www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Location aware routing in software defined network

K. Tamil Selvi[1], Dr. R.Thamilselvan[2]

[1]Assistant Professor, Department of CSE, Kongu Engineering College.
[2]Professor, Department of IT, Kongu Engineering College.

ABSTRACT

Today's communication is based on Internet Protocol (IP), where IP packets are routed from source to destination hosts via one or more intermediate nodes. The location based routing can be used to route flows for location based services, but cannot be adapted with the current IP networks. Obtaining geospatial location using IP address is not a direct relation. The large volume of traffic flow in Internet obstructs the routing of data flows using geospatial information. The IP header is rigidly structured and provides no space for addition of extra information. The augmentation of geospatial information in IP packet can accomplished using Software Defined Networking (SDN). SDN allows the facility to control network flows by separation of data plane and control plane in the network. The actions associated with the centralized controller paves ways for modification of IP packet. Thus the geotags can be added to the IP header during encapsulation at the SDN controller and encapsulation at the destination. The satellite data can be disseminated on geotags based routing which provides improved quality of service. Further new application can be built using enrichment of packets using geotags including geofencing, network security related applications. Theoretical results are presented to assess the benefits of proposed geotags based routing and its performance is compared to the traditional dissemination of data flows.

Keywords: IP, SDN, Geotags, geospatial, Satellite data

INTRODUCTION

The Internet Protocol (IP) is the fundamental protocol for identifying hosts on the Internet. Every host on the Internet has unique IP address. This address is used to forward packet from source host to the destination host. The IP packet is associated with source IP address and destination IP address. On the other hand, the association of IP address to the geographical location is loose. The intermediate nodes which route the packets to the destination are unaware of the geographical location of the source or destination of the packet.

The routing of packet to the destination host is mainly using the IP address. Mining the source or destination geographical location of a packet in Internet is unpractical, due to rapid flow of packets through nodes of the network. The translation of IP address to geospatial location is not simple, and is based on table lookups. The Source IP address can be spoofed and manipulated, so the applications are unable to relay on them [1-5].

An approach for geotagging IP packet is to add geotag which contain location and time of the IP packet. A packet may be tagged just at the location where it is originated, or may accumulate tags as it visits nodes on its route to its destination. The geotags finds its application in various streams like to improve network management, support location based services and network security applications.

Adding geotags to IP packet is not a direct relation. The headers of the IP packets are rigidly structured and there is no space for provision of extra information. The payload portion of the IP

Author for correspondence:
Department of CSE, Kongu Engineering College.

packet also does not provide space for geotags. To overcome the above challenges, SDN can be used for augmenting geotags to the IP packets.

Network Function Virtualization (NFV) can used to build network application. It provides virtualization of tasks than that is executed on hardware. These functions could be chained with other virtualized functions. This chaining result in better network management system, effective load balancing systems, etc., depends on the application. The SDN and NFV provide flexibility and enhanced control over packet routing.

In this paper, the importance of using SDN and NFV for geotagging IP packet is described. Section 2 provides insight SDN and NFV. Section 3 illustrates how to add geotags to IP Packets. Section 4 exploits the applications of geotagging for location aware data dissemination. Section 5, analysis the performance enhancement of geotag based routing and finally the paper concludes.

SOFTWARE DEFINED NETWORKING

Software Defined Networking (SDN) is an open architecture that separates the control plane from the data plane in the communication nodes. The SDN architecture is shown in Fig 1. In SDN, the centralized controller controls the entire flow in the network. It has access to the networking devices like routers, switches of the network.

The SDN controller can alter the network flow by modifying the flow instructions in the flow table of the network elements using Open Flow protocol interface. The controller can add different types of action instruction to the flow table. When the packet is arrived at the network elements, matches an action rule, the corresponding action is performed on the packet. The action includes forwarding packets to other nodes, sending a copy of packet to the controller, increasing a counter or dropping a packet. [6-10].

The SDN controller can add an action that can modify packet header, which provides space for adding information to the IP packet. By this mechanism, the controller can instruct the routers or switches to add spatial – temporal information to the packets. Thus the geotag can be encapsulated in the IP packet and can be used for location based services like dissemination of satellite data based on user location.

