International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Recovery Management in All Optical Networks Using Biologically-Inspired Complex Adaptive System

Inadyuti Dutt, Soumya Paul, S.N. Chaudhuri

***Abstract* - All-Optical Networks have the ability to display varied advantages like performance efficiency, throughput etc but their efficiency depends on their survivability as they are attack prone. These attacks can be categorised as active or passive because they try to access information within the network or alter the information in the network. The attack once detected has to be recovered by formulating back-up or alternative paths. The proposed heuristic uses biologically inspired Complex Adaptive System, inspired by Natural Immune System. The study shows that natural immune system exhibit unique behaviour of detecting foreign bodies in our body and removing them on their first occurrences. This phenomenon is being utilised in the proposed heuristic for recovery management in All-optical Network.**

***Keywords* – All-optical Network (AON), Swarm Intelligence, Honey Bee Algorithm.**

I. INTRODUCTION

Once an attack has been detected, proper recovery or back-up paths are designed to ensure the normal functioning of the network. Attack recovery may be defined as the method of re-establishing traffic continuity in the event of an attack being detected on a networking node, by rerouting the signals on diverse facilities after the attack. Clearly, recovery from an attack is a crucial aspect for the successful deployment of today's telecommunications networks. Most users rely heavily on their telecommunications networks. Users can range from individual clients to institutions, hospitals, banks, stock marketing firms, schools, government agencies, military operations, etc. In many such institutions, frequent or lengthy periods of service disruptions can affect the normal operations of the business. An attack that remains unattended for a longer period of time can become bottleneck problem and may cause both tangible as well as non-tangible losses for the organizations. A prolong disruption of service can damage the credibility as well as reputation of the organization. The clients on the other hand, might not attempt to single-handedly join hands with such organizations whose service operations become disrupted due to attack on the network.

Thus it becomes a necessity to employ certain recovery methods or techniques which would introduce alternative or back-up paths. This chapter presents some interesting survey of the existing recovery techniques in optical networks as an introduction and then explicitly describes the recovery methods or techniques formulated overcome such attacks.

A. Attack Recovery Classifications

A network is defined as survivable if it is capable of attack recovery in the event of attack occurrence. The degree of survivability is determined by the network's ability to survive single or multiple attacks. Fast and reliable recovery methods are essential to efficiently protect the network against any such attacks. The main objective of recovery management technique is to employ accurately, rapidly and without incurring additional cost for rerouting the traffic.

In the first half of the 1990s most of the attack recovery techniques in optical networks employed point-to-point systems and Self-Healing Rings(SHRs), as natural extensions of the SONET recovery techniques. Protection methodologies used in SONET were widely accepted as simple and reliable. It was only in the second half of the 1990s and beyond that recovery techniques included Tellium implementation of commercial equipment, Shared Backup Path Protection (SBPP). Different recovery methods have their advantages and disadvantages. For example, one recovery method can be very fast but can use excessive redundant capacity while the other can be slower but can use redundant capacity very efficiently. Depending upon the customers' needs and how critical their services are, the recovery methods can be selected for implementation.

Recovery methods can be classified depending upon the survivability definitions presented below:

- Protection signifies techniques with which the back-up or alternative paths are pre-computed before the occurrence of an attack. It may be noted that such back-up routes have been pre-computed but not pre-configured prior to attack occurrence. This holds true for the recovery techniques used in point-to-point and Self-Healing Ring (SHR) architechture of WDM or SONET.
- Restoration denotes recovery techniques where the back-up or alternative paths are nor pre-computed prior to attack occurrence but calculated in real time after an attack has been actually detected. Switching equipments and spare capacity in conjunction with rerouting schemes are then used to reroute the traffic. Recovery in such situations is accomplished by employing intelligence that resides at a centralised network manager or controller or at individual switching nodes.

