

QoS-Aware Ant Routing with Security Constraints in Optical Fibre Networks by Using RGB Pheromones

Mohammed Al-Momin, Pavlos I. Lazaridis, John Cosmas, Zaharias D. Zaharis, Stavros Kalafatis, Alben Mihovska, and Ian Glover

Abstract— The traditional ant routing protocol provides an efficient way for dynamic routing in continuously changing networks. Due to their social behaviour, ants tend to find optimized paths based on network status information such as the path length and capacity. However, the conventional ant routing protocol tends to satisfy acceptable Quality of Service (QoS) requirements for the whole network traffic. The major problem is that different traffic types request different QoS requirements, and the traditional ant routing lacks the ability of providing different levels of QoS parameters for these different traffic types. In this paper, a novel technology is proposed to satisfy the requirements of different traffic types which vary in terms of bandwidth, latency and security. Oyster Optics Technology has been used to introduce the security as a new significant QoS factor.

Keywords— Ant routing, QoS, load balance, traffic types, routing, optical networks.

I. INTRODUCTION

Ant Colony Routing (ACR) was inspired from the social behaviour of ants. Despite the limited intelligence of single ants, the collective behavior enables them to find the shortest path to food [1], [2]. Ants belong to a special category of social insects that deposit a volatile chemical substance called pheromone on the path they pass through. In addition, ants tend to follow paths with more deposited pheromone than others [3], [4]. Due to volatility, the concentration of pheromone depends on the path length. By assuming multiple paths that lead ants to the food, the ant which takes the shortest path will reach the food faster than the other ones. Then, this ant returns by passing through the same path, since the pheromone deposited in the path has hardly evaporated and thus the pheromone concentration attracts the ant to use the same path.

Mohammed Al-Momin is with Southern Technical University, Basra, Iraq. John Cosmas is with the School of Engineering and Design, Brunel University, London UB8 3PH, UK. Pavlos I. Lazaridis and Ian A. Glover are with the School of Computing and Engineering, University of Huddersfield, HD1 3DH, UK. Zaharias D. Zaharis is with Aristotle University of Thessaloniki, GR-54124 Thessaloniki, Greece. Stavros Kalafatis is with Texas A&M University, USA, and Alben Mihovska is with Aalborg University, Denmark.

During its return journey, the ant reinforces the path with more pheromone, while ants on longer paths are still on their way to the food source. Other ants coming from the nest follow the shortest path due to its increased pheromone concentration. Consequently, the concentration of pheromone on the shortest path will dramatically increase compared to other paths. Finally, all ants will follow the shortest path leaving the pheromone on other paths to gradually evaporate. This swarm foraging behaviour has been imitated to solve many problems, and one of these problems is network routing [5], [6].

Each outgoing ant is represented by a small packet in routing theory, and therefore this packet is called *forward ant*. During its journey, this packet records information about the path it passes through to reach its destination. Then, the destination node (i) receives ants which used different paths to reach the node, (ii) calculates the *goodness* of every path according to a specific goodness function which is based on the path status, and (iii) deletes each forward ant and returns a respective backward packet called *backward ant* to the source node of the forward ant through the same path. This backward ant updates the selection probability (alternative term for pheromone) of each node it traverses according to the result of the goodness function [5], [6].

The goodness function is an expression of Quality of Service (QoS) and is defined according to the requirements of the traffic type over the network. In the traditional swarm routing, two QoS factors are taken into account. These are the delay along the path and the current congestion over that path. However, traffic generated due to different services of the network correspond to different values of QoS factors. There are traffic types where congestion is more critical than delay, while in other traffic types delay is more important than congestion. This paper presents a novel way of providing levels of QoS factors that are better matched with the requirements of each category of applications [6]. *Security* is introduced in the present study as an additional QoS factor. This paper is based on the first author's PhD thesis, [7].

