Emerging Function Concept Applied to Photonic Packet Switching Network

Antonio de Campos Sachs, Ricardo Luis de Azevedo da Rocha, Fernando Frota Redigolo, Tereza Cristina Melo de Brito Carvalho.

Departamento de Engenharia de Computação e Sistemas Digitais (PCS)
Escola Politécnica da Universidade de São Paulo (EPUSP)
São Paulo, Brazil
antoniosachs@larc.usp.br; luis.rocha@poli.usp.br; fernando@larc.usp.br; carvalho@larc.usp.br

***Abstract*—Aiming to contribute to a solution for the number of nodes scalability problem, a transparent Optical Packet Switching (OPS) network is treated in a new approach that considers the network as a complex system. This treatment allowed the investigation of a network based on large number of autonomous OPS nodes connected in a mesh topology. The network operates in a bottom-up organization and the long distance signalization, one of the main factors responsible for the number of nodes limitation, is avoided and the scalability is enabled. Desirable characteristics (scalability, traffic organization, protection, restoration, etc.) result from simple rules executed by individual nodes. All those characteristics are referred to as Emerging Functions. It is possible to create those simple rules, or fundamental individual functions executed by individual nodes, in order to potentiate those Emerging Functions. As an example, a set of node interactions with their next neighbors is described. That will result in a Protection Emerging Function able to maintain the network operation after failure and to confine the network degradation just around the failure position. That segregation of the failure effects represents a new feature that could be observed due to the new approach.**

Keywords-complexity; emerging function; photonic packet switching; protection

I. INTRODUCTION

One important limit factor for the scalability of the number of nodes in a network is the long time necessary for communication between two distant nodes. The current approach, which treats the OPS network as a complex system and the network nodes as autonomous entities, was previously described in [1]. That approach avoids long distance signalization. A packet is sent from source to destination without any previous path determination. Routing activities needs to use a shortest path table previously calculated at the moment of the network initialization. From that shortest path table each node knows the number of the output port that corresponds to the shortest path connecting itself to any other node. Each packet carrying the destination address can find the path from source to destination from node to node in a multi hop schema using the output port corresponding to the shortest path or the alternative port in those cases in which the preferred one is not available.

Simple switching device without optical buffers that forwards the arriving packet without delay to the preferential output port or to the alternative one is a procedure referred to as "hot potato routing" [2]. That operation can be performed by using an optical sample removed before a FDL (fiber delay lane). This sample can be converted into electrical media for the logical treatment performed by conventional electronic circuitry and the optical switch, based on SOA (Semiconductor Optical Amplifiers) devices, can be positioned before the arrival of the packet that is traveling through the FDL. Such operations have been adopted since the precursor projects KEOPS [3] and DAVID [4]; but, nowadays, the conversion from optical to electrical media is not necessary and new photonic devices can do all the jobs (including logical operations), and the switching operation can be performed in a fully optical process [5]. The network described herein works for any technology utilized for reading the address and forwarding the packet to the output port. Apart from the technology used inside the node, the network can operate as a complex system, with a bottom-up organization. Each node has the autonomy to carry on the switching operation, performing its work exclusively with locally obtained information.

The utilization of large number of nodes with large number of alternative paths, provided by the mesh topology, is known to be important for the network survivability. Since the beginning of the digital telecommunication technology, Baran [2] worked with mesh topology and got very strong robustness for a network with a large number of nodes. Today, the survivability of a complex network is associated to the intrinsic robustness of complex systems [6, 7]. Carlson and Doyle [6] claims that all complex systems are intrinsically robust for the most frequent daily events; however they are very fragile due to rare and unexpected environment events. Reference [7] declares that "hubs make the network robust against accidental failures but vulnerable to coordinated attacks". All agree that complexity is intrinsically related to robustness.

Next, Section II describes generically aspects related to Emerging Functions applied to a network and Section III describes the network operation. Section IV describes the adopted theory, calculations aspects and discussions analyzing the failure distribution effect for a 256-node case study. Section V presents the final conclusions.

