SDN Based Content-Centric QoS-Guaranteed for Wireless Multimedia Sensor Networks

Gaolei Li, Jun Wu(✉), Jianhua Li, Kuan Wang, and Shan He

School of Electronic Information and Electrical Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{gaolei_li, junwuhn, lijh888, wangkuanfyfy, hszoe1995}@sjtu.edu.cn

Abstract. As the deployment of wireless multimedia sensor networks (WMSNs) increases sharply, the control granularity of traditional quality of service (QoS) technologies present weak assistance to satisfy the various application requirements. In this paper, we propose a novel architecture of software-defined network (SDN) based content-centric QoS-guaranteed (SCQG) for WMSNs. The SDN is an innovative network paradigm, which has capability to uniformly monitor and control the WMSNs' infrastructures automatically. In proposed architecture, we formulate proper priority for each content based on its popularity in WMSNs. And also, we extend the SDN controller to match the content and make flow tables each content requests. Besides, we design an k-nearest neighbor (KNN) based machine-learning algorithm to identify the popularity of different contents.

Keywords: Wireless multimedia sensor networks (WMSNs)
Software-defined network (SDN) · Content-centric QoS-guaranteed
Popularity · k-nearest neighbor (KNN)

1 Introduction

Wireless multimedia sensor networks (WMSNs) aims to provide more comfortable urban life, enriching data acquisition methods with videos, pictures and voices [1]. As the increasing deployment of WMSNs, the control granularity of traditional quality of service (QoS) technologies present weak assistance to support various future smart applications in smart city [2].

Recently, concept of software defined networks (SDN) has been considered as an innovative architecture with tremendous potential for utilization by the underlying infrastructures [3]. Firstly, SDN decouples control plane from data plane, breaking the vertical OSI model. States of all underlying infrastructures in the whole network are monitored and controlled centralizedlly. Secondly, to provide efficient information exchange between control plane and data plane, OpenFlow protocol, which has become the most popular southbound application programmable interface (S-API), defines a pipeline processing model [4, 5]. Rules of packets forwarding are handed out together with flow tables from SDN controller. When a packet arrives, switch will look up flow tables one by one. Once the corresponding flow table is matched, the packet will be

Y. Chen and T. Q. Duong (Eds.): INISCOM 2017, LNICST 221, pp. 40–48, 2018.
https://doi.org/10.1007/978-3-319-74176-5_4

forwarded according to rules in the flow table. If there is no appropriate flow table, packet will be sent into SDN controller for analysis (such as routing path, firewall, and load balancing). In summary, centralized control and global forwarding optimization accelerate packet forwarding speed significantly [6–9]. However, the rules for packet forwarding are designed only relying on the information from layer1 (L1) to layer4 (L4) of OSI model so that control granularity of OpenFlow protocol is inadequate for provisioning quality of services (QoS) satisfactorily. Particularly, priority can not be configured for each traffic dynamically. Therefore, some important sessions especially for multimedia data delivery may be interrupted when congested. Thus, SDN needs a new traffic engineering technique that can see deeper into the packet and identifies behaviors of every traffic, then classifies traffic according to these diverse identified behaviors in a fine-grained way. Content-awareness is perceived as a very imperative technology to provision optimal QoS for communication networks [10–13]. However, different from matching the static information from L1 to L4 of OSI model of TCP/IP simply, huge overhead of traffic behavior identification may lead to sharp degradation of network performance in traditional network.

In this paper, we propose SDN based content-centric QoS-guaranteed (SCQG) architecture which incorporates content-aware capability into SDN. The behavior identification is based on deep packet inspection (DPI), which is a typical traffic engineering technique and this function is shifted into the control plane of SDN in a previous work [14]. The SCQG specify the priority for each content appropriately according to its popularity, mapping from behaviors and the real-time network states adaptively. Priority control relies on dynamical modification of flow table. We present the designation principles and discuss how the SCQG will facilitate the provision of QoS. Many significant advantages in network performance such as delay, delay variation (including jitter and drift), packet loss and throughput can be improved promissingly.

The main contributions of our work contain three aspects. Firstly, we formulate proper priority for each content based on its popularity in WMSNs rather than the information in packet header. Secondly, we extend the SDN controller to match the content and make flow tables each content requests. Finally, we design an k-nearest neighbor (KNN) based machine-learning algorithm to identify the popularity of different contents.

We push content-awareness to SDN controller that has the whole view of network. The controller identifies popularity of each content and the underlying infrastructures rewrites flow table to determine which action to use for a packet and which packets to drop when congested. The scheme allows us to configure priority for each packet dynamically according to the comprehensive analysis about users' demands.

