Simulation of Performance Enhancement in the AAA Protocol*

Ji-Sun Kim, Eun-Chul Cha, and Hyoung-Kee Choi
School of Information and Communication Engineering, Sungkyunkwan University
Suwon, South Korea
E-mail: {jsk,iris1212,hkchoi}@ece.skku.ac.kr

Abstract: Nowadays managing the network is a laborious task. The reason is that boundary of the network has become ambiguous due to the combination of various forms of network and active access of mobile equipments.
The Authentication Authorization Accounting (AAA) is the system and protocol that controls access for network, applies access of policies, and collects the charges for the service used. The role of AAA could be highlighted under the complicated network environment. The AAA is related not only to the network security and mobile access but also to the service providing process. Consequently, the improved performance of AAA affects the whole network service system.
This paper analyzes the AAA performance improvement issues and the solution provided by IETE AAA WG, and measures the actual level of the performance improved. The issues of The Head-Of-Line (HOL) and Silly Window Syndrome (SWS) and their solutions have been adapted for this study since they are connected to AAA protocol. Also, the NS-2 simulator has been used as a simulator, and IEEE 802.16 has been selected as the network framework.
The results showed that the solution of HOL and SWS enhanced the performance of AAA 37.5 %, 30%, respectively.

1. Introduction

The fact is that network service is the most valuable commodity in the world. Multitudes of people desire to use network service. Every potential use of a service is valuable to a network service provider. Authentication Authorization Accounting (AAA) is a system that authenticates the identity of a user accessing a service, authorizes a user to access an available service and accounts for service utilization. Most operators in wired and wireless networks manage service supply via AAA. Since AAA is intimately associated with network architecture, eliminating redundancy of AAA operation is important. Many studies were conducted to improve AAA performance [1]. Specially, IETF AAA WG [2] resolves several issues of the AAA protocol [3][4][5]. Among the remainder, we focus on Head-of-Line (HOL) and Silly Window Syndrome (SWS) problem. They are closely related to the AAA protocol and much less rigorous analysis was done on them. We implement solutions of HOL and SWS. Then, we study their impact on AAA performance.

* "This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2008-C1090-0801-0028)

The reminder of this paper is organized as follows. In section 2, we provide background information about AAA. In section 3, we describe HOL and SWS issues and the existing solution. Section 4 presents the results of simulation. Finally, we conclude in Section 5.

2. AAA overview

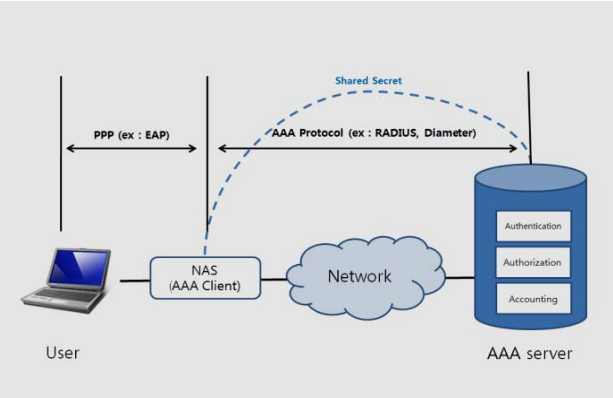

Figure 1. AAA architecture

Figure 1 represents a generic AAA client-server architecture. The AAA server is the core which performs authentication, authorization and accounting. Between the user and the AAA server, Network Access Server (NAS) works effectively with an AAA client. A user and NAS connect via point-to-point. NAS and an AAA server connect via practical multi-hop. NAS converts a point-to-point protocol format to an AAA protocol format. Remote Authentication Dial In User Service (RADIUS) [6] and Diameter [7] are designed for transmission of the AAA protocol. RADIUS utilizes User Datagram Protocol (UDP) as the transport layer. UDP does not guarantee reliability, delivery or duplicate protection. Diameter operates via a reliable transport protocol such as Transmission Control Protocol (TCP) and Stream Control Trans-mission (SCTP) [8]. TCP and SCTP are connection-oriented. Multi-homing and multi-streaming features distinguish SCTP from TCP.

