

## A BAT algorithm based Enhancement of physical layer security in a Multi Domain-Elastic Optical Network

<sup>1</sup>Mr.J.Kumarnath,

Assistant Professor, Electronics and Communication Engineering, PSNACET

email:jkumarnath@gmail.com

<sup>2</sup>Dr.K.Batri,

Associate Professor, Electronics and Communication Engineering, PSNACET

email: krishnan.batri@gmail.com

**Abstract:** Now a day's optical networks are subjecting notable changes, imposed by the advocate growth of traffic due to multimedia services and by the increased uncertainty. Multidomain elastic optical networks (MD-EONs) improve network scalability, extend service coverage, and facilitate good interoperability to orchestrate administrative domains managed by different carrier. Other domain users can attack the physical layer of optical domain. In this work, the realistic scenario that does not treat all the inter domain light paths as malicious ones, and try to arrange the light paths routing and spectrum assignment (RSA) schemes with the help of the game theory to balance the security level of the domain and BAT algorithm for Routing. The proposed algorithm is evaluated with evolutionary algorithm called BAT to improve its effectiveness. The BAT algorithm is used for routing Wavelength assignment. We use bat algorithm for global optimization. Bat is based on echolocation character oh micro bats with varying pulse rate of emission and loudness.

**Keywords**—Game Theory;Bat Algorithm;physical layer Security;

### I. INTRODUCTION

Recently, due to the exponential increase of high-throughput and dynamic traffic demands in backbone networks, network operators' expectation on highly-efficient and flexible optical networking technologies is becoming more and more urgent. However, the traditional fixed-grid wavelength division multiplexing (WDM) networks only have limited flexibility in the optical layer[1].Under this circumstance, the elastic optical networks (EONs), which can

allocate optical spectrum in a flexible-grid way and thus achieve agile bandwidth management in the optical layer, have attracted intensive interests recently [1]. Specifically, the bandwidth-variable transponders (BV-Ts) and bandwidth-variable wavelength selective switches (BV-WSS') in EONs operate on narrow-band frequency slots (FS') at 12.5 GHz or even less and groom them adaptively to realize both sub-wavelength and super-channel transmissions [2], [3].Meanwhile, except for their appealing potential, EONs are still facing a few challenges. An important one of them is how to achieve efficient service provisioning in multi-domain EONs (MD-EONs). Since a backbone network usually covers a relatively large geographical area and can be managed by multiple network operators, the multi-domain scenario of EONs has to be addressed properly. Previously, people have considered the cross-domain orchestration in MD-EONs and proposed a few network architectures in [4]–[5].The intra domain virtual topology (ID-VT) helps to protect the domain privacy and improves the physical-layer security within each domain. However, this is far from enough as malicious users can still launch physical-layer attacks from outside of the domain and put the intra-domain resources/requests in danger. In optical networks, optical components, e.g., fibers, amplifiers and cross-connects (OXC's), can be vulnerable to various physical-layer issues [7]. When multiple light-paths share optical components, they can affect one another's performance due to these issues and a physical-layer attack can be launched by a malicious user therein [8]. The protocol designing will also play a key role to protect against the physical and optical layer security and hence understanding in this area has to be made before providing a solution to RSA [9], This work considered optically translucent domains and proposed several attack-aware service provisioning schemes to enhance the physical-layer security in MD-EONs cost-efficiently. More specifically, tried to minimize the sharing of optical components between intra- and inter domain light-paths .Even though the schemes which is proposed in [9] are apparently more cost-efficient than the

idea of building opaque domains, their efficiencies can still be improved. The schemes were developed based on the consideration that treats every inter-domain light-path as a malicious one. Note that the basic premise for an MD-EON to operate normally is that most of its users should be harmless and trusted ones since this ensures the mutual trust among the domains. Therefore, it would be better if the domain manager could intelligently categorize inter-domain light-paths into harmless and malicious ones based on the network status and then apply the corresponding routing and wavelength assignment (RSA) schemes on them. This actually motivates us to seek help from the game theory. Specifically, if consider the domain manager and the users from other domains as the players in an attacker/defender game [10], it can leverage the Bayesian game to further improve the performance of attack-aware service provisioning. In this work, the problem of attack-aware service provisioning in one domain of an MD-EON, which considers both inter- and intra-domain light-paths, i.e., using a network model has been addressed that is similar as that in [9]. Nevertheless, we consider a more realistic scenario that does not treat all the inter domain light-paths as malicious ones, and try to arrange the light-paths RSA schemes with the help of game theory to balance the spectrum utilization and security-level of the domain better. The importance of parametric analysis has been analyzed in-depth in the dynamic optical network which can be useful in understanding the elastic optical network with respect to parametric approach [6].

