Fine-Grained Data Traffic Management System Based on VPN Technology

Yiming Liu[1], Zhen Cheng[1], Ziyu Wang[2], Shihan Chen[1],
and Xin Su[1](✉)

[1] College of IOT Engineering, Hohai University, Changzhou 213022, China
15995086362@163.com, lte_5g@yeah.net,
1299068532@qq.com, leosu8622@163.com
[2] NanJing Ivtime, U2-1205 NO. 12 East Mozhou Road,
Town of Future Network, Nanjing 210000, China
wangziyu@ivtime.com

Abstract. With the development of the wireless network and mobile Internet service, the bandwidth of wireless network has increased obviously, and the number of wireless network user and data traffic generated by user terminal are steadily on the increase. Development in different economic and social sectors not only require higher network speed but also need low-cost information networks. The market needs a complete set of solutions, which can provide a comprehensive management system for the operation and billing of fine-grained data traffic. In this paper, we focus on the management system of fine-grained data traffic operation, which is support reverse charge and realize the fine-grained data traffic. Therefore, the proposed method can save user's cost and improve economic efficiency.

Keywords: Fine-grained data traffic · VPN technology
Data flow identification

1 Introduction

With the development of the wireless network and mobile Internet service, the bandwidth of the wireless network have increased obviously, and the number of wireless network user and data traffic generated by user terminal are steadily on the increase.

Development in different economic and social sectors not only require higher network speed but also need low-cost information networks. At present, there has been a contentious issue that users should pay operators when they use mobile phones to surf the Internet. For example, a transportation company called "Tencent" runs a bus called "WeChat" carrying nearly nine hundred million Internet users to "mobile internet", and who will pay the tolls? It is obvious that the bus driver should pay the tolls. However, the current situation cannot meet fine-grained data traffic management. The market needs a complete set of solutions, which can provide a comprehensive management system for the operation and billing of fine-grained data traffic [1–3].

J. J. Jung et al. (Eds.): BDTA 2017, LNICST 248, pp. 19–25, 2018.
https://doi.org/10.1007/978-3-319-98752-1_3

In order to provide users with better experiences and eliminate their expense concerns, we hope to implement a detailed and fine-grained billing of data traffic according to the types of business or user's custom. The research target of this paper is aimed at developing a fine-grained data traffic management system which can provide a detailed and fine-grained billing of data traffic. The user's various applications will be processed uniformly like data collection, statistical analysis, data mining, safety management, and other processing, to achieve a goal of detailed and fine-grained billing according to the types of applications, business or specific data traffic packages [4].

2 Analysis on Data Traffics

Through China-mobile Communication Corporation in Changzhou, we obtained the monthly average data traffic of 4 base stations in Hohai University (in the first half of 2016). E-UTRAN Cell Global Identifier (ECGI) of four base stations respectively is 4600-871713-12 (31.8193° N, 119.97166° E), 4600-872639-1 (31.82152° N, 119.97886° E), 4600-341532-1 (31.81869444° N, 119.9787778° E), 4600-341533-1 (31.8206° N, 119.975° E). Figure 1 shows the exact location and monthly data traffic of the four base stations, and the difference between the monthly data traffic of 4600-341533-1 and 4600-341532-1 is significant. After analysis, the former is close to the student dormitory and the traffic users are mostly students. Students are the majority of the current traffic users and live 24 h a day on campus. The latter is close to office buildings and classrooms, and part of traffic users are teachers, while they use traffics mainly during the day.

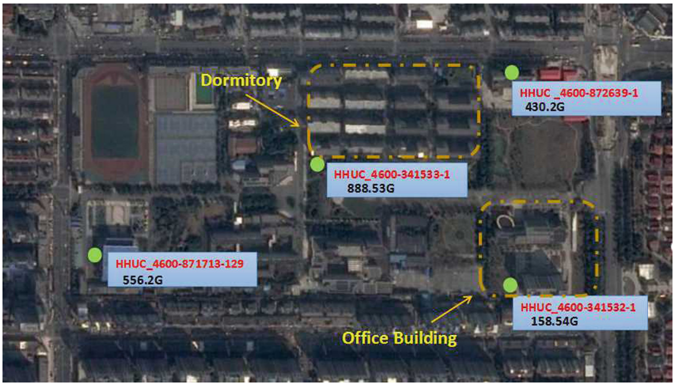

Fig. 1. Four base stations at Hohai University of Changzhou Campus.