II. EMERGING FUNCTIONS APPLIED TO A NETWORK

The term Emerging Function is utilized in a number of different areas, such as physics, chemistry or biology. Although there is no single formal definition for the term, two main definitions can be inferred:

 ISBN: 978-1-61208-239-4

- A function that is not regularly present in a system and appears or is activated automatically in an emergency situation;
- A function that is always present in a system (it characterizes the system) and emerges from simple operations executed by its individual parts.

An emerging function is associated to the whole system and not to its individual parts although its emergence is the result of small changes in the normal operations (first definition) or of regular operations of individual parts of the system (second definition).

A system based on emerging functions can be characterized as a bottom-up organization system or, equivalently, a self-organized system [8] and it is associated with a complex system composed by a large number of individual units following simple operation rules. It is difficult to deal with such complex systems, with a large number of elements, in a classical and reversible treatment that calculates all the possible events in all the system components. The models considering the probability of transition from one state to the next one to describe the system evolution seem to be a more feasible strategy. That is also the same strategy found in the chaos theory [9], in which the final consequences cannot be derived from the initial conditions because there is a high sensitivity to tiny fluctuations in those initial conditions.

The network routing function herein is not controlled by the network layer (OSI network layer 3). It emerges from simple fundamental functions executed by each node individually. There is no high entity accounting for switches operation or for the path followed by each packet in the network. Instead, the node operation is based on the local situation and on the packet header information: each packet is sent to the preferred output port, or sent to the available port if the preferred one is occupied. This operation rule, by itself, turns the network auto-organized or bottom-up organized, and provides autonomic network operation. Therefore, it is possible to consider "routing" as a function emerging from individual nodes operations or, in other words, that routing is an Emerging Function.

Traffic distribution, which can be considered the set of all routes, is also an Emerging Function. As the shortest path is not always the one which is chosen, the traffic distribution obtained is better than the one obtained utilizing only the shortest path.

The access to the network is made only if there is a time interval to accept the new packet without collision. This is possible because of a fiber delay line (FDL) positioned before any input port. Collision avoidance can also be interpreted as an Emerging Function, since it is not executed by any higher protocol layer, but it results from the careful local insertion procedure.

Protection is an important network function that can be enabled through the insertion of an extra individual node operation function based on a backward signalization sent to all the input ports. The output ports integrity can be checked through the signalization received from the next node. Protection can also be considered as an Emerging Function and its architecture is presented in detail in Section III.

III. NETWORK OPERATION

The network architecture is based on the "Hot Potato Heuristic Routing Doctrine" [2] made up by network nodes executing simple well-defined rules. A set of Emerging Functions arise from those simple rules. The network complexity is related to its size and the number of nodes. Each node, in contrast, is idealized to be simple. The first simplification is the omission of optical buffers. Without optical buffers, it is necessary to use symmetrical nodes in order to avoid packet losses. In symmetrical nodes, with the same number of input and output ports, there is always a free output port for any arriving packet.

Manhattan-Street Network (MSN) [10] was chosen as the main topology for the development of this work, but any other mesh topology can be considered. This particular choice facilitates the calculations for increasing the number of nodes without changing the network symmetry.

To implement the protection emerging function, it is necessary to differentiate the two output ports in order to define links sub-domains as described in [1]. Figure 1 is a MSN showing clockwise and counterclockwise sub-domains. Each node belongs to two sub-domains and each sub-domain contains four nodes.

