Key Caching Mechanism for AAA over Mobile IP

Shin-Ming Cheng, Phone Lin, and Wei-Hou Chen
Department of Computer Science & Information Engineering,
National Taiwan University, Taipei, Taiwan
Email: shimi@pcs.csie.ntu.edu.tw, plin@csie.ntu.edu.tw, cwh@pcs.csie.ntu.edu.tw

***Abstract*— RFC 2977 proposes the** *Authentication, Authorization, Accounting* **(AAA) framework architecture for mobile IP to protect signaling messages from eavesdropping by malicious attackers. The AAA server in the home network (i.e., AAAH) generates and distributes session keys to** *Mobile Node* **(MN),** *Foreign Agent* **(FA), and** *Home Agent* **(HA), which is known as the authentication procedure. The procedure for session key distribution introduces extra signaling overhead in the mobile IP network, which is not considered in RFC 2977. To resolve this issue, this paper proposes a key caching algorithm named AKC. With AKC, the MN can be authenticated locally without involving the AAAH. The simulation experiments are conducted to investigate the performance of the AKC algorithm.**

I. Introduction

With the rapid development of the mobile networking technologies, mobile computing over Internet has become one of the major research directions. Users with mobile equipment enjoy Internet services through wireless networks anywhere and any time. To efficiently route the packets for the mobile users in the Internet, the working group, *Internet Engineering Task Force* (IETF), proposed Mobile IP [1] as the routing protocol. With Mobile IP, the *Mobile Node* (MN) can receive the data in the foreign network by using the IP address assigned by the home network. Two kinds of assistant nodes are introduced in the mobile IP network, including the *Home Agent* (HA) in the home network and *Foreign Agent* (FA) in the foreign network. The HA and FA are responsible to route the packets for an MN through the home network and foreign network, respectively.

In mobile IP, before delivering the user data, signals are exchanged among MN, FA, and HA to establish routing tables for the MN, which is known as the registration procedure. Details of the registration procedure can be found in [1]. The registration procedure plays a very important role in the mobile IP network due to the fact that all security attacks (including the eavesdropping attack, the replay attack, and the man-in-middle attack [2], etc.) may be initiated through this procedure. To make sure the legal access of an MN to the FA in the registration procedure, the working group IETF proposes the RFC 2977 [3], the mobile IP *Authentication, Authorization, Accounting* (AAA) framework architecture. The AAA server in the home network (also known as AAAH) generates and distributes session keys to the MN, FA, and HA. The procedure for session key distribution introduces extra signaling overhead in the mobile IP network, which is not considered in the RFC 2977.

To resolve this issue, the previous works [4][5][6][7][8] were conducted. [4] proposed a mechanism to minimize the number of the signaling messages. In [4], the authors only proposed the mechanism but didn't conduct any performance evaluation to justify the advantages of the proposed mechanisms. [5][6] proposed a mechanism to resolve this issue in the heterogeneous network (e.g., WLAN/3G network) by applying the authentication mechanism of the cellular network on WLAN, which needs heavy modification of the mobile IP protocol, and is not easily deployed. [7][8] attempted to modify the AAA procedure in the mobile IP AAA framework to reduce the signaling overhead, which is also difficult to be implemented in the existing mobile IP network.

In this paper, based on the standard mobile IP AAA framework, we propose a key caching algorithm named AKC to resolve this issue[1]. Our algorithm is considered practical and to be easily installed in the existing mobile IP network. In AKC, when the MN is authenticated by the home network at the first time, it can bring sets of session keys back to the local AAA server for the following authentication. The MN can be authenticated locally without involving the AAAH, and the signaling cost can be reduced. We conduct simulation experiments to evaluate the performance of the AKC algorithm.

The rest of the paper is organized as follows. Section II describes the mobile IP AAA authentication framework. Section III proposes the key caching algorithm, AKC. Section IV evaluates the performance of the AKC algorithm. Finally, section V concludes our study.

