An Efficient Online Algorithm For Dynamic SDN Controller Assignment In Data Center Networks

T. Jayanthi[1], N.Nikhil Reddy[2], N.Raja Kumar Reddy[3]
[1]Asst.Prof, Dept of CSE
[2, 3]Dept of CSE
[1, 2, 3] Sri Chandrasekhrendra Saraswathi Viswa Mahavidyalaya, Deemed to be University Kanchipuram, Tamil Nadu, India

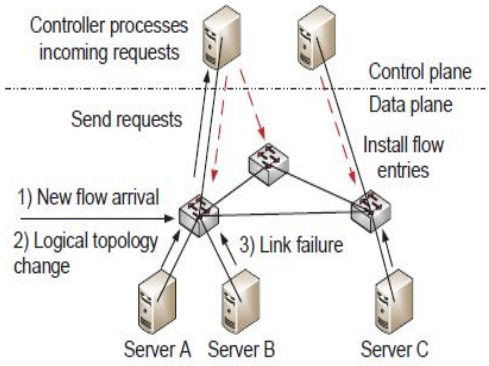
Abstract- *It is mainly to investigate the dynamic BS switching, active BS transmitting time and BS energy consumption association in the wireless network. SDN-based strategy, called PSESA-MinAir, is proposed to save energy in a wireless network during low traffic hours. When the traffic is low, on the guarantee of users' QoS, PSESA-MinAir tries to allocate traffic to as few BSs as possible. Those spare BSs are able to be switched into sleeping mode for energy saving. Then PSESA-MinAir minimizes active BS transmission airtime to low down active BS load and reduce BS power. When the traffic load is low, it reduces the energy consumption of BSs effectively. In addition, it is also necessary to identify the impact of energy consumption parameters on the energy-saving effect of our proposed strategy.*

Keywords- Dynamic BS switching, SDN, PSESA-MinAir, QoS.

I. INTRODUCTION

SOFTWARE defined networking (SDN) has emerged as anew paradigm that shifts network control from distributed protocols to a logically centralized control plane. With itssupport of flexible network management and rapid deployment of new functionalities there is an increasing interest in deploying SDN in both inter-data center and intra-data center scenarios. To improve scalability and avoid a single point of failure the SDN control plane is typically implemented as a distributed system with a cluster of controllers Switches are then statically assigned to one or multiple controllers However, static assignment between switches and controllers results in long and highly varying controller response. Times since traffic in data center networks (DCN) fluctuates frequently. Spatially, switches in different layers of the topology experience significantly different flow arrival rates and traffic variability. Temporally, the aggregate traffic usually peaks in daytime and falls at night. Moreover, traffic variability also exists in shorter time scales even when the total traffic remains the same. All these factors cause hot spots among some controllers, leading to excessively long response times for the switches they manage. Although the controller response time may not be significant for elephant flows it fundamentally limits the network's ability to quickly react to events such as failures and may cause transient congestion to last for a long time. Further, maintaining a cluster of controllers needs special care considering their synchronization cost, since this synchronization among controllers directly affects the scalability and management of the control plane. Consistent network states should be maintained otherwise the network performance may significantly degrade. The synchronization among controllers requires all-to-all communications which means the more controllers there are, the more the maintenance costs.Hence, it is critical to apply dynamic controller provisioning and assignment to a software defined DCN, for lower controller response time and better utilization of controller resources. Dynamic switch migration across controllers is technically feasible as demonstrated by past work such as . We formulate the dynamic controller assignment problem (DCAP) as an online optimization problem aiming at minimizing the total cost. In this problem, each controller has capacity in terms of the maximum request rate it can manage. The switches are dynamically mapped to controllers when traffic varies. One key challenge is then to develop an efficient solution algorithm, so that switches can be re-assigned in atimely fashion in response to variations of network conditions, even in a large-scale DCN. To solve the long-term DCAP online, we apply the Randomized Fixed Horizon Control (RFHC) framework to decompose the long-term optimization into a series of onetime- slot assignment problems. However, even in each time slot, the assignment problem remains challenging. From the switch's perspective, it prefers a controller with lower response time to improve performance. From the controller's perspective, it is more willing to manage topologically closer switches to reduce the control traffic overhead. This is important as communication between switches and controllers is frequent and occupies scarce bandwidth resources. First, stable matching is competitive in its outcome and efficiency. The deferred acceptance algorithm to generate a stable matching can be easily implemented in a centralized manner with low time complexity, which is suitable for large scale DCN. Second, the two phases are complementary. The solution of the stable matching phase serves as the input of the coalitional game and accelerates the