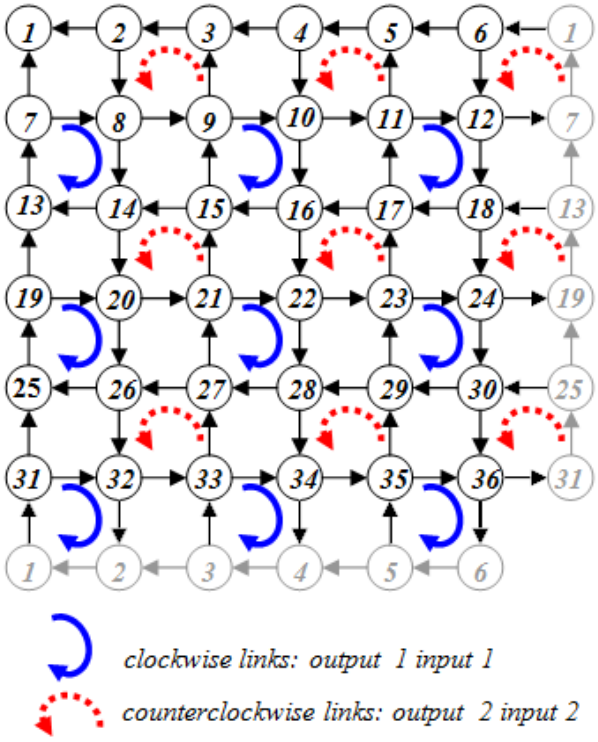

Figure 1: MSN organized with clockwise and counterclockwise link sub-domains [1].

After organizing the network links in small sub-domains, it is possible to create the protection function by including an operation rule for all network nodes. This operation rule is composed by a continuous optical signal which is sent

backward through the two input ports and the operation of reading the arriving signal from the two output ports. This signal is named integrity signal, as the integrity of a link sub-domain is signalized by the optical signal continuously traveling in the opposite direction of the optical packet signal. When a failure occurs in one link, the backward integrity signal is interrupted and the node, which is just before that link, is immediately aware of the failure and no longer uses that output port. The action rule for all nodes is to turn off the integrity signal forwarded to the input port belonging to the failed sub-domain.

In this work, a second signalization was added, sent backward to inform the nodes outside the failed sub-domain that the link is working properly but the next node belongs to a failed sub-domain.

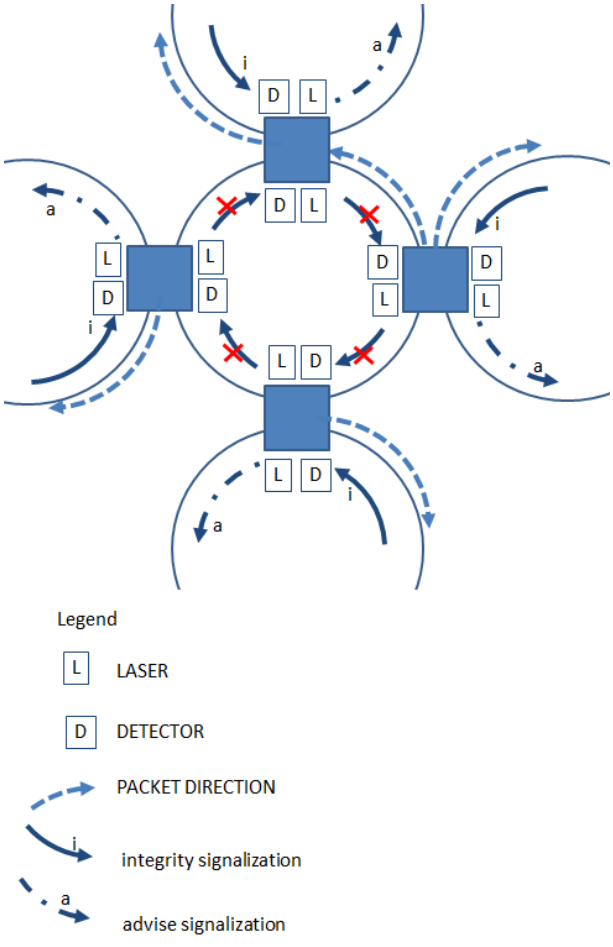

Figure 2: First signalization (link integrity DC laser signal) and second signalization (square wave advise signalization).

Figure 2 shows four nodes with four links in a counterclockwise sub-domain. Each node has a DC laser sending a continuous laser signal in clockwise direction (opposite direction of the counterclockwise packets) and has a detector placed to receive the laser signal sent by the next neighbor belonging to the same counterclockwise sub-domain. In case any one of those four links is interrupted, the detector that first stops receiving the signal turns off the laser corresponding to the same sub-domain. All the four links in the ring are forced to be interrupted. The four lasers are turned off. Each node belongs to two sub-domains and uses a second laser as well as a second detector for integrity signalization of that second sub-domain. In a normal process, without failure, all signalization is of the first type (continuous laser signal), but in the case of failure, the signalization is interrupted in the failed sub-domain and changed from continuous signal to square wave signal in the second sub-domain (four next neighbor sub-domains). The failure causes four links to stop the first signalization (integrity signalization) and to start the second signalization (advise signalization) outside the failed sub-domain.