The rest of this paper is organized as follows. Section 2 introduces the preliminaries. Section 3 describes the basic model and every component of SCQG architecture. Section 4 describes the designation principles and its work process. Ultimately, Sect. 5 concludes this paper.

2 Preliminaries

In this section, we consider the possible existing technologies that may be utilized to implement the proposed SDN based content-centric QoS-guaranteed (SCQG) architecture as follows.

2.1 OpenFlow Protocol

The emerge of OpenFlow protocol greatly accelerates the development of SDN. Now it has become a standardized communication protocol for interconnection between control plane and data plane of SDN. Flow table has been central to OpenFlow protocol and it consists of matches, actions and counters mainly. Intelligent functions separated from the underlying infrastructures are integrated into flow tables. When a packet arrives, switch will match its IP header (L1–L4) by looking up the local flow tables one by one fastly. If there is no appropriate flow table, this packet will be sent into SDN controller for further analysis. Otherwise, it will be forwarded according to actions defined in the flow table. In this process, packets can be classified rapidly according to information from L1 to L4 and routing path is selected through computing some statistical characteristics about states of communication links. OpenFlow makes it flexible to reconfigure network elements dynamically and improves network performance significantly [18].

2.2 Quality of Services and Priority Control

QoS refers to ability of a network that can use a variety of basic technology, to provide better services for the specified network communication. QoS is a kind of network security mechanism, and it is often used for solving the problem of network delay when congested [14]. It is very important for network stability ensuring to implement better QoS policy in time-critical network such as wireless sensor networks (WSNs) [15], Smart Grid [16] and multimedia networks [17]. Usually, different applications have different requirements for QoS in different networks. The more characteristics of traffic flows are recognized, the more fine grained rules for QoS services can be provided. Priority control is the most popular approach to provide QoS services. In IP based network, DSCP is originally designated to distinguish the priority of each packet but not adopted practically.

2.3 Content Popularity Awareness

In traditional network, content-awareness is commonly treated as behavior identification of users. Therefore, deep packet inspection (DPI) originally is designed to enhance the security of the network. It combines the functionality of intrusion detection system (IDS) and intrusion prevention system (IPS) with a stately traditional firewall. The basic concept of DPI contains content analysis of the captured packets as well as accurate and timely discrimination of the traffic generated by different Internet protocols. Nowadays, DPI has been the most widely used method for application-awareness [19, 20].

Implementing application-awareness allows network to provide fine-grained traffic control by inspecting packets and identifying their application behaviors.

In this paper, we treat content-awareness as investigating the content's popularity. Implementing this content-awareness capability in SDN has two additional benefits. Firstly, popularity based content-awareness enables privacy security by hiding the identity of each user. Secondly, popularity based content-awareness is flexible for network elements to reduce the overhead QoS management.

3 SDN Based Content-Centric QoS-Guaranteed

It is generally assumed that there are two elements that have affect on the QoS performances of a communication system: (1) users' demands, and (2) network resources allocation. SDN treats all contents from the same local network as a group. In the past, networking technology care more about the connection between hosts. Popularity of contents are not considered when users call for content processing services. QoS services provided by SDN is often implemented through network monitoring and control. Multi-path is an effective approach to provide QoS guarantees. However, for resource constrained and time-critical scenarios such as wireless multimedia sensor networks (WMSNs), scale of delivered data in real-time is so large that every node and link may be being occupied. To ensure non-interrupted of important sessions, the importance of priority control is highlighted again. Therefore, we propose SDN based content-centric QoS-guaranteed architecture, in which the SDN controller can identify popularity of each content and classify them according to their popularity, and then maps the popularity into priority to control the QoS performances.

3.1 Constrains and Assumptions

This section shows the motivation of this paper and the significance of our work. Constrains of the scene are described as follows.

- Multimedia data delivery. Data exchanged in the specified communication system is mixed with diverse types of information including texts, voices, pictures, flashes and videos. We assume that the priority is positively proportional to content popularity.
- Time-critical & fault-tolerance. To ensure stability and availability of the network, it is imperative to transmit content with high priority from one to anther precisely in real time.
- Costs optimization. Either energy, bandwidth or cache of each network node in WMSNs are limited respectively, Moreover, continual join and quit my lead to unavailability of multi-path because energy of each node can't be aware of in real time.

Besides, we also assume that the SDN control is a trusted control center, and this center is maintained by trusted operators. Actually, this scene can be found out in the real word easily.