## II. EXISTING METHODOLOGY

To determine how expert's composition affect system wide network protection, we analyze 3 distinct N -players security games which has k selfish experts ( $0 \leq k \leq N$ ) and  $N - k$  players. We assume that the experts understand the dynamics of each game and choose strategies to maximize their own expected payoffs, while the N-k players choose whether to protect based on a simple cost-benefit analysis comparing protection costs to their individual expected loss in the event of protection failure. For expert agents, we distinguish between knowledge conditions about other players' expected losses. In a complete information environment, each expert has full knowledge of the expected losses of all players resulting from network protection failure. In an incomplete information environment, each expert knows her own expected loss in the event of protection failure, but only knows the distribution on these expected losses for all players (the uniform distribution). Finally, to illustrate the drawbacks of selfish equilibria more generally, we compute the social optimum strategy for each game. To facilitate comparisons with the scenario involving selfish experts, we characterize the social optimum from the individual perspective of N cooperative agents.

### A. Game Assisted Routing Spectrum Assignment

EON is considered a promising method to improve the spectral efficiency of optical networks. One of the most important planning challenges of elastic optical networks is the problem of NP-hard routing and spectrum assignment. Here, an EON is the optical network that can adapt the

channel bandwidth, data rate, and transmission format for each traffic demand in order to offer maximum throughput. In elastic filter less networks, the presence of unfiltered signals resulting from the drop-and-continue node architecture must be considered as an additional constraint in the RSA problem. In this work, the RSA problem in elastic filter less networks is formulated by using an integer linear program to obtain optimal solutions for small networks. Due to the problem complexity, two efficient RSA heuristics are also proposed to achieve suboptimal solutions for larger networks in reasonable time. Simulation results show that bandwidth is saved significantly in elastic filter less networks compared with the fixed-grid filter less solutions. The proposed approach is further tested in multi-period traffic scenarios and combined with periodical spectrum defragmentation, leading to additional improvement in spectrum utilization of elastic filter less optical networks.

### B. Maintaining the Integrity of the Specifications

In this section, we shall discuss how to solve the Bayesian game above to provision an inter-domain request from.

#### BNE

As explained in the previous section, the players (i.e., user and domain manager) need to find their mutual best responses to maximize their utilities. This actually can be achieved by analyzing the Nash equilibrium of the Bayesian game formulated in Section IV, since a BNE represents a strategy profile in which neither  $q-m$  nor  $qm$  can increase its utility by adjusting the strategy unilaterally [10]. Note that, even when  $q-m$  is malicious, it will report its ingress node honestly after each game, since changing its ingress node unilaterally would make  $q-m$  deviate from its best response to the strategy of  $qm$  and hence result in utility loss.

**Theorem 1:** The Bayesian game formulated in has at least one mixed-strategy BNE. *Proof:* In the game, there are two players, i.e.,  $q-m$  and  $qm$ . We can see that each player only has two pure strategies. Hence, the game is a finite one. As every finite Bayesian game has at least one mixed-strategy BNE [10], we prove the theorem. In the following, we derive the general form of the BNE in the game and formulate a nonlinear programming model (NLP) to obtain it.

#### Parameters:

- 1)  $\lambda$ : the priori probability that  $qm$  believes that  $q-m$  is malicious.
- 2)  $\Phi_m a$ : the utility matrix of  $qm$  under all the pure strategy pairs, if  $q-m$  is malicious.
- 3)  $\Phi_{-} a m$ : the utility matrix of  $q-m$  under all the pure strategy pairs, if  $q-m$  is malicious.
- 4)  $\Phi_m u$ : the utility matrix of  $qm$  under all the pure strategy pairs, if  $q-m$  is harmless.
- 5)  $\Phi_{-} u m$ : the utility matrix of  $q-m$  under all the pure strategy pairs, if  $q-m$  is harmless.

6)  $L-m$ : the value of the smallest element in  $\Phi^- a m$  for a malicious  $q-m$  or in  $\Phi^- u m$  for a harmless  $q-m$ .