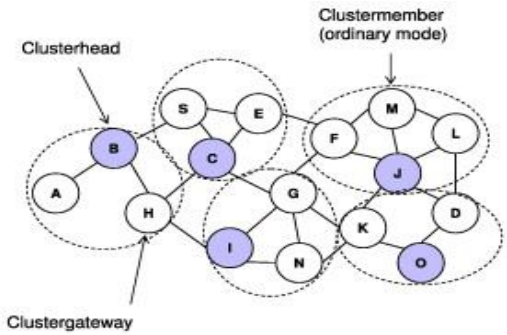
convergence of the second phase, while the coalitional game makes transfers to further improve response time.



SDN Functional Process

I: CLUSTER FORMATION

Nodes cooperate to form clusters, and each cluster consists of a CH along with some Cluster Members (CMs) located within the transmission range of their CH. While a node takes part in the network, it is allowed to declare itself as a CH. In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in this CH's transmission range can accept the packet to participate in this cluster as cluster members. On the other hand, when a node is deemed to be a CM, it has to wait for CHP. Upon receiving CHP, the CM replies with a CM Hello Packet (CMP) to set up connection with the CH. Afterward, the CM will join this cluster; meanwhile, CH and CM keep in touch with each other by sending CHP and CMP.



II. MODEL AND FORMULATION

In this section, we introduce the Dynamic Controller Assignment Problem (hereafter denoted as DCAP) along with the system model. We focus on understanding how to dynamically provision the control plane's capacity (i.e., the number of active controllers) and decide the assignment between switches and controllers so as to minimize the total cost in the data center deployed with SDN.

A. Network Model

Though the physical topology of a DCN varies communication between switches and controllers can be logically viewed as taking place in a two-tier structure between the control and data plane, as shown in Fig. 1. Note the SDN controllers can be running on dedicated hardware or software appliances in virtual machines.

B.Controller Response Time Model

Since today's data center topology can provide high bisection bandwidth the propagation delay in dispatching forwarding rules is less significant than the controller CPU processing time Thus we only model the request processing time on the controller

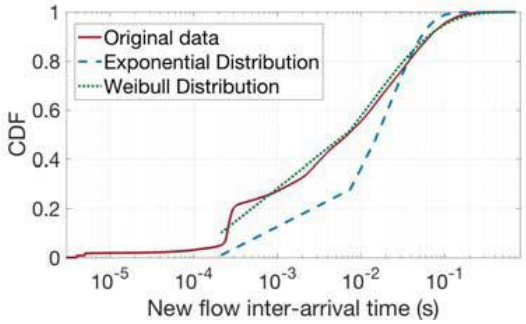


Fig. 2. CDF of flow inter-arrival times in the UNI1 DCN traffic dataset [1] publicly released by [10]. Best-fit curves for Exponential and Weibull distributions are depicted

C. Dynamic Controller Assignment Problem

Our objective is to decide the number of active controllers and the proper assignment between switches and controllers to minimize the cost of the system, which can be divided into two categories

We now describe each type of cost in detail.

Operating Cost: The operating cost consists of two main components:

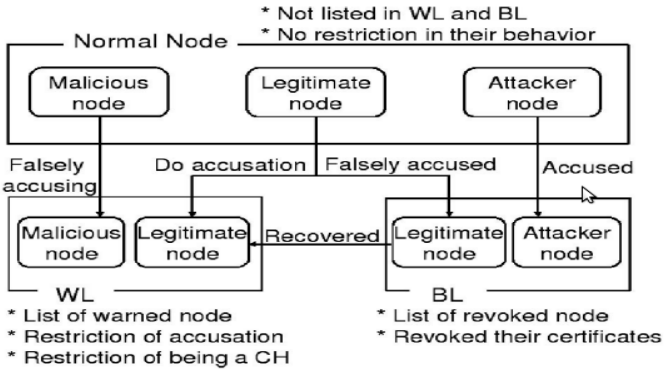
(a) Delay cost: Compared with traditional networks, the deployment of SDN introduces additional processing time in the control plane.

(b) Maintenance cost: The large number of controllers complicates the management of the control plane. Particularly, to hold a consistent global view of the network, the controllers constantly communicates with each other to synchronize the network states

Switching Cost: We define δas the unit cost of transitioning one controller from the sleep state to active state. The cost of transitioning from active to sleep is assumed to be zero. Thus, the switching cost for changing the number of active controllers from time.