B. Biologically-Inspired Complex Adaptive Systems (CASs)

Biologically-Inspired Complex Adaptive Systems (CASs) have evolved as an emerging inter-disciplinary field which exploits tools and techniques across a range of different areas to understand the behaviour of systems found in Nature. CAS generally refers to a dynamical network of self-similar and independent agents that interact with each other in many different ways and give rise to a previously unknown collective behaviour (Waldrop, 1992; Holland, 1995; Dooley, 1996). Complex Adaptive Systems (CAS), a term coined by John H. Holland et al. at the Santa Fe Institute in1980s (Waldrop, 1992) focuses on the understanding and managing of

complex inter-disciplinary field of science. The field of CAS is basically inspired by Nature and offers wide range of techniques and analysis tools that are truly motivated from the fields of Biology and Sociology. Techniques such as Artificial Immune Systems, Artificial Neural Networks and Swarm Intelligence are some of the few examples which encourage problem solving in varied fields of study and research. Natural CAS is robust and flexible in nature as because they can adapt to environmental changes and can constantly change their states for their betterment. Due to their unique characteristics like self-similarity, self-organization, emergent behaviour, highly decentralised control and adaptivity they are now widely used in the field of Computer Networks and Security.

Ever since the computers have evolved, there has been large transformation from a small scale, restricted set of computers in a secured network connecting a few operators to the large scale, unbounded internetworks of networks providing the backbone of today's omnipresent computing environment. Recent researches (Baraba´ si and Albert, 1999) have shown that the large scale, heterogeneous computer networks like Internet, WWW and semantic web share similar topological features as exhibited by many of the networks found in Nature such as metabolic networks of living organisms and various social networks. These networks have been considered as ''scale free'', i.e. the degree distribution (probability of a node having a certain number of links) of these networks follows a power law. When these networks have few nodes with high connectivity (known as the hubs) and many nodes with only few connections, they exhibit the so called ''small world'' phenomenon, which essentially means that each node on the network is accessible from another node within a small number of hops. This class of networks is referred to as complex networks. Leading to this discovery, it has outmoded the classical Erdos–Renyi model (Erdo¨ s and Re´nyi, 1960) which assumed the large scale networks to be random in nature.

As the Complex Adaptive System is composed of many self-similar agents interacting with each other in many ways, large scale computer networks are also composed of numerous end hosts interacting with each other in many different ways with each individual exhibiting a self-similar network traffic pattern. Nevertheless, it is evident that the network traffic patterns of the local nodes cannot predict the traffic trend of the global network in a very similar manner to a CAS where the collective behaviour of the system emerges from the interaction of the individuals; the holistic network behaviour emerges from the communication between the individual hosts on the network.

C. Complex Adaptive Systems (CAS) and Natural Immune System

The main objective of CAS is to check the whole system in conducting an "immune surveillance" to identify self and non-self cells so as to recognise and eliminate the harmful non-self cells. During the generation of T-cells, receptors are made through a pseudo-random genetic rearrangement process. They undergo a censoring process in the thymus, called negative selection. There, T-cells that react against self-proteins are destroyed and those that do not bind to self-proteins are allowed to leave the thymus thus, demonstrating self tolerance [Timmins and Knight; 2002]. These matured T-cells then undertake immune surveillance to pick up Major Histocompatibility Complex molecules (MHC). Thus, adaptive immunity launches an attack against invaders that the innate system cannot remove and is directed towards invaders made up of lymphocytes3. It is the B and T-cells that aid in recognising and destroying specific substances even if it has never faced an invader before [Castro and Von Zuben, 1999].

Adaptive immunity is the main focus because of its vital features of learning, adaptability and memory which are important for emerging agents to adapt and evolve for optimum immunity. T-Lymphocytes participates in cell mediated immune reactions which reacts by killing altered self-cell thus, activation of various phagocytic cells, enables them to phagocytose and kill micro-organisms more effectively. The adaptive immune system is made up of lymphocytes which are called B and T cells (Timmis, 2001). The process of detecting between different types of pathogens is explained using the principle of ''self'' and ''non-self''. Not all the pathogens are harmful and thus it is central to the working of immune system that it can distinguish between the harmless antigens (i.e. self) and the harmful antigens (i.e. non-self) (Hofmeyr and Forrest, 2000). The discrimination process, known as negative selection (Forrest et al., 1994), occurs during the generation of T cells in the thymus. During negative selection the immature T cells that match self proteins are destroyed. Once the infectious antigens are detected they are eliminated with the help of B cells. This primary response invokes to generate a large number of B cells through a process called clonal selection (Timmis, 2001 for references). During clonal selection the B cells are cloned and mutated to produce a diverse range of antibodies that might match a similar infection in future.