3. AAA issues and solutions

3. 1 Head-Of-Line

In Diameter, it is quite inefficient to configure a TCP or SCTP connection for every authentication request from users. For instance, a 48-port NAS may have to maintain up to 48 TCP connections with the AAA server. Instead, a single persistent connection in the AAA server is better suited to resource management. Multiple authentication requests from different users can be pipelined via a single persistent connection.

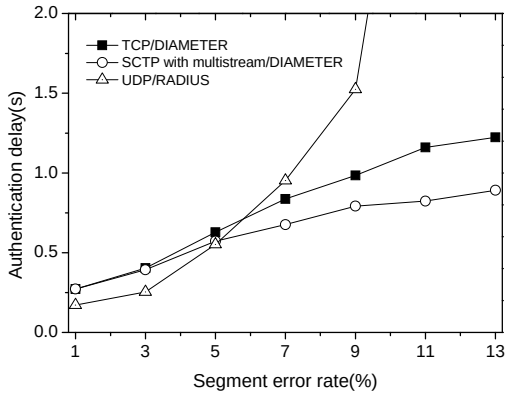

Figure 2. Delay difference TCP and SCTP

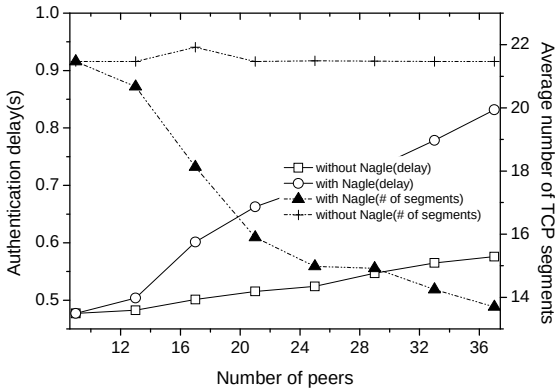

Figure 3. The comparison with and without the Nagle's algorithm

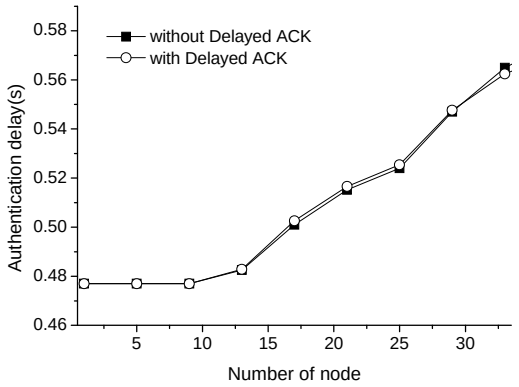

Figure 4. The comparison with and without the Delayed ACK

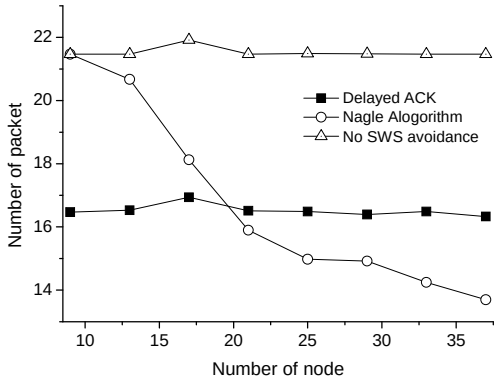

Figure 5. Network traffic load for SWS avoidance solutions

In this case, the pipelining request in the TCP connection may cause a problem. If one TCP segment is dropped or lost, HOL blocking may cause delays in all segments in the sender's TCP buffer, until the dropped segment is recovered. SCTP adopts a multi-stream feature to alleviate this kind of problem. SCTP is allowed to open a number of independent connections via logical streams. Because connections in different streams are independent, segments in different streams don't affect each another. Hence, HOL blocking is a problem within a stream, not across streams. By applying SCTP to the Diameter protocol, a single persistent connection is maintained between NAS and the AAA server. A number of authentication requests from different users are delivered via multiple streams, in which one authentication request corresponds to one stream. A pipelining request is not necessary, because streams are independent.

