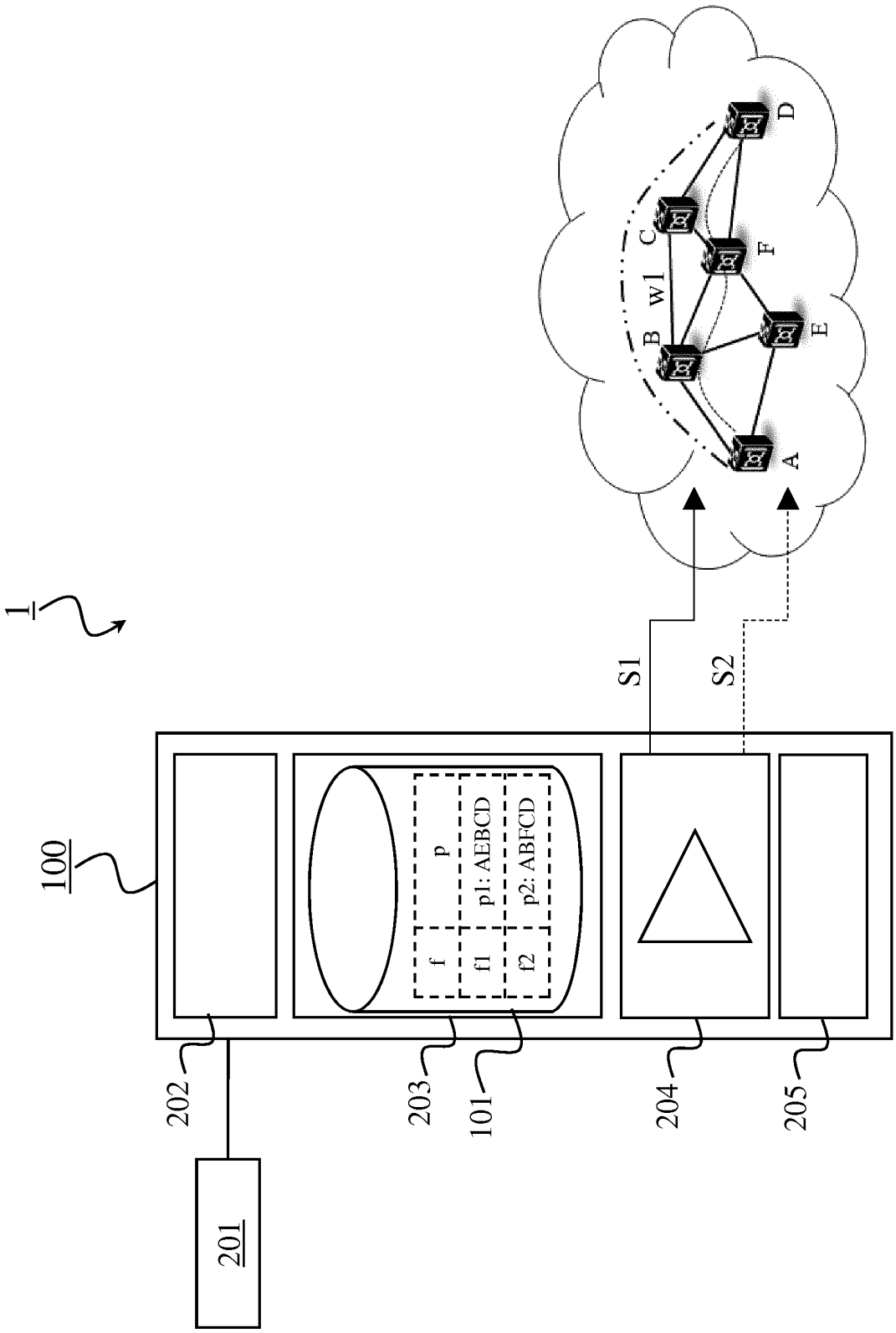
1
100
201
202
203
101
204
205
S1
S2
p
f
f1
f2
p1: AEBCD
p2: ABFCD
A
B
C
D
E
F
w1