The implementation of that second level of information can be performed by a square wave light signal replacing the DC light signalization or, alternatively, a DC laser can be used with half optical power to differentiate from the full optical power of the regular link integrity signalization. The implementation of both signalization types, indeed, can also be made by smart photonic devices in a fully optical process.

All the nodes at a failed sub domain operate with only one input and one output. All the other nodes, far from the failure, have no information about the failure and their procedure remains the same, including the utilization of the same preferential output port matrix. The action of the node receiving the second signalization is to deflect all packets to the other output port (the port that is receiving the first signalization type), with the exception of the packets addressed to those nodes that are sending the second signalization type. That is the only way a failed sub-domain node can receive a packet. That deflection corresponds to an adaption in the preferential port table.

As an example, consider a failure in the counterclockwise sub-domain connecting nodes 17, 16, 22, 23 in Figure 1. Those four nodes extend the information failure to the remaining input by changing the backward continuous wave light source to square wave light-source. That signalization is a sign for the preferential port adaption in nodes 18, 10, 21 and 29.

That new feature was implemented in the calculations, and the results are shown in Figure 3 for 16 nodes (N=16) and 256 nodes (N=256). The caption termination “F” refers to the first level protection schema, characterized by not using the second signalization type. The caption termination “F2” refers to the second level protection schema that includes a second signalization type. For 16 nodes, the second level protection schema (N=16F2) shows that the interference of the failure is remarkably smaller than that observed at the first level protection schema (N=16F).

One additional feature is the correction of a strange behavior for low charge condition. In that region (Link Load < 50%) the failure causes a large number of hops enhancement and it is quite odd to see the number of hops decreasing for higher load condition (curve N=16F in Figure 3). That behavior can be explained by the fact that in the low load condition, the packets take the preferential output port more often as compared to the large charge condition and are

 ISBN: 978-1-61208-239-4

forced to proceed through the failed region. The failure is more efficiently avoided with the second signalization, minimizing such effect. All the unnecessary trial through the failed region is avoided.

IV. CALCULATIONS

To deal with scalability, the number of nodes can be higher than practical calculations can support. It is impossible to implement calculations for an arbitrarily large number of nodes. In order to minimize the time and memory utilization, connection matrix "c" and preferential output port matrix "pp", were calculated separately. Data were saved in files that could be interpreted by the main program. The shortest path calculation is presented in sub-section A. The algorithm description for the mean number of hops calculation is presented in sub-section B. The model validation carried out by comparison with the simulation model is presented in sub-section C. One important result, the segregation of the failure effect, is presented in sub-section D.

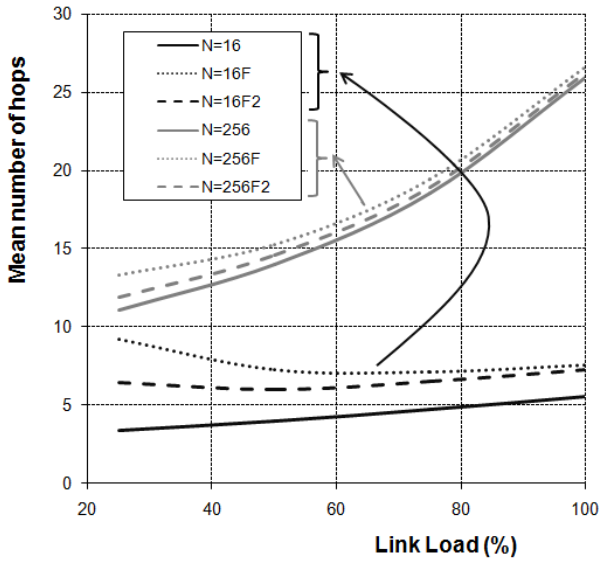

Figure 3: Number of hops increases after failure for two types of signalizations.