7)  $U-m$ : the value of the largest element in  $\Phi^- a m$  for a malicious  $q-m$  or in  $\Phi^- u m$  for a harmless  $q-m$ .

8)  $Lm$ : the value of the smallest element in  $\Phi m a$  and  $\Phi m u$ .

9)  $Um$ : the value of the largest element in  $\Phi m a$  and  $\Phi m u$ .

Variables:

1)  $sm$ : the mixed-strategy vector ( $sm\ 1, sm\ 2$ ) T that indicates how  $qm$  formulates its strategy. Specifically,  $sm\ 1$  and  $sm\ 2$  are the probabilities that  $qm$  chooses to use MDAa-RSA and KSP-FF, respectively.

2)  $sa$ : the mixed-strategy vector ( $sa\ 1, sa\ 2$ ) T that indicates how a malicious  $q-m$  formulates its strategy. Specifically,  $sa\ 1$  and  $sa\ 2$  are the probabilities that  $q-m$  chooses to access  $Gm$  from  $vm\ b, 1$  and  $vb, m2$ , respectively.

3)  $su$ : the mixed-strategy vector ( $su\ 1, su\ 2$ ) T that indicates how a harmless  $q-m$  formulates its strategy. The definitions of  $su\ 1$  and  $su\ 2$  are similar as those of  $sa\ 1$  and  $sa\ 2$ .

4)  $\Psi m$ : the expected utility of  $qm$ .

5)  $\Psi-m$ : the expected utility of  $q-m$ .

6)  $Zm$ : the best response functions of  $qm$ .

7)  $Za$ : the best response functions of a malicious  $q-m$ .

8)  $Zu$ : the best response functions of a harmless  $q-m$ .

9)  $\Gamma m$ : the optimal utility of  $qm$ .

10)  $\Gamma-m$ : the optimal utility of  $q-m$ .

Objectives: The objective of  $q-m$  is

$$\text{Maximize } \Psi^{-m} = \begin{cases} (s^a)^T \Phi_a^{-m} s^m, & \text{malicious} \\ (s^u)^T \Phi_u^{-m} s^m, & \text{harmless} \end{cases}$$

Where the expression of  $\Psi^{-m}$  depends on the actual type of  $q-m$  since different types could lead to different decisions, i.e.,  $sa$  might not be the same as  $su$ .

$$\text{Maximize } \Psi^m = \lambda (s^a)^T \Phi_a^m s^m + (1 - \lambda) (s^u)^T \Phi_u^m s^m$$

Where the expected utility contains two parts, each of which is weighted by the corresponding prior probability. The first part is for when  $qm$  believes that  $q-m$  is malicious, while the second part is the other way around. With the objectives in Eqs. (2)–(3), and we can get the best response functions as

$$\begin{cases} z^a(s^m) = \arg \max_{s^a} \Psi^{-m}, & \text{malicious} \\ z^u(s^m) = \arg \max_{s^u} \Psi^{-m}, & \text{harmless} \end{cases}$$

$$z^a(s^a, s^u) = \arg \max_{s^m} \Psi^m.$$

Specifically, given a mixed-strategy of  $qm$  (i.e.,  $sm$ ),  $q-m$  uses Eq. (4) to obtain its best response (i.e.,  $za$  or  $zu$ ). Similarly,  $qm$  leverages Eq. (5) to get its best response  $zm$ . Then, by definition, BNE is expressed as  $(za, zu, zm)$ , if Eqs. (4) (5) can be satisfied simultaneously. In order to figure out  $(za, zu, zm)$ , we adopt the method in [25], which reduces the problem of finding a BNE to solving the optimization of the NLP below.

$$\text{Minimize } f = |\Gamma^m - \Psi^m| + |\Gamma^{-m} - \Psi^{-m}|$$

Where  $f$  is the summation of two items that denote the gaps between the optimal utility and the expected utility of  $qm$  and  $q-m$ . By minimizing  $f$  to 0, we obtain a BNE.