3.2 Components Description

As illustrated in Fig. 1, the proposed architecture consists of four core modules including ***content requests monitoring module***, ***popularity identification module***, ***priority mapping module*** and ***QoS-guaranteed policy module***.

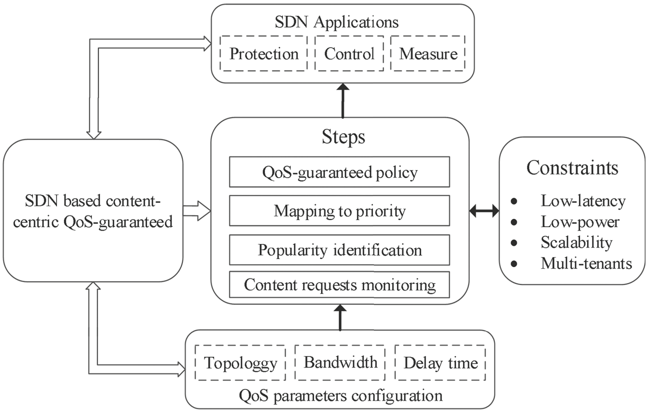

Fig. 1. The system model of SDN based content-centric QoS-guaranteed architecture.

Different from tradition network in which QoS requirements are mapped into differentiated service control protocol (DSCP) markings at the side of hosts, in our scheme QoS requirement of each content is identified by monitoring the popularity of diverse content. The priority-marking of each content coming from any user is set as zero initially. ***Content requests monitoring module*** consists of content requests collection, content inspection and information analysis. Content requests collection unit is designed to collect the content names which are the first time to enter into this network and must be sent to SDN controller for identification. This unit is deployed on the network elements in data plane. Content inspection unit is designed to identify application layer's information from the sent content. The application layer's information related to L7 visibility is provided as network services for orchestration of QoS guarantees. Information analysis unit is designed to provide an interface for synchronization between L7 information and states of whole network.

When the next same content arrives, priority-marking unit on the switch will match its priority-marking with flow tables one by one. If there is no corresponding flow table for this packet, it will be sent into traffic collection unit and then be sent into content inspection unit for identification. Applications of QoS guarantees unit in SDN converts these L7 information into a series of priority values, then priority control unit distributes them into data plane together with the corresponding flow table about forwarding. Rules in the flow table will contain policy about how to deal with the priority-markings. Therefore, the scheme allows us to configure priority for each content dynamically according to the comprehensive analysis about network states and users' QoS demands.

4 Design Principles

In SCQG scheme, the content popularity awareness is formulated to KNN algorithm. It allows priority for each content to be configured appropriately according to their popularity and the real-time network states automatically. Priority control also relies on dynamical modification of DSCP label. In this section, we will present the design principles and discuss how SCQG architecture to facilitate the provision of QoS in WMSNs. The main contribution of our work that hosts are the wrong place to map priority onto per-content will be introduced in detail. We push priority-mapping to SDN controller to identify popularity of each content. DSCP field is rewritten for determine which content to drop when congested and marking the identified contents. SCQG scheme enables inter-network priority-making. The proposed scheme makes it possible to dynamically configure priority for each content in a fine-grained way.

4.1 Priority-Mapping from Popularity

Forwarding policy for every content with a fixed priority is unelastic, priority marking defined by hosts can't be change in real-time with network states. As introduced in advance, the main contribution of our work is that hosts are the wrong place to map priority onto per-content. We push priority-mapping to a trusted SDN controller which has view of the whole network. Priority-marking of each packet coming from any host is set to zero initially.

The priority-mapping from popularity is based on KNN algorithm. The steps of KNN algorithm is showed as follows.

(1) Initialization of training set: We compute out the 42 different stochastic values in training set and compare them with many cautiousness in training set. We denote the eigen matrix in training set by $X = \{X_1; X_2; \ldots; X_n\}$, in which X_i presents stochastic values with significant difference. Therein, n represents the total number of training set, and the stochastic values with significant difference in training set is denoted as $X_i = \{x_1^i, x_2^i, \ldots, x_l^i\}$, $1 \le l \le 14$; $l, n \in N^+$. The $i-th$ training content is labeled with priority λ_i, $\lambda_i \in \{\text{'a'}, \text{'b'}\}$.