II. Mobile IP AAA Framework

This section illustrates the mobile IP AAA framework. As shown in Figure 1, the AAA server is introduced in the mobile IP network to provide authentication, authorization, and accounting services. The AAA servers involved in the home network and foreign network are called as Home AAA server (AAAH) and Foreign AAA server (AAAF), respectively. The Diameter protocol [9] is run between AAAH and AAAF, between HA and AAAH, and between FA and AAAF to support secured message delivery among these nodes. To simplify our description, we use ADA and SDA to denote the service area of an agent (i.e., FA and HA) and the service

[1]This paper is the prior work of the paper "Study on Key Caching for Mobile IP AAA" that has been submitted to IEEE JSAC.

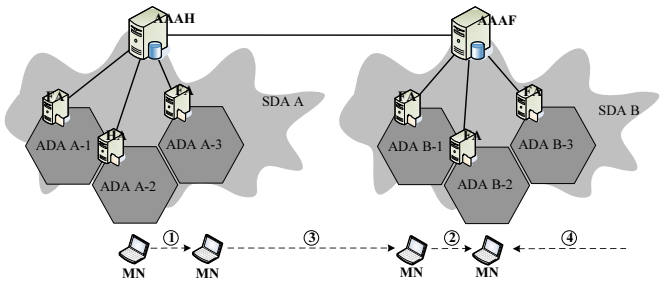

Fig. 1. The mobile IP AAA framework architecture

area of an AAA server, respectively. One SDA may cover one or more ADAs. In this framework, the mobile IP AAA authentication procedure is exercised to update MN's location information when the MN moves between two ADAs. Suppose that the MN moves from ADA x to ADA y. Four cases are considered for user movement.

Case I: Intra AAAH Movement. ADA x and ADA y are within the same SDA served by the AAAH, e.g., from ADA A-2 to ADA A-3; see Figure 1 (1).

Case II: Intra AAAF Movement. ADA x and ADA y are within the same SDA served by the AAAF, e.g., from ADA B-1 to ADA B-2; see Figure 1 (2).

Case III: Inter AAAH and AAAF Movement. ADA x and ADA y are within the SDA (served by the AAAH) and the SDA (served by the AAAF), respectively, e.g., from ADA A-3 to ADA B-1; see Figure 1 (3).

Case IV: Inter AAAF Movement. ADA x and ADA y are within different SDAs served by different AAAFs; see Figure 1 (4).

Figure 2 illustrates the message flow for the mobile IP AAA authentication procedure. We consider Case III, Inter AAAH and AAAF user movement. For other cases, the message flows are similar, whose details are not presented in this paper. Through the Diameter protocol, Mobile Security Associations (MSAs) are pre-set up between AAAH and AAAF, between HA and AAAH, and between FA and AAAF. The MSA between MN and AAAH is set up when the mobile user subscribes the service. The MSA supports the mutual authentication on a message delivery between two network nodes. An MSA consists of a hash algorithm, a shared session key, and an agreement on the Security Parameter Index (SPI). The hash algorithm is used to compute keyed hashes over messages. The shared session key is the secret for the hash algorithm. The SPI indicates the type of the hash algorithm and secret, and is the identifier of the MSA. For more details of an MSA, readers may refer to [1]. To simplify our description, we use k_{x-y} to denote the shared session key of network nodes x and y. To enable authentication of a message (sent from node x to node y), node x appends an authenticator to this message, and then sends it to node y. Node y checks the authenticator by taking the following three actions: (i) looks up the MSA based on the SPI; (ii) re-computes the keyed hash by using the shared session key k_{x-y}; (iii) verifies whether the re-computed

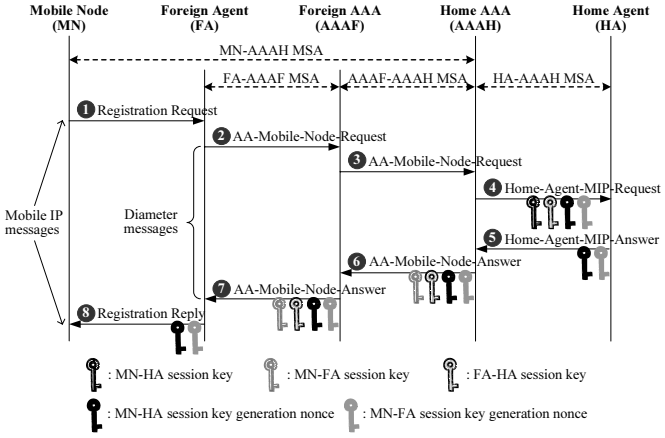

Fig. 2. The message flow for the mobile IP AAA authentication procedure

result is equal to the content in the received authenticator. A validation timer is maintained for the shared session key k_{x-y} to prevent the shared key from exposing by malicious crackers. When the validation timer of a shared session key expires, a new session key is regenerated.