Constraints:

$$\begin{cases} \Phi_a^{-m} s^m \leq (\Gamma^{-m}, \Gamma^{-m})^T, & \text{malicious,} \\ \Phi_u^{-m} s^m \leq (\Gamma^{-m}, \Gamma^{-m})^T, & \text{harmless,} \end{cases}$$

$$\text{Maximize } \Psi^m = \lambda (s^a)^T \Phi_a^m s^m + (1 - \lambda) (s^u)^T \Phi_u^m s^m \leq (\Gamma^m, \Gamma^m).$$

Eq. (7)–(8) ensures that none of the players can increase its utility by changing its own strategy.

$$\Gamma^{-m} \in [L^{-m}, U^{-m}],$$

$$\Gamma^m \in [L^m, U^m],$$

Eqs. (9)–(10) ensure that  $\Gamma^{-m}$  and  $\Gamma^m$  are within right ranges

$$\sum_{i=1}^2 s_i^a = \sum_{i=1}^2 s_i^u = \sum_{i=1}^2 s_i^m = 1$$

$$s_i^m, s_i^a, s_i^u \in [0, 1] \forall i = 1, 2.$$

Eqs. (11)–(12) ensure regularity and nonnegative constraints. We then use the sequential quadratic programming based quasi-Newton (SQP-qN) method [26] to solve the NLP. Note that the performance of this method would be affected by the initial searching point, which means that we will find the BNE that is the closest to the initial searching point [26]. To handle this issue, we design Algorithm 1. Lines 1–2 are for the initialization. Here, by saying a “pure strategy profile”, we mean that the elements in  $sa$ ,  $su$ , and  $sm$  can only be 0 or 1, i.e.,  $qm$  or  $q-m$  selects one of its strategies deterministically. The for-loop that covers Lines 3–8 uses all the pure strategy profiles as the initial searching points to solve the NLP for BNEs. Lines 4–5 calculate an initial searching point with a pure strategy profile and input it to the NLP. The NLP is solved in Line 6 with SQP-qN for a BNE. Line 7 stores the obtained BNE. With Lines 9–13, we try to get the best BNE as the one with a pure strategy profile, and only when no pure strategy BNE exists, we select a mixed-strategy one. Since either  $qm$  or  $q-m$  only has two pure strategies, the search space defined by  $|S| =$

8 is very small and thus the complexity of Algorithm 1 only depends on that of using SQP-qN to solve the NLP, which has been verified as time-efficient in [25].

### C. Game-Assisted Service Provisioning

In addition to those in *Rex*, we also need to provision the light-paths in *Rin* and *Rlv* in *Gm*. Algorithm 2 shows the procedure of our proposed game-assisted service provisioning. Lines 1–2 are for the initialization. The for-loop that covers Lines 3–19 is to provision all the requests. Specifically, for various types of light-paths, we adopt different RSA algorithms, i.e., MDAA-RSA for *Rin*, KSP-FF for *Rlv*, and the Ga-RSA for *Rex*. In Lines 13–19, we try to provision each light-path using the obtained RSA scheme. The complexity of MDAA-RSA is  $O_1 = O(K \cdot |Vbm| \cdot 2 \cdot (|R| + |Vm| \cdot |Em| + F \cdot (|Vm| + |Em|)))$  according to [9]. Hence, if we denote the complexity of Algorithm 1 as  $O_2$ , the complexity of Algorithm 2 would be  $|R| \cdot \max(O_1, O_2)$ .

## III. PROPOSED METHODOLOGY

Now a day's meta-heuristic algorithms are becoming more powerful methods for solving many high level optimization problems [3-7, 11]. The wide majority of heuristic and meta heuristic algorithms have been derived for global optimization bat algorithm is one of the meta heuristic algorithm. Bat was a superlative algorithm since it uses the echolocation character of micro bats, with varying pulse rates of emission and loudness. Xin-She Yang who developed the bat algorithm in 2010.

From the behavior of biological systems and/or physical systems in nature. For example, PSO was developed based on the swarm behaviour of fish and birds [7, 8], while simulated annealing was based on the annealing process of metals [9]. New algorithms such as harmony search and firefly are also emerging.