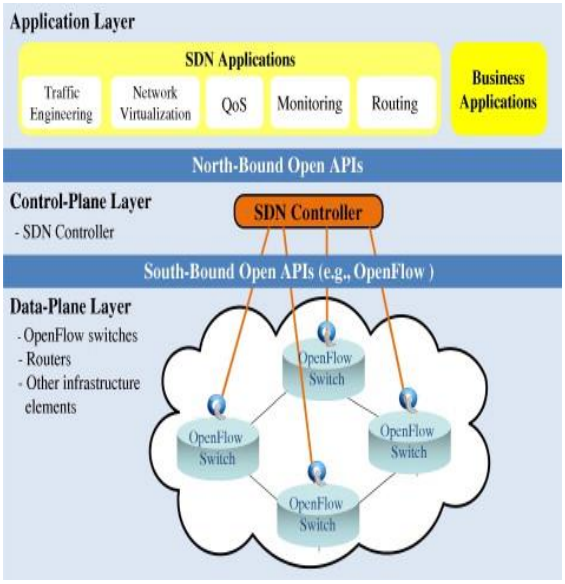

Fig 1. SDN Architecture

(Source: W-SDN: Towards next generation Wireless networks, Broadband Wireless Networking Laboratory)

In non-SDN network, network rules are computed in decentralized fashion. The routing protocols are hardcoded in the hardware and

difficult to modify and expensive. SDN adds flexibility to the network. SDN can be used for associating network flow with spatial and temporal information. This new set of capabilities allows for implementing location-aware SDN, where spatial – temporal information is combined with routing of IP packets [11-15].

The geotagging application could be virtual network functions (VNF) using Network Function Virtualization. VNF provides virtualization of tasks that runs as service on hardware. The dissemination of satellite based on user location can be implemented as VNF. This service can be chained with load balancer and other application for enhanced network management.

GEOTAGGING

Geotagging of IP packet is the process of adding a tag that contains geographical location of the network node and time of addition of the information. When the IP packet arrives at the network node, the geotag is added to the packet. The authentication of the tag can be endowed with certificate attesting the genuineness of the network node. The geotag can be unwrapped before the packet reaches destination or at the destination node which is depicted in Fig.2

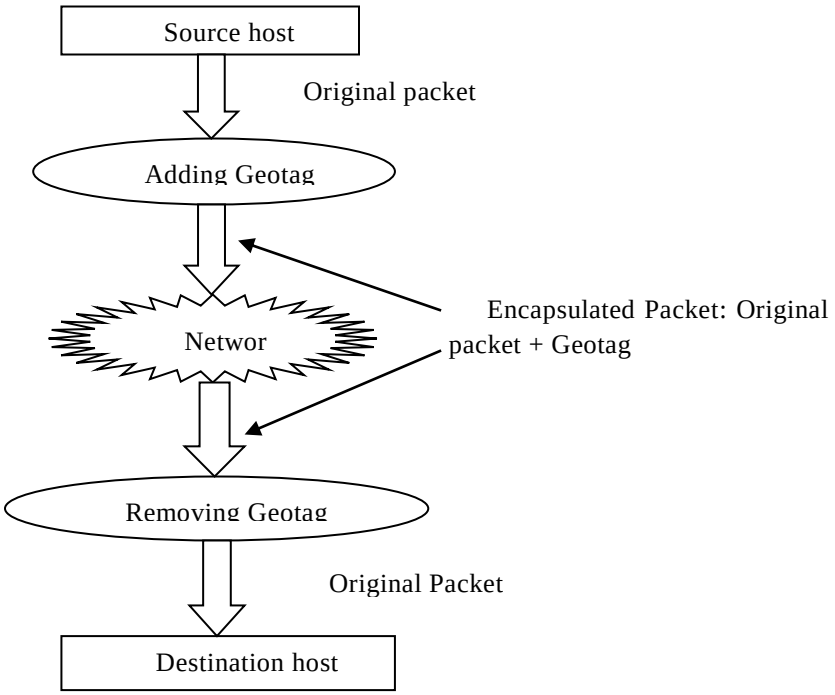

Fig 2. Geotagging IP Packet

Based on the instruction of the SDN controller, the encapsulation and unwrapping of geotags is executed by different nodes as the packet travels along the path. In encapsulation, the packet and the geotag are concatenated, a new payload is created. The existing packet remains unchanged. Thus geotagging is a part of Network layer and does not affect Transport layer.