It is the B-cells that are primarily responsible for hurmoral immunity and it is the reaction of antigens that result in cloning, enabling cells that recognize the antigen proliferate via the cloning selection principle in an attempt to produce sufficient antibodies [Timmins and Knight; 2002, Castro and Timmins; 2002]. Instead of the expected clonal deletion of all self-reactive cells, occasionally B lymphocytes were found that had undergone receptor editing: these B cells had deleted their low affinity receptors and developed entirely new ones through recombination (Nussenzweig, 1998).

Natural Immune Systems (IS) provide an excellent platform for applying CAS. IS provide an excellent mechanism by which an organism, which is exposed to trillions of previously unknown antigens of varying types, can combat them efficiently with ease. First the physical barrier like skin prevents the viruses and bacteria to enter the body. If this layer is breached then the innate immune system provides an immediate response without targeting to any specific pathogens. During subsequent surveillance the initial encounter and removal of foreign substances is referred to a primary response in which "a quantity of B-

cells remain in the IS and acts as an immunological memory" [Timmins and Knight; 2002]. Even though it begins to degrade the secondary response causes a more rapid growth in the quantity of B-cells and antibodies which results in a faster response during secondary exposure. This attribution to memory cells does not require a new immunity to be built up thus, acts as a self-organising and self-regulatory system which can capture antigen information.

II. Proposed Recovery Management Algorithm Based on Artificial Immune System (AIS)

A. Artificial Immune Systems (AIS)

Just like Complex Adaptive System in Immune Systems, the computer networks are exposed to multitude of attacks. IS silently tackles all these pathogens without us realizing that our immune system is constantly defending against the intruders. IS are highly distributed, dynamical, self organized, adaptive and robust information processing systems (Hofmeyr and Forrest, 2000). IS provide a multi-layered protection to the organisms. The adaptive immune system comes into action if the innate system is evaded (Somayaji et al., 1997).

Due to the inherent resemblance between the working of an IS and the requirements of computer security various researchers have used AIS based approaches. In a typical AIS based IDS (Hofmeyr and Forrest, 1999; Jungwon and Bentley, 2001), the normal behaviour is considered as self and the intrusive behaviour as non-self. Initially the detectors or patterns of the network traffic or the host activities are randomly generated to mimic the generation of T cells. During training the negative selection process occurs where these detectors are exposed to the normal events and any matching detectors are removed from the detector sets. The remaining detectors are then used to detect the abnormal behaviour. The detectors which correctly match the anomalous behaviour are memorised for future use. These detectors also go under the clonal selection process which is simulated using a Genetic Algorithm (GA).

Various approaches have been proposed in the literature that aim to mimic the behaviour of IS for computer security. Somayaji et al. (1997) provided various possible architectures of AIS for computer security. DasGupta (1998) and Aickelin et al. (2004) provided a good review of the field. Many early researchers have shown the success of AIS based intrusion detection and have provided frameworks for host and network based Intrusion Detection Systems, e.g. Forrest et al. (1996), Hofmeyr (1998), Dasgupta (1999), and Jungwon and Bentley (2001).