3. 2 Silly Window Syndrome

In environments in which the sender application generates messages slowly or the receiver application uses them slowly, or both cases occur simultaneously, SWS can arise. For example, if TCP sends segments containing only one byte of data, this is one byte of user data in a 41-byte datagram. The overhead, however, is 40 bytes, which indicates that the operation is quite inefficient. A number of mechanisms to avoid SWS were proposed. The two mechanisms of particular interested in this paper are Nagle's algorithm and Delayed Acknowledgment. Nagle's algorithm works with the sender TCP. This algorithm constrains the sender TCP to delay until either the acknowledgments return or sufficient data has accumulated to fill a maximum-size segment (MSS). Nagle's algorithm is not used in SCTP. Delayed Acknowledgment (Delayed ACK) is proposed for a slow receiver application. The receiver TCP with Delayed ACK does not immediately send an acknowledgment. The receiver TCP delays until there is a reasonable amount of memory available in its receiver buffer. In Delayed ACK, the acknowledgment should not be delayed more than 500 ms.

4. Simulation

We utilize the NS-2 [9] simulator for the simulation. In particular, we selected IEEE 802.16 [10] for the access network in the model. The IEEE 802.16 network uses PKM for authentication. PKMv2 can now support Extended Authentication Protocol (EAP) [11] for authentication. We used the ns-2 simulation module for WiMAX developed by NIST [12]. In the model, a hundred Mobile Stations (MSs) are connected to the Base station (BS) via the IEEE 802.16 access network. Mobile Stations act as peers, and BS acts as an authenticator (AUTH). A peer generates a request for

authentication at a rate given as a parameter in the simulation. AS is two hops from AUTH via the public Internet. Diameter and TCP were selected as the AAA protocol and the transport protocol, respectively. The connection between AUTH and the AAA sever was set to 1.5 Mbps with a 10 millisecond delay.

We examine the effectiveness of the multi-stream in SCTP in the simulation. As shown in Figure 2, we compare the authentication delay with respect to the error rate in the connection between NAS and the AAA server. Figure 2 compares the three different combinations of the AAA protocol; Diameter/SCTP, Diameter/TCP and RADIUS/UDP. The operation of Diameter and RADIUS is quite similar in EAP. These two protocols handle the same number of EAP messages. The differences are in the transport protocol and in the size of the overhead incurred in the EAP message.

As the error rate increases, the delay difference between TCP and SCTP increases. With SCTP, authentication delay is reduced by a maximum of 37.5%. If the error rate is 5%, the difference in the authentication delay between TCP and SCTP is about 0.5 seconds. The error rate increases to 19%, and, the difference increases by about 1.25 seconds. The reason is that SCTP's multi-stream prevents HOL blocking, because the effect of packet loss in one stream is isolated within that stream. In Figure 2 we also compare the authentication delay between UDP and TCP/SCTP. UDP is free of HOL blocking. Therefore, the authentication delay is less than both TCP and SCTP at a lower error rate. However, as the error rate increases, the authentication delay in UDP increases exponentially, because of retransmission in RADIUS, to recover from a UDP segment error.

Figure 3 shows the comparison of two parameters with and without Nagle's algorithm: The parameters are the authentication delay and the number of TCP segments transmitted. As shown in Figure 3, Nagle's algorithm increases the authentication delay as the number of nodes increases. This is because of the size of messages generated by Diameter. In general, Diameter messages are smaller than those in MSS. Hence, a message can be delayed until either the size of data scheduled for transmission is greater than MSS or until the acknowledgments return. This extra delay increases the overall authentication delay. However, a comparison with respect to the number of TCP segments is contrary to this result. Here, we calculate the average number of TCP segments, to authenticate a single peer. The basic idea of Nagle's algorithm is to combine small segments into a single large segment. That is why the average number of TCP segments with Nagle's algorithm is smaller than without Nagle's algorithm. Nagle's solution increases the efficiency by 38%.

Figure 4 shows a comparison with and without delayed ACK. Figure 4 indicates that Delayed ACK does not influence the authentication delay, in contrast to Nagle's algorithm. Because most receivers participating in the authentication protocol respond to a message immediately, Delayed ACK doesn't occur.

