

Chapter 20

An Intelligent Traffic Engineering Method Over Software Defined Networks for Video Surveillance Systems Based on Artificial Bee Colony

Reza Mohammadi

Shiraz University of Technology, Iran

Reza Javidan

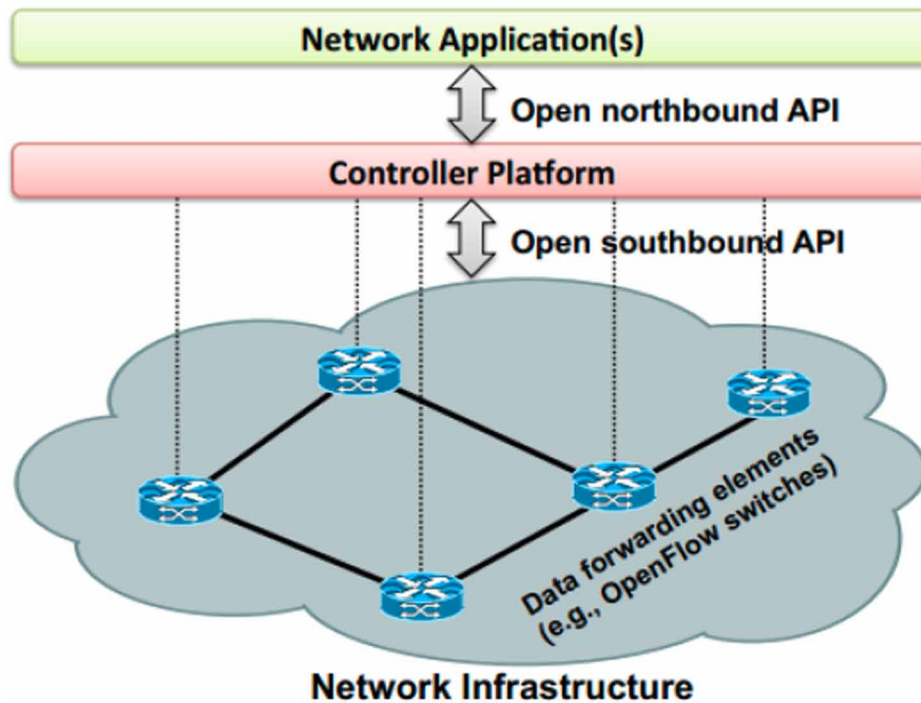
Shiraz University of Technology, Iran

ABSTRACT

In applications such as video surveillance systems, cameras transmit video data streams through network in which quality of received video should be assured. Traditional IP based networks cannot guarantee the required Quality of Service (QoS) for such applications. Nowadays, Software Defined Network (SDN) is a popular technology, which assists network management using computer programs. In this paper, a new SDN-based video surveillance system infrastructure is proposed to apply desire traffic engineering for practical video surveillance applications. To keep the quality of received videos adaptively, usually Constraint Shortest Path (CSP) problem is used which is a NP-complete problem. Hence, heuristic algorithms are suitable candidate for solving such problem. This paper models streaming video data on a surveillance system as a CSP problem, and proposes an artificial bee colony (ABC) algorithm to find optimal solution to manage the network adaptively and guarantee the required QoS. The simulation results show the effectiveness of the proposed method in terms of QoS metrics.

DOI: 10.4018/978-1-5225-7113-1.ch020

Figure 1. A simplified view of SDN (Kreutz et al., 2015)



1. INTRODUCTION

Nowadays, due to growing multimedia data type, providing Quality of Service (QoS) for multimedia applications is a main agenda for network providers. Traditional networks are complex, and hard to manage dynamically (Kreutz et al., 2015), because network administrators must configure each individual network device separately. In traditional networks such as IP and ATM, network devices are vendor specific further control and data plane are coupled (Akyildiz, Lee, Wang, Luo, & Chou, 2014). Due to these limitations, there are a few successful traffic engineering methods for providing QoS in traditional networks. One of the most popular traffic engineering schemas in IP networks is MPLS (Xiao, Hannan, Bailey, & Ni, 2000). Nevertheless, MPLS is not suitable for real time applications such as online multimedia streaming (Egilmez, Civanlar, & Tekalp, 2013), because MPLS requires many signaling messages between routers for assigning labels and managing the routes themselves. IntServ (Clark, Shenker, & Zhang, 1992) and DiffServe (Ito & Tasaka, 2008) are other solutions for providing QoS in the traditional networks. These methods are based on hop by hop manner of IP routing and do not care about overall network resources, hence they are not truly successful in all type of networks for multimedia applications (Egilmez, Civanlar, & Tekalp, 2013). Moreover, due to lack of global network view in legacy networks, it is difficult to guarantee QoS with respect to such constraints.

To overcome such limitations, Software Defined Networks (SDN) can be used. In SDN, the control plane and data plane of network are separated, and network providers will be able to control the whole network with a controller (Akyildiz, Lee, Wang, Luo, & Chou, 2014). Separation between control and data plane helps network administrators to manage the network dynamically. SDN provides network programmability, hence network administrators will be able to program and configure their networks per-flow and dynamically (Kim & Feamster, 2013). Figure 1 shows the simplified view of SDN architecture.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/an-intelligent-traffic-engineering-method-over-software-defined-networks-for-video-surveillance-systems-based-on-artificial-bee-colony/213811

Related Content

Risks, Security, and Privacy for HIV/AIDS Data: Big Data Perspective

Md Tarique Jamal Ansari and Dhirendra Pandey (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications* (pp. 58-74).

www.irma-international.org/chapter/risks-security-and-privacy-for-hiv-aids-data/213794

Living While Being Watched

(2022). *Modern Day Surveillance Ecosystem and Impacts on Privacy* (pp. 184-201).

www.irma-international.org/chapter/living-while-being-watched/287150

Security in Transnational Interoperable PPDR Communications: Threats, Requirements and Architecture Solution

Ramon Ferrús, Oriol Sallent, Cor Verkoelen, Frank Fransen, Keld Andersen, Christian Bjerrum-Niese, Jaakko Sajonmaa, Claudia Olivieri, Michel Duits, Anita Galin, Franco Pangallo and Debora Proietti Modi (2019). *National Security: Breakthroughs in Research and Practice* (pp. 859-879).

www.irma-international.org/chapter/security-in-transnational-interoperable-ppdr-communications/220920

Towards Intelligent Human Behavior Detection for Video Surveillance

Swati Nigam, Rajiv Singh and A. K. Misra (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications* (pp. 884-917).

www.irma-international.org/chapter/towards-intelligent-human-behavior-detection-for-video-surveillance/213837

Privacy Concerns with Digital Forensics

Neil C. Rowe (2016). *Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance* (pp. 145-162).

www.irma-international.org/chapter/privacy-concerns-with-digital-forensics/145566