FIG. 2

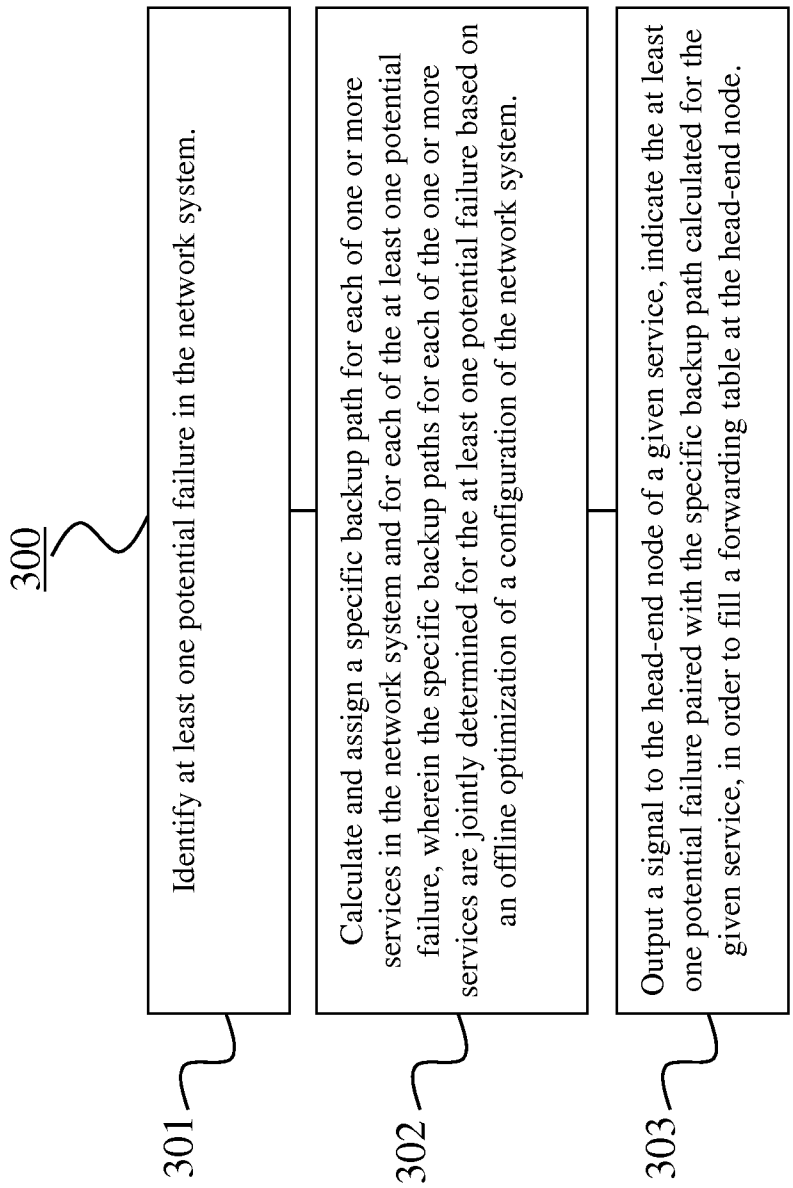
300
Identify at least one potential failure in the network system.
301
Calculate and assign a specific backup path for each of one or more services in the network system and for each of the at least one potential failure, wherein the specific backup paths for each of the one or more services are jointly determined for the at least one potential failure based on an offline optimization of a configuration of the network system.
302
Output a signal to the head-end node of a given service, indicate the at least one potential failure paired with the specific backup path calculated for the given service, in order to fill a forwarding table at the head-end node.
303