AIS highlight these characteristics which include [Timmins and Knight; 2002, Harmer et al; 2002, Timmins et al; 2004]:

- Recognition – its ability to differentiate between self and non-self cells and further, recognise and eliminate harmful molecules.
- Uniqueness - each system possesses its own IS, with its particular vulnerabilities and capabilities;
- Feature extraction - ability to extract features of the antigen by filtering molecular noise from the antigen before being presented to the lymphocytes.
- Diversity – a diverse range of antibodies repertoire is created in response to an antigen via hypermutation.
- Learning and Memory – interaction within the immune network theory and IS maintaining a memory of antigens encountered enables future responses to the same pathogens are faster and stronger.
- Anomaly detection - The IS can detect and react to pathogens that the body has never encountered before.
- Distributed detection - There is no one point of overall control; each lymphocyte is specifically stimulated and responds to new antigens.
- Imperfect detection (noise tolerance): an absolute recognition of the pathogens is not required, hence the system is flexible;
- Self regulation - IS dynamics are such that the IS population is controlled by local interactions and not by a central point of control.
- Metadynamics - New immune cells are created, and the old and useless cells are eliminated. This process of continually maintaining the immune cells is called metadynamics.

B. Description

The proposed algorithm for recovery management begins with initialization of the network with optical nodes and confirming the source and destination nodes from the user. The data packets are being sent by the source node and they are received by the destination node. Once the source and destination nodes are confirmed, all the possible routes between the two nodes are determined.

Then the algorithm generates T-cells as attack detector cells for detecting attacks in the network. T-cell attack detectors just like the natural IS imitate to detect foreign antibodies or intruders in the body or network. Upon detecting an attack on a specific node in between the source and destination nodes, the B-cells are then generated to determine the alternative, back-up paths in the network and to remove the attacked node from these paths. Thus the main objective of B-cells is to remove the affected node from the back-up paths created for normal functioning of the network.

C. Proposed Algorithm

Step1: Enter the number of nodes "n" in the network between which the packets of data needs to be transferred.
Step2: Enter the adjacency matrix a[n] [n] showing the connection between the nodes.
Step3: Give the source node (node from which the packets need to be transferred) "p" and the destination node (node in which the packets should reach) "q".
Step4: To show the direct path between source node and destination node.
Step5: To show all the indirect routes.
Step6: Generate the attack detector cells (T-cells) for detecting attack between node 'p' and 'q'.

International Journal of Electronics Communication and Computer Engineering
Volume 4, Issue 1, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Step7: Enter the node in which attack is detected. Remove this node from the routes. (i.e. all the routes which does not include the attacked node are shown)
Step8: If an attack is detected on a node between 'p' and 'q', generate recovery cell (B-cells) to determine the alternative, back-up paths.
Step9: Display the direct paths between source node and destination node, excluding the attacked node.
Step10: Display the indirect paths between source node and destination node.

D. Example Illustration

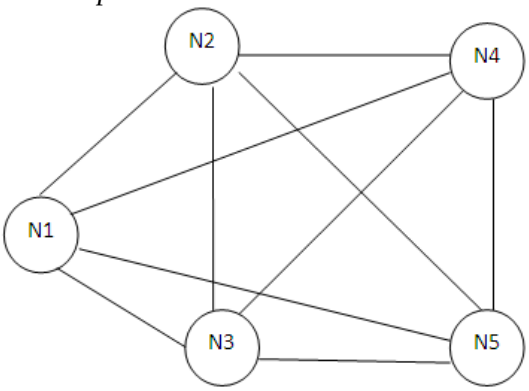


Fig.1. Mesh network with five nodes

Consider the above network in which there are five computing nodes, N1, N2, N3, N4 and N5. Between each node there exist certain distances which is as specify. A fully connected network has been considered for detecting attacks by a third party or a third network. Suppose we consider the source and destination of attack detection and alternative path identification to be N1 and N3. The primary path would be either the path which is having a direct connection from source to destination. Since the nodes are fully connected we get direct path links among the source and destination.

A computing node is said to be a source node if it send any kind of message or packet to any other node.

A destination node or network is that which receives message and packets from any destination.

Thus the primary path N1 to N3 is N1- N3.

The attack if detected between this path we try to find an alternative solution to the problem by implementing alternative paths. These alternative paths are known as backup or recovery paths. This in here they said N1 to N3; the backup paths might be.

