A Dynamic Security Association Control Scheme for Efficient Authentication in Wireless Networks

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

Abstract— **In this paper, we present a dynamic security association control scheme to improve system performance during authentication in wireless networks. First, a new architecture composed of licensed authentication centers (LACs) for inter-domain authentication is introduced, in which security associations (SAs) are created and modified on demand, thus reducing the number of SAs and dynamically adjusting the lifetime of an SA. Then, a dynamic SA (DSA) control scheme is developed to determine an optimal threshold time for DSAs by using a utility function for maximizing the bandwidth efficiency. Simulation results reveal the effectiveness of the proposed scheme in terms of the improvement in authentication latency, bandwidth efficiency, and the number of SAs.**

Key Words: *Authentication, security association.*

I. Introduction

The development of wireless networks provides convenience to people at the expense of exposing sensitive data in open mediums [1]. To secure communications in open mediums, authentication is proposed to identify mobile nodes (MNs), which includes the establishment of security association (SA), encryption and decryption of credentials, etc [2], [3]. An SA is a trust relationship that can afford security service with keys and cryptographic algorithms. The distribution of keys and the complexity of the algorithms determine the security of the network and the efficiency of communication. Thus, an SA becomes a critical part for the authentication to affect network security and the communication efficiency [4], [5].

A strong authentication mechanism in wireless networks can guarantee the security with complicated processes, such as certificate verification, to set up an SA for communications. However, due to the complex algorithms or the remote distance to establish an SA, the authentication produces extensive overhead, which further degrades many parameters such as bandwidth efficiency, authentication delay, cost and call dropping probability [4]–[7]. If the authentication lasts for a long time, the bandwidth efficiency may be reduced due to bandwidth idle for authentiation, which may worsen if bandwidth is reserved before authentication [8]. Because the establishment of an SA is time-consuming due to either complex algorithms or remote distance, many protocols are developed to distribute an SA before the MN's roaming [9], [10].

A centralized authentication architecture requires a central authentication server, which is unrealistic for mass environments of wireless networks [9]. Then, two solutions are introduced for Mobile IP networks [11]. The first solution is a distributed authentication architecture, which requires a local authentication, authorization, accounting server (AAAL) to share SAs with the other AAALs in Mobile IP networks. However, this configuration may cause a quadratic growth in the number of SAs when the number of AAALs increases, which is identified as a problem by ROAMOPS group in IETF [10]. The second solution in [11] uses hierarchical AAA brokers (AAABs) trusted by AAALs to relay credentials, which goes through higher AAABs when an AAAB cannot find an SA for two networks. Thus, the number of SAs can be reduced and the manageability of networks can be maintained. However, the hierarchical architecture may take a long time to search upper AAABs in inter-domain authentication, and chaining AAA servers may result in a number of security threats such as man-in-middle attack [10].

To improve the bandwidth efficiency during authentication, we develop a dynamic SA control scheme for efficient authentication. First, a new distributed authentication architecture is proposed, which utilizes fewer SAs than the hierarchical architecture. Second, a dynamic SA control scheme is presented to improve the bandwidth efficiency and the network security by assigning an optimal life time to the SA. Third, a utility function with pricing models is constructed to obtain the optimal life time of the SA, which considers the bandwidth efficiency, traffic pattern, risk assessment, and number of SAs, simultaneously. Most of all, our proposed scheme can be implemented in various wireless networks, in which one authentication center is used at one autonomous network. For example, we can run our scheme on AAA servers in Mobile IP networks by adding a parameter of life time for a dynamic SA into AAA messages.

The rest of this paper is organized as follows: Section II describes the proposed authentication architecture in wireless networks. In Section III, the dynamic security association control scheme for efficient authentication is proposed based on a utility function with pricing models. Section IV explains the simulation scenarios and provides the simulation results of our control scheme on the new architecture. Finally, we present our conclusion in Section V.

II. A New Authentication Architecture for Wireless Networks

In this section, we first introduce the hierarchical authentication architecture in wireless networks for future its good scalability and applications. Then, some terminologies used in the new architecture are explained. Lastly, the new authentication architecture is illustrated, with which we develop a dynamic SA control scheme for efficient authentication in Section III.