Each of these algorithms has certain advantages and disadvantages. For example, simulating annealing can almost guarantee to find the optimal solution if the cooling process is slow enough and the simulation is running long enough; however, the fine adjustment in parameters does affect the convergence rate of the optimization process. A natural question is whether it is possible to combine major advantages of these algorithms and try to develop a potentially better algorithm. This work is such an attempt to address this issue. In work is intended to propose a new Meta heuristic method, namely, the Bat Algorithm (BA), based on the echolocation character of bats. By using echolocation, the micro bats can find the prey and differentiate various types of insects even in the darkness. The first analyze is to formulate the bat algorithm by idealizing the echolocation behaviour of bats. The practical work has been framed and simulated and then the comparison has been made other existing algorithms. Finally, we will discuss some implications for further studies. Caustics of Echolocation Though each pulse only lasts a few thousandths of a second (up to about 8 to 10 ms), however, it has a fixed frequency which is usually in the region to 150 kHz from 25 kHz. The typical range of frequencies for most bat species are in the region between 25 kHz and 100 kHz,

though some species can emit higher frequencies up to 150 kHz. Each and every ultrasonic fragment may last typically 5 to 20 ms, and micro bats emit about 10 to 20 such sound bursts every second. When hunting for prey, the rate of pulse emission can be sped up to about 200 pulses per second when they fly near their prey. Such short duration sound crack implies the fantastic ability of the signal processing power of bats. The existing results shows the integration time of the bat ear is typically about 300 to 400  $\mu$ s. As the speed of sound in air is typically 340 m/s, the wavelength of the ultrasonic sound bursts with a constant frequency is given by

$$\lambda = v/f$$

Which is in the range of 2mm to 14mm for the typical frequency range from 25 kHz to 150 kHz? Such wavelengths are in the same order of their prey sizes. The emitted pulse could be as loud as 110 dB, and, fortunately as they are in the ultrasonic region it is harmless. The loudness also varies from the loudest when searching for prey and to a quieter base when homing towards the prey. The travelling range of such short pulses is typically a few meters, depending on the actual frequencies [12]. Micro bats can manage to avoid obstacles as small as thin human hairs.

The target's distance and orientation can be detected and it identifies the prey type and even the moving speed of the prey such as small insects. Indeed, studies suggested that bats seem to be able to discriminate targets by the variations of the Doppler Effect induced by the wing-flutter rates of the target insects [1]. Most of bats have very sensitive smell and also by known fact bats have very good eyesight. In reality, they will use all the senses as a combination to maximize the efficient detection of prey and smooth navigation. However, here we are concentrated in the echolocation and the related behavior. Such echolocation behaviour of micro bats can be formulated in such a way that it can be associated with the objective function to be optimized, and this makes it possible to formulate new optimization algorithms. We will first outline of the Bat Algorithm's (BA) basic formation and then discuss the implementation and comparison in detail. If we idealize some of the echolocation characteristics of micro bats, we can develop various bat-inspired algorithms or bat algorithms. The following idealized rules are used for simplification:

1. To sense distance and to know the difference between prey and background barriers they use echolocation technique.

2. With varying wavelength  $\lambda$  and loudness  $A_0$  and with velocity  $v_i$  at position  $x_i$  with a fixed frequency  $f_{min}$  to search their prey. By adjusting the wavelength and rate of pulse emission automatically where  $r \in [0, 1]$ , and depending on the proximity of their target.

Objective function  $f(x)$ ,  $X = (x_1 \dots x_d)^T$

Initialize the bat population  $x_i$  ( $i=1, 2, \dots, n$ ) and  $v_i$

Define the pulse frequency  $f_i$  at  $x_i$ .

Initialize the pulse rate  $r_i$  and loudness  $A_i$ .

While ( $t < \max$  no of iteration)

Generate new solutions by adjusting frequency.  
 And updating velocity and solutions.  
 If (rand<ri)  
     Select a solution among the best solutions.  
     Generate a local solution in the best solution.  
 End if  
     Fly randomly and generate a new solution.  
 If (rand<Ai&&f(x1)<f(x2))  
     New solutions are to be accepted.  
     Reduce Ai and increase ri.  
 End if  
     Rank the bats and find current best solution.  
 End while  
 Process the result and visualize it.

$$f_i = f_{min} + (f_{max} - f_{min})\beta,$$

$$V_i^t = V_i^{t-1} + (X_i^t - X_*) f_i$$

$$X_i^t = X_i^{t-1} + V_i^t$$

Where  $\beta \in [0, 1]$  is a random vector drawn from a uniform distribution. Here  $x^*$  is the current global best location (solution) which is located after comparing all the solutions among all the  $n$  bats. As the product  $\lambda f_i$  is the velocity increment, we can use either  $f_i$  (or  $\lambda f_i$ ) to adjust the velocity change while fixing the other factor  $\lambda f_i$  (or  $f_i$ ), depending on the type of the problem of interest. In our implementation, we will use  $f_{min} = 0$  and  $f_{max} = 100$ , depending the domain size of the problem of interest. Initially, each bat is randomly assigned a frequency which is drawn uniformly from  $[f_{min}, f_{max}]$ . For the local search part, once a solution is selected among the current best solutions, a new solution for each bat is generated locally using random walk