The purposes of the mobile IP AAA authentication procedure include: (i) to identify and authenticate an MN; (ii) to update MN's correspondent IP address in the HA; (iii) to authorize an MN to use the services in the foreign network; (iv) to distribute the shared session keys, k_{MN-FA}, k_{MN-HA}, and k_{FA-HA}. As shown in Figure 2, the mobile IP AAA authentication procedure consists of eight steps, and the details are given below:

Mobile IP AAA Authentication Procedure:

Step 1. When an MN roams from the home network to the foreign network, it sends a mobile IP message, Registration Request, to the FA, which contains the *Network Authentication Identity* (NAI). A NAI consists of two parts, user part and realm part, and is in the form of "user@realm". The user part indicates MN's identity, and the realm part stores the network identity of MN's home domain.

Step 2. Upon receipt of the Registration Request message, the FA updates its visitor list (containing the NAIs of all MNs residing in its ADA). Suppose that the FA is served by the AAAF. Then the FA sends the AAAF a Diameter message, AA-Mobile-Node-Request, which encapsulates the Registration Request message.

Step 3. When receiving the AA-Mobile-Node-Request message, the AAAF detects that the requested MN is not in its SDA by checking the realm part of MN's NAI. Then the AAAF forwards the AA-Mobile-Node-Request message to MN's AAAH by using the realm part in the NAI.

Step 4. The AAAH checks the AA-Mobile-Node-Request message to determine whether the MN is a legal user by using the MSA between the MN and the AAAH. Then, the AAAH generates three session

keys $(k_{MN-FA}, k_{MN-HA}, k_{FA-HA})$ and two nonces[2] (n_{MN-FA}, n_{MN-HA}) for this MN.

The AAAH sends the HA a Diameter message, Home-Agent-MIP-Request, which contains the two session keys (k_{MN-HA}, k_{FA-HA}), two nonces (n_{MN-FA}, n_{MN-HA}), and the Registration Request message.

Step 5. Upon receipt of the Home-Agent-MIP-Request message, the HA extracts the Registration Request message from this message. The two session keys (k_{MN-HA}, k_{FA-HA}) will be used to make sure the legal delivery for the signaling between MN and HA, and between FA and HA, respectively. The HA generates a mobile IP message, Registration Reply, to encapsulate the two nonces (n_{MN-FA}, n_{MN-HA}) in this message. Then the HA sends a Diameter message, Home-Agent-MIP-Answer, to the AAAH, where the Registration Reply message is carried in this message.

Step 6. When receiving Home-Agent-MIP-Answer, the AAAH generates a Diameter message, AA-Mobile-Node-Answer, which encapsulates the Registration Reply message and the two session keys (k_{MN-FA}, k_{FA-HA}) obtained in Step 4. Then the AAAH sends the AA-Mobile-Node-Answer message to the AAAF.

Step 7. The AAAF forwards the received AA-Mobile-Node-Answer message to the FA.

Step 8. Upon receipt of the AA-Mobile-Node-Answer message, the FA retrieves the two session keys (k_{MN-FA}, k_{FA-HA}) from this message. The two keys are for the secured message delivery between MN and FA and between FA and HA, respectively. Then the FA sends the MN the Registration Reply message which contains the two nonces (n_{MN-FA}, n_{MN-HA}).

After receiving Registration Reply, the MN uses the two nonces (n_{MN-FA}, n_{MN-HA}) to derive two session keys (k_{MN-FA}, k_{MN-HA}). The two session keys will be used to secure the message delivery between MN and FA and between MN and HA. The MN starts a validation timer for the two session keys. When the validation timer expires, or the MN moves to another ADA, the mobile IP AAA authentication procedure will be exercised to get a new session key set.