A. Shortest Path Calculation

The shortest path to reach the destination is calculated once for a non-failed topology. As the packet can be deflected to any output port, it must be able to find out the destination shortest path from any place in the network and not only from the origin. The packet is informed about the shortest path through a preferential port matrix "pp" with dimensions *NxN*, were *N* is the total number of nodes. Each column of the pp matrix represents the actual position of a packet and the matrix elements are numbers indicating the best option: number 1 for output 1 or number 2 for output 2 or number 3 to indicate that there is a shortest path starting from both outputs.

Before the calculation of the preferential port matrix pp, it is necessary to know the connection matrix "c". That matrix is a sparse *NxN* matrix representing the considered topology. Each column in the c matrix represents the actual position of a packet and each line represents the destination to be reached in one hop. With the exception of the two directly connected nodes, all the *N-2* elements in any column of the c matrix are equal to zero. In addition to the information of the directly connected nodes, the non-zero elements also inform the link sub-domain type number. The positions of the matrix elements correspond to the directly connected nodes and the matrix element itself represents the sub-domain type 1 (output 1) or sub-domain type 2 (output 2). Type 1 could be, as an example, the clockwise type and type 2 the anticlockwise type (see Figure 1).

Starting from connection matrix c, the preferential port matrix pp is constructed. This is done column by column, in an adaptive tree procedure [11] that is nondeterministic just at the beginning of the algorithm. That procedure is nondeterministic because it is necessary to calculate the smallest path starting from all possible packet positions.

B. Mean number of hops calculation

The network performance is measured by the mean number of hops $<H>$ a packet completes from origin to destination. The main program, utilized for the main number of hops calculation, is based on the evolution of a vector $P(x)$ with N dimensions. The x variable is the discrete position for the packet $(x = 1, 2, ..., N)$. Each vector represents the probability of finding a hypothetical packet in etch node. That is called probability distribution vector. The mathematical treatment for the evolution of a probability distribution along time corresponds to the application of an operator *"U"* to the probability vector $P_t(x)$ at any instant of time "t" to obtain the probability vector $P_{t+1}(x)$ at the instant of time "t+1" after a discrete time interval. The unitary increment of time corresponds to one hop from one node to the following in the packet traveling from source to destination.

$$P_{t+1}(x)=UP_t(x) \quad (1)$$

Operator U is analogous to the "Perron-Frobenius operator" utilized in the chaos theory for the calculation of the time evolution of a probability distribution [9]. An analogy can be constructed with the chaos theory, in which the idea of trajectory is abandoned and replaced by the evolution of a probability distribution. In this work, the idea of a path that a packet should follow from its origin to its destination is replaced by the probability distribution vector time evolution described in [1]. Acampora and Shah [12] consider similar statistical procedure to describe the behavior of a store-and-forward routing as a comparison with hot-potato routing. Due to the fact that the probability to go directly from one node to the other is zero for almost all nodes except for the two directly connected nodes, most of the elements in operator U are zero. Each column has only two non-zero elements. The preferential output port has probability *Ppp* and the alternative port, corresponding to the deflection port, has probability *Pd* given by:

 ISBN: 978-1-61208-239-4

$$Pd = 1 - Ppp \quad (2)$$

A packet is sent to the preferential port in tree cases:

a) There is no other packet in the competitor link that could arrive before it.
b) There is another packet that could arrive before it, but that has a local final address and is going to be removed before competition.
c) There is another packet arriving before it that is not a local packet, but it has a different preferential output port.

The link occupation probability *Poc* defines the probability of the first case to be $1 - Poc$. Given that case a) is not true, the local packet probability *Plp* defines the second case probability term as $Poc*Plp$. Finally, given that case a) and case b) do not apply, considering *Pop* as the probability of the competitor packet to have a different preferential port (another port), the third term is defined as $Poc*(1-Plp)*Pop$. The final probability of a packet to go through the preferential port *Ppp* is given by:

$$Ppp = 1 - Poc + Poc*Plp + Poc*(1-Plp)*Pop \quad (3)$$

In (3), *Poc* is the occupation probability that is associated to the link load. It is considered that a fully loaded link (not considering the FDL length) corresponds to $Poc=1$. The probability of a packet preference pointing to another port *Pop* is assumed to be 50% and $Pop=0.5$ in all cases. The local packet probability *Plp* is evaluated to be $1/<H>$, with $<H>$ calculated as a preliminary mean number of hops obtained with a first guess value $Plp=1/(N-1)$.