FIG. 3

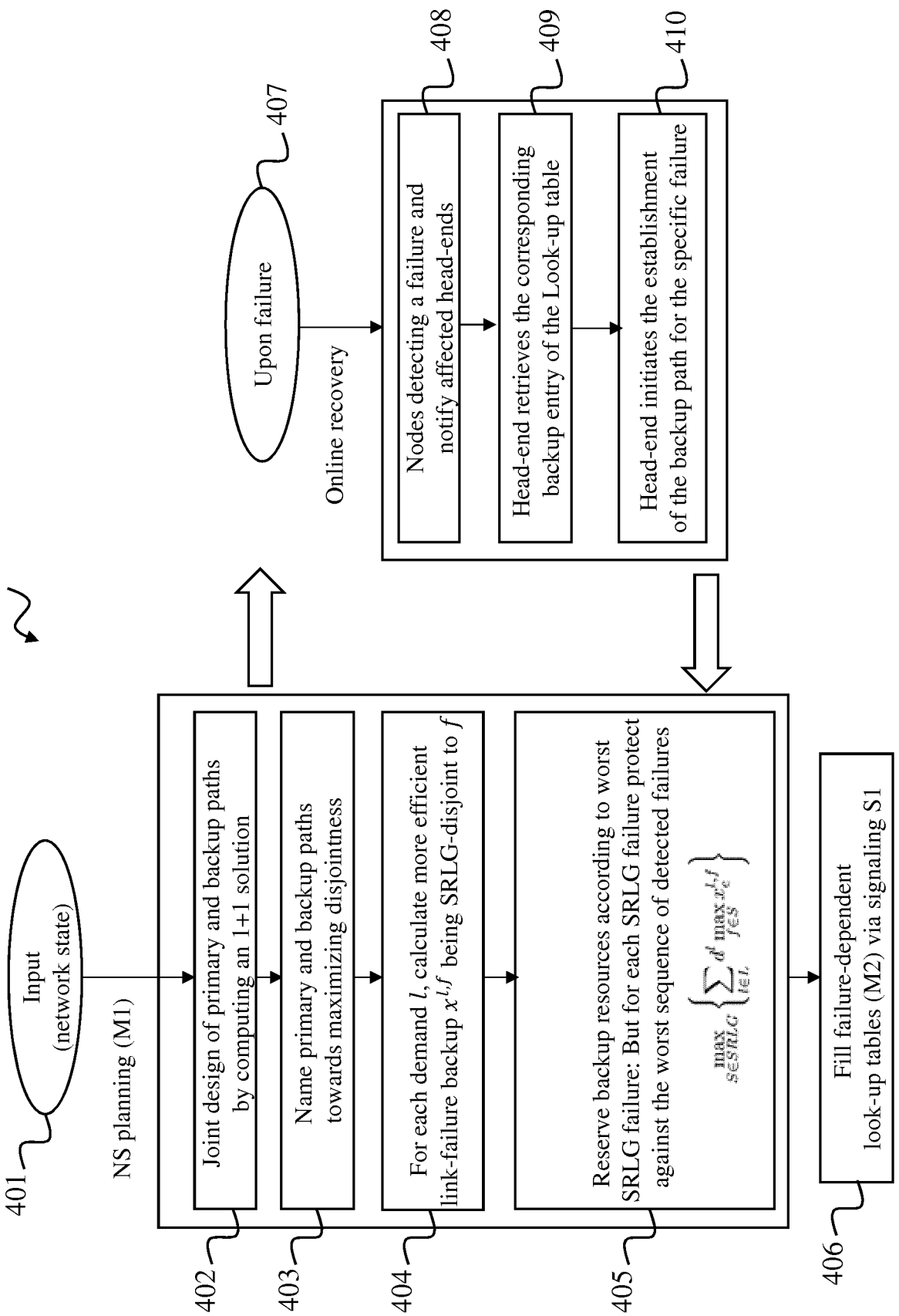
400
401
Input
(network state)
NS planning (M1)
Joint design of primary and backup paths by computing an 1+1 solution
Name primary and backup paths towards maximizing disjointness
For each demand l, calculate more efficient link-failure backup $x^{l,f}$ being SRLG-disjoint to f
Reserve backup resources according to worst SRLG failure: But for each SRLG failure protect against the worst sequence of detected failures
$\max_{s \in SRLG} \left\{ \sum_{l \in L} d^l \max_{f \in S} x_e^{l,f} \right\}$
Fill failure-dependent look-up tables (M2) via signaling S1
402
403
404
405
406
Online recovery
Upon failure
407
Nodes detecting a failure and notify affected head-ends
Head-end retrieves the corresponding backup entry of the Look-up table
Head-end initiates the establishment of the backup path for the specific failure
408
409
410