After the execution of the mobile IP AAA authentication procedure, the signaling exchanges for the mobile IP protocol among the MN, FA, and HA are secured.

For Case I (i.e., intra AAAH movement), Steps 1, 3, 4, 5, 6, and 8 are executed. For Cases II and IV (i.e., intra AAAF movement and inter AAAF movement), Steps 1-8 are executed.

We note that in this procedure, when the validation timer of a session key set expires, or the MN moves to another ADA, the Mobile IP AAA authentication procedure should be exercised to get a new session key set from AAAH. Extra signaling overhead is introduced into the mobile IP network. To resolve this issue, in the next section, we propose a key caching algorithm AKC for the mobile IP AAA authentication procedure.

[2]The nonces n_{MN-FA} and n_{MN-HA} are used to generate session keys k_{MN-FA} and k_{MN-HA}, respectively [10]. An MN will get these two nonces in the Registration Reply message and derive the corresponding session key by the shared session key in MN-AAAH MSA [11].

III. The AKC Algorithm

This section describes the AKC algorithm. With AKC, the MN can be authenticated locally (i.e., through AAAF) without involving the AAAH server. We add caches in AAAF and HA to cache session key sets. The mobile IP AAA authentication procedure is slightly modified so that the authentication procedure can be finished in the foreign network. We discuss the AKC algorithm in two cases:

Case 1: *The MN moves into a new SDA, or all cached session key sets are run out.* Steps 4-7 in the mobile IP AAA authentication procedure are modified: In Step 4, the AAAH generates K session key sets and K nonce sets, $(k_{MN-FA,1}, k_{MN-HA,1}, k_{FA-HA,1})$ $(n_{MN-FA,1}, n_{MN-HA,1}), (k_{MN-FA,2}, k_{MN-HA,2},$ $k_{FA-HA,2})(n_{MN-FA,2}, n_{MN-HA,2})$, ..., $(k_{MN-FA,K},$ $k_{MN-HA,K}, k_{FA-HA,K})(n_{MN-FA,K}, n_{MN-HA,K})$ for the MN. Then the AAAH sends the HA the Home-Agent-MIP-Request message containing K two-key sets and two-nonce sets, $(k_{MN-HA,1}, k_{FA-HA,1})(n_{MN-FA,1}, n_{MN-HA,1})$, $(k_{MN-HA,2}, k_{FA-HA,2})(n_{MN-FA,2}, n_{MN-HA,2})$, ..., $(k_{MN-HA,K}, k_{FA-HA,K})(n_{MN-FA,K}, n_{MN-HA,K})$. In Step 5, upon receipt of the Home-Agent-MIP-Request message from AAAH, the HA caches the K two-key sets and encapsulates K two-nonce sets in the Registration Reply message. In Step 6, the AAAH sends the AAAF the AA-Mobile-Node-Answer message containing the Registration Reply message and K two-key sets $(k_{MN-FA,1}, k_{FA-HA,1})$, $(k_{MN-FA,2}, k_{FA-HA,2})$, ..., $(k_{MF-HA,K}, k_{FA-HA,K})$. Note that to enable the authentication done in the AAAF (i.e., locally), there should be an MSA existing between AAAF and MN. This MSA can be established by sending all related information for the MSA (between AAAH and MN) to the AAAF in Step 6. In Step 7, upon receipt of the AA-Mobile-Node-Answer message, the AAAF caches K two-key sets and K two-nonce sets.

Case 2: *If there are valid cached session key sets, the MN moves from one ADA to another belonging to the same SDA, or the validation timer of the currently used session key set expires.* When the validation timer of the currently used session key set expires, only Steps 1, 2, 7, and 8 need be performed for the local authentication through AAAF. In the end of Step 2, after the AAAF receives the AA-Mobile-Node-Request message, the AAAF authenticates the MN by using the MSA between MN and AAAF. In Step 7, the AAAF replies the FA the AA-Mobile-Node-Answer message containing a cached two-key set.

When the MN moves from one ADA to another belonging to the same SDA, besides Steps 1, 2, 7, and 8, the FA

and HA exchange two mobile IP messages, Registration Request and Registration Reply, between Steps 7 and 8 to update MN's location information in the HA.