At the same time, B2C mode is asymmetric, charge between companies and consumers cannot reverse. However, companies want to provide a better user experience, for example, let users under any circumstances to be able to shop or play games online, etc. Therefore, Alibaba and some other companies are willing to cooperate with the three operators to pay the fee to consumers and attract consumers to buy their products. However, many small and medium Internet enterprises are not willing to reverse the charge, because the present marketing system, management analysis system, network management, billing system of all operators does not support the reverse charge. Only upgrade system can achieve this goal but they are not willing to bear the upgrade cost. Because of this, the reverse charge plan is difficult to conduct.

3 Analysis of Existing VPN Technologies

Traffic transmitted through a tunnel, such as a VPN or protocol agency. In this paper, we use the mature, controllable and secure VPN technology. Currently, there are several common VPN technologies [3–6]:

3.1 Point to Point Tunneling Protocol (PPTP)VPN

The Point to Point Tunneling Protocol (PPTP) is a new enhanced security protocol developed based on the Point to Point Protocol (PPP). The protocol supports VPN, and can enhance security through Password Authentication Protocol (PAP), Extensible Authentication Protocol (EAP), etc. The PPTP can create, maintain and terminate a tunnel through connection control, and can encapsulate PPP frames by using the Generic Routing Encapsulation (GRE). Before encapsulation, the PPP frames' payload, that is effective transmission data, need a mixed process of encryption and compression first, and then make the remote users directly connect the Internet or other network by accessing the Internet Service Provider (ISP). The PPTP VPN is developed by Microsoft and is standardized. The GRE tunnel is created dynamically with TCP controlling tunnel (plaintext), and the GRE tunnel encapsulating real user data traffic—the PPP payload. The encryption of payload is merely based on a self-contained encryption protocol—MPPE, the head of GRE is all clear, and security level is not high. Moreover, other details are not transparent.

3.2 Layer 2 Tunneling Protocol (L2TP) VPN

L2TP is a kind of Virtual Private dial-up Network (VPDN) tunnel protocol. VPDN refers to accessing the public network using the dial-up function of public networks (such as ISDN or PSTN), and realize a virtual private network which can provide access services for enterprises, small Internet service provider (ISP) and mobile workforce, etc. VPDN can provide an economical and effective point-to-point connection between remote users and private enterprise networks. L2TP is an industry-standardized Internet tunnel protocol, which is similar to the PPTP protocol, for example, both of them require encryption of network data flow. The difference is that, for example, PPTP requires Internet Protocol (IP) network, while L2TP requires packet-oriented point-to-point connection. PPTP uses a single tunnel and L2TP USES multiple tunnels; L2TP provides the header compression, tunnel verification, while PPTP does not support.

3.3 Internet Protocol Security (IPsec) VPN

IPSec works like packet-filtering firewall, which can be viewed as an extension of packet-filtering firewall. When an IP packet is received, the packet-filtering firewall uses its header to match in a rule table. When a matching rule is found, the received IP packets will be processed by the packet-filtering firewall in accordance with the method decided by the rule table. There are only two processing works here: discarding or forwarding. The IPSec decides the process of IP packets received by searching the Security Policy Database (SPD). But unlike the packet-filtering firewall, IPSec handles the IP packet with the IPSec process except discarding, directly forwarding (bypassing the IPSec). It is because the new process that more network security than packet-filtering firewall can be provided.