The $Plp=1/<H>$ hypothesis is originated by the fact that all packets, at any time, belong to his path from origin to destination. The mean number of hops in all possible paths is $<H>$ and the packet is considered to be a local packet only in the last of those hops. That means that *Plp* is the probability of a packet to be positioned at the last hop of its path from origin to destination.

Without failure, the Manhattan Street network architecture belongs to a symmetry group called automorphism [10]. In this group, it is impossible to differentiate any node from the other concerning its position in the network. The mean number of hops is the same regardless the position of the final address node. But introducing a failure, the symmetry is broken and the mean number of hops may assume different values for different final destinations. In this case, it is necessary to calculate the mean number of hops for all possible destinations and to adopt the arithmetic mean of those values as the final network mean number of hops.

One more consideration should be made about the "don't care" nodes. They are already identified and signalized by number 3 in the preferential port matrix pp. In that case, it is considered that the packet plays no role in the decision of the preferable output port. The position of the switch may be adjusted to the preferred output port of the packet eventually arriving in the competitor link. That procedure corresponds to considering $Ppp=Pd=50\%$ in all "don't care" situations.

The number of hops is obtained recursively by (1) starting with $P_1(x)$, that represents the probability to reach the destination with one hop, to calculate $P_2(x)$, that represents the probability to reach the destination with two hops. That procedure is repeated k times while the total probability is less than 100%, with an arbitrary criteria chosen to be $\Delta P=10^{-6}$. Further reduction of that criterion interferes only with the calculation time and no change is observed in the results for $\Delta P=10^{-5}$.

As an example, for a network with four nodes ($N=4$), the initial probability to find a packet addressed to node number one, in any place is considered to be zero to node number one and 1/(N-1) for all the other nodes. That condition is represented by the initial probability vector $P_1(x)$ given in (4).

$$P_1(x) = \begin{bmatrix} 0 \\ 1/3 \\ 1/3 \\ 1/3 \end{bmatrix} \quad (4)$$

The mean number of hops for each destination x is calculated by the equation:

$$< H >= \sum_{1}^{k} t P_t(x) \quad (5)$$

With the condition:

$$1 - \Delta P < \sum_{1}^{k} P_t(x) \leq 1 \quad (6)$$

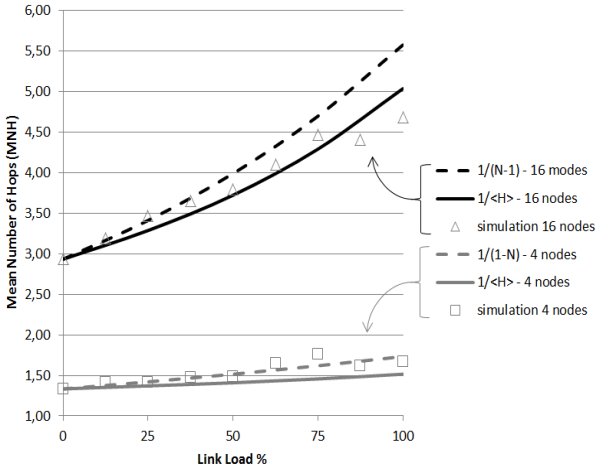

Figure 4: Analytical and simulation models.

C. Simulation model

The time domain simulation model (TDSM) was developed over the OMNET++ platform. The simulation model considers all the nodes sending packets to all the others and following the same rules used for the analytical model. Every packet arriving to one *2x2* node is addressed to the better output port, unless the node is already occupied with a competitor packet. In that case, the packet is sent to the available output port. The destination and the exact instant of packet generation are randomly chosen. Each link