(2) Initialization of testing set: We compute out the 42 different stochastic values in training set and compare them with many cautiousness in testing set. By comparing, we select 14 different eigen values, which are denoted by a matrix $Y = \{Y_1; Y_2; \ldots; Y_m\}$. Therein, m represents the total number of testing set; We denote the eigen matrix in testing set by $Y_j = \{y_1^j, y_2^j, \ldots, y_l^j\}$, $1 \le l \le 14$; $l, m \in N^+$.

(3) KNN based priority-awareness:
To complete the priority prediction of each content in testing set, we calculate the euclidean distance between vectors in training set and testing set $D_{ij} = d(X_i, Y_j) = \sqrt{\sum_{i}^{n} (x_l^i - y_l^j)^2}$. When we want to predict the priority of $j-th$ content,the contents in $j-th$ column of D_{ij} are ranked from high to low. We select K lowest values and their corresponding i, and re-label them as

$\{i_1, i_2, \ldots, i_K\}$. In the algorithm, the priority counter is initialized as $C_a = 0$ and $C_b = 0$ firstly; Then, we retrieve the $\{\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_K}\}$, if $\lambda_{i_k} = 'a'$, then $C_a = C_a + 1$; if $\lambda_{i_k} = 'b'$, then $C_b = C_b + 1$. Consequently, if $C_b > C_a$, then the priority label is set as 'b', otherwise, the priority label is set as 'a'. Recycling the above process can finish the priority prediction. Actually, by the classification of KNN algorithm, the most popular content will be configured as the highest priority.

4.2 Packet Matching

The priority configuration is implemented by setting the DSCP value. When content arrives in switch supporting OpenFlow protocol, DSCP field will be matched firstly, if it is equal to zero, this content will be mirrored into SDN controller through "Packet In" message, and then it will be inspected by content popularity aware module. If malicious behaviors are found, this content will be dropped. Therefore, there no doubt that our scheme also can prevent malicious programs stepping into the networks additionally. Otherwise, a new flow table with DSCP value representing for priority will be distributed into OpenFlow switches.

As defined in advance, if it is the first time for this content to step into network, DSCP field will be set to zero and there is no corresponding flow table for it. Hence, it will be sent to SDN controller through a secure channel for analysis. Steps of content matching related to IP priority on the OpenFlow switch are introduced as follows

(1) Check whether DSCP field are NULL (every bit is zero).
If not, continue to match. Otherwise, go to step (5).
(2) Matching flow table one by one. If not found, go to step (5) Otherwise, continue.
(3) Forward content to the next switch.
(4) Execute instructions in action sets and update the counter.
(5) Send content to controller.

4.3 DSCP Field Marking

As introduced in advanced, the main contribution of our work is that hosts are the wrong place to map application behaviors onto per-content. In our scheme, application behaviors are identified by application-aware technology, and service priority are marked by set DSCP field. Moreover, DSCP field is filled out according to network states in real time dynamically by network operators rather than settled by hosts (users). Values of DSCP field are distributed together with the corresponding flow table through "Packet Out" message. Before this content is forwarded to the next switch, its DSCP field will be rewritten by the distributed values.

4.4 Optimization of Content-Awareness

Overhead of content-aware technology is very large and both efficiency and accuracy of it still need to be improved, in this paper we adopt three methods to optimize it as introduced in followings.

(1) DSCP field in the packet header is used to mark QoS priority of diverse applications uniquely. When a marked content arrives again, the corresponding flow table which has been formulated when the data content arrives for the first time is executed. In another word, content is inspected only when it arrives for the first time.
(2) A high-speed traffic collection unit is deployed in data plane to line the contents up, and this unit also set up an agent to pre-process and classify these contents. Both when and where the content arrives will be recorded and these records will be stored in a management information (MIB). They are also provided for diverse applications by the general interface.
(3) Content popularity-awareness is provided as services. Different application-aware instances can be allocated on demands. Scalability and efficiency of it can be improved significantly.

5 Conclusion

In this paper, a novel architecture with content-aware traffic control was proposed for WMSNs, popularity based priority configuration was integrated into the SDN controller. The global network view, status, flow patterns/characteristics and behaviors of the traffic flows were exploited to meet the diverse requirements of network applications for better stability, scalability and flexible scheduling. The proposed architecture contained content popularity aware module and the traffic control module. Besides, we adopted some mathematical models to quantitatively evaluate the performances of the proposed architecture. We designed an k-nearest neighbor (KNN) based machine-learning algorithm to identify the popularity of different contents.

Acknowledgments. This work was supported by the National Science Foundation of China (Grant No. 61401273 and 61431008) and Shanghai Science and Technology Committee (Grant No. 15PJ1433800 and 14DZ1104903).