II. RELATED WORK

Ant routing protocols have been an interesting research topic in the last two decades. Research papers in this area can be classified into two categories. Papers in the first category, such as [8], and [9], aim at improving ant routing techniques by accelerating the network learning phase in order to make

the results converge in a shorter period of time. On the other hand, papers in the second category try to achieve ant routing with better QoS [10]-[12]. This research category focuses on the optimality function of ants to compromise among different QoS parameters. Most of this research takes into account only two QoS parameters, which are the end-to-end delay and the path congestion. What was never taken into account in the QoS research so far is the *security* parameter.

In [13], we proposed a QoS-aware centralised routing protocol that takes into account the QoS requirements of different traffic types. This idea has been broadened in this paper by applying it to a distributed ant based routing algorithm. The traditional traffic-blind routing algorithm has been replaced by a novel security enabled traffic-aware routing algorithm which adopts the idea of classifying traffic into different classes according to their QoS requirements aiming to provide satisfactory levels of QoS factors to each class. This will of course increase the overall QoS offered by the network. In this paper, Oyster Optics Technology (OOT), [14], has been exploited to add the security as a crucial QoS factor that should be taken into account when private information is transmitted.

III. ANT ROUTING BACKGROUND

By imitating ant behavior, a distributed routing algorithm can be implemented for communication networks, [15]. According to this algorithm, some nodes are chosen to send small packets (forward ants) to random destinations in order to explore periodically the available paths towards these destinations. Each node i within a N -node network has its own routing table constructed from $N-1$ rows and M columns, where M is the number of neighbours of that node. Each row corresponds to a certain destination, while columns represent neighbours through different paths. Each entry in the routing table is addressed by the destination node d ($d=1, \dots, N-1$), the next neighbour node j ($j=1, \dots, M$), and the probability $\tau(i, j, d)$ to choose node j at the next hop when an ant moves from node i to node d . The value of τ varies between 0 and 1 and the sum of probabilities of each row is equal to 1. The forward ant records information about the path, such as the load of the different links which construct that path, the total number of hops of the path, etc. When this ant reaches its destination (i.e., destination node d), a backward ant is sent back along the same path to update the routing tables of the nodes visited by the forward ant. For each i th node reached by the backward ant, all entries (i, j, d) , $j=1, \dots, M$, of the node's routing table are updated. By assuming that node k was reached by the backward ant before node i , the update is applied by increasing the probability $\tau(i, k, d)$ and by decreasing all other probabilities $\tau(i, j, d)$, $j=1, \dots, k-1, k+1, \dots, M$, according to the following expressions:

$$\tau_{i,k,d}(t+1) = \frac{\tau_{i,k,d}(t) + \delta_r}{1 + \delta_r} \quad (1)$$

$$\tau_{i,j,d}(t+1) = \frac{\tau_{i,j,d}(t)}{1 + \delta_r}, \quad j = 1, \dots, M, \quad j \neq k \quad (2)$$

Where: δ_r is the reinforcement parameter which is extracted from the path information (collected by the forward ant) as follows:

$$\delta_r = a. \delta_p + b. \delta_c + c. \delta_s, \text{ with } a + b + c = 1 \quad (3)$$

where, δ_p and δ_c are reinforcement components extracted respectively from the length and business of the path, while δ_s is a new reinforcement component introduced in this paper that depends on the path security. Also, parameters a , b and c reflect the importance of each component in (3) and specify the type of application where traffic needs to be routed. The values of these parameters are specified in Table I. In addition, δ_p , δ_c and δ_s are extracted as given below:

$$\delta_p = e^{-\alpha \Delta p}, \quad \Delta p = p - p_{min} \quad (4)$$

$$\delta_c = e^{-\beta c} - 1 \quad (5)$$

$$\delta_s = e^{-\gamma s} - 1 \quad (6)$$

where: p is the actual path length, p_{min} is the length of the shortest path found by ants, c is the percentage of free capacity along the path, and s is the percentage of path security. Furthermore, α , β and γ are design parameters used to control the performance of the algorithm. No particular criteria exist for choosing the values of these parameters. Their optimal values depend on the topology of the network and the amount of the input traffic [6], [16]. In the present study, α , β and γ were assigned values equal to 0.8 since it was found by trial that these values achieve the best performance in terms of network convergence speed (speed of training) and solution accuracy. The percentages of path free capacity and path security can be respectively estimated according to the following expressions:

