A Lightweight Authentication Protocol with Local Security Association Control in Mobile Networks

Wei Liang Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University, Raleigh, NC 27695

Abstract— **In this paper, we propose a new lightweight authentication protocol with local security association (SA) control to locally authenticate an inter-domain roaming user efficiently based on its mobility and traffic patterns in mobile networks. We first design a protocol to establish a local SA for authenticating the roaming user securely. Then, in order to determine the life time for the local SA, an authentication cost function is proposed to evaluate the authentication efficiency with the concern of risk, mobility and traffic patterns. The optimal life time of the local SA is determined by minimizing the authentication cost function. The performance of the proposed protocol is analyzed with respect to authentication cost under different mobility and traffic patterns. Comparing to DIAMETER, the proposed approach outperforms DIAMETER for macro-mobility users with high volume of authentication requests.**

Key Words: *Mobile networks, authentication, security association.*

I. Introduction

The increasing demand for communications over mobile networks has imposed challenges on security and quality of service (QoS) due to unprotected and bursty open mediums. To protect the service in mobile networks, authentication is proposed to identify mobile users (MUs) and negotiate secret credentials such as keys and cryptographic algorithms [1].

A strong authentication protocol can guarantee the security by protecting the information secrecy, data integrity and resource availability with negotiated secret credentials and complicated cryptographic algorithms. In an authentication process, an MU is required to submit secret materials such as certificates and challenge/response values for verification. The verification is performed with a security association (SA), which is a relationship that affords security services with parameters such as keys and algorithms. As a result, the authentication can protect authorized access to network resource for legitimate users. The information secrecy and data integrity can also be guaranteed by using the negotiated secret credentials for encryption and message authentication, which is extremely critical to the MUs in military movement.

Meanwhile, the authentication has great effect on the QoS such as authentication latency and cost due to additional overheads in mobile networks [2], [3]. When public/private-key based authentication mechanism is applied, the computation complexity of encrypting/decrypting data with public/private keys consumes much time and power [2]. Furthermore, denial of service (DoS) attack to public/private-key based authentication is found although it can be mitigated with client puzzle technique [4]. Therefore, secret key based challenge/response authentication mechanism is widely used in mobile networks [5]–[7]. In challenge/response authentication, due to the lack of end-to-end SA between the foreign access router and the home network of the roaming MU, the credentials of the MU are encrypted and transmitted from a foreign network to a home network hop-by-hop among authentication servers [8]. The transmission and encryption/decryption of credentials affect many QoS parameters such as authentication cost in terms of signaling and encryption/decryption cost and authentication delay, which further affect other parameters such as call dropping probability.

Since the authentication affects both of security and QoS, the design of an authentication protocol should consider security and efficiency, simultaneously. To this end, many authentication protocols are proposed [1], [5]–[15]. These papers either focus on providing strong security to the communication [6], [9], [12]–[15], or consider how to improve the authentication efficiency with fast key distribution or re-authentication in a special scenario [1], [5], [7], [8], [10], [11]. But the effects of the mobility and traffic patterns of the MU on the authentication efficiency as well as the risk that credentials are being cracked are not considered, all of which are extremely important for military operation. In the basic challenge/response authentication [9], the MU is required to be authenticated from the home authentication server (HAS) *each time* before the MU obtains service. Thus, the accumulated authentication cost is greatly increased with the traffic pattern of authentication requests. Although a permanent local SA in the foreign network can reduce the authentication costs, the establishment of local SA incurs the overhead of signaling. Moreover, the long term existing SA will compromise the security due to potential brute-force attacks.

In this paper, we propose a lightweight authentication protocol with local SA control for efficient authentication in mobile networks. We first propose an authentication protocol to establish a local SA for a visiting MU out of its home network. Then, the total authentication cost for the MU, which includes the risk estimation of the local SA, is evaluated with the concern of the traffic and mobility patterns of the MU. Based on the evaluation of the cost, an optimal life time of

the local SA is determined to minimize the authentication cost.

The rest of this paper is organized as follows. In Section II, we introduce the security association and authentication architecture needed to implement our protocol with local SA control. We propose a lightweight authentication protocol with local SA control in Section III by describing the proposed authentication protocol and deriving the optimal life time of the local SA based on the authentication cost function. In Section IV, we evaluate the proposed protocol with local SA control by comparing to DIAMETER. Finally, we draw a conclusion in Section V.

II. Security Association and Authentication Architecture

In this section, we introduce the concept of *security association* (SA) first. Then, we illustrate an authentication architecture in mobile networks. The SA and the authentication architecture make up the environment in which we implement our proposed authentication protocol with local SA control.