A. Hierarchical Authentication Architecture

A hierarchical authentication architecture for wireless networks is proposed in [11], in which a proxy authentication center (PAC) is introduced to manage static SAs (SSAs) for a group of authentication centers (ACs). The PACs are organized in groups and are controlled by a higher-level PAC. Suppose each network has only one AC and let M_H be the number of ACs in hierarchical authentication architecture. The total number of inter-domain SAs, denoted as N_H, is obtained by:

$$N_H = \underbrace{2(M_H + \frac{M_H}{v} + \frac{M_H}{v^2} + \cdots + v)}_{log_v^{M_H}} = \frac{2v}{v-1}(M_H - 1), \quad (1)$$

where v is the number of ACs or PACs controlled of one PAC. Here we suppose $log_v^{M_H}$ is an integer.

Hierarchical architecture has good manageability and scalability by reducing the number of SAs [10], [11]. However, this architecture may not provide end-to-end protection between ACs without direct SAs between ACs. This may cause many security problems such as man-in-middle attack [10]. In addition, searching for the SA of a network may take a long time, further deteriorating bandwidth efficiency of the system.

B. Dynamic and Static Security Association

An SA is a one-way trust relationship between communicators that affords security service on the traffic with parameters such as key, lifetime, and cryptography algorithm. A *dynamic SA* (DSA) is an SA created *on demand* and can be established with four-way handshake protocol in transport layer security (TLS) and changed by adjusting its parameters [12].

The number of SAs between wireless networks is an important factor to evaluate manageability and reliability of wireless networks [10]. A huge number of SAs impose a great effort to manage and secure the SAs at ACs [10]. In addition, an SA is easily attacked due to its long existence time, especially in the open medium of wireless networks [13]. The number of SAs can be reduced with DSAs and the short existence time of DSA can limit the analysis of the SA, while the establishment of a DSA may cause long authentication delays, further deteriorating bandwidth efficiency [4].

Therefore, we propose a new authentication architecture, on which a DSA control scheme for authentication is implemented based on the evaluation of the bandwidth efficiency, risk assessment of DSA, and average number of SAs.

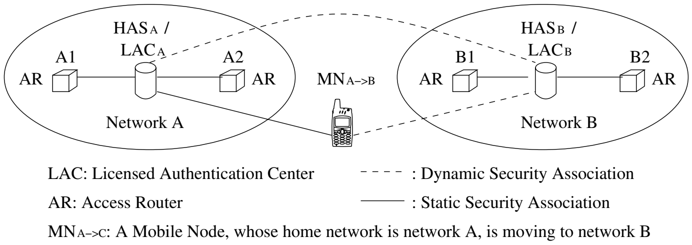

HASA /
LACA
A1
A2
AR
AR
Network A
MNA->B
HASB /
LACB
B1
B2
AR
AR
Network B
LAC: Licensed Authentication Center
- - - - : Dynamic Security Association
AR: Access Router
—— : Static Security Association
MNA->C: A Mobile Node, whose home network is network A, is moving to network B

Fig. 1. Proposed New Authentication Architecture.

C. Infrastructure of New Authentication Architecture

In the proposed architecture, a licensed authentication center (LAC) is defined as a central authentication authority in an autonomous wireless network, which only has one LAC in it. Every access router (AR) in a wireless network shares a static SA with the LAC. All the MNs in their home network are trusted by a home authentication server (HAS), which is also an LAC for visiting MNs. The LACs are connected to each other by DSAs. An example of the proposed architecture is shown in Fig. 1 with two wireless networks A and B. LAC_A and LAC_B are LACs in network A and B, respectively. $A1$ and $A2$ are two ARs trusted by LAC_A in network A. $B1$ and $B2$ share static SAs with LAC_B in network B.