Note that AKC does not modify the authentication procedure of the MN, and the MN executes the authentication procedure as usual.

IV. Performance of AKC with Fixed Cache Size

This section conducts simulation experiments to investigate the performance for AKC with a fixed cache size K. The simulation technique used in the paper is similar to that used in [12], and the details are omitted. Let N be the number of session key-set retrievals from AAAH while the MN resides in an SDA with the cache size K. Let $C(K)$ be the total bandwidth consumption for signaling cost of AKC with fixed cache size K while an MN resides in an SDA. In order to preciously calculate $C(K)$, we assume β, γ, and δ as the sizes of a mobile IP message (see Steps 1 and 8 in Figure 2), a Diameter message (see Steps 2-7 in Figure 2), and a shared session key or a nonce, respectively. Let N_m and N_d denote the number of mobile IP message and the number of Diameter message exchanged in the mobile IP network while the MN resides in an SDA with the cache size K, respectively. Let N_k denote the number of session key and nonce carried in the signaling messages (i.e., mobile IP and Diameter messages) exchanged in the mobile IP network while the MN resides in an SDA with the cache size K. The $C(K)$ function for AKC with the cache size K, is expressed as follows:

$$C(K) = \beta * N_m + \gamma * N_d + \delta * N_k,$$

In this paper, we investigate the expected value $E[N]$ of N and the $C(K)$ performance for AKC algorithm with the fixed cache size K. Assume that the validation time of a session key set, t_v, is exponential distribution with mean $\frac{1}{\mu_v}$. The ADA residence times are assumed to be exponentially distributed with mean $\frac{1}{\eta_a}$. The impacts of several input parameters are discussed as follows.

Effects of K and Ratio μ_v/η_a on $E[N]$. Figure 3 plots $E[N]$ against K with various μ_v/η_a setups. This figure indicates that $E[N]$ increases as μ_v/η_a increases. A larger μ_v/η_a implies that the setup for the expiration timer of shared session keys is shorter. It is more likely that the MN changes the key. Thus more key-set retrievals from the AAAH are executed.

The figure also shows that $E[N]$ is a decreasing function of K, which indicates that as the key cache size increases, the MN has better chance to be authenticated locally. When $K \geq 16$, this phenomenon becomes insignificant.

Effects of K and Ratio μ_v/η_a on $C(K)$. Figure 4 plots $C(K)$ as functions of K and μ_v/η_a. This figure shows that as K increases, $C(K)$ decreases and then slightly increases. As K increases, we have the following two facts:

Fact 1. The number of session key-set retrievals form AAAH drops (i.e., $E[N]$ decreases), which causes smaller $C(K)$ values.

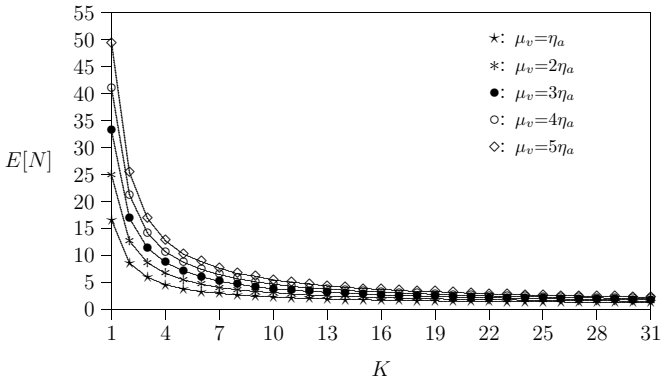

Fig. 3. Effects of μ_v/η_a and K on $E[N]$

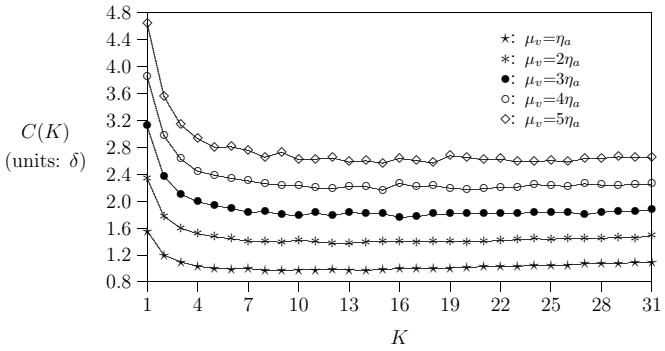

Fig. 4. Effects of μ_v/η_a and K on $C(K)$ ($\alpha = 1$, $\beta = 3\delta$, and $\gamma = 12\delta$)

Fact 2. More bandwidth are consumed to deliver the multiple key sets from AAAH, which increases the $C(K)$ cost.