A. Security Association

As defined in IP security architecture (IPsec), a security association (SA) is a one-way relationship between communicators that affords security services to the traffic with parameters such as security parameters index (SPI), lifetime, cryptographer algorithm, and keys [16]. When an SA is established and modified, these parameters can be modified simultaneously with authentication protocols.

The SAs can be established and modified by using Internet security association and key management protocol (ISAKMP), secure socket layer (SSL) or transport layer security (TLS). In these protocols, SSL and TLS are two protocols commonly used in mobile networks. SSL is a standard for encrypted client/server communication between network devices, working with public/private keys. TLS is an IETF standard with the goal to produce an Internet standard version of SSL [17]. However, the algorithms applied in this protocol are time-consuming, especially when the client is an MU with limited calculation capability [2]. The extended authentication time affects many QoS parameters such as packet delay and call dropping probability.

In order to facilitate the authentication in mobile networks, secret key based authentication is widely adopted [9]. In particular, challenge/response authentication requires the roaming MU to submit a response value for authentication *each time*, which is encrypted with a challenge value, a random value, and an SA shared between the MU and its home network. The challenge and response values are delivered to the home network of the MU for verification. An authentication approval message is returned if the authentication is granted. However, whenever an MU initiates a service request or crosses the boundaries of subnetworks, authentication will be triggered, which is related with the mobility and traffic patterns of the roaming MU and imposes a heavy burden to deliver the authentication messages between networks.

Therefore, we propose a lightweight authentication protocol to establish a controlled local SA and avoid remote authentication with the consideration of mobility and traffic patterns of the roaming MU. The protocol is based on the authentication architecture introduced as follows.

B. An Authentication Architecture in Mobile Networks

In order to deliver the authentication messages between mobile networks, many authentication architectures are proposed [8], [18], [19]. In our paper, we consider the authentication, authorization, and accounting (AAA) architecture that is initially proposed by IETF for Mobile IP networks and is being deployed in 3G systems.

An AAA architecture is composed of local AAA servers (LASs), home AAA servers (HASs), and proxy AAA servers (PASs). An LAS is an AAA server that serves for the visiting MUs in a network domain for AAA functions. An HAS is an AAA server in a network domain that only serves for the MUs who subscribe services in the network domain. A PAS is an AAA server that takes charge of relaying the AAA messages between different AAA servers. All of these AAA servers are organized hierarchically with shared SAs between the AAA server in lower layer and the AAA server in higher layer.

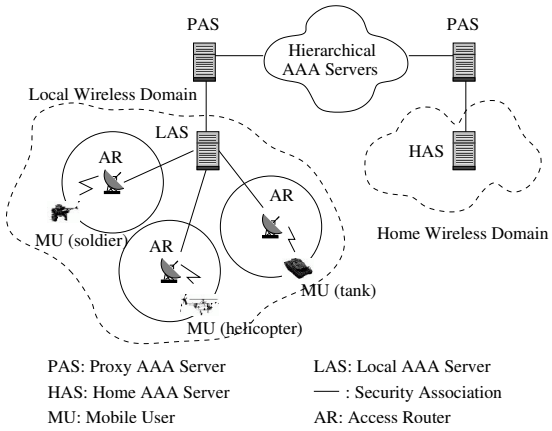


Fig. 1. AAA Architecture in Mobile Networks.

An example of this AAA architecture is shown in Fig. 1. As we can see, an LAS is located in a local mobile network, serving for visiting MU. There are many access routers (ARs) in a mobile networks that share SAs with the LAS. These ARs also provide communication services for the roaming MUs. When an MU requests network service from an AR, the LAS will relay the authentication request of the MU to its HAS through the PASs and the hierarchical AAA servers. If the authentication is granted, the MU can obtain the network resources. Otherwise, the request for services is rejected. If the MU roams from one subnet to another in the mobile network, same authentication process is required. If the distance between the LAS and the HAS is long, the authentication efficiency in terms of signaling cost for authentication should be considered seriously. Therefore, some methods are proposed to distribute a permanent local SA for

the visiting MU in the local mobile network [7]. However, they do not account for the mobility and traffic patterns of the MU and the permanent life time of the SA will induce the risk of being hacked, which compromises the network security, furthermore may endanger the military operation due to the cracked SA of an MU such as a soldier or a plane.

To consider the efficiency and security with different mobility and traffic patterns, we propose a lightweight authentication protocol with local SA control, which can be implemented based on the AAA architecture. Therefore, it can be applied in various mobile environments including 3G, such as CDMA-2000 and UMTS, and 802.11 networks because AAA architecture has been deployed in these networks.