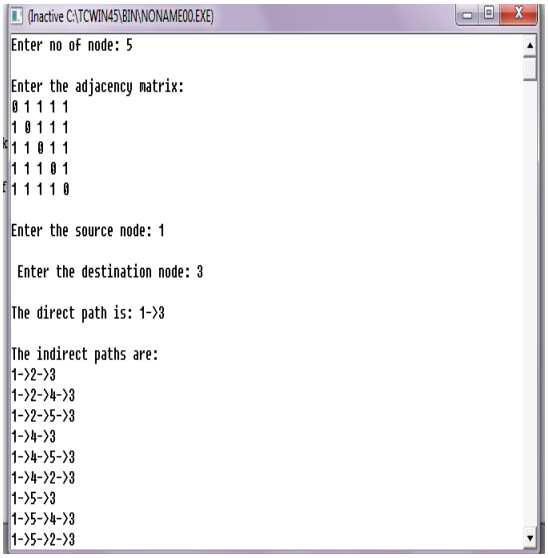
N1- N2-N3
N1- N2-N4-N3
N1-N2-N5-N3
N1-N4-N3
N1-N4-N2-N3
N1-N4-N5-N3
N1-N5-N3
N1-N5-N4-N3
N1-N5-N2-N3

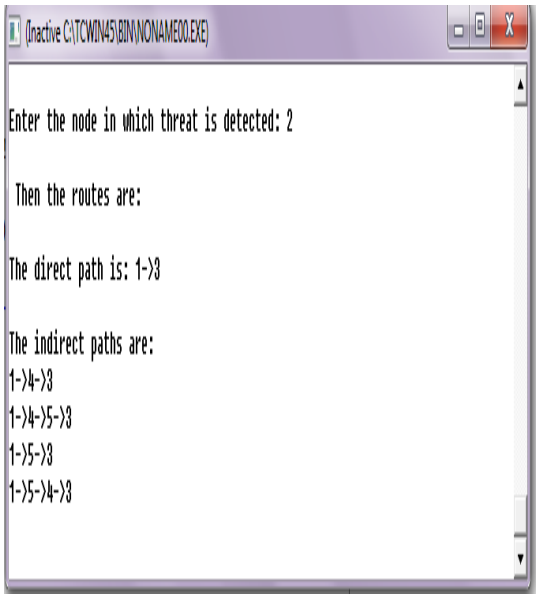
The attack detection system works as a B cell in the human body by trying to find the foreign particle in the network. The attack would be detected between N1 to N3 by sending finite number of packets or messages between them. Say between N1 to N3 50 packets have been send and if it is seen that less than the 50% packets have not being received then the attack can be detected. A probability of more than 0.5 or ½ will suggests that there remain no attack between the source and destination.

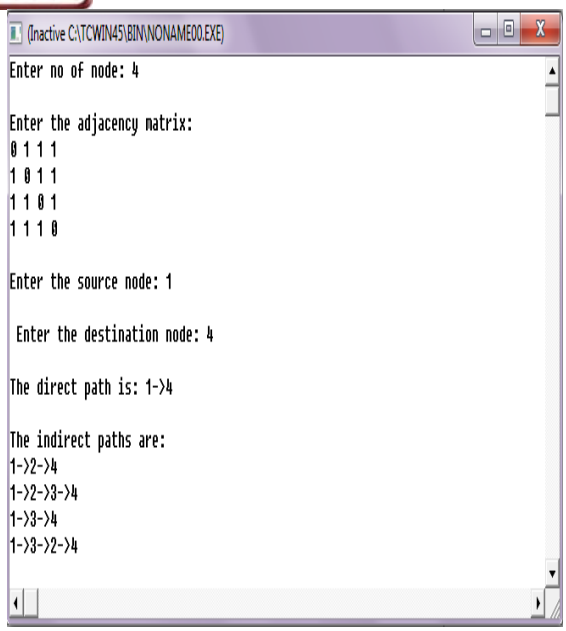
After detection of the attack the alternative paths are identify by another system called backup or recovery system. It acts as the T cell in the human body by capturing those nodes which are attacked. So in this case if attack has been detected N1 to N3 then the recovery system will identify the backup path.