$$c = \frac{\text{used bandwidth}}{\text{total path capacity}} \quad (7)$$

$$s = \frac{\text{number of secure hops in the path}}{\text{total number of path hops}} \quad (8)$$

To track any abnormality, such as link or node failures, or the redistribution of population among the network nodes, ants are required to be repeatedly generated at fixed time intervals. Another issue is the gradual increase in the pheromone concentration on the former best path, which attracts ants to continue following that path even though another path has become more preferable. To avoid such a problem, the deposited pheromone evaporates after a period of time [17], [18]. To increase the exploration ability of ants and thus make them capable of observing any change in the network state, an exploration probability P is used [19]. Therefore, an ant found at node i may select the next node either at random with probability P or according to the routing table of node i with probability $1-P$. In our simulations, P was assigned the value of 0.12.

Two main advantages of such a routing technique can be observed: first, there is no dominant managing entity, which

monitors the status of the whole network, provides routing decisions and thus needing a huge amount of memory for large networks. On the contrary, nodes communicate with each other to exchange routing information and link states in a distributed manner. Second, the ants are periodically generated, enabling thus the network to discover any change in the routes and consequently to update the routing tables. It is important to note that the network needs first to be trained by sending a number of packets (forward ants) across different paths. During this stage, no data should be sent since nodes have no information about the locations and states of other nodes. Therefore, all the entries of the routing tables are initially set to zero. Furthermore, in cases of dynamic network changes, the network keeps on using the former routing tables until it is trained again to track the changes according to a set of predefined QoS requirements of the various traffic types.

IV. TRAFFIC TYPES

Traffic over the network is categorised according to the requirements regarding three orthogonal QoS factors. These factors are (i) the residual bandwidth of the path, (ii) the delivery speed, and (iii) security (see Table I). As mentioned before, goodness (G) is an expression of QoS and is defined according to the requirements of the traffic type over the network. Goodness can be defined inside the range $[0,1]$, where $G=1$ indicates an extremely good route and $G=0$ implies an extremely bad route. Each QoS factor has its own impact on the value of G of a certain path. The respective impacts a , b and c of residual bandwidth, delivery speed and security for a particular traffic type are denoted in this paper by the 3-tuple (a, b, c) , which represents the QoS requirements pattern. Different traffic types correspond to different values of QoS factors. However, the sum of impact of all the QoS factors on G is equal to 1.

Table I. Traffic Type Categories.

Red Traffic	Green Traffic	Blue Traffic
$(a, b, c) =$ (10%, 50%, 40%)	$(a, b, c) =$ (70%, 30%, 0%)	$(a, b, c) =$ (30%, 70%, 0%)
VoIP	Web Browsing	Interactive
Video	P2P File Sharing	Gaming
	Streaming Video	IPTV
	Miscellaneous	Streaming Audio
	Audio/Video up/downloads	

According to the QoS requirements pattern, each category of traffic is assigned a distinct color. Red color is assigned to traffic that needs to be routed with high speed, high security and any available bandwidth and thus is represented by the pattern (10%, 50%, 40%). Blue color is assigned to delay-sensitive traffic and thus is represented by the pattern (30%, 70%, 0%). Finally, green color is assigned to traffic that

considers bandwidth as the most important QoS factor and thus makes use of pattern (70%, 30%, 0%). Therefore, green traffic avoids congested paths and is required to be routed through paths with sufficient residual bandwidth. In this way, green traffic contributes to balancing off the load over the different network links and consequently improves network link utilisation.