3.4 Secure Sockets Layer (SSL) VPN

SSL is encrypted between the fourth and fifth layers and is often certified with digital certificates. Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is a type of client less SSL VPN, and it is vulnerable to man-in-the-middle. Currently, apple IOS 10. X does not support PPTP VPN, while the high version of android only supports IPsec VPN and L2TPVPN. Therefore, considering the compatibility and safety of the scheme, this paper mainly adopts IPsec VPN to realize traffic fine-grain operation management system. At the same time, for security, we use the Internet Key Exchange version 2 (IKEv2) protocol allows server better preventing Disk Operation System (DOS) attack in terms of the secret key exchange control. And the building of ISAKMP SA in Phase 1 only need 4 message exchanges instead of 6. IKEv2 is used to add a notify payload, and whenever there is a client connection to IKE server, the server responds a notify payload containing a cookie. Meanwhile, the client receives the notify message and contains the cookie in the next connection request. The connection will be established if the cookie is verified legal, otherwise, it will be viewed as a DOS attack, and dose not establish a connection. The server side simply saves a cookie that occupied a few bytes of memory and can be released quickly. IKEv2 is used in authentication, negotiate encryption, hash algorithm, the encryption of data traffic and the establishment of IKE SA, IP SEC SA. Security is ensured by the certification (Pre-shared password, digital certificate), Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Secure Hash Algorithm (SHA), Message Digest Algorithm (MD5), Anti-replay window.

The main software part proposed in this paper and its description are illustrated in Table 1.

4 System Design Objectives and Requirements

In this article, the flow fine-grain operation management system constructed based on the principle of standardization, will strictly follow the requirements of the relevant technical standards and business to practice overall planning and unified construction arrangement; In the meantime, based on the principle of openness, the system follows

Table 1. Software components and its descriptions of the system

Software components	Descriptions
APP client	Data flow identification and distribution It is suggested to provide the channel download business application and provide the starting entrance of the APP
SDK (Android version)	Android version SDK can provide the fine-grained data separating capacity and can realize APP packaging call
Data forwarding server (tunnel forwarding, security encryption)	Forwarding the data flow in server Making the security encryption and forwarding

an open architecture and adopts an open interface protocol and development platform to provide users with a unified and open capability call. In addition, business maintenance and development are not dependent on equipment manufacturers to ensure the continuous upgrading and development of the business. In terms of security, our system will be designed strictly according to the application of the telecommunications level. The system software and hardware architecture should fully consider the security strategy and mechanism of the whole system operation. In view of the security requirements of various business processes, various security technologies are adopted to provide users with perfect security. Finally, a software design framework with mature and stable operation instance is adopted [2, 4, 5].

5 System Architectures

The type of applications installed in users' equipment will be identified automatically when the user starts the data flow workshop SDK or APP. The network configuration information will automatically synchronize with data traffic management gateway. Data traffic management gateway will send feedback to users based on the current traffic load of network and the information. When the user adds a certain application to the directional flow packet, the flow workshop SDK or APP will create the pre-defined corresponding VPN tunnel to the traffic load device according to the type of applications. Data traffic packets are generated by a specific APP, and local SDK or APP can identify the packet by identifying the APP ID of the application started by users. And then according to the relevant protocol of VPN tunnel and the group package way of flow workshop SDK or APP to re-group packages, send to the specified tunnel, the flow is unpacked at the end of the tunnel, and then to the business server of SP. The data reverse process is similar.

Figure 2 shows the flow of VPN-call. It is initiated by the APP to register the login authentication, and the policy server manages the terminal users and data service nodes to perform uniform user access configuration. The APP internally make traffic identification according to the product used, and identifies the dynamic IP address of the current SP to bind with APPID temporarily. The APP server launch VPN resource request to the policy server, and make the policy server choose the nearest data server to access based on the IP address of the APP itself. Meanwhile, policy configuration will be forwarded to data load server based on the dynamic IP address of SP recognized by the APP. When the resource is ready, the server request APP to return the confirmation message and SA. The APP user uses the data server information and SA to log in the specified data load server, establish the virtual traffic tunnel for the identified APP data traffic. These four steps complete the establishment of VPN, and the identification and forwarding of data traffic [3–6].