III. NODE CLASSIFICATION

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their certificates in order to guarantee network security. A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers. In particular, it is able to falsely accuse a legitimate node to revoke its certificate successfully. The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network.These nodes can be further classified into three categories based on their reliability: normal node, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal node with high reliability that has the ability to accuse other nodes and to declare itself as a CH or a CM. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes. Nodes that are listed in the warning list are deemed as warned nodes with low reliability. Warned nodes are considered suspicious because the warning list contains a mixture of legitmate nodes and a few malicious nodes. Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they are unable to accuse neighbors any more, in order to avoid further abuse of accusation by malicious nodes. The accused nodes that are held in the blacklist are regarded as revoked nodes with little reliability. Revoked nodes are considered as malicious attackers deprived of their certificates and evicted from the network.

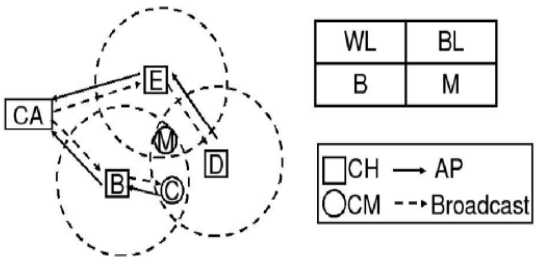


IV. CERTIFICATE REVOCATION

To revoke a malicious attacker's certificate, we need to consider three stages

- Accusing
- Verifying
- Notifying

The revocation procedure begins a detecting the presence of attacks from the attacker node. Then, the neighboring node checks the local list BL to match whether this attacker has been found or not. If not, the neighboring node casts the Accusation Packet (AP) to the CA. Note that each legitimate neighbor promises to take part in the revocation process, providing revocation request against the detected node. After that, once receiving the first arrived accusation packet, the CA verifies the certificate validation of the accusing node: if valid, the accused node is deemed as a malicious attacker to be put into the BL. Meanwhile, the accusing node is held in the WL. Finally, by broadcasting the revocation message including the WL and BL through the whole network by the CA, nodes that are in the BL are successfully revoked from the network.



V. CONCLUSION

In particular, we prove that the algorithm asymptotically minimizes a network cost and establish the relationship between the network cost and the corresponding

weight construct. Although our theoretical result is an asymptotic result, our experimental results show that the algorithm in fact performs very well under a wide range of traffic conditions and different data centre networks. While the algorithm has low complexity, the real implementation depends on how fast the weight updates and least weight paths can be computed in practical data centres (e.g., based on SDN). One possible way to improve the computation timescale is to perform the computation periodically or only for long flows, while using the previously computed least weight paths for short flows or between the periodic updates.

REFERENCES

[1] X. Han, X. G. Cao, E. L. Loyd, and C.-C. Shen, "Fault-tolerant relay node placement in heterogeneous wireless sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 5, pp. 643–656, May 2010.

[2] A. Krause, R. Rajagopal, A. Gupta, and C. Guestrin, "Simultaneous optimization of sensor placements and balanced schedules," IEEE Trans. Autom. Control, vol. 56, no. 10, pp. 2390–2405, Oct. 2011.

[3] D. Yang, S. Misra, X. Fang, G.Xue, and J. Zhang, "Two-tiered constrained relay node placement in wireless sensor networks: Computational complexity and efficient approximations," IEEE Trans. Mobile Comput., vol. 11, no. 8, pp. 1399–1411, Aug. 2012.

[4] H. Liu, X. Chu, Y.-W. Leung, and R. Du, "Minimum-cost sensor placement for required lifetime in wireless sensor-target surveillance networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1783–1796, Sep. 2012.

[5] A. E. Roth and M. A. O. Sotomayor, Two-Sided Matching: A Study in Game-Theoretic Modeling and Analysis. Cambridge, U.K.:Cambridge Univ. Press, 1992.

[6] A. Roy, H. Zeng, J. Bagga, G. Porter, and A.C. Snoeren, "Inside the social network's (datacenter) network," in Proc. ACM SIGCOMM, 2015,pp. 123–137.

[7] A. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sherwood, "On controller performance in software-defined networks," in Proc. USENIX HotICE, 2012, pp. 1–6.

[8] L. Zhang et al., "Moving big data to the cloud: An online costminimizing, approach," IEEE J. Sel. Areas Commun., vol. 31, no. 12, pp. 2710–2721, Dec. 2013.