Figure 5 illustrates how Nagle's algorithm and Delayed ACK can reduce the network traffic load. With Delayed

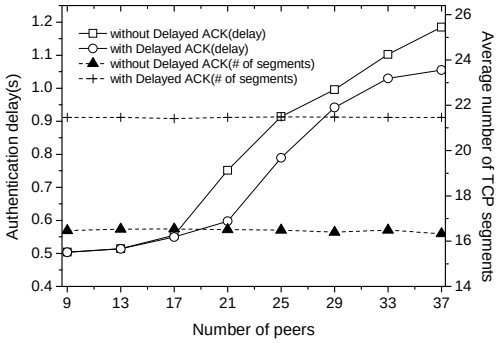

Figure 6. Comparison with and without Delayed ACK for traffic congestion

ACK, the number of packets in the network is 70% less than the case where there is no SWS avoidance mechanism, because of a reduction in the number of ACK messages. With Nagle's algorithm, the number of packets in the network is not much greater than the case where there are no SWS avoidance solutions. If there are 9 nodes in the network, the number of packets is 21. The number of nodes increases to 37 and the number of packets is reduced to 13. The number of packets in Nagle's algorithm and Delayed ACK increase by 38% and 23%, respectively.

A reduction in the total number of packets is obvious for traffic congestion. Traffic congestion arises from multiple connections between NAS and the AAA server. More rarely, problems of power supply cause traffic overflow. If the AAA server is disabled, all messages are blocked. Then, restoration of the AAA server results in its flooding with numerous messages and authentication requests. SWS avoidance mechanisms deal with network congestion via a decrease in the number of packets.

Figure 6 shows the comparison of performances with and without Delayed ACK for traffic congestion. The left-hand and right-hand axes in Figure 6 show a comparison of the authentication delay and the average number of TCP segments, respectively. The average number of TCP segments is constant with respect to the number of nodes, but only if the difference is constant. This is because the number of segments required to authenticate a peer is constant. Authentication delays with and without Delayed ACK are quite similar up to 17 nodes. The reason is that segments from the 17 peers do not incur congestion in the network. As the number of peers exceeds 17, TCP with Delayed ACK outperforms TCP without Delayed ACK. Fewer segments decrease the queuing delay, which decreases the overall authentication delay. We observe that the solution with Delayed ACK is an average of 23% better than without Delayed ACK, in terms of the number of packets.

5. Conclusion

The expansion of the Internet and the coexistence of various network services is at the heart of information flooding. AAA handles important information associated with the user and the service provider. Note that the efficiency of the AAA system influences the overall

network performance. Despite the fact that the problems and solutions for AAA performance are known, very few attempts were made to verify their effectiveness. We concentrated on two AAA issues: HOL and SWS. We analyzed these problems and verified existing solutions. As a result of the simulation using NS-2, we conclude that well known solutions to HOL and SWS problems increase the performance of AAA by an average improvement of 33%.

References

[1] B. Aboba *et al.*, "Authentication, Authorization and Accounting (AAA) Transport Profile," RFC 3539, Jun. 2003.

[2] IETE AAA WG(Working Group). *available at* http://tools.ietf.org/wg/aaa/

[3] R Ekstein *et al.*, "AAA Protocols: Comparison between RADIUS, Diameter, and COPS", *IETF NASREQ WG INTERNET-DRAFT*, draft-ekstein-nasreq-protcomp-00.txt, Oct. 2000.

[4] P. Calhoun *et al.*, "Diameter mobile IPv4 application," RFC 4004, Aug. 2005

[5] A. Yegin *et al*,, "AAA Mobile IPv6 Application Framework", *IETF MIP6 WG, INTERNET-DRAFT*, draftyegin-mip6-aaa-fwk-00.txt, Aug. 2004.

[6] C. Rigney *et al.*, "Remote Authentication Dial In User Service (RADIUS)," RFC 2058, Jun. 2000.

[7] P. Calhoun *et al.*, "Diameter base protocol," RFC 3588, Sep. 2003.

[8] R Ekstein *et al*., "AAA Protocols: Comparison between RADIUS, Diameter, and COPS," *IETF NASREQ WG INTERNET-DRAFT*, draft-ekstein-nasreq-protcomp-00.txt, Oct. 2000.

[9] Network Simulator NS-2. *available at* http://www.isi.edu/nsnam/ns/

[10] IEEE 802.16-2004, IEEE standard for local and metropolitan area networks part 16: air interface for fixed broadband wireless access systems, Oct. 2004.

[11] B. Aboba *et al.*, "Extensible Authentication Protocol (EAP) ," RFC 3748, Jun. 2004.

[12] NIST homepage. *available at* http://w3.antd.nist.gov/seamlessandsecure/toolsuite.html.