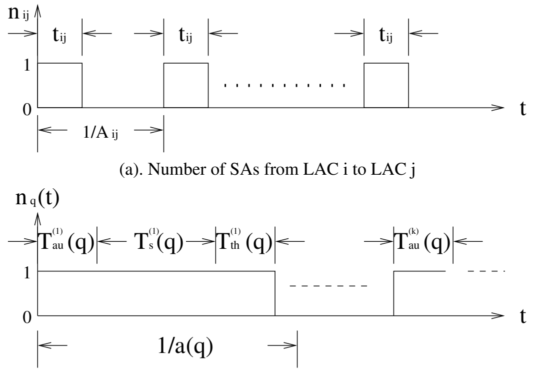
We define *the average number of SAs* between LACs in a period of time as N_N, which is shown as:

$$\begin{aligned} N_N &= \lim_{T_p \to \infty} \frac{\sum_{i=0}^{M_N-1} \sum_{j=0, j\neq i}^{M_N-1} \int_0^{T_p} n_{ij}(t)dt}{T_p} \\ &= \sum_{i=0}^{M_N-1} \sum_{j=0, j\neq i}^{M_N-1} t_{ij} A_{ij} \\ &\leq \sum_{i=0}^{M_N-1} \sum_{j=0, j\neq i}^{M_N-1} t_m A_m = t_m A_m M_N (M_N - 1), \quad (2) \end{aligned}$$

where M_N is the number of LACs in our architecture, T_p is an observation time within which we count the number of SAs, i and j are the indices of the LACs in a wireless network. t_m is the maximal lifetime of DSA between any two LACs, A_m is the maximal arrival rate of inter-domain authentication requests. Because the unit of t_m is milliseconds and A_m in a second is also small in reality, the condition $t_m A_m << 1$ is satisfied in most cases. If the DSA is alive, the value of $n_{ij}(t)$ is 1 for there only exists one DSA from the LAC i to the LAC j, and the value of $n_{ij}(t)$ is 0, if the DSA does not exist. Then, $n_{ij}(t)$ can be shown in Fig. 2 (a).

III. Dynamic Security Association Control Scheme for Efficient Authentication

In this section, we first present a dynamic security association control scheme for efficient authentication to describe the operation of the LAC in the proposed architecture. In order to optimize the bandwidth efficiency with the consideration of risk assessment and average number of SAs, we develop an algorithm using a utility function to determine an optimal threshold time for the lifetime of a DSA.



(a). Number of SAs from LAC i to LAC j

(b). Number of SAs between visiting MN q and LAC

Fig. 2. Number of SAs in Two DSA Controls.

A. Operation of LACs

In our proposed scheme, an LAC has two types of authentication functions. One is to process the intra-domain authentication and the other is for inter-domain authentication. Here, we focus on inter-domain authentication and control the DSAs at the LAC during inter-domain authentication, while having the intra-domain authentication processed by other authentication mechanisms such as DIAMETER [2].