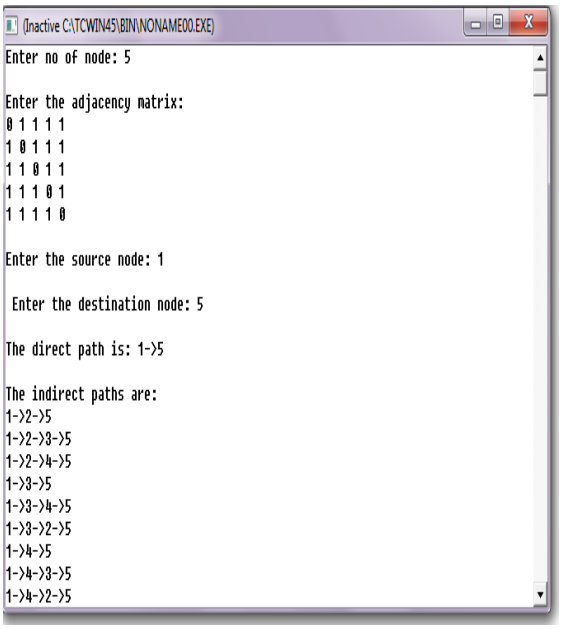
III. RESULTS

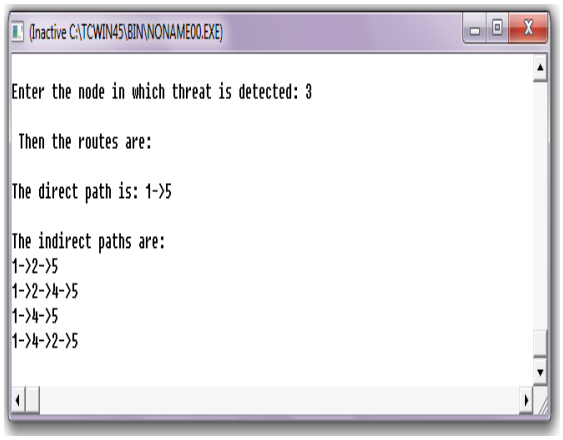
The results show that the proper determination of alternative, back-up paths between a source and destination node. The usage of local path occurs when there is no attack in the AON whereas the usage of global paths is due when there occurs attack on the network. Thus the proposed heuristic not only determines the primary path but also calculates their back-up paths. Figures represent the depiction the results of both local and global paths in the network.

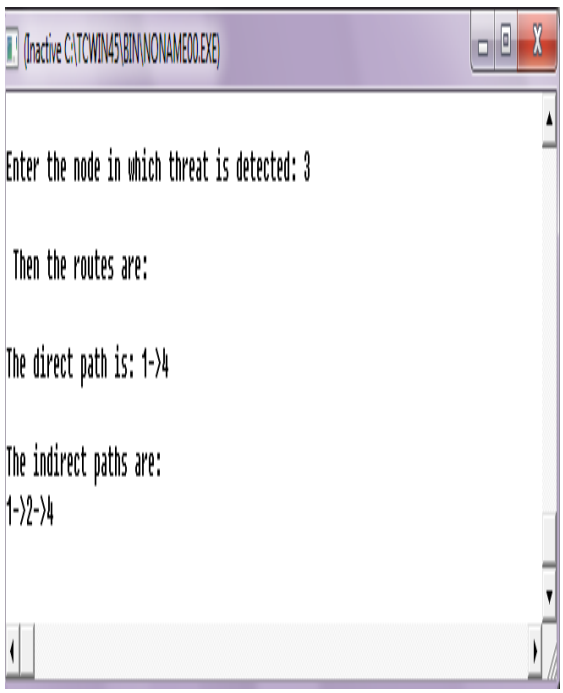












IV. Conclusion

The proposed heuristic uses biologically inspired Complex Adaptive System, inspired by Natural Immune System. The study shows that natural immune system exhibit unique behaviour of detecting foreign bodies in our body and removing them on their first occurrences. This phenomenon is being utilised in the proposed heuristic for recovery management in All-optical Network**.** The results in the above section reveals the efficiency of the proposed heuristic in identifying the attacks on the network and in addition to it provides recovery paths for the attacked network.