To distinguish between the geotag and payload, the structure of the structure of the encapsulate packet is shown in Fig.3. The length of the original packet is indicated in first two bytes. Then there is the entire packet. After the original packet, geotag is appended. When a node adds geotag to already encapsulated packet, the size of the payload in the packet header must be changed accordingly.

The packet can be partitioned when it is too big for encapsulation. The first part of the payload is inserted into the first encapsulated packet, and the second part into the second encapsulated packet. And the both part contain the relevant geotag.

The location is represented as a pair of latitude and longitude coordinates. However many switches are expected to have the same location. For efficient representation of the location, hash codes can be used. When using hashing, the hash code of the location can be stored in the packet instead of the coordinates. The translation from a hash code to location or from location to hash code can be done using VNF. Hence there is no need to use physical machine to implement geotagging

.

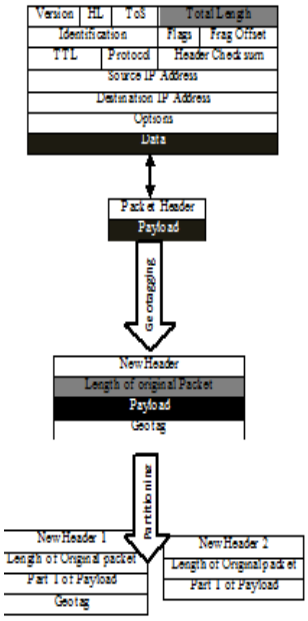

Fig 3. Encapsulating and Partitioning IP Packet

LOCATION AWARE DATA DISSEMINATION

Verified Source based Approach

The Verified source based approach is used to identify the location of the user rather than GPS and IP address. In this approach, the access point, where the user device access the network, would add to the first packet of the flow or to all the packets, a geotag. Now the geotag may include location, the reception strength of mobile devices. Authentication information can be added to geotag to indicate the authenticity of the access point.

The advantages of verified source based approach are: First in case of mobile devices, the location of the user device could be estimated more accurately by the services by including the reception strength. Second, the location of the user could be carried on to the destination, even when changed by intermediate nodes like NAT, because it is a part of payload. Third, by cryptographically signing the location, the system could rely on the information, and is less vulnerable to spoofing. Thus this approach facilitates the implementation of location proofs and location collaboration.

Dynamic Network Provisioning

The dynamic network provisioning concept is a solution to provide flexibility and service customization in the existing networks via sharing the network resources, which includes physical resources (e.g., computation, storage, etc.) and logical resources (e.g., network functions, etc.) among various service providers. Generally, this concept relates to the optimization problems in resources allocation, to segment the network into network slices which support specific QoS requirements offered services.

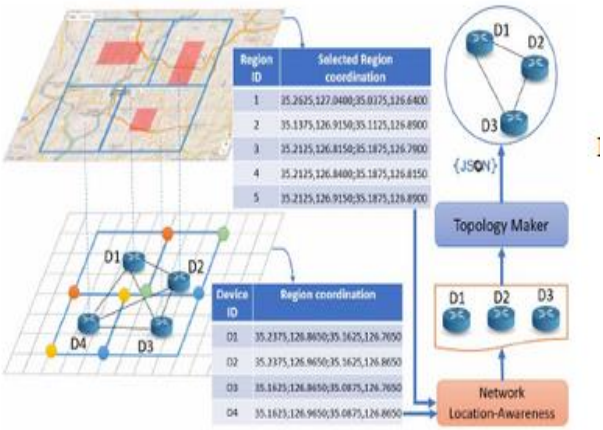

Fig 4. Modelling Network location-awareness

The network slice is generated dynamically based on the requested location of the user to provide dynamic location-aware network provisioning which is shown in Fig 4. The requested location is sent to SDN controller, which identify the geographical local of the SDN switches. The controller setup a location-aware network slice.

NETWORK SLICING

Network slices are defined as end-to-end logical networks running on common underlying physical or virtual network. These networks can be created on demand and are mutually independent with independent control and management. These self-contained networks are flexible to accommodate diverse application from multiple users on common infrastructure.

Network orchestration is a continual process of selecting resources to satisfy client requests in optimal way. SDN controller plays the role of orchestration. It will coordinate diverse network processes for creating, managing and delivering network services. Through orchestration, SDN controller optimally dispatches the selected resources to the requested client.

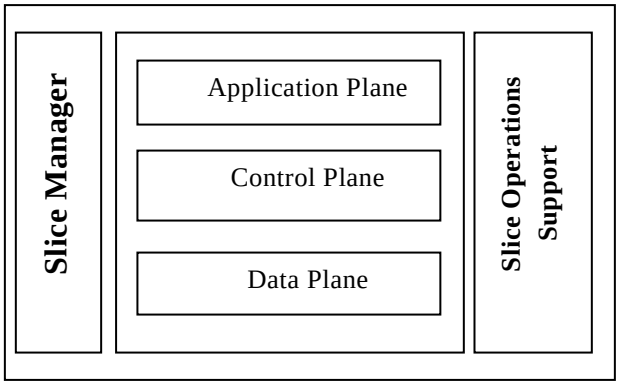

Fig 5. Generic structure of Network Slice

Each network slice is composed of data, control and application plane as shown in Fig 5. A Network slice instance is built over physical or logical resources that are fully or partially isolated from the resources. The network slicing finds its application in 5G communication.

The generic framework for network slicing consists of three layers namely Infrastructure layer, Network Function Layer and Service Layer. The infrastructure layer depicts the physical network devices. Many SDN techniques are encapsulated to

provide resource abstraction within the core network and medium access network.

Network Function layer executes all the required functions to manage virtual resources and network functions life cycle. The service layer is composed of applications that use the services provided by the network. SDN and NFV play a vital role in facilitating efficient management and orchestration of network resources.

NETWORK MODELING AND ANALYSIS

Network calculus is a tool used to analyses the flow control problems in the network. It is used to formulate deterministic guarantees on delay, throughput, queue length and other metrics of network. A SDN switch is a network element with Input: I, Output: O and Flow Table: C, such that O=C(I(t)), at time t. q(t) is length of queue inside SDN Switch at time slot t. μ is Constant Service rate.

The packet forwarding rate of SDN switch is given by

$$Q(t+1) = (q(t) + I(t+1) - \mu) \text{ with } q(0) = 0$$

The output flow cumulative process of SDN switch is

$$O(t) = I(t) - q(t)$$

$$O(t) = \min \{I(s) + \mu(t-s)\}, t \geq 0$$

The SDN network consists of numerous SDN switches which are centrally controlled by SDN controller. The network model of SDN controller and SDN switches is shown in Fig 6. Let A1 and A2 be the overall arrival process of SDN switch and SDN controller. FC (t) and FS(t) be the respective output processes.

$$A1(t) = A1(t) + S21(FC(t)),$$

$$A2(t) = A2(t) + S12(FS(t))$$

The cumulative arrival process A2 represents packet input from SDN switches which are controlled by SDN controller. A part of the flow control command, which leaves SDN controller is forwarded to SDN switch S1 and rest to other switches in network controlled by SDN controller.

The output packet stream of S1 (FS (t)) is divided into two parts. One part is forwarded to SDN controller S12 (FS (t)), which represent the packet flows, for which the SDN switch has no flow-entry in its flow table. The other part represents the packet flows, for which an existing flow entry table is available in the flow table of the switch. Assume that cumulative arrival processes are upper constrained.

Then the queue length of SDN controller (QC) and SDN switch (QS) is given by

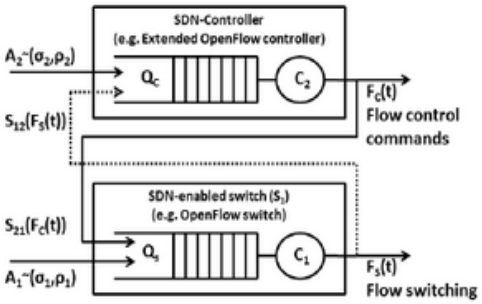

Fig 6. Network Model of SDN Controller and SDN Switch

$$Q_C \leq \sigma_1 + \gamma_{21}\sigma_2 + \delta_{21}$$

$$Q_S \leq \sigma_2 + \gamma_{12}\sigma_1 + \delta_{12}$$

Where σ is burst rate, δ is arrival rate and σ is constraint parameter. The flow controlling function S12 ~ (δ12, γ12) and S21 ~ (δ21, γ21) are upper constrained.

CONCLUSION

Geotagging IP packet improves routing by adding location and time to the packet. With the help of SDN capabilities, adding tags to the IP packet is done effectively and flexibly. NFV provides provision for processing of added tags without additional overhead. Generating network slice dynamically based on requested location of

the user provides the way for provision of user based services. Based on the cumulative arrival process, the proposed SDN switch model capture the closed form of the packet delay and buffer length.

Given the cumulative arrival process and flow control functionality of SDN Controller, an upper bound estimate of packet delay and buffer requirement of SDN switch can be calculate. This deterministic modelling of network helps in identifying the resource requirement of the specific application. The stochastic modelling of SDN deployment will be the future trends for adhoc network applications.

REFERENCES

[1]. Tamraparni Dasu, Yaron Kanza, Divesh Srivastava, "Geotagging IP Packets for Location-Aware Software-Defined Networking in the Presence of Virtual Network Functions", Proceeding of the 25th ACM SIGSPATIAL International Conference on Advances in Geographical Information Systems

[2]. Sharma, Vicky, et al. "Dynamic network provisioning for time-varying traffic." Journal of Communications and Networks 9.4, (2007), 408-418.

[3]. Li, Yong, and Min Chen. "Software-defined network function virtualization: A survey." IEEE Access 3, (2015): 2542-2553.

[4]. Nguyen, Choi, et al. " Location-aware dynamic network provisioning" , 19th Asia-Pacific Network operations and Management Symposium, 2017.

[5]. Chatras, Bruno, U. Steve Tsang Kwong, and Nicolas Bihannic. "NFV enabling network slicing for 5G." Innovations in Clouds, Internet and Networks (ICIN), 20th Conference on. IEEE, 2017.

[6]. KaustubhJoshiandTheophilusBenson.2016. Network Function Virtualization. IEEE Internet Computing (2016), 7–9.

[7]. Jiebo Luo, Dhiraj Joshi, Jie Yu, and Andrew Gallagher. 2011. Geotagging in multimediaandcomputervision—asurvey. Multimedia Tools and Applications 51, 1, 2011, 187–211.

[8]. Keith Kirkpatrick. 2013. Software-defined networking. Commun. ACM 56(9), 2013, 16–19.

[9]. J.-Y. Le Boudec and P. Thiran, Network calculus: a theory of deterministic queuing systems for the internet. Springer-Verlag, 2001.

[10]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev., vol. 38(2), 2008, 69–74.

[11]. M. Caesar, D. Caldwell, N. Feamster, J. Rexford, A. Shaikh, and J. van der Merwe, "Design and implementation of a routing control platform," in Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2(05), Berkeley, CA, USA, 2005, 15–28.

[12]. Tootoonchian, S. Gorbunov, Y. Ganjali, M. Casado, and R. Sherwood, "On controller performance in software-defined networks," in Proceedings of the 2nd USENIX conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services, Berkeley, CA, USA, 2012.

[13]. Openflow controller performance comparison, [Online].Available: http://www.openflow.org/wk/index.php/Controller Performance Comparisons last access. 2013.

[14]. "A calculus for network delay. ii. network analysis," Information Theory, IEEE Transactions on, 37(1), 1991,132–141.

[15]. Joshua Reich, Christopher Monsanto, Nate Foster, Jennifer Rexford and David Walker, "Modular SDN programming with Pyretic" Technical Reprot of USENIX, 2013.