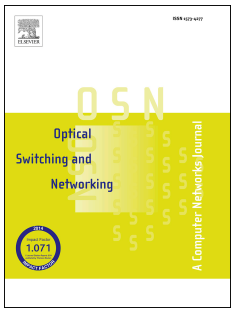
Accepted Manuscript



Decision tree rule learning approach to counter burst header packet flooding attack in Optical Burst Switching network

Adel Rajab, Chin-Tser Huang, Mohammed Al-Shargabi

PII: S1573-4277(17)30176-5

DOI: 10.1016/j.osn.2018.03.001

Reference: OSN 475

To appear in: *Optical Switching and Networking*

Received Date: 31 August 2017

Revised Date: 10 March 2018

Accepted Date: 11 March 2018

Please cite this article as: A. Rajab, C.-T. Huang, M. Al-Shargabi, Decision tree rule learning approach to counter burst header packet flooding attack in Optical Burst Switching network, *Optical Switching and Networking* (2018), doi: 10.1016/j.osn.2018.03.001.

Decision Tree Rule Learning Approach to Counter Burst Header Packet Flooding Attack in Optical Burst Switching network

Adel Rajab[1,2], Chin-Tser Huang[1], Mohammed Al-Shargabi[2]

[1]Department of Computer Science and Engineering,
University of South Carolina,
Columbia, SC, USA, 29208
rajaba@email.sc.edu; huangct@cse.sc.edu
[2]College of Computer Science and Information System,
Najran University,
Najran, KSA, 1988
adrajab@nu.ed.sa; mashargabi@nu.edu.sa

Abstract

An Optical Bust Switching (OBS) network is vulnerable to a range of issues. One of the most significant issues is Burst Header Packet (BHP) flooding attacks, which can negatively impact on the Quality of Service (QoS) and create more urgent issues such as Denial of Service (DoS). Existing techniques correcting BHP flood attacks usually display a low accuracy in detecting misbehaving nodes leading to BHP attacks. By contrast, Machine Learning (ML) is a widely adopted and powerful data analysis technique which has showed a high degree of predictive performance in multiple application domains due to its ability to discover beneficial knowledge for decision-making. This study investigates the use of predictive ML to counter the risk of BHP flooding attacks experienced in OBS networks, proposing a decision tree-based architecture as an appropriate solution. This contains a learning algorithm that extracts novel rules from tree models using data processed from several simulation runs. The results show that the rules derived from our learning algorithm will accurately classify 93% of the BHP flooding attacks into either Behaving (B) or Misbehaving (M) classes. Moreover, the rules can further classify the Misbehaving edge nodes into four sub-class labels with 87% accuracy, including: Misbehaving-Block (Block), Behaving-No Block (No Block), Misbehaving-No Block (M-No Block), and Misbehaving-Wait (M-Wait). The results clearly show that our proposed decision tree model is a viable solution compared to decisions undertaken by expert domains or human network administrators.

Keywords: Optical Burst Switching (OBS) Network; Burst Header Packet (BHP) Flooding Attack; Binary Classification; Machine Learning (ML); Decision Tree.

1. Introduction

An Optical Network (ON) is commonly used to transmit data from a source to its destination, using light via an optical fibre medium [1]. In contrast to traditional networks, ON features efficient quality performance indicators such as bandwidth and speed. Thus, it is a preferable option for Internet infrastructure [2]. In order to make use of the huge bandwidth of ON, Optical Burst Switching (OBS) was proposed in [3] as being the next generation of optical switching technology. Once it has obtained the User Datagram Protocol (UDP) packets, an OBS network will assemble the packets from the clients at the edge nodes (ingress node) into a data burst (DB) and a burst header packet (BHP), which will be transmitted in advance to preserve the network resources required before the DB is actually sent. Security and QoS performance issues are two important issues that need to be addressed to guarantee OBS network reliability. The work in [4,5,6] have discussed malicious attacks in Layer-1 in optical networks, and proposed solutions to reduce the impact of Layer-1 attacks. However, Layer-3 flooding attack still pose open threats, and attackers can exploit this, making an ingress node (source node) overload (flood) the network with BHPs that reserve the resources without transmitting the actual DB [7]. It is important, therefore, to ensure that prevention of BHP flooding attacks is a high priority in OBS, potentially