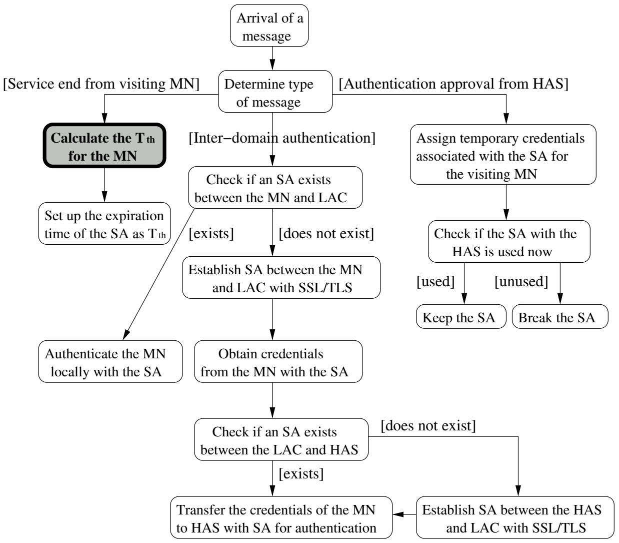

Arrival of a message
Determine type of message
[Service end from visiting MN]
[Authentication approval from HAS]
Calculate the T_{th} for the MN
[Inter−domain authentication]
Assign temporary credentials associated with the SA for the visiting MN
Check if an SA exists between the MN and LAC
Set up the expiration time of the SA as T_{th}
[exists]
[does not exist]
Check if the SA with the HAS is used now
Establish SA between the MN and LAC with SSL/TLS
[used]
[unused]
Keep the SA
Break the SA
Authenticate the MN locally with the SA
Obtain credentials from the MN with the SA
Check if an SA exists between the LAC and HAS
[does not exist]
[exists]
Transfer the credentials of the MN to HAS with SA for authentication
Establish SA between the HAS and LAC with SSL/TLS

Fig. 3. Operation of LACs.

During inter-domain authentication, the LAC has to manage two types of DSAs. One is between the visiting MN and the LAC; the other is between the LAC and the HAS of visiting users. The proposed scheme is shown in Fig. 3, which works according to received messages at the LAC. If the message is an authentication approval from an HAS, the scheme decides whether to keep the DSA with the HAS. In the case of a notification of service termination from a visiting MN, the scheme calls an algorithm to calculate an optimal threshold time, T^*_{th}, to keep an SA for the MN. When the message is an inter-domain authentication request, our scheme asks the LAC to either authenticate the visiting MN locally with existing DSA or forward the credentials of the MN to its HAS for authentication if no DSA exists between the MN and LAC.

In this scheme, the most important is the algorithm to calculate T^*_{th} for each DSA, which is highlighted in Fig. 3. Next, we introduce a utility function to calculate T^*_{th}.

B. Utility-based Control Scheme

1) Utility Function with Pricing Models: We develop a utility function with pricing models, Γ, in which bandwidth efficiency, risk assessment of a DSA and the average number of SAs used by an MN are considered. Γ is defined as:

$$\Gamma = U(f(q)) - \alpha(q)R(q) - \beta(q)n_c(q), \tag{3}$$

where $f(q)$ is the bandwidth efficiency of a visiting MN q, $U(f(q))$ is a utility function increased with increasing of $f(q)$. $R(q)$ is the risk function of a DSA used by MN q, and $n_c(q)$ is the average number of SAs used by MN q. $\alpha(q)$ and $\beta(q)$ are the coefficients of $R(q)$ and $n_c(q)$, respectively. The definitions and applications of $f(q)$, $R(q)$ and $n_c(q)$ are explained as follows.

- $f(q)$ is defined as:

$$f(q) = \frac{B_s(q) \cdot T_s(q)}{B_{un}(q) \cdot T_{au}(T_{th}(q)) + B_s(q) \cdot T_s(q)}, \tag{4}$$

where $B_s(q)$ is the service bandwidth for MN q and $B_{un}(q)$ is the bandwidth unavailable for service caused by the authentication of MN q. $T_s(q)$ is the service time for MN q, $T_{th}(q)$ is the threshold time to keep the DSA for MN q after the end of service, and T_{au} is the authentication time for MN q, which is defined as the time from when the authentication request is sent to when the MN receives the authentication reply. T_{au} is a function of $T_{th}(q)$. We assume that $B_s(q)$, $B_{un}(q)$ and $T_s(q)$ have constant mean values, then adjust T_{th} for each MN to maximize the bandwidth efficiency for an MN, furthermore optimizing the *total* bandwidth efficiency, F, for a total number of Q inter-domain roaming MNs during authentication. F is defined as:

$$F = \frac{\sum_{q=1}^{Q} B_s(q) \cdot T_s(q)}{\sum_{q=1}^{Q} B_{un}(q) \cdot T_{au}(T_{th}(q)) + \sum_{q=1}^{Q} B_s(q) \cdot T_s(q)}. \tag{5}$$