Where  $q \in [-1, 1]$  is a random number, while  $A_t = \langle A_i \rangle$  is the average loudness of all the bats at this time step. The update of the velocities and positions of bats have some similarity to the procedure in the standard particle swarm optimization [7] as  $f_i$  essentially controls the pace and range of the movement of the swarming particles. To a degree, BA can be considered as a balanced combination of the standard particle swarm optimization and the intensive local search controlled by the loudness and pulse rate. Furthermore, the loudness  $A_i$  and the rate  $r_i$  of pulse emission have to be updated accordingly as the iterations proceed. As the loudness usually decreases once a bat has found its prey, while the rate of pulse emission increases, the loudness can be chosen as any value of convenience. For example, we can use  $A_0 = 100$  and  $A_{min} = 1$ . For simplicity, we can also use  $A_0 = 1$  and  $A_{min} = 0$ , assuming  $A_{min} = 0$  means that a bat has just found the prey and temporarily stop emitting any sound. Now we have

$$A_i^{t+1} = \alpha A_i^t, \quad r_i^{t+1} = r_i^0 [1 - \exp(-\gamma t)]$$

Where  $\alpha$  and  $\gamma$  are constants. In fact,  $\alpha$  is similar to the cooling factor of a cooling schedule in the simulated annealing [9]. For any  $0 < \alpha < 1$  and  $\gamma > 0$ , we have

$$A_i^t \rightarrow 0, \quad r_i^t \rightarrow r_i^0, \text{ as } t \rightarrow \infty$$

In the simplicity case, we can use  $\alpha = \gamma$ , and we have used  $\alpha = \gamma = 0.9$  in our simulations. The choice of parameters requires some experimenting. Initially, each bat should have different values of loudness and pulse emission rate, and this can be achieved by randomization. For example, the initial loudness  $A_0$  can typically be  $[1, 2]$ , while the initial emission rate  $r_0$  can be around zero, or any value  $r_i \in [0, 1]$  if using (6). Their loudness and emission rates will be updated only if the new solutions are improved, which means that these bats are moving towards the optimal solution.

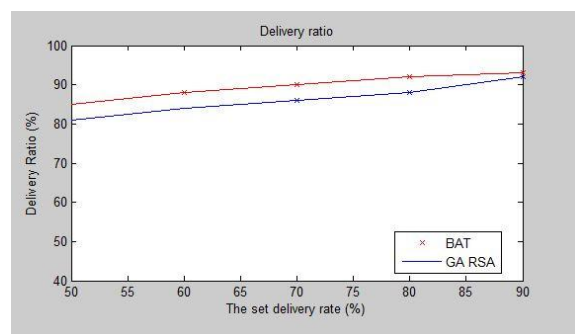


Fig.1 delivery ratio.

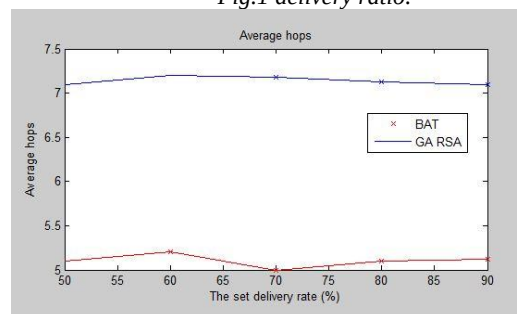


Fig.2 Average hops.

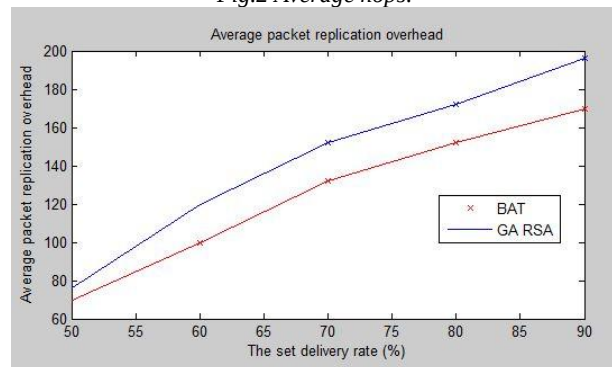


Fig.3 Average packet replication overhead.