Since goodness values are defined inside the range $[0,1]$, probability $\tau(i, j, d)$ can be used to express the goodness of every route. Therefore, G can be evaluated by using (1) and (2) and by taking into account the values of the 3-tuple (a, b, c) according to each particular application type.

V. NETWORK MODELLING

The US National Science Foundation (NSF) network with 14 nodes, shown in Fig. 1, is used here to demonstrate the feasibility of the proposed QoS-aware ant routing protocol. Each node of the network represents a whole Regional Area Network (RAN) with a presumed number of 4,000,000 users and 20Gbps link capacity. Seven out of twenty bidirectional links have been secured by replacing the input and output transceivers in their hosting nodes by secure Oyster Optics ones [14]. These secured links are coloured red in Fig. 1. The amount of traffic flow on the different links is estimated using the application specifications of usage statistics. To expedite the network training process, every node sends streams of ants to random destinations across the network. In fact, three types of ants (belonging to three ant colonies) are launched from each node. The first type deposits red-coloured pheromone, which is specialised in estimating the security of paths. The second type deposits green-coloured pheromone to calculate the amount of residual bandwidth of paths. In addition, blue-coloured pheromone is deposited by ants of the third type to determine the delay of paths. Ants are not allowed to visit a node which was previously visited. If there is no way to a destination except through a previously visited node, then the ant is eliminated. Ants are also eliminated if they exceed their preset lifetime, also known in the ant routing terminology as *time to live* (TTL).

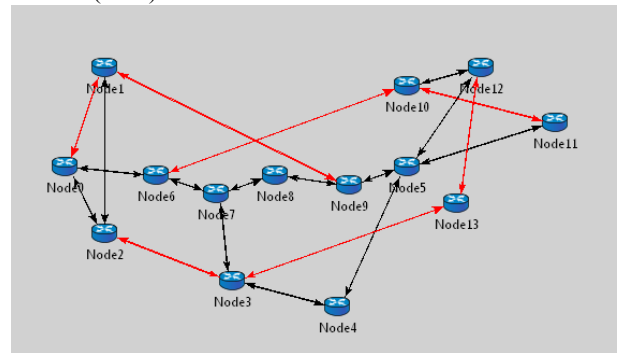


Fig. 1. NSF network.

VI. TRAFFIC FLOW MODELLING

Different types of traffic flow through the network as flow batches, where each batch is identified by three fields: the source address, the destination address and the type of

application that generated this traffic. The various network applications responsible for providing different network services have been classified into ten application types where any network application currently in use can be incorporated in one of these types. These types are: web browsing, streaming audio, streaming video, IPTV, VoIP, video communications, gaming, P2P file sharing, other miscellaneous audio up/downloads, and other miscellaneous video up/downloads. For the purpose of analysis each bidirectional link in the network will be split into two unidirectional links. Thus, the amount of traffic through the link in each direction can be determined.

VII. RESULTS AND DISCUSSION

Fig. 2 shows the distribution of blue traffic over different network links. Since traffic in such a category is delay-sensitive and therefore it tends to follow paths with the minimum number of hops, the load is concentrated on those links that construct the minimal hop paths to the destinations (such as links 7-8, 6-0, 3-4, 0-2 and 4-5 of Fig. 1), even though such links are highly loaded. In fact, routers will route this traffic mostly depending on the path shortness (in terms of the number of hops) and paying only a little attention to the congestions over these links with no regard to security, since the QoS requirements pattern of blue traffic is (30%, 70%, 0%). This is why some links in Fig. 2 are highly loaded whereas other links have low loads over them. On the other hand, Fig. 3 displays the load distribution of green traffic, which is considered as bandwidth-sensitive. Routers distribute the load over minimally congested paths to prevent any bandwidth insufficiency on their routes. As a consequence, a better load balance is provided and a better load link utilisation is achieved for such traffic. Green traffic in Fig. 3 seems to be distributed somewhat more evenly than blue traffic in Fig. 2. Moreover, Fig. 4 shows that red traffic tries to compromise between security and delivery speed by mostly using secure links and short paths. Therefore, the most congested links are secure links (coloured red in Fig. 3) which provide fast end-to-end delivery, such as links 0-1, 1-9, 3-13, 10-6 and 13-12. Although link 0-6 is not secure, it is highly congested because it forms a part of the shortest path to node 0 from most of the other network nodes.