- $R(q)$ is defined as:

$$R(q) = P_r(q) \cdot C(q), \tag{6}$$

where $P_r(q)$ is the probability that one DSA between MN q and a local LAC is hacked, and $C(q)$ is a risk value. It is reasonable to assume $P_r(q)$ relates to the lifetime of a DSA because the brutal attack is associated with the duration time of a DSA [13]. Furthermore, we assume $P_r(q)$ is exponentially distributed and independent of different MNs for simplicity. Then, $P_r(q)$ becomes:

$$P_r(q) = \int_0^{(T_{au}(T_{th}(q)) + T_s(q) + T_{th}(q))} \lambda(q) e^{-\lambda(q)t} dt, \tag{7}$$

where the sum of $T_{au}(T_{th}(q))$, $T_s(q)$ and $T_{th}(q)$ is the lifetime of the DSA between MN q and the LAC, which is shown in Fig. 2 (b). $\lambda(q)$ is the successful attack rate on this SA. We consider $C(q)$ a risk value assigned to a security level. We assign two values of $C(q)$ to two security levels. When an MN is in its home network, the security level and $C(q)$ are low, which means the user trusts its surroundings. When an MN is in a foreign network, the security level and $C(q)$ are accordingly high because the MN may face more threats such as denial of service due to lack of confidentials.

- $n_c(q)$ is defined as:

$$n_c(q) = \frac{\sum_{k=1}^{K(q)} (T_{au}^{(k)}(q) + T_s^{(k)}(q) + T_{th}^{(k)}(q))}{T_p}, \quad (8)$$

where T_p is the observation time, k is the kth request from MN q, and $K(q)$ is the number of authentication requests from MN q in time T_p. Let $a(q)$ be the arrival rate of authentication requests from MN q and let $T_p = 1/a(q)$, then $K(q) = 1$. Suppose all of the time variables are the same in different sessions, then $n_c(q)$ becomes:

$$n_c(q) = \min\{a(q)(T_{au}(T_{th}(q)) + T_s(q) + T_{th}(q)), 1\}. \quad (9)$$

The first value of $n_c(q)$ in 9 is obtained by substituting $T_p = 1/a(q)$ and $K(q) = 1$ into (8) if $T_{au}(T_{th}(q)) + T_s(q) + T_{th}(q) \leq 1/a(q)$. When $T_{au}(T_{th}(q)) + T_s(q) + T_{th}(q) > 1/a(q)$, because observation time is in $1/a(q)$, the value of $n_c(q)$ should be 1. The curve of $n_c(q)$ is shown in Fig. 2 (b).

2) Optimal Threshold T_{th}^*: To maximize the bandwidth efficiency, we need to maximize function Γ with respect to $T_{th}(q)$. Therefore, the optimization of function Γ becomes:

$$\begin{aligned} maximize \quad & \Gamma(Tth(q)) \\ over \quad & T_{th}(q) \geq 0. \end{aligned} \quad (10)$$

In order to obtain T_{th}^* for each MN, we need to study the relationship between T_{au} and T_{th} first. In our control scheme, the relationship between T_{au} and T_{th} can be written as:

$$T_{au}(T_{th}(q)) = \begin{cases} TS_{au} & \text{if } T_{th}(q) \geq t_2 \\ TN_{au} & \text{if } 0 \leq T_{th}(q) < t_1 \\ (TS_{au} + TN_{au})/2 & \text{if } t_1 \leq T_{th}(q) < t_2 \\ 0 & \text{Otherwise} \end{cases}, \quad (11)$$

where $t_1 = 1/a(q) - TN_{au}(q) - T_s(q)$ and $t_2 = 1/a(q) - TS_{au}(q) - T_s(q)$. $TN_{au}(q)$ is the authentication time needed to verify MN q from its HAS, and $TS_{au}(q)$ is the authentication time to re-authenticate MN q locally with the existing DSA between MN q and LAC. $TS_{au}(q)$ is the sum of message transmission time, propagation time, data encryption/decryption time at the MN, AR and LAC and data verification time at LAC. $TN_{au}(q)$ is composed of similar time variables as $TS_{au}(q)$, except that $TN_{au}(q)$ includes additional DSA establishment time between MN and LAC and possible DSA establishment time between LAC and HAS. Therefore, we can see that $TS_{au}(q) < TN_{au}(q)$ and $t_1 < t_2$.