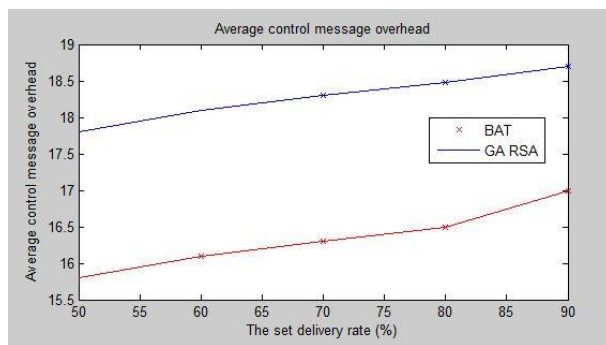


Fig. 4 Average control message overhead.

## Conclusion

The BAT algorithm thus proves to be an effective addition for the Game assisted RSA selects the superior path with proper maximized parametric solution. Though various algorithm has been proposed early with the genetic as well as bio inspired approach, The proposed algorithm consider the novel characteristic of the BAT, which is proved to produce better spectrum assignment, increase in the delivery ratio and hop count reduction. With respect to the security concepts, this work considers game theory approach to provide satisfactory solution to the security issues. The future work would be to improve the efficiency by adding more secure light paths i.e the game theory can be modified in a better way in the for coming work.