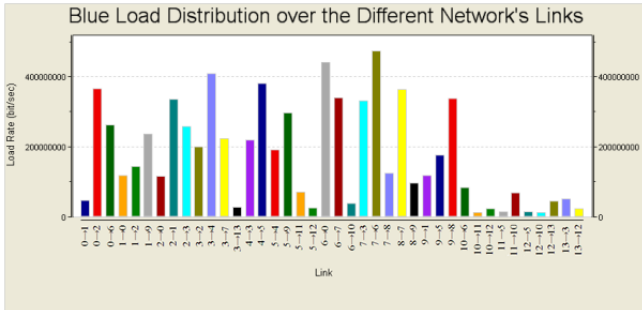


Fig. 2. Blue load distribution over different network links.

Fig. 5 shows the overall traffic over different network links. Since the dominant part of network traffic belongs to applications in the green load category, such as P2P file sharing and web browsing (i.e., applications causing the

heaviest traffic), the total load over the links will exhibit the distribution of green load to a larger extent.

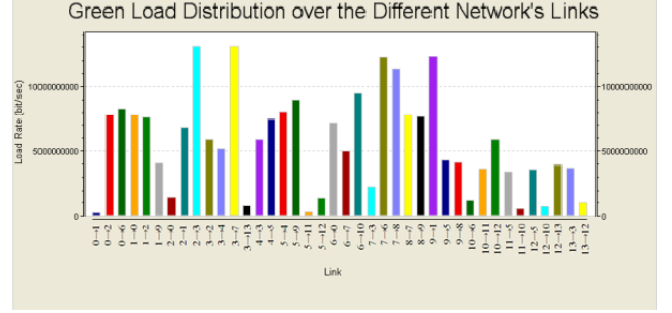


Fig. 3. Green load distribution over different network links.

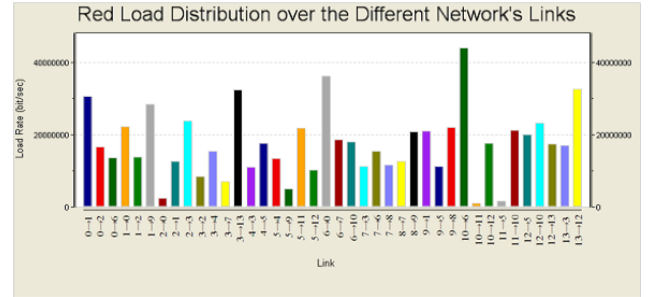


Fig. 4. Red load distribution over different network links.

This may be considered as a merit for our proposed scheme, since the overall network traffic is balanced to a certain extent. By supposing that an Optical-Electronic-Optical switch is required per each main router and by neglecting the very low propagation delays in optical fibres, the switching time and the queuing time required for each routing process make the number of hops the most significant factor that affects the overall end-to-end delay. Therefore, the delays in Fig. 6 are computed in terms of the number of hops. The applications in Figs. 6 and 7 are: web browsing, streaming audio, streaming video, IPTV, VoIP, video communications, interactive gaming, P2P file sharing, miscellaneous audio up/downloads, and miscellaneous video up/downloads, respectively.