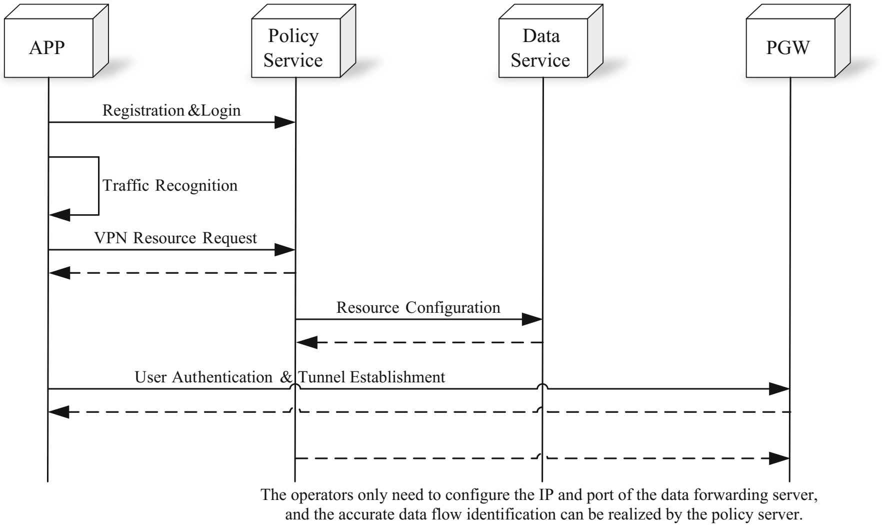
APP
Policy Service
Data Service
PGW
Registration &Login
Traffic Recognition
VPN Resource Request
Resource Configuration
User Authentication & Tunnel Establishment
The operators only need to configure the IP and port of the data forwarding server, and the accurate data flow identification can be realized by the policy server.

Fig. 2. The flow of VPN-call in typical business scenario.

The operators only need to configure the IP and port of the data forwarding server, and the accurate data flow identification can be realized by the policy server. Operators' billing management platform can obtain traffic statistics information through API docking. The way of billing can also be developed by the policy server itself.

6 Conclusions

With the development of the wireless network and mobile Internet service, the bandwidth of the wireless network have increased obviously, and the number of the wireless network user and the data traffic generated by user terminal are steadily on the increase. Development in different economic and social sectors not only require higher network speed but also need low-cost information networks. The market needs a complete set of solutions, which can provide a comprehensive management system for the operation and billing of fine-grained data traffic. In this paper, we focus on the management system of fine-grained data traffic operation, which is support reverse charge, and can realize the fine-grained division of data traffic. We bring a new type of consumption model for customers to save money based on traffic data reverse charge for customers. We use VPN to encapsulate applications separately that will help operators easily calculate the flow data for each application and reversely charge from online enterprises. Many online enterprises will be willing to cooperate with operators to pay the fee to consumers because they want to provide a better user experience, for example, let users under any circumstances to be able to shop or play games online, etc., and attract consumers to buy their products. We have experimentally employed the proposed reverse charge system, and the questionnaires have shown that this is a win-win model for both customers and online enterprises. We hope the proposed system will be finally implemented in practice.

Acknowledgements. This research is supported by the Natural Science Foundation of Jiangsu Province under Grant BK20160287.

References

1. Wan, H., Lin, Y., Zhihao, W., Huang, H.: Discovering typed communities in mobile social networks. J. Comput. Sci. Technol. **27**(3), 480–491 (2012)
2. Hou, J., Xu, B., Xu, L., Wang, D., Xu, J.: A testing method for web services composition based on data-flow. Wuhan Univ. J. Nat. Sci. **13**(4), 455–460 (2008)
3. Yan, T., Wang, B.: Grid architecture model of network centric warfare. J. Syst. Eng. Electron. **17**(1), 121–125 (2006)
4. Chen, J., Chen, Z., Wang, Q., Fang, Y.: Spatial database management system of China geological survey extent. J. China Univ. Geosci. **14**(3), 250 (2003)
5. Xiao, Y., Chen, Y.: Effcient distributed skyline queries for mobile applications. J. Comput. Sci. Technol. **25**(03), 523–536 (2010)
6. Jianming, Y., Guoxin, W., Junming, W.: Rebuilding the extrant's architecture with VPN. J. Southeast Univ. (English Edition), (1), 69–74 (1999)