## References

- [1] P. Lu et al., "Highly-efficient data migration and backup for big data applications in elastic optical inter-datacenter networks," *IEEE Netw.*, vol. 29, pp. 36–42, Sept./Oct. 2015.
- [2] R. Mao et al., "Overcoming the challenge of variety: Big Data abstraction, the next evolution of data management for AAL communication systems," *IEEE Commun. Mag.*, vol. 53, pp. 42–47, Jan. 2015.
- [3] Z. Zhu et al., "Demonstration of cooperative resource allocation in an OpenFlow-controlled multidomain and multinational SD-EON testbed," *J. Lightw. Technol.*, vol. 33, pp. 1508–1514, Apr. 2015.
- [4] "Control and management of flexi-grid optical networks with an integrated stateful R. Casellas et al., path computation element and OpenFlow controller," *J. Opt. Commun. Netw.*, vol. 5, pp. A57–A65, Oct. 2014.
- [5] S. Yoo, "Multi-domain cognitive optical software defined networks with market-driven brokers," *Proc. of ECOC 2014*, pp. 1–3, Sept. 2014.
- [6] J. Kumamath et al., "A Novel parametric Analysis of the performance dynamicity of Optical Network" *Advances in Natural and Applied sciences*, vol. 11, pp. 166–173, July 2018
- [7] M. Medard, D. Marquis, R. Barry, and S. Finn, "Security issues in all-optical networks," *IEEE Netw.*, vol. 11, pp. 42–48, May 2017.
- [8] K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection prevention," in *Proc. of MILCOM 2004*, pp. 711–716, Oct. 2004. [9] R. Rejeb, M. Leeson, and R. Green, "Fault and attack management in all-optical networks," *IEEE Commun. Mag.*, vol. 44, pp. 79–86, Nov. 2016
- [9] J. Kumamath and J. Vetrimanikumar, "A Survey Of Routing Protocols In Optical Network," *International Journal of Engineering & Science Research*, vol. 3, pp. 2266–2272, Jan 2013.
- [10] Y. Du, F. Xue, and S. Yoo, "Security enhancement of SPECTS O-CDMA through concealment against upstream DPSK eavesdropping," *J. Lightw. Technol.*, vol. 25, pp. 2799–2806, Sept. 2007.
- [11] M. Fok, Z. Wang, Y. Deng, and P. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 725–736, Sept. 2011.
- [12] A. Lazzez, "All-optical networks: Security issues analysis," *J. Opt. Commun. Netw.*, vol. 7, pp. 136–145, Mar. 2015.
- [13] N. Skorin-Kapov and M. Furdek, "Limiting the propagation of intra-channel crosstalk attacks in optical networks through wavelength assignment," in *Proc. of OFC 2009*, pp. 1–3, Mar. 2012.
- [14] M. Furdek, N. Skorin-Kapov, and M. Grbac, "Attack-aware wavelength assignment for localization of in-band crosstalk attack propagation," *J. Opt. Commun. Netw.*, vol. 2, pp. 1000–1009, Nov. 2016.
- [15] N. Skorin-Kapov, J. Chen, and L. Wosinska, "A new approach to optical networks security: Attack-aware routing and wavelength assignment," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 750–760, Jun. 2017.
- [16] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proc. of ICTON 2014*, pp. 1–4, Jul. 2014.
- [17] K. Manousakis and G. Ellinas, "Attack-aware planning of transparent optical networks," *Opt. Switch. Netw.*, vol. 19, pp. 97–109, Jan. 2016.
- [18] W. Shi, Z. Zhu, M. Zhang, and N. Ansari, "On the effect of bandwidth fragmentation on blocking probability in elastic optical networks," *IEEE Trans. Commun.*, vol. 61, pp. 2970–2978, Jul. 2013.
- [19] M. Zhang, C. You, H. Jiang, and Z. Zhu, "Dynamic and adaptive bandwidth defragmentation in spectrum-sliced elastic optical networks with time-varying traffic," *J. Lightw. Technol.*, vol. 32, pp. 1014–1023, Mar. 2014.
- [20] Y. Wang, X. Cao, and Y. Pan, "A study of the routing and spectrum allocation in spectrum-sliced elastic optical path networks," in *Proc. of INFOCOM 2011*, pp. 1503–1511, Apr. 2016.
- [21] K. Christodouloupoulos, I. Tomkos, and E. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical networks," *J. Lightw. Technol.*, vol. 29, pp. 1354–1366, May 2011.
- [22] L. Gong, X. Zhou, W. Lu, and Z. Zhu, "A two-population based evolutionary approach for optimizing routing, modulation and spectrum assignments (RMSA) in O-OFDM networks," *IEEE Commun. Lett.*, vol. 16, pp. 1520–1523, Sept. 2012.
- [23] X. Zhou, W. Lu, L. Gong, and Z. Zhu, "Dynamic RMSA in elastic optical networks with an adaptive genetic algorithm," in *Proc. of GLOBECOM 2012*, pp. 2912–2917, Dec. 2012.
- [24] W. Lu and Z. Zhu, "Dynamic service provisioning of advance reservation requests in elastic optical networks," *J. Lightw. Technol.*, vol. 31, pp. 1621–1627, May 2013.
- [25] L. Gong, W. Zhao, Y. Wen, and Z. Zhu, "Dynamic transparent virtual network embedding over elastic optical infrastructures," in *Proc. of ICC 2013*, pp. 3466–3470, Jun. 2013. [26] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, "Dynamic service provisioning in elastic optical networks with hybrid single-/multi-path routing," *J. Lightw. Technol.*, vol. 31, pp. 15–22, Jan. 2013. [27] Y. Yin, M. Zhang, Z. Zhu, and S. Yoo, "Fragmentation-aware routing, modulation and spectrum assignment algorithms in elastic optical networks," in *Proc. of OFC 2013*, pp. 1–3, Mar. 2013. [28] S. Ma et al., "Demonstration of online spectrum defragmentation enabled by OpenFlow in software-defined elastic optical networks," in *Proc. of OFC 2014*, pp. 1–3, Mar. 2014.
- [26] C. Chen et al., "Demonstrations of efficient online spectrum defragmentation in software-defined elastic optical networks," *J. Lightw. Technol.*, vol. 32, pp. 4701–4711, Dec. 2014.
- [27] N. Skorin-Kapov, M. Furdek, R. Aparicio Pardo, and P. Pavon Marino, "Wavelength assignment for in-band crosstalk attacks in optical network- s: ILP formulations and heuristic algorithms," *Eur. J. Oper. Res.*, vol. 222, pp. 418–429, Nov. 2012. [31] Z. Zhu et al., "Jitter and amplitude noise accumulations in cascaded all-optical regenerators," *J. Lightw. Technol.*, vol. 26, pp. 1640–1652, Jun. 2008.
- [28] Energy-efficient translucent optical transport networks with mixed regenerator placement," *J. Lightw. Technol.*, vol. 30, pp. 3147– 3156, Oct. 2012