FIG. 4

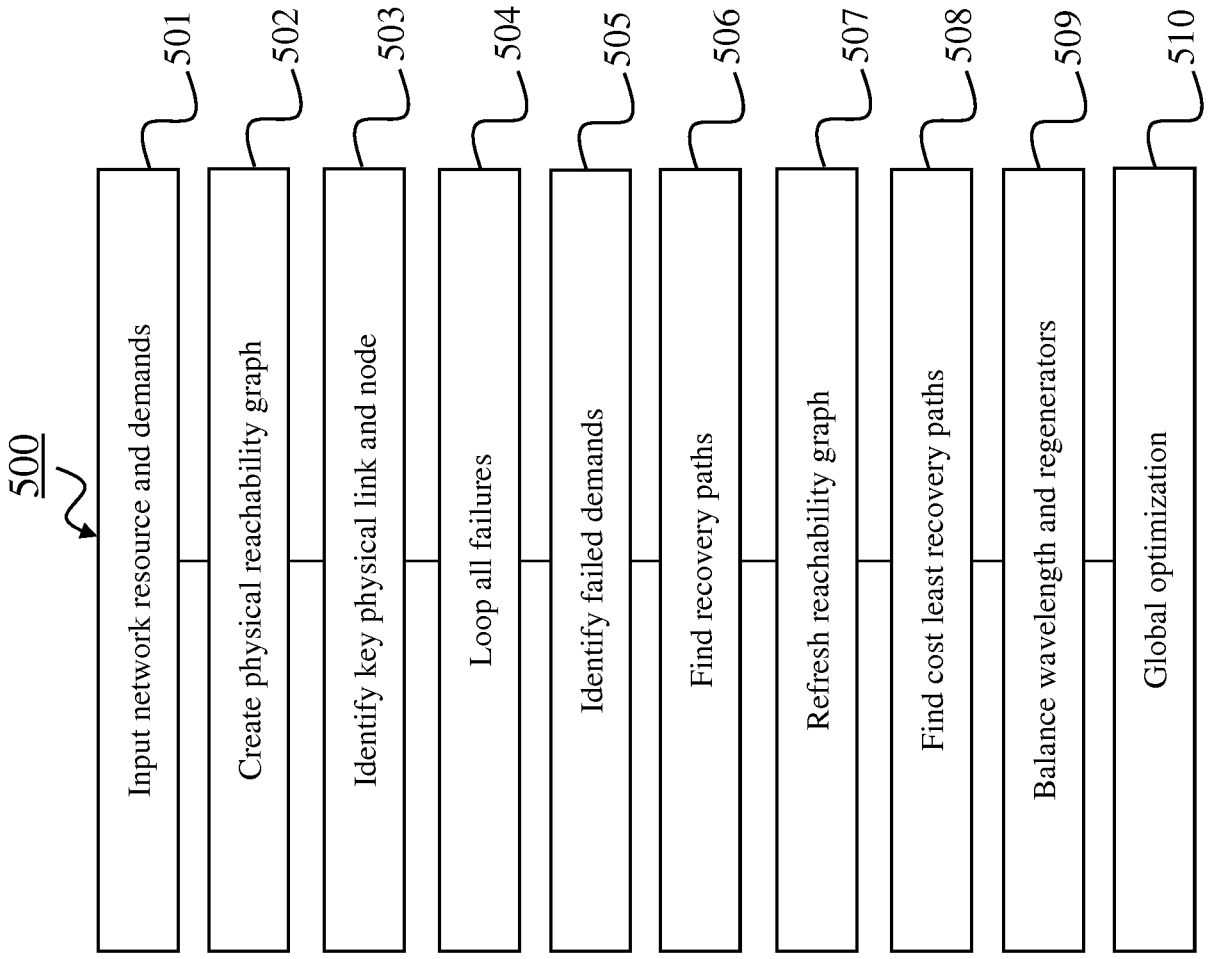
500
Input network resource and demands
501
Create physical reachability graph
502
Identify key physical link and node
503
Loop all failures
504
Identify failed demands
505
Find recovery paths
506
Refresh reachability graph
507
Find cost least recovery paths
508
Balance wavelength and regenerators
509
Global optimization
510

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2018/074147

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04J3/14 H04J3/16 H04L12/703 H04L12/707 H04L12/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04J H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SRINIVASAN RAMASUBRAMANIAN ET AL: "Comparison of failure dependent protection strategies in optical networks", PHOTONIC NETWORK COMMUNICATIONS, KLUWER ACADEMIC PUBLISHERS, BO, vol. 12, no. 2, 9 September 2006 (2006-09-09), pages 195-210, XP019437238, ISSN: 1572-8188, DOI: 10.1007/S11107-006-0028-Z abstract page 195, right-hand column, paragraph 2 - page 196, left-hand column, paragraph 2 page 196, right-hand column, paragraph 3 - page 197, left-hand column, paragraph 1; figure 3 page 197, right-hand column, paragraph 4 page 198, left-hand column, paragraph 2 -/--	1-14

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March 2019	29/03/2019

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Roldán Andrade, J

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	page 200, right-hand column, paragraph 5; table 1 page 202, left-hand column, paragraph 4; figure 5 -----	
X	RAMASUBRAMANIAN S: "On failure dependent protection in optical grooming networks", DEPENDABLE SYSTEMS AND NETWORKS, 2004 INTERNATIONAL CONFERENCE ON FLORENCE, ITALY 28 JUNE - 1 JULY 2004, PISCATAWAY, NJ, USA,IEEE, 28 June 2004 (2004-06-28), pages 440-449, XP010710806, DOI: 10.1109/DSN.2004.1311917 ISBN: 978-0-7695-2052-0 abstract page 441, left-hand column, paragraph 3 - paragraph 4 page 441, right-hand column, paragraph 2 - page 442, left-hand column, paragraph 2 page 443, right-hand column, paragraph 3 - page 446, left-hand column, paragraph 4 -----	1-14
X	JALALINIA SHABNAM S ET AL: "Green and resilient design of telecom networks with shared backup resources", OPTICAL SWITCHING AND NETWORKING, vol. 23, 1 January 2017 (2017-01-01), pages 97-107, XP029839120, ISSN: 1573-4277, DOI: 10.1016/J.OSN.2016.06.007 abstract page 97, right-hand column, paragraph 2 - page 98, left-hand column, paragraph 2 page 100, left-hand column, paragraph 1 -----	1-14
A	EP 1 633 068 A1 (CIT ALCATEL [FR]) 8 March 2006 (2006-03-08) paragraph [0010] -----	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2018/074147

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1633068 A1	08-03-2006	AT 364270 T	15-06-2007
		CN 1744479 A	08-03-2006
		DE 602004006865 T2	31-01-2008
		EP 1633068 A1	08-03-2006
		US 2006045007 A1	02-03-2006