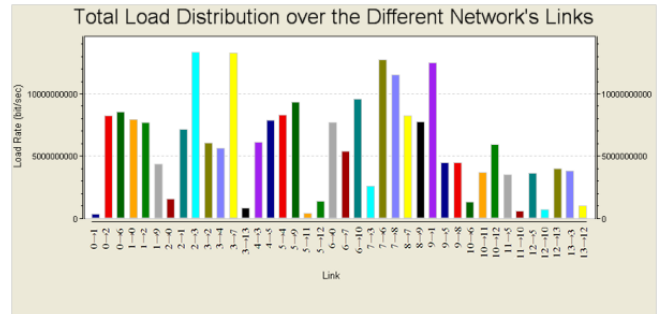


Fig. 5. Total load distribution over different network links.

The merit of the proposed routing protocol can be derived from Figs. 6 and 7. Fig. 6 shows that blue applications are served very quickly to minimise end-to-end delay. This result is in good agreement with the high impact value (70%) of delivery speed in blue traffic. Red traffic in Fig. 6 comes after the blue traffic in terms of the number of hops because it has a

delivery speed impact of 50%. Finally, green applications are not delay-sensitive and thus routers do not take into account the path shortness to serve such applications. On the other hand, Fig. 7 shows the end-to-end security of different traffic types. It is obvious that secure applications, such as VoIP and video communications, are given the higher importance in terms of security when delivered.

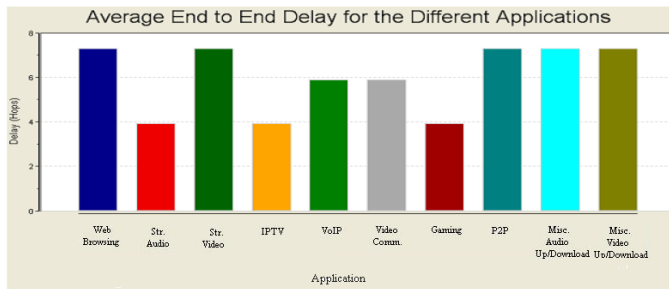


Fig. 6. Average end-to-end delay for different applications.

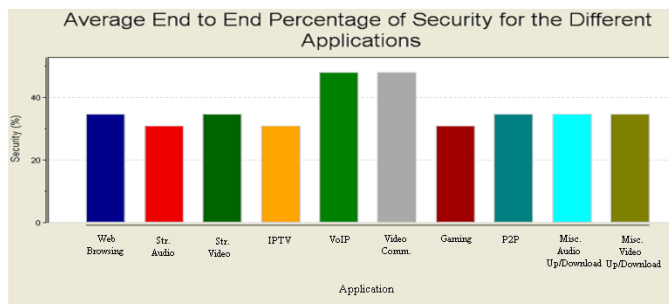


Fig. 7. Average end-to-end percentage of security for different applications.

VIII. CONCLUSIONS

According to the QoS requirements, applications were organised into three traffic types. Applications in the same type require the same levels of bandwidth, speed and security. Oyster Optics security technique has been used to secure seven bidirectional 40Gbps links out of 20 links aiming to provide secure transmission for private data over the network. For each traffic type, a respective type of ants was launched over the network links to test the suitability of the different available paths between each source-destination pair. Each one of the ant types deposits pheromone of a distinct colour (red, green or blue) specialised in estimating the level of bandwidth availability, speed and security of the path.

Red pheromone was used to test the path security, whereas green pheromone was used to calculate the amount of free bandwidth over the path. Furthermore, blue pheromone was utilised to calculate the delay through the path. Consequently, unlike the traditional ant routing protocol which considers only one pheromone type to accommodate for a single mix of QoS requirements for the entire network traffic, the proposed ant routing technique is capable of dealing in a precise manner with the QoS requirements of the network traffic.

Results clearly show the merits of our proposed routing protocol in satisfying the QoS requirements of traffic generated due to running different network applications. Better security was achieved in routing private information,

faster end-to-end communication was gained for speed-demanding applications, and congestions were avoided in cases of bandwidth consuming applications. Results show that the proposed technique outperforms conventional ant routing in terms of load balancing, end-to-end delay and security.

