Information Sciences 340–341 (2016) 27–40

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Analysis of Ant Colony Optimization-based routing in optical networks in the presence of byzantine failures

Gustavo Sousa Pavani*, Anderson de França Queiroz, Jerônimo Cordoni Pellegrini

Centro de Matemática, Computação e Cognição – Federal University of ABC (UFABC) Rua Abolição, s/n. Santo André–SP CEP: 09210-180, Brazil

ARTICLE INFO

Article history:
Received 11 June 2015
Revised 22 October 2015
Accepted 1 January 2016
Available online 11 January 2016

Keywords:
Routing and wavelength assignment
Ant Colony Optimization
Control plane security
Byzantine failures

ABSTRACT

Byzantine failures during the execution of the routing algorithm may degrade or disrupt the normal operation of the network. Ant Colony Optimization (ACO)-based routing algorithms are especially vulnerable to those failures. In this work, we propose the use of crankback re-routing extensions associated to the ACO algorithm in wavelength-routed optical networks to deal with byzantine failures. We investigate three different byzantine failure scenarios: misdirection of forward ants, dropping of forward ants and dropping of backward ants. Those failures affect the routing information of the network, but they are very hard to detect and cannot be fully addressed by integrity and authentication techniques. Without any need for a byzantine failure detection mechanism, simulations have demonstrated that the proposed approach is effective in mitigating the impact on the blocking probability due to network nodes exhibiting a byzantine behavior.

1. Introduction

Ant Colony Optimization (ACO) algorithms have been successfully applied in a great number of difficult routing problems in communication networks [6]. Inspired by the foraging behavior of natural ants, these algorithms are characterized by a type of indirect communication that relies on the environment to stimulate subsequent actions, which is called stigmergy [8].

Stigmergy is a key component of ACO algorithms, being responsible by the emergent and self-organizing behavior of the ant colony. Indeed, an artificial ant lays down information on the visited nodes about the performance of its traversed path along the network, in the form of artificial pheromone level. The deposited pheromone levels can be locally sensed by other wandering ants, which can reinforce a previously found good route.

ACO algorithms can be used in optical networks, being straightforwardly incorporated in their control plane as the replacement of the routing protocol while maintaining the signaling protocol unaltered [16]. The process of finding good routes in the network is fully distributed and based on local information, being resilient to link or node failures [14–16].

* Corresponding author. Tel: +55 1149968334.
E-mail addresses: gustavo.pavani@ufabc.edu.br, gupavani@gmail.com (G.S. Pavani), contato@andersonq.eti.br (A.d.F. Queiroz), jeronimo.pellegrini@ufabc.edu.br (J.C. Pellegrini).

http://dx.doi.org/10.1016/j.ins.2016.01.008
0020-0255/

However, ACO algorithms are vulnerable to a hostile environment, where an attack can exploit the security issues found on stigmergic algorithms [25]. For instance, there is no mechanism that guarantees the integrity or the authenticity of the information carried by the ants. In addition, there is an implicit trust among the network nodes [25].

Well-known, standard cryptography techniques can be used to counter many of those problems in order to provide secure routing. However, they cannot avoid problems due to an authenticated node that is misconfigured or compromised [1,2,24].

Indeed, a byzantine failure at the routing protocol occurs whenever an authenticated network node exhibits arbitrary or faulty behavior that degrades or even disrupts the routing service [1,17]. Additionally, byzantine failures can be regarded as a security vulnerability of the routing protocol.

The proposal of this work is to associate crankback re-routing extensions to the ACO algorithm [7,16] to deal with byzantine failures in Wavelength-Routed Optical Networks (WRON). The crankback mechanism [7] helps the computation of constrained-based paths in (G)MPLS networks that may use out of date or inaccurate routing information. Byzantine failures may also affect the routing information of the network. Therefore, the crankback mechanism can also be used to improve the routing performance in the presence of byzantine failures. Since the crankback mechanism can operate over out of date or inaccurate routing information, there is no need to detect or locate the byzantine failures.

To our knowledge, this is the first work that uses crankback re-routing extensions to deal with byzantine failures. It is also the first work that deals with security issues targeting the ants or their processing by the nodes on the control plane of optical networks routed by means of ACO algorithms.

In this work, we assess the performance and robustness of the proposed approach using three different byzantine failure scenarios: misdirection of forward ants, dropping of forward ants and dropping of backward ants. Simulations demonstrate that it is possible to achieve routing survivability in a WRON with byzantine failures by using ACO routing with a crankback mechanism and securing the signaling protocol layer of the control plane.

The remaining of the paper is organized as follows. Firstly, in Section 2, we briefly discuss some related works in security and resilience of routing protocols. In Section 3, we introduce our routing ACO algorithm for transparent WRON and its associated crankback mechanism. Then, in Section 4, we present the byzantine failure model considered in this work and the motivation for the use of a crankback mechanism to deal with byzantine failures. We detail the simulations carried out to evaluate the ACO algorithm under byzantine failures in Section 5. The results obtained through simulations are then shown and discussed in Section 6. Finally, in Section 7, the conclusions are drawn.

2. Related work

Very few works have focused on the security issues of ACO algorithms. In [25], the authors show that AntNet [5], which belongs to the class of ACO algorithms, is vulnerable to three types of attacks: fabricating of ant packets, dropping of ant packets and tampering with the information in ant packets. For mitigating the fabrication attack, they propose the use of unique identifiers while for countering the tampering attack, they suggest the use of public key cryptography.

In AntNet, forward ants rely on the current node to be forwarded to the next hop. A malicious node can misdirect a forward ant, ignoring the information on the pheromone routing table. In [22], this threat is addressed and a new protocol is proposed to protect the forwarding ant process. The proposal can detect malicious behavior of a node in most occasions. However, it is vulnerable to collusion of two adjacent nodes and it significantly increases the network load generated by the ants.

Another work related to security issues on AntNet is proposed in [12], which is suited for Wireless Mesh Networks (WMN). *AntSec* is the first solution presented. It makes the AntNet algorithm resilient against forging, modification and dropping attacks by the use of public key cryptography. Other solutions proposed are *WatchAnt*, which is used to detect misbehaviors in the forwarding of ant and data messages, and *AntRep*, which is a reputation management system used in conjunction with *WatchAnt*.

An analysis of the security threats of *BeeHive*, which is a nature inspired routing protocol with a trust problem similar to AntNet, is presented in [23]. Byzantine failures caused by malicious nodes are studied and methods based on public key cryptography are shown to counter the attacks that could disrupt the correct protocol routing behavior. Due to substantial increase in the size of the agents as a result of the digital signatures carried by them, the communication overhead is substantially increased in the network.

On the other hand, the authors in [24] argue that the administrative and cryptography mechanism necessary to secure the routing protocol is an excessive burden. They also argue that a better way is to enhance the availability of the routing service in the presence of compromised nodes or communication, which can be achieved with the use of multiple paths.

A similar argument can be found in [1,2]. Since an authenticated node can exhibit a byzantine behavior, the focus has to be on providing routing survivability. Thus, those works rely on detecting byzantine faults in order to circumvent them during the path establishment.

3. Ant Colony Optimization

The observation of the foraging behavior of natural ants is the source of inspiration to the class of algorithms known as Ant Colony Optimization. ACO algorithms are based on artificial stigmergy, where artificial pheromone levels have positive or