References

[1] Kamran Shafi Hussein A. Abbass, “Biologically-inspired Complex Adaptive Systems approaches to Network Intrusion Detection, Defence and Security Applications” Research Centre (DSARC), University of New South Wales at the Australian. Defence Force Academy, Canberra ACT 2600, Australia Elsevier.

[2] Nobel laureate Karl von Frisch, ‘The Dance Language and Orientation of Bees’, Harvard University Press, 1993.

[3] Deepika Chaudhary, “Bee-Inspired Routing Protocols for Mobile Ad HOC Network (MANET)”, Journal of Emerging Technologies in Web Intelligence, Vol. 2, pp. 86-88, May, 2010.

[4] Horst F. Wedde, Muddassar Farooq, and Yue Zhang, “BeeHive: An Efficient Fault-Tolerant Routing Algorithm Inspired by Honey Bee Behavior”, M. Dorigo et al. (Eds.): ANTS 2004, LNCS 3172, pp. 83–94, 2004, Springer-Verlag Berlin Heidelberg 2004.

[5] Omid Bozorg Haddad, Abbas Afshar and Miguel A. Martin, “Honey-Bees Mating Optimization (HBMO) Algorithm:A New Heuristic Approach for Water Resources Optimization”, Water Resources Management (2006) 20: 661–680, DOI: 10.1007/s11269-005-9001-3.

AUTHOR'S PROFILE

Inadyuti Dutt

has been in the field of academics and research for more than ten years and is currently the Assistant Professor in the Department of Computer Application of B. P. Poddar Institute of Management & Technology, Kolkata, West Bengal, India. .Earlier, she held several technical positions in National Informatics Centre, Kolkata and Semaphore Computing Networks Pvt. Ltd. respectively. She has earned Master's Degree in Computer Application and currently pursuing her research in Computer Science and Engineering. She has more than 15 publications to her laurels and her research interest is specifically in the field of Optical Networking, Security and Genetic Algorithms. She has also been Member, Editorial Board in journal publications like International Journal of Software Engineering & Research.

Soumya Paul

Assoc. Professor and Head, Department of Computer Application in B. P. Poddar Institute of Management & Technology, Kolkata, has been in teaching and research for over 12 years. He holds a Master's Degree in Technology, Computer Application as well as in Mathematics and has gathered vast experiences in the same. He received his M.Sc. (Mathematics) from Visva Bharati University and stood 1st class 1st. He received MCA from National Institute of Technology, Rourkella and M. Tech (CSE) from AAI-Deemed University and pursuing Ph. D in Computer Science and Engineering. He served as a faculty member and visiting faculty member in various Institutes and Universities like RCCIIT, Visva Bharati University, University of Calcutta, Bardhaman University, West Bengal University of Technology etc. He has delivered numerous lectures across India in the field of his research interest, Optical Networks and Genetic Algorithms. He is an author/co-author of several published articles in International Journals and International Conferences. He has chaired an International Conference technically supported by IEEE communication. He has more than 15 research publications and currently Reviewer and Member, Editorial Board in many conferences and journals like International Journal of Data Modelling and Knowledge Management.

Prof. Dr. S. N. Chaudhuri

Director, Kanad Institute of Engineering & Management, Manakar, Burdwan, West Bengal is a renowned Academician as well as Scientist. He has a working experience for nearly 40 years in different National and International Institutions. As a visiting Professor, he visited different foreign Universities. He has number of publications to his credit and his name has been included in Who is Who Indian Personages.