III. Lightweight Authentication Protocol with Local SA Control

We propose a lightweight authentication protocol with local SA control in this section. First, we provide an overview of the control process. Then, two critical parts of our protocol are introduced. One is to establishment a local SA; the other is to determine the optimal life time of the SA to minimize the authentication cost, which is also effective to reduce the latency and the risk of being attacked.

A. Overview of Lightweight Authentication Protocol

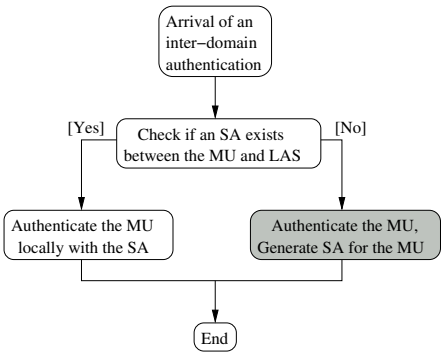
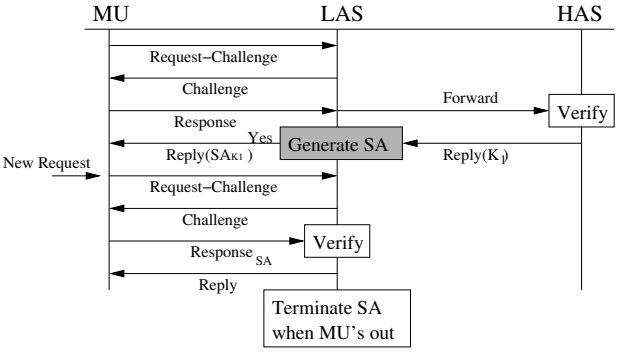


Fig. 2. Overview of Lightweight Authentication Protocol.

The overview of our proposed protocol is illustrated in Fig. 2. When an inter-domain authentication request from a visiting MU comes to the LAS, the LAS first checks if a local SA exists for the MU. If the local SA exists, the LAS authenticates the roaming MU with this SA. Otherwise, the LAS relays the credentials of the roaming MU through AAA architecture to the HAS for authentication. When the authentication is granted, a local SA is generated for the roaming MU. The sequential authentication requests arriving within the life time of the local SA will be processed efficiently with the local SA.

Many papers provide the authentication protocols with shared SA between an MU and an LAS [9]. Therefore, we do not focus on the authentication of the MU locally with shared SA. Instead, we focus on the establishment of the local SA in a mobile network for the roaming MU, which is highlighted in Fig. 2. The establishment of a local SA involves with two problems. One is how to distribute the key securely and efficiently; the other is how to determine the life time of the local SA to minimize the authentication cost and risk.

B. Authentication and Local SA Establishment Protocol



LAS: Local Authentication Server SA: Security Association
HAS: Home Authentication Server MU: Mobile User

Fig. 3. Authentication and Local SA Establishment Protocol.

The signaling diagram of the protocol to authenticate a roaming MU and establish a local SA for sequential authentication requests is shown in Fig. 3. When a foreign MU is requesting services in the local network, an authentication request is sent out to the LAS. The LAS replies a challenge value, a random value, to the MU. The MU encrypts the challenge value with an SA shared with the HAS. The result is a response value and returned to the LAS. Because the LAS has no SA shared with the MU, the LAS relays the response value to the HAS of the roaming MU through the AAA architecture. The HAS of the MU decrypts the response value and compares the result with the challenge value transfered by the LAS. If these two values are matched, the MU is authenticated. Then, a key K_{u1} is generated with the SA shared between the MU and its HAS as follows:

$$K_{u1} = HMAC - MD5(K_0, \{R_1 \| ID_{MU}\}), \tag{1}$$

where K_0 is the pre-shared key in the SA between the MU and its HAS, R_1 is a random value of at least 64 bits. ID_{MU} is the MU's identity. $HMAC - MD5$ is a hash function implemented with MD5. The symbol $\|$ means the two values are linked together. Then, the message that includes the following data is sent to the LAS:

$$\{K_{u1}, ALGORITHM, F_0, F_i, \{R_1, ALGORITHM, F_0\}_{K_0}\}_{K_i}, \tag{2}$$

where K_{u1} is the key generated for the local SA shared between the MU and the LAS, $ALGORITHM$ is the description of the algorithm for the local SA selected by the HAS that will be used for local authentication, F_i is a random number used to avoid replay attack between AAA servers i and $i-1$ in the AAA chaining servers shown in Fig. 4, F_0 is a random number used to avoid replay attack between the MU and the LAS, K_0 is the pre-shared key in the SA between the

MU and its HAS, K_i is the pre-shared key in the SA between AAA servers i and $i-1$ in the AAA chaining servers shown in Fig. 4, the subscripts K_0 and K_i mean that the data in the parenthesis are encrypted with K_0 or K_i, respectively.

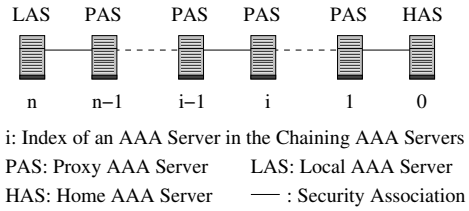


Fig. 4. Demonstration of Chaining AAA Servers.

Then, when the HAS, PAS, LAS and the visiting MU receive the message, the operations of them are shown as:

- *Operation of HAS*: when an HAS receives an authentication request transfered from the associated PAS, the HAS authenticates the MU first. If the authentication is granted, the HAS generates a key K_{u1} with (1) and replies a message like (2) to the PAS.
- *Operation of PAS*: when the PAS receives a message like (2) from an AAA server, the PAS decrypts the message with key K_i and corresponding algorithm in the pre-shared SA. Then, the PAS replies an encrypted value of $F_i - 1$ to the source AAA server to avoid replay attack. After replacing F_i with a new random value, encrypting the message with another pre-shared SA, the PAS sends a message like (2) to the next AAA server.
- *Operation of LAS*: when the LAS receives an authentication approval with the message shown in (2), the LAS decrypts the message with the key and algorithm in the SA shared with the upstream PAS and replies value $F_n - 1$ to the PAS to avoid replay attack, where n is the number of chaining AAA servers. Then, the LAS sends a message $\{R_1, ALGORITHM, F_0\}_{K_0} \| \{LIFETIME\}_{K_{u1}}$ to the visiting MU. Here, $LIFETIME$ is the life time of the local SA and it is calculated at the LAS by optimizing the authentication cost in the next section.
- *Operation of visiting MU*: when the visiting MU receives the replied message from the LAS, the MU decrypts the first part of the message to obtain the value R_1 and generates the key K_{u1} with (1). With key K_{u1}, the value of $LIFETIME$ is obtained. Then, the MU replies value $F_0 - 1$ to avoid replay attack.

When the above operations are finished, a local SA can be established at the visiting MU and the LAS as follows:

SA::={*UID; SPI; ALGORITHM; DIRECTION; KEY; LIFETIME*},

where UID is the unique user identification of the MU that the local SA is used for. In the local SA at the LAS, UID is the identification of the MU. In the local SA at the MU, UID is the identification of the LAS. SPI (Security Parameter Index) is the identification number of the association to differentiate the SA uniquely. ALGORITHM is a description of the algorithm used in this local SA. DIRECTION specifies the association used for packets arriving or leaving, KEY provides the encoding and decoding key for the authentication, which is $K1$ in our proposed protocol. LIFETIME is a time period to keep the SA, which is determined and transfered by the LAS.

Then, the sequential authentication requests sent by the MU can be authenticated with the local SA by using challenge/response mechanism. When the life time of the local SA expires and the MU still stays in current network domain, the local SA is refreshed by sending a message from the LAS to the MU with new key and life time of the new SA. The new key is generated as follows:

$$K_{u2} = HMAC - MD5(K_{u1}, \{R_2 \| ID_{MU}\}), \tag{3}$$

where K_{u2} is the new key, K_{u1} is the old key in the old local SA, R_2 is a new random value, ID_{MU} is the identification of the MU. By encrypting R_2 and life time of the new local SA with the old SA, the parameters of the new local SA can be sent to the MU securely from the LAS.

From the operations of the HAS, PAS, LAS, and the MU, we can see that the security to distribute the key K_{u1} is guaranteed. First, the messages transmitted between the AAA servers are encrypted with the SAs between each two of them with nonce technique. Thus, information secrecy, data integrity are provided and replay attack can be defeated. Second, the transmission of key K_{u1} to the visiting MU from the HAS is done through a random value R_1 with an SA shared between the MU and its HAS, which avoids direct key distribution on the unprotected medium since no encryption is implemented between the visiting MU and the LAS before the authentication. This operation guarantees secure transmission of K_{u1} from the HAS to the MU.

The life time of the SA has great effect on the sequential authentication requests sent by the visiting MU in current network domain. If the authentication requests come within the life time of the local SA, the visiting MU can be authenticated locally with challenge/response mechanism. If the life time of the local SA expires, a new local SA will be generated with additional cost, which affects the authentication efficiency. On the other hand, if the life time of the local SA is very long, the possibility that an SA is being cracked will increase. Therefore, we propose an authentication cost function next with the consideration of the risk that an SA is being cracked. By minimizing the authentication cost function, the optimal life time of the local SA can be obtained.

C. Determination of Optimal Life Time

In order to determine the optimal life time for the local SA, we evaluate the total authentication cost with a cost function, which is related with the life time of the local SA.

The *authentication cost* is defined as the signaling cost for one authentication request sent by a visiting MU in a foreign network domain. The *total authentication cost*, $C(T)$, is defined as the sum of the authentication cost to process all the authentication requests sent by a visiting MU in a foreign

network domain. In $C(T)$, we consider the risk that one SA is being cracked as part of the authentication cost because an additional SA, i.e., the local SA, increases the possibility that the security is compromised due to unpredicted events such as unknown attacks. Then, $C(T)$ can be written as:

$$C(T) = \begin{cases} \lambda\tau c_m & \text{if } T = 0 \\ \frac{\tau}{T}(\lambda T c_n + c_r e^{\beta T}) + \frac{\tau c_c}{T} + c_m & \text{if } 0 < T \leq \tau \\ \lambda\tau c_n + c_r e^{\beta T} & \text{if } T > \tau \end{cases}, \quad (4)$$

where λ is the arrival rate of session authentication requests, which is defined as the authentication initiated to begin a new service for the MU. Therefore, λ is equal to the call arrival rate of the MU. T is the life time of the local SA. Once we determine the life time, we use the same value of T whenever we refresh the local SA. c_n is the authentication cost for one authentication with local SA, c_m is the authentication cost for one authentication with remote authentication to the HAS of the MU, c_r is the cost to compensate the risk that one SA is cracked. For example, if the crack of the local SA induces data loss, the compensation cost is the cost to recover the original data from the backup data. β is an factor of the increasing speed of the risk, τ is the residence time of the MU in the network, and c_c is the signaling cost to refresh a local SA.

The first line of $C(T)$ in (4) is the total authentication cost without the local SA. In this case, the life time of the local SA is set to 0. Therefore, when a session authentication request arrives, the LAS must authenticate the visiting MU from its HAS because of the lack of local credentials. The total authentication cost is equal to the sum of the cost for the authentication requests sent by the MU when it resides in current network domain.

The second line of $C(T)$ in (4) is the total authentication cost with our proposed protocol if $0 < T \leq \tau$. $\lambda T c_n + c_r e^{\beta T}$ is the total authentication cost and the risk that a local SA is being cracked within the life time T. Once a local SA is established through our proposed protocol, the authentication requests arrive within the life time T of the SA can be processed locally. At the same time, the existence of the local SA has the risk of being hacked, which is increased with the existence time of the local SA. In our cost function, we use $c_r e^{\beta T}$ to present this risk. To decrease the risk, we refresh the local SA when the life time of the SA expires. Therefore, if $0 < T \leq \tau$, the times to refresh an SA is $\frac{\tau}{T}$ because the LAS refreshes the local SA every T minutes, thus the signaling cost to refresh the local SA is $\frac{\tau c_c}{T}$. And the total authentication cost should include the signaling cost to establish the local SA for the first time, i.e., c_m.

The third line of $C(T)$ in (4) is the total authentication cost with the proposed protocol if $T > \tau$. In this case, it is clear that the total authentication cost is equal to the sum of authentication cost for all the authentication requests sent by the MU in the foreign network domain and the cost to compensate the risk that the SA is being cracked in time T.

The authentication cost for one local authentication request, c_n, can be evaluated with the number of signalings. As shown in Fig. 3, $c_n = 4$. Similarly, c_m can be represented with the number of signalings between the visiting MU and its HAS. Therefore, $c_m = 4 + 2 * n$, where n is the number of hops between the LAS and the HAS. For c_c, we evaluate it with the number of signalings to refresh a local SA. When the life time expires, the local SA can be refreshed with two signalings. One is sent by the LAS to notify the MU with necessary new data such as new key; the other is sent by the MU to confirm the reception of the message. So $c_c = 2$. For the cost to compensate the risk that a local SA is being cracked, i.e., c_r, we evaluate it with the number of destroyed records of the MUs caused by the crack of the local SA. We assume one local SA only affects one record of the visiting MU. Therefore, $c_r = 1$. In our proposed protocol, we ask the MU to save its traffic and mobility patterns in its profile in terms of call arrival rate, λ, and average residence time of the MU in a subnet, $\overline{T}_r$. When the MU needs authentication, these data should be sent to the LAS. Then, The call arrival rate, λ, and average residence time of the MU in a subnet, $\overline{T}_r$, can be obtained from the MU's profile. For the residence time of the MU in a network domain, i.e., τ, we use its average value, $\overline{\tau}$. Then, if the visiting MU is assumed to be uniformly roaming in current network domain, $\overline{\tau}$ can be evaluated as [20]:

$$\overline{\tau} = \frac{(M+1)\overline{T}_r}{2}, \quad (5)$$

where M is the number of subnets in current network domain.

In our proposed protocol, we assign a life time to the local SA that meets the condition $0 < T \leq \tau$. Then, the optimal value $C^*(T^*)$ can be obtained by taking derivative of $C(T)$ with respect of T as follows:

$$C^*(T^*) = \frac{\overline{\tau}}{T^*}(\lambda T^* c_n + c_r e^{\beta T^*}) + \frac{\overline{\tau} c_c}{T^*} + c_m, \quad (6)$$

T^* is the solution of $e^{\beta T^*}(\beta T^* - 1) = c_c/c_r$, which can be obtained with discrete method.

By calculating T^* at the LAS and transmitting it to the visiting MU with the protocol shown in III-B, the local SA can be established securely and efficiently, and the authentication cost with the consideration of risk evaluation, mobility and traffic patterns can be minimized, simultaneously.

IV. Numerical Results and Discussion

In this section, we show the numerical results for our proposed protocol by comparing to DIAMETER used in AAA architecture. We assume a visiting MU is roaming in a foreign network domain that is composed of M subnets. The corresponding parameters are shown in Table I.

We assume that there are 100 subnets in a network domain where the visiting MU is roaming. The distance, n, is represented in terms of hops between the LAS and the HAS, which is set to 10. The related authentication costs in terms of number of signalings or the number of records associated with the risk of one local SA are 24, 4, 1, and 2 for c_m, c_n, c_r, and c_c, respectively, which have been evaluated in Section III-C. By assuming that $\overline{T}_r = 10$ minutes, $\overline{\tau}$ can be obtained with 5 as 505 minutes. The call arrival rate of the visiting MU is assumed to be 0.3 times per minute. The coefficient β in our

TABLE I
SIMULATION PARAMETERS.

M	n	c_m	c_n	c_r	c_c	$\overline{T}_r$ (minutes)	$\overline{\tau}$ (minutes)	λ (per minute)	β
100	10	24	4	1	2	10	505	0.3	0.8

proposed protocol is assumed to be 0.8, which can be adjusted according to the knowledge of the risk in the environments. For example, if the historical data show that many attacks succeeded recently, the environment can be thought unsafe, and the value of β can be set to a big value, which indicates the risk increases very fast. If the historical data show that the attacks to the local SAs did not succeed frequently, the value of β can be set to a small value to demonstrate a slow increase of the risk with the time. The estimation of a good value for β in an environment is out of the discussion of our paper, and we will discuss it in our future work.

We evaluate the effects of residence time, call arrival rate, number of hops between LAS and HAS, and number of subnets in a network domain on the total authentication cost. The numerical results are shown in Fig. 5, Fig. 6, Fig. 7, and Fig. 8, respectively.

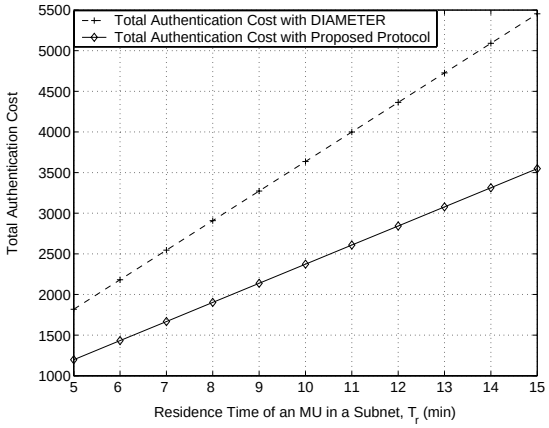


Fig. 5. Total Authentication Cost vs. Residence Time of an MU in a Subnet.

In Fig. 5, the total authentication cost is increasing with the increase of residence time of a visiting MU in a subnet. The longer the MU stays in current network domain, the more authentication requests the MU sends. Therefore, the total authentication cost increases due to the large amount of authentication requests. This increasing trend is same to DIAMETER and our proposed protocol. However, the total authentication cost with our proposed protocol outperforms that with DIAMETER because the authentication with local SA avoids the remote authentication signalings. The improvement is about 34.3% when $T_r = 6$ and 34.8% when $T_r = 12$.

Fig. 6 shows a trend in both DIAMETER and our proposed protocol that the total authentication cost increases with the increase of call arrival rate of a visiting MU. Whenever a call is initiated, an authentication request is sent out. Then, the number of authentication requests in current network domain

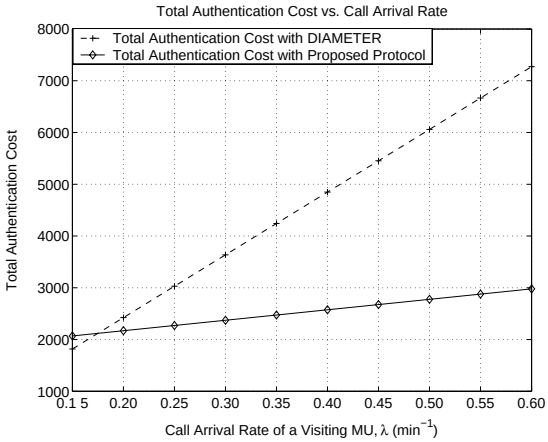


Fig. 6. Total Authentication Cost vs. Call Arrival Rate of a Visiting MU.

increases with the call arrival rate. Accordingly, the total authentication cost increases with the increase of call arrival rate. In some cases that $\lambda < 0.18$, the total authentication cost with DIAMETER is less than our proposed protocol. It is because the proposed lightweight protocol needs to establish, refresh, and keep a local SA, which takes costs. If the call arrival rate, i.e., the number of authentication requests during residence time in a network domain, is too small, the costs spent with the proposed protocol is not worthy. However, if the call arrival rate is bigger than 0.18 times per minute, the proposed lightweight protocol economizes much authentication cost. The improvement of authentication costs increases with the call arrival rate. When $\lambda = 0.3$, the improvement of our proposed protocol is about 34.7%.

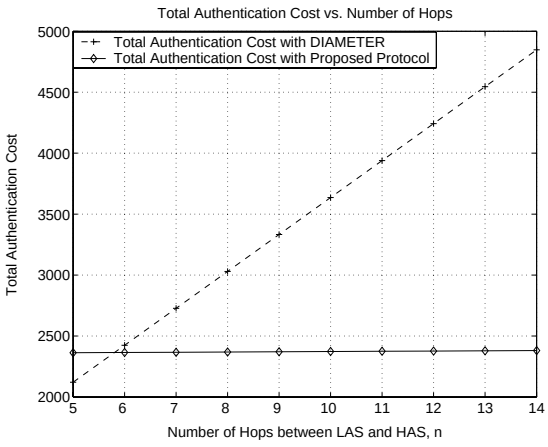


Fig. 7. Total Authentication Cost vs. Distance between LAS and HAS.

The relationship between the total authentication cost and

the number of hops between LAS and HAS is shown in Fig 7. We can see that the authentication cost with DIAMETER increases with the increase of the number of hops between LAS and HAS, while the authentication cost with the proposed lightweight protocol remains constant with the increase of the number of hops between LAS and HAS. The reason is that whenever a session authentication is initiated, the challenge/response authentication in DIAMETER needs the LAS to authenticate the MU from the HAS, which requires remote delivery of the credentials. Therefore, the authentication cost with DIAMETER increases with the number of hops between the LAS and HAS. In the proposed lightweight protocol, after the first authentication, the rest of the authentication requests for the visiting MU become local authentication, which has no relation with the number of hops between the LAS and the HAS. Therefore, the authentication cost with proposed lightweight protocol remains constant.

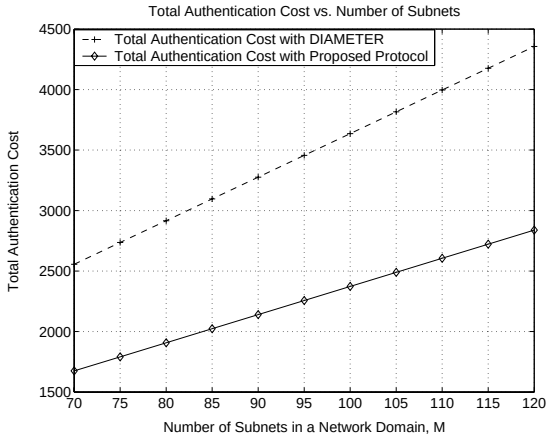


Fig. 8. Total Authentication Cost vs. Number of Subnets in a Network.

In Fig. 8, we illustrate the effect of number of subnets in a network domain on the total authentication cost. The total authentication cost increases in DIAMETER and our proposed protocol with the increase of number of subnets in a network domain. When the number of subnets in a network domain increases, the residence time of an MU in a network domain increases according to (5) if the other conditions such as residence time in a subnet do not change. Therefore, the number of authentication requests becomes big with the increase of residence time in a network domain. Accordingly, the total authentication cost increases. However, the total authentication cost with our proposed protocol is far less than that with DIAMETER because of the implementation of local authentication with the local SA. The improvement with our proposed is about 34.8% when $M = 100$.

V. Conclusion

In this paper, we propose a lightweight authentication protocol with local security association control to establish a local security association for efficient authentication in mobile networks. In the proposed protocol, we first design a light weight method to establish a local security association, which can guarantee the secure transmission of information. In order to determine the life time of the local security association, an authentication cost function, which considers traffic, mobility patterns as well as risk evaluation, is proposed. By minimizing the authentication cost, the optimal life time of the local security association is obtained. The numerical results reveal that our protocol outperforms DIAMETER greatly under various conditions such as long residence time and high volume of call arrival rate. In summary, we provide an applicable lightweight authentication protocol on AAA architecture, which combines the authentication efficiency with mobility pattern, traffic pattern and risk evaluation, and improves the authentication efficiency greatly.

References

[1] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "The Evolution of Wireless LANs and PANs - Efficient Authentication and Key Distribution in Wireless IP Networks," *IEEE Personal Communications on Wireless Communications*, vol. 10, pp. 52–61, December 2003.

[2] V. Gupta, S. Gupta, and S. Chang, "Performance Analysis of Elliptic Curve Cryptography for SSL," in *WiSe'02-ACM Workshop on Wireless Security*, September 2002.

[3] A. Hess and G. Schafer, "Performance Evaluation of AAA / Mobile IP Authentication," in *http://www-tkn.ee.tu-berlin.de/publications/papers/pgts2002.pdf*, 2002.

[4] C. Fung and M. Lee, "A Denial-of-Service Resistant Public-Key Authentication and Key Establishment Protocol," in *21st IEEE International Performance, Computing, and Communications Conference, 2002.*, pp. 171–178, 2002.

[5] H. Kim and H. Afifi, "Improving Mobile Authentication with New AAA Protocols," in *IEEE International Conference on Communications*, vol. 1, pp. 497–501, 2003.

[6] W. Simpson, "PPP Challenge Handshake Authentication Protocol (CHAP)," *RFC1334*, August 1996.

[7] S. Shieh, F. Ho, and Y. Huang, "An Efficient Authentication Protocol for Mobile Networks," *Authentication Protocol Journal of Information Science and Engineering*, vol. 15, pp. 505–520, 1999.

[8] S. Glass, T. Hiller, S. Jacobs, and C. Perkins, "Mobile IP Authentication, Authorization and Accounting Requirements," *RFC2977*, October 2000.

[9] C. Perkins and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions," *RFC3012*, November 2000.

[10] M. Xu and S. Upadhyaya, "Secure Communication in PCS," in *Vehcular Technology Conference, 2001. VTC 2001. IEEE*, pp. 2193–2197, 2001.

[11] B. Lee, T. Kim, and S. Kang, "Ticket-based Authentication and Payment Protocol for Mobile Telecommunications Systems," in *International Symposium on Dependable Computing, 2001. Proceedings.*, pp. 218–221, 2001.

[12] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," *RFC2716*, October 1999.

[13] L. Blunk and J. Vollbrecht, "PPP Extensible Authentication Protocol," *RFC2284*, March 1998.

[14] L. Dell'Uomo and E. Scarrone, "The Mobility Management and Authentication/Authorization Mechanisms in Mobile Networks beyond 3G," in *Personal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium on*, vol. 1, pp. c44–c48, September 2001.

[15] *http://standards.ieee.org/getieee802/download/802.1X-2001.pdf*.

[16] W. Stallings, "Network Security Essentials," *Applications and Standards*, 2000.

[17] T. Dierks and C. Allen, "The TLS Protocol," *rfc2246*, January 1999.

[18] M. Barton, D. Atkins, J. Lee, S. Narain, D. Ritcherson, K. Tepe, and K. Wong, "Integration of IP Mobility and Security for Secure Wireless Communications," in *2002 IEEE International Conference on Communications,*, pp. 1045–1049, 2002.

[19] T. Braun, L. Ru, and G. Stattenberger, "An AAA Architecture Extension for Providing Differentiated Services to Mobile IP Users," *Proceedings. Sixth IEEE Symposium on Computers and Communications, 2001.*, pp. 472–478, 2001.

[20] W. Wang and I. Akyildiz, "Intersystem Location Update and Paging Schemes for Multitier Wireless Networks," in *Proc. of ACM/IEEE MobiCom'2000*, pp. 99–109, August 2000.