 ISBN: 978-1-61208-239-4

load condition is governed by the packet size. A packet with half the link size is used to simulate the 50% link load condition. Each packet that reaches the destination stimulates the insertion of a new one, addressed to a new randomly chosen destination. That procedure insures the maintenance of the link load condition all along the simulation time. A 40Gbps bit rate and one kilometer link length were considered. The delay line fiber length is considered to be equal to the link length, the same hypothesis utilized in the analytical model. Figure 3 shows the simulation results compared to the analytical model results for two hypotheses utilized for the evaluation of the local packet probability *Plp*. The agreement between models is better for hypothesis *Plp=1/<H>* as compared to the hypothesis of the first guess *Plp=1/(N-1)*. In fact, that first guess is very close to simulation results for the small number of nodes but tends to decrease faster than *Plp=1/<H>* producing wrong results for a higher number of nodes. The simulation time is far higher than the analytical calculation time, limiting its utilization for scalability issues.

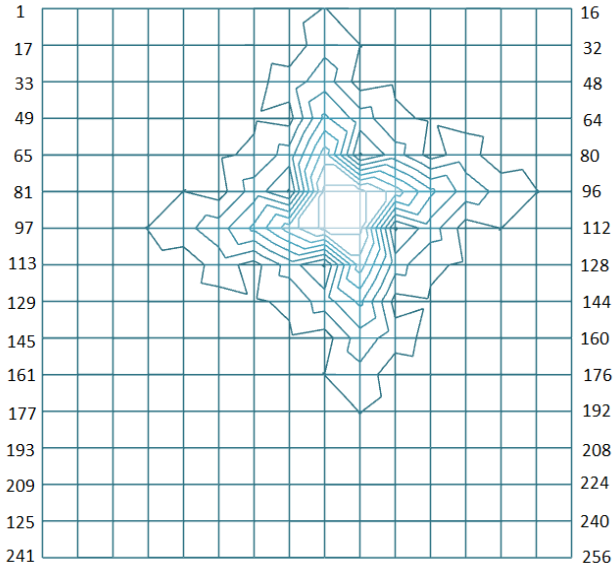

Figure 5: Failure segregation. Each contour line corresponds to one more hop from source to destination. Outside the contour lines, the Average Number of Hops (ANH) is less than 26. Inside all lines, the ANH is less than 34.

D. Failure effect distribution map

The last calculation performed was the failure distribution effect. In case of failure, the symmetry is broken and the mean number of hops is no longer the same for any destination. Then, it was necessary to calculate the mean number of hops executed by an arbitrary packet addressed to all the 256 nodes. The overall mean value was considered to be the arithmetical median of those previously calculated values. Considering the full load traffic condition (100% link load), the map in Figure 5 shows an important distribution characteristic. The map shows nodes 1 to 16 in the first line and 16 nodes per line up to node number 256. The failure occurs in a link belonging to the clockwise sub-domain connecting nodes 89, 90, 106 and 105. Most of the destination nodes are not perturbed by the failure and remain with the same average number of hops (ANH) they had before failure (ANH<26). The ANH increases only for the destinations near the failure. Outside the contour lines, the ANH is less than 26. Crossing one contour line, the ANH is less than 27. Increased by one unit after crossing each contour line, the ANH will be less than 34, near failure, after crossing 8 contour lines.

V. CONCLUSION AND FUTURE WORK

The approach of treating large number of nodes network as a complex system, working as a bottom-up organization system, was analyzed with a statistical analytical model and a simulation model. It was possible to investigate a Protection Emerging Function. Protection is achieved by local signalization that modifies only the nodes operations around the failure. No signalization needs to be transmitted over a long distance regardless of the size of the network. A map with the number of hops after failure illustrates that the network performance degradation occurs only around the failure. The segregation of the failure effects represents a new feature that could be observed due to the new approach. All results can be reproduced for any topology. Reference [13] shows preliminary results for the National Science Foundation Network (NFSnet) treated as a complex system in a bottom-up type of organization. Future work will furnish more details about the complex behavior trough the utilization of the same statistical analysis. With more nodes new Emerging Functions can be emphasized [1]. Several new features can be proposed or investigated. Traffic distribution, protection and restoration functions can also be analyzed as Emerging Functions. The bottom-up organization and the complex system treatment permits better performance and to increase the robustness of large number of nodes network.