References

1. Baccarelli, E., Chiti, F., Cordeschi, N., Fantacci, R., Marabissi, D., Parisi, R., Uncini, A.: Green multimedia wireless sensor networks: distributed intelligent data fusion, in-network processing, and optimized resource management. IEEE Wirel. Commun. **21**(4), 20–26 (2014)
2. Gaolei, L., Mianxiong, D., Kaoru, O., Jun, W., Jianhua, L., Tianpeng, Y.: Towards QoE named content-centric wireless multimedia sensor networks with mobile sinks. In: IEEE International Conference on Communication (ICC) (2017)
3. Kreutz, D., Ramos, F.M.V., Esteves Verissimo, P., Esteve Pothenberg, C., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2015)
4. McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J.: OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)

5. Lara, A., Kolasani, A., Ramamurthy, B.: Network innovation using OpenFlow: a survey. IEEE Commun. Surv. Tutor. **16**(1), 493–512 (2014)
6. Akyildiz, I.F., Lee, A., Wang, P., et al.: A roadmap for traffic engineering in SDN-OpenFlow networks. Comput. Netw. **71**(4), 1–30 (2014)
7. Agarwal, S., Kodialam, M., Lakshman, T.V.: Traffic engineering in software defined networks. In: INFOCOM, 2013 Proceedings IEEE, pp. 2211–2219. IEEE (2013)
8. Yassine, A., Rahimi, H., Shirmohammadi, S.: Software defined network traffic measurement: current trends and challenges. Instrum. Meas. Mag. IEEE **18**(2), 42–50 (2015)
9. Yong, C., Shihan, X., Chunpeng, L., Stojmenovic, I., Minming, L.: Data centers as software defined networks: traffic redundancy elimination with wireless cards at routers. IEEE J. Sel. Areas Commun. **31**(12), 2658–2672 (2013)
10. Qazi, Z.A., Lee, J., Jin, T., et al.: Application-awareness in SDN. ACM SIGCOMM Comput. Commun. Rev. **43**(4), 487–488 (2013)
11. Zhenyun, Z., Tae-Young, C., Raghupathy, S., Aravind, V.: Application-aware acceleration for wireless data networks: design elements and prototype implementation. IEEE Trans. Mob. Comput. **8**(9), 1280–1295 (2009)
12. Amemiya, K., Abiru, K., Ishihara, T.: Application-aware traffic control for network-based data processing services. In: IEEE International Conference on Intelligence in Next Generation Networks (ICIN), pp. 142–147 (2012)
13. Jarschel, M., Wamser, F., Hohn, T., Zinner, T., Tran-Gia, P.: SDN based application-aware networking on the example of YouTube video streaming. In: 2013 Second European Workshop on Software Defined Networks (EWSDN), vol. 87, no. 92 (2013)
14. Gaolei, L., Mianxiong, D., Kaoru, O., Jun, W., Jianhua, L., Tianpeng, Y.: Deep packet inspection based application-aware traffic control for software defined networks. In: IEEE Global Communication Conference, pp. 1–6 (2017)
15. Chang-Su, M., Sun-Hyung, K.: A study on the integrated security system based real-time network packet deep inspection. Int. J. Secur. Appl. **8**(1), 113–122 (2014)
16. Al-Anbagi, I., Erol-Kantarci, M., Mouftah, H.T.: A survey on cross-layer quality-of-service approaches in WSNs for delay and reliability aware applications. IEEE Commun. Surv. Tutor. **18**(1), 525–552 (2016)
17. Kaulbars, D., Schweikowski, F., Wietfeld, C.: Spatially distributed traffic generation for stress testing the robustness of mission critical smart grid communication. In: IEEE Globecom Workshops (GC Wkshps) (2015)
18. Spachos, P., Toumpakaris, D., Hatzinakos, D.: QoS and energy-aware dynamic routing in wireless multimedia sensor networks. In: IEEE International Conference on Communications (ICC), pp. 6935–6940 (2015)
19. Kogan, K., Nikolenko, S., Culhane, W., et al.: Towards efficient implementation of packet classifiers in sdn/OpenFlo. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 153–154 (2013)
20. Dainotti, A., Pescape, A., Claffy, K.C.: Issues and future directions in traffic classification. IEEE Netw. **26**(1), 35–40 (2012)
21. Finsterbusch, M., Richter, C., Rocha, E., Muller, J.-A., Hanssgen, K.: A survey of payload-based traffic classification approaches. IEEE Commun. Surv. Tutor. **16**(2), 1135–1156 (2014)