When K is small, Fact 1 dominates. On the other hand, when K is large, Fact 2 balances the effects of Fact 1. Thus, we observe that as K increases, $C(K)$ decreases and then slightly increases. The figure also shows that as μ_v/η_a increases, $C(K)$ increases. As μ_v/η_a increases, the $E[N]$ increases, and larger $C(K)$ values are observed.

V. Conclusion

In mobile IP AAA, the authentication procedure (from the MN to the AAA server in the home network) is exercised for every location update and every expiration of the shared session keys, which introduces extra signaling overhead into the mobile IP network. To resolve this issue, this paper proposed a key caching algorithm, AKC, to reduce the signaling overhead introduced by the mobile IP AAA procedure. With AKC, when the MN is authenticated by the home AAA server (i.e., AAAH) at the first time, it can bring multiple session key sets to the key cache in the local AAA server (i.e., AAAF), and then the MN can be authenticated locally without involving AAAH. Simulation experiments were conducted to investigate the performance of our proposed algorithm. We observed the following results.

- Increasing the cache size, K, can significantly decrease the expected number $E[N]$ of session key-set retrievals

from AAAH while the MN resides in an SDA. When cache size is large enough (in our study, $K \geq 16$), the improvement becomes insignificant.

- The bandwidth consumption cost, $C(K)$, for AKC with cache size K, are concave curves. That is, as K increases, $C(K)$ drops quickly, and then slightly increases. There exists an optimal K value that minimizes $C(K)$.

REFERENCES

[1] C. E. Perkins, "IP mobility support for IPv4," RFC 3344, Aug. 2002.

[2] J. D. Solomon, *Mobile IP the Internet Unplugged*. Prentice Hall, 1998.

[3] S. Glass, T. Hiller, S. Jacobs, and C. E. Perkins, "Mobile IP authentication, authorization, and accounting requirements," RFC 2977, Oct. 2000.

[4] M. Cappiello, A. Floris, and L. Veltri, "Mobility amongst heterogeneous networks with AAA support," in *Proc. IEEE ICC'02*, vol. 4, Apr. 28–May 2, 2002, pp. 2064–2069.

[5] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun. Mag.*, vol. 10, no. 6, pp. 52–61, Dec. 2003.

[6] H. Kim and H. Afifi, "Improving mobile authentication with new AAA protocols," in *Proc. IEEE ICC'03*, vol. 1, May 11–15, 2003, pp. 497–501.

[7] M. Long, C.-H. Wu, and J. D. Irwin, "Localized authentication for wireless LAN internetworking roaming," in *Proc. IEEE WCNC'04*, vol. 1, Mar. 13–17, 2004, pp. 264–267.

[8] C. Politis, K. A. Chew, N. Akhtar, M. Georgiades, R. Tafazolli, and T. Dagiuklas, "Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun. Mag.*, vol. 11, no. 4, pp. 76–88, Aug. 2004.

[9] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter base protocol," RFC 3588, Sept. 2003.

[10] P. Calhoun, T. Johansson, C. E. Perkins, T. Hiller, and P. J. McCann. (2004, Aug.) Diameter mobile IPv4 application. Internet draft. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-mobileip-20.txt

[11] C. E. Perkins and P. Calhoun, "Authentication, authorization, and accounting registration keys for mobile IPv4," Mar. 2005.

[12] S.-R. Yang and Y.-B. Lin, "Performance evaluation of location management in UMTS," *IEEE Trans. Veh. Technol.*, vol. 52, no. 6, pp. 1603–1615, Nov. 2003.