ACKNOWLEDGMENT

The authors thank FAPESP – The State of São Paulo Research Foundation – sponsor of the KyaTera Project. The authors also thank Lucas Pauli Simões for the contributions to the simulation results.

REFERENCES

[1] A. Sachs, C.M.B. Lopes, and T.C.M.B. Carvalho, Protection schema for optical packet switching network with large number of nodes, Microwave and Optoelectronics Conference (IMOC) 2009 SBMO/IEEE MTTS-International, 3-6 Nov 2009, pp. 47-50.

[2] P. Baran, On Distributed Communications Netwoks, IEEE Transactions on Commnications Systems, CS-l2 (1964), pp. 1-9.

[3] C. Guillemot, M. Renaud, P. Gambini, C. Janz, I. Andonovic, R. Bauknecht, B. Bostica, M. Burzio, F. Callegati, M. Casoni, D. Chiaroni, F. Clerot, S.L. Danielsen, F. Dorgeuille, A. Dupas, A. Franzen, P.B. Hansen, D.K. Hunter, A. Kloch, R. Krahenbuhl, B. Lavigne, A. Le Corre, C. Raffaelli, M. Schilling, J.C. Simon, L. Zucchelli, Transparent Optical Packet Switching: The European ACTS KEOPS Project Approach, J of Lightwave Technology, 16 (1998), pp. 2117-2134.

 ISBN: 978-1-61208-239-4

[4] L. Dittmann, C. Develder, D. Chiaroni, F. Neri, F. Callegati, Member, IEEE, W. Koerber, A. Stavdas, M. Renaud,, A. Rafel, J. Solé-Pareta, W. Cerroni, N. Leligou, Lars Dembeck, B. Mortensen, M. Pickavet, N. Le Sauze, M. Mahony, B. Berde, and G. Eilenberger; The European IST Project DAVID: a Viable Approach towards Optical Packet Switching; JSAC Special Issue on High-Performance Optical/Electronic Switches/routers for High-Speed Internet II. IEEE Journal on Selected Areas in Communications, 21 (2003), pp 1026 – 1040.

[5] C. Stamatiadis, M. Bougioukos, A. Maziotis, P. Bakopoulos, L. Stampoulidis and H. Avramopoulos, All-Optical Contention Resolution using a single optical flipflop and two stage all-optical wavelength conversion, paper OThN5 Proceedings of OSA / OFC/NFOEC 2010. Available at: <http://www.photonics.ntua.gr/PCRL_web_site/OFC_10_OThN5.pdf>. Retrieved: July, 2012.

[6] J.M. Carlson and J. Doyle, Complexity and Robustness, Proceedings of the National Academy of Sciences - PNAS, February 19, vol. 99, suppl. 1, 2002, pp. 2538–2545.

[7] A.L. Barabási, The Architecture of Complexity, IEEE Control Systems Magazine, 27(2007), pp. 33-42.

[8] D.L. Turcotte and J.B. Rundle; Self-organized complexity in the physical, biological, and social sciences, in Proceedings of the National Academy of Sciences – PNAS, February 19, vol. 99, suppl. 1, 2002, pp. 2463–2465.

[9] I. Prigogine, Le leggi del caos, Roma-Bari, Editori Laterza, 1993.

[10] A.G.Greenberg and J.Goodman, Sharp approximate models of adaptative routing in mesh networks. Telegraffic Analysis Computer Performance Evaluation. Elsevier Science -North Holland, pp. 255-269, 1986.

[11] H. Pistori; J.J. Neto; M.C. Pereira, Adaptive Non-Deterministic Decision Trees: General Formulation and Case Study. INFOCOMP Journal of Computer Science, Lavras, MG, 2006. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1885&rep=rep1&type=pdf>. Retrieved: July, 2012.

[12] A.S. Acampora and S.I.A. Shah, Multihop lightwave network: a comparison of store-and forward and hot potato routing, IEEE Transactions on Communications, 40(1992), pp. 1082-1090.

[13] A.C. Sachs, Rede auto-organizada utilizando chaveamento de pacotes ópticos. 2011. Doctoral Theses (Digital Systems) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2011. Available at: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-05082011-152444/>. Retrieved: July, 2012.

 ISBN: 978-1-61208-239-4