REFERENCES

- [1] Blum C., Merkle D. (Eds.), *Swarm Intelligence: Introduction and Applications*, Springer, Natural Computing Series, 2008.
- [2] Gupta A. K., Sadawarti H., Verma A. K., "MANET routing protocols based on Ant Colony Optimization", *Int. Journal of Modeling and Optimization*, Vol. 2, No. 1, February 2012.
- [3] Dorigo M., Birattari M., and Stützle T., "Ant Colony Optimization Artificial Ants as a Computational Intelligence Technique", *IEEE Computational Intelligence Magazine*, November 2006.
- [4] Varela G. N., Sinclair M. C., "Ant Colony Optimisation for Virtual-Wavelength-Path Routing and Wavelength Allocation", *Proceedings of the Congress on Evolutionary Computation*, 1999.
- [5] G. Di Caro and M. Dorigo "AntNet: Distributed Stigmergetic Control for Communications Networks", *Journal of Artificial Intelligence Research*, Volume 9, pp. 317-365, 1998.
- [6] Liu Z., "Ant Based Algorithm and Robustness Metric in Spare Capacity Allocation for Survivable Routing", PhD thesis, University of Canterbury, Christchurch, New Zealand.
- [7] Al-Momin M., "QoS - Aware content oriented flow routing in optical computer network", PhD thesis, Brunel University London, London, UK, 2013.
- [8] Yoo J. H., La R. J., and Makowski A. M., "Convergence of ant routing algorithms – Results for a simple parallel network and perspectives," Technical Report CSHCN 2003-44, Institute for Systems Research, University of Maryland, College Park, 2003.
- [9] Purkayastha P. and Baras J. S., "Convergence Results for Ant Routing Algorithms via Stochastic Approximation and Optimization", *Proceedings IEEE Conference on Decision and Control*, New Orleans, LA, USA, pp. 340-345, Dec. 12-14, 2007.
- [10] Yan X., Wang L. and Li L., "Ant Agent-Based Multicast Routing with QoS Guarantees", *1st International Symposium on Pervasive Computing and Applications*, Xinjiang, China, 2006.
- [11] Deepalakshmi P., Radhakrishnan S., "Ant Colony Based QoS Routing Algorithm For Mobile Ad Hoc Networks", *International Journal of Recent Trends in Engineering*, Vol. 1, No. 1, pp. 459-462, May 2009.
- [12] Attia R., Rizk R. and Mariee M., "A hybrid multi-path ant QoS routing algorithm for MANETs", *IFIP International Conference on Wireless and Optical Communications Networks WOCN '09*, Cairo, 2009.
- [13] Mohammed Al-Momin, John Cosmas, and Saman Amin "Adaptive Three-Layer Weighted Links Routing Protocol for Secure Transmission over Optical Networks", *WSEAS Transactions on communications*, Issue 8, Volume 11, pp. 287-298, August 2012.
- [14] US Patents, *Securing Fiber Optic Communications against Optical Tapping Methods*, Oyster Optics, Inc. 2003.
- [15] Martina Umlauf, "A concept for ant-routing with colored pheromones in wireless mesh networks," *IEEE conference on Intelligent Systems*, 2008.
- [16] S. Ngo, X. Jiang and S. Horiguchi, "An Ant-Based Approach for Dynamic RWA in Optical WDM Networks," *Photon. Network Commun.*, vol. 11, no. 1, pp. 39-48.
- [17] Kamali S. and Opatrny J., "A Position Based Ant Colony Routing Algorithm for Mobile Ad-hoc Networks", *Journal of Networks*, Vol. 3, No. 4, pp. 31-41, April 2008.
- [18] Roy B., Banik S., Dey P., Sanyal S., and Chaki N., "Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3, No. 1, pp. 10-14, January 2012.
- [19] Son Hong Ngo, Xiaohong Jiang and Susumu Horiguchi "An ant-based approach for dynamic RWA in optical WDM networks", *Photonic Network Communications*, Volume 11, No. 1, pp. 39-48, 2006.