There are three states between MN q and the LAC during authentication. The first state is the least time-consuming state, in which $T_{th}(q)$ is long enough to accommodate each authentication request of MN q. Therefore, the authentication time for this request is TS_{au} as shown in Fig. 2 (b). In the second state, the authentication request of MN q reaches the LAC after the shared SA expires. Thus, the authentication time in the second state is TN_{au}, and the condition to get this time can also be derived from Fig. 2 (b). In the third state, when $T_{th}(q)$ is between t_1 and t_2, the authentication time of this state oscillates between TS_{au} and TN_{au}. Thus, the authentication time and the conditions in these three states can be shown in (11).

After we get the relationship between $T_{au}(q)$ and $T_{th}(q)$ in (11), the maximal Γ function, Γ_{max}, becomes:

$$\begin{aligned} \Gamma_{max} = max\{ & \Gamma(T_{th}(q))|_{T_{th}^*(q)=0}, \\ & \Gamma(T_{th}(q))|_{T_{th}^*(q)=t_1}, \ \Gamma(T_{th}(q))|_{T_{th}^*(q)=t_2}\}. \end{aligned} \quad (12)$$

When $T_{th}(q) \in [0, t_1)$, because the authentication time is TN_{au}, $U(f(q))$ is a constant though $R(q)$ and $N_c(q)$ increase as the increase of $T_{th}(q)$. Thus, the local Γ_{max} is obtained at $T_{th}(q) = 0$ when $T_{th}(q) \in [0, t_1)$. Similar analysis can be applied when $T_{th}(q) \in [t_1, t_2)$ and $T_{th}(q) \in [t_2, \infty)$, then Γ_{max} can be obtained at the points of 0, t_1, or t_2.

IV. Simulation

In this section, we evaluate *average authentication latency*, *bandwidth efficiency* and *average number of SAs* of the proposed scheme on the new authentication architecture. We define the average authentication latency, T_{av}, as the ratio of the sum of the authentication latencies of inter-domain authentication requests over the number of these requests. Bandwidth efficiency, F, and average number of SAs, N_N, are defined in (2) and (5), respectively.

TABLE I

Simulation Parameters.

Parameters	Values	Parameters	Values
Radio Channel BW	3840 (kbps)	$U(f)$	$e^{(k*f)}$
B_s	50(kbps)	$\lambda \ (sec^{-1})$	$\frac{1}{600}$
B_{un}	B_s	k	50
T_s	1 (sec)	α	0.1
A_{MN}	0.2 (calls/sec)	C	5
MAC Access Delay	0.01 (sec)	β	0.5
Trans. and Propa. Time (Hier. Arch.)	0.07 (sec)	T_V/T_{VH}	0.1 (sec)
Trans. and Propa. Time (Proposed Arch.)	0.05 (sec)	T_{int}	10 (sec)

We compare the efficiency of inter-domain authentication on the new architecture with schemes on hierarchical architecture. Two networks are considered in the simulation with one LAC and two ARs in a network. For the hierarchical architecture, one PAC is used to control two ACs. Important parameters are defined in Table I. All of the time variables are supposed to be exponentially distributed. A_{MN} is arrival rate of new inter-domain authentication requests, and T_{int} is a time interval defined as $T_{int} = 1/a - T_{au} - T_s$ according to Fig. 2 (b). The mean time variables are obtained from [4], [5]. Since we know the least time to hack an SA in WEP is around 10 minutes [13], we use 10 minutes as the value of $1/\lambda$.

In Fig. 4, we observe that T_{av} is reduced greatly with the proposed scheme. Compared with T_{av} in hierarchical architecture without the control scheme, the improvement is up to 34%. The benefit is obtained as some of previously authenticated MNs can be authenticated locally by the LAC with the proposed scheme. However, when A_{MN} increases, the number of new visiting MNs is increased. They cannot obtain the benefit from the management of SA between an MN and the LAC in our control scheme. Therefore, T_{av} increases with the increase of A_{MN}.

