Peer-to-Peer 기법을 이용한 Eduroam

소카세인 라자시리, 뉴엔 트리 투안 힙, 황성민, 김경백
전남대학교 전자컴퓨터공학부
{sokasaners, tuanhiep1232, hsmvirus}@gmail.com, kyungbaekkim@jnu.ac.kr

Peer-to-Peer Approach for Eduroam

Rajashree S. Sokasane, Hiep Nguyen Tri Tuan, Sungmin Hwang, Kyungbaek Kim
School of Electronics and Computer Engineering
Chonnam National University

Abstract

Nowadays, the use of mobile devices is increased in academic world. Almost all mobile devices have wireless connectivity facility to easily get access to network everywhere. The eduroam is a secure worldwide wireless network which allows users to access the Internet with their own credentials at visiting institution during roaming. The eduroam is based on hierarchical structured RADIUS proxy servers. However, the RADIUS based tree structured approach of eduroam has some scope for improvements. Existing RADIUS based tree structure of edoroam is not self configurable; Joining/leaving of node is not automatically handled by existing approach and an authentication process takes high communication delay. In this paper, we propose peer-to-peer approaches for eduroam in two types: flat layer model with domain mapping table and DHT(Distributed Hash Table) based model, in order to improve the scalability of eduroam with self configurable feature and reduce authentication delay.

1. Introduction

Nowadays, the use of mobile devices is increased in academic world. Almost all mobile devices have wireless connectivity facility to easily get access to network everywhere. Wi-Fi Technology has become increasingly popular due to its flexibility and mobility. A user can access to the Internet by establishing a connection with a Wi-Fi access point. However, in order to use Wi-Fi connections users needs to pass through authentication process because of various reasons such as privacy and management [9]. For example, Wi-Fi access points run by an educational institute should be accessible only to faculties, students and staffs of the institute.

The authentication process of eduroam is based on the tree structured RADIUS servers. However, the tree structured RADIUS approach has some room for improvements. All authentication traffic flows through the whole tree hierarchy even though a user is only of interest to the information of a leaf RADIUS server of the tree, and it causes long authentication delay.

Process/machine	Time in μs
Request Forwarding	357
Authentication	270
Response Forwarding	162
Network latency	204191

(Table I) Composition of authentication process time in eduroam with RADIUS servers over WAN

Table I shows the composition of authentication processing time in eduroam. It is observed that request forwarding almost takes more time than response forwarding time. Request forwarding time is almost twice of response forwarding time. In request forwarding process, request is checked by every node, processed it and then forwarded to next node according to mapping; this process takes place on every node so it takes more time. When

request reaches at destination node, it is authenticated on that particular node and response is forwarded to user. In response forwarding process, it simply forwards the response gained from destination RADIUS node; so it takes less time to forward. From results given in table below, we can say that increasing intermediate node, increases network latency.

In this paper, we proposed a per-to-peer based eduroam, in order to improve the scalability and the performance of the authentication process of an eduroam-like Wi-Fi access point sharing service. We consider the two approaches of a peer-to-peer based eduroam. First, the Flat Layer RADIUS server model, and second DHT based RADIUS server model. The Flat Layer RADIUS server model is based on domain mapping table. In a domain mapping table, a domain name is mapped to a corresponding RADIUS server. It always takes O(1) message to lookup. The Flat Layer RADIUS server model has the ability to reduce communication delay. But it takes high maintenance cost as compared to DHT based RADIUS server model. It is because DHT update affects only set of RADIUS server rather than every RADIUS server in the network. However, DHT based RADIUS server model takes O(log N) message to lookup. That is, there is a tradeoff between the operation cost and the maintenance cost.

The rest of the paper is organized as fallows. Section 2 provides background of eduroam, RADIUS server and distributed hash table. Section 3 describes the proposed p2p approaches for eduroam in detail. Finally, Section 4 covers discussions and conclusion.

2. Background

In this section we give an overview of the eduroam, authentication process and each protocol that related to, such as Remote Authentication Dial-In User Service (RADIUS) and DHT.

2.1 Eduroam

eduroam originally proposed by TERENA (Trans-European Research and Education Networking Association). eduroam allows students, researchers and staff from home institutions to obtain Internet connectivity when visiting other other institutions. The eduroam principle[7] is based on the fact that the user's authentication is done by the user's home institution, whereas the authorization decision allowing access to the network resources is done by the visited network. eduroam is based on the most secure encryption and authentication standards in existence today [7]. It gives an access to authorized users only.

2.2 RADIUS AAA server

The RADIUS server is used as authentication server. It checks the credentials entered by the users and reply whether the user is valid or not. It also keeps a record of network usage. RADIUS is a networking protocol that provides centralized Authentication, Authorization and Accounting [8] management for computers to connect and use a network service [6]. RADIUS works a server as well as proxy; A proxying capability is used to give service to roaming user whenever they move, such as in eduroam [9].

2.3 Distributed Hash Table

In a peer-to-peer system, every node in the system plays same role; each node has a piece of system data. In this case, looking up data has an important role in distributed system. Distributed Hash Table provides a lookup service to help peer-to-peer system or other distributed applications to locate data more efficiently. DHT uses key that is generated by hashing function to locate node which contains the value [11][12][13].

3. Peer-to-Peer based eduroam

Although eduroam is secure roaming system between research and educational institutions; it has some disadvantages especially with its RADIUS based tree structure. Every authentication traffic flows through the whole hierarchy [4] even though it is only of interest to a leaf RADIUS server that causes high communication delay. Also, existing RADIUS based tree structure is not self configurable and it arises scalability issues.

To mitigate the disadvantages, we proposed a peer-to-peer based eduroam approach in order to improve the scalability issue of eduroam.

3.1 Flat Layer RADIUS server model

In this approach we used domain mapping based flat layer RADIUS structure instead of RADIUS based tree structure. In the Flat Layer RADIUS server model, each RADIUS is directly communicate with each other, i.e. without using any intermediate RADIUS proxy servers. By using this Flat Layer RADIUS server model we can reduce authentication delay. Flat layer RADIUS server model is self configurable. In addition to that it may avoid single point failure.

In the Flat Layer RADIUS server model, each RADIUS server maintains a domain mapping table with mappings between domain name and other RADIUS. To do this we must take for granted that each RADIUS server in a network has known about other RADIUS servers. With the Flat Layer RADIUS server model, an authentication request is forwarded directly to a

destination RADIUS by referring the domain mapping table with the requested name.

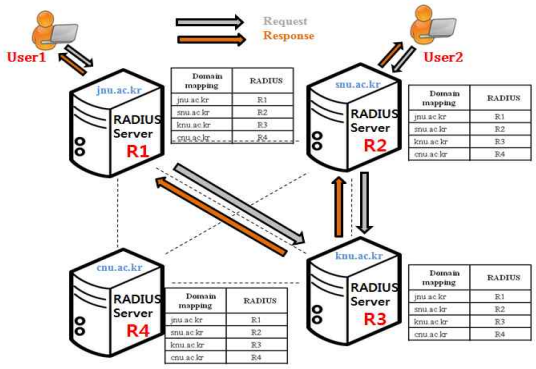

Figure 1: Overview of flat layer RADIUS server model

For example, let's assume that an eduroam-like Wi-Fi access point sharing system has four RADIUS servers namely R1, R2, R3 and R4. Like Figure 1, in this case each RADIUS server has a domain mapping table with tuples like (R1, jnu.ac.kr), (R2, snu.ac.kr), (R3, knu.ac.kr), (R4, cnu.ac.kr).

If request arises at R1 for user@knu.ac.kr then R1 is directly connected to the R3. In this case there is no need to use R2 as intermediate RADIUS proxy to connect with R3; I.e. Path for authentication is R1→R3 instead of R1→R2→R3. Authentication takes place on R3 and response is forwarded to R1. By using this Flat Layer RADIUS server model we need not to travel through unnecessary RADIUS proxies, we can directly communicate with the RADIUS which is corresponding to the requested domain.

Even though it is self configurable and reduces authentication delay, it has some scalability problem. If new node is joined in network then all existing nodes in network are need to be updated. If the number of nodes is increased with large number in network, then the cost for data transferring and maintaining data is very big. Distributed Hash Table is good option for domain mapping table to maintaining scalability of eduroam.

3.2 DHT based RADIUS server model

In Distributed Hash Table, data is distributed across nodes by using hash function; and a routing scheme is implemented to efficiently look up node on which data item is located. In DHT based RADIUS server model, each node knows information about related nodes only. DHT provides a protocol for looking up node in which data item is located [14]. DHT has some functionality such as scalability, availability [12], self configuration and affected a set of nodes rather than every other node in system. When a new node joins system, system will redistribute data. New node automatically configured to build its routing table. This process will affect to a small set of nodes in the system instead of affecting all nodes in the system. It helps to reduce data transferred cost.

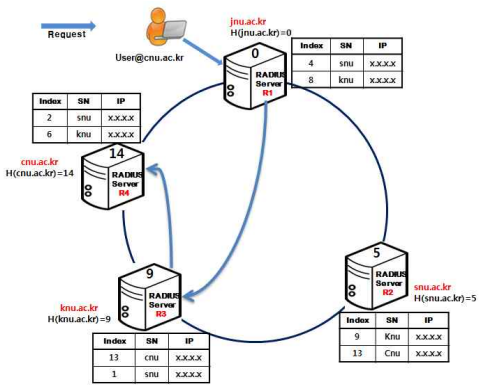

Figure 2: Overview of DHT based RADIUS server model

Each node in DHT based RADIUS server model has an identifier in m bit circle identifier space. Node identifier is generated by hashing domain name or IP address of RADIUS server. Each node in DHT based RADIUS server model, maintains its own routing table; based on it, visited RADIUS server can find the home RADIUS server where the user data is located. Figure 3 shows DHT based RADIUS server model with m=4. User with User@cnu.ac.kr is authorized user of RADIUS Server R4 (cnu.ac.kr). While roaming, the user is visited to RADIUS Server R1 (jnu.ac.kr). User wants to access the internet through Wi-Fi connectivity at visited institution with its own credentials. In this case by using DHT based RADIUS server model when user sent a request to RADIUS Server R1, it check its own routing table to send user information to its corresponding domain. Jnu.ac.kr doesn't have the information related to cnu.ac.kr then it forwards the request to node whose index key is nearest to cnu.ac.kr index. Then the intermediate node knu.ac.kr get the request, it check its own routing table for cnu.ac.kr, and it finds the index key related to cnu.ac.kr then the request for authentication of user is sent to its domain i.e. cnu.ac.kr.

4. Discussions and Conclusion

In this paper we presented concept of peer-to-peer based eduroam with two approaches, flat layer RADIUS server model and DHT based RADIUS server model respectively. In flat layer RADIUS server model, we use domain mapping table to map domain names to corresponding RADIUS server. In this approach we must consider that each node in the system knows about

every other node; and all nodes need to update after every joining and leaving of node. So, with this approach we may face some scalability problems.

DHT based RADIUS server model is self configurable and in case of joining and leaving of node DHT only affects the set of related domain (RADIUS servers) rather than all nodes in the network. It has low maintenance cost as compared to flat layer RADIUS server model. In aspect of scalability, DHT based RADIUS server model is better than flat layer RADIUS server model.

Flat layer RADIUS server model takes O (1) message to lookup and DHT based RADIUS server model takes O (log N) massages to lookup, where N is the total number of servers. DHT based RADIUS server model takes more time delay for looking up the data than flat layer RADIUS server model.

Currently, we already have an implementation of the flat layer RADIUS server model, and we are implementing the DHT based RADIUS server model. As a future work, we will conduct in-depth comparison of the authentication performance between these two p2p approaches for eduroam.

Acknowledgement

This research was supported by the MSIP(Ministry of Science, ICT&Future Plan-ning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2013-H0301-13-3005) supervised by the NIPA(National IT Industry Promotion Agency).

References

[1] Lisa Phifer , “Using RADIUS For WLAN Authentication, Part I ”

[2] Wikipedia. http http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access accessed 20 may 2013

[3] Y. Watanabe, H. Goto, H. Sone, “Resource Access Control for Wireless LAN Roaming Systems”, International Symposium on Applications and the Internet, 2008 p. 281-284.

[4] K. Wierenga, L. Florio, “eduroam: Past, Present and Future”, Computational Method in Science and Technology, vol. 11 (2005) pp. 169-173, 2005

[5] Yoshinori MIYAMOTO, Yasuhiro YAMASAKI, Hideaki GOTO Hideaki SONE “Optimization System of IP Address Using Terminal ID in eduroam” 2011 IEEE/IPSJ International Symposium on Applications and the Internet.

[6] Wikipedia. http://en.wikipedia.org/wiki/RADIUS accessed 05 may 2013

[7] eduroam. https://www.eduroam.org accessed 05 may 2013

[8] RADIUS.http://www.wifi.keller.com/CNIT107HW7.html

[9] L. Florio, K. Wierenga, "eduroam, providing mobility for roaming users."

[10] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[11] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker. “A scalable content-addressable network”, In Proc. ACM SIGCOMM’01, San Diego, CA, Aug. 2001.

[12] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for Internet applications. In Proc. ACM SIGCOMM’01, San Diego, CA, Aug. 2001

[13] A. Rowstron and P. Druschel. Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems. Accepted for Middleware, 2001, 2001.

[14] http://en.wikipedia.org/wiki/Distributed_hash_table

[15] Rajashree Sokasane, Kyungbaek Kim. Flat Layer Radius Model: Reducing Authentication Delay in eduroam. In Proceedings of the 2nd International Conference on Smart Media and Applications (SMA 2013), October 14-17, Kota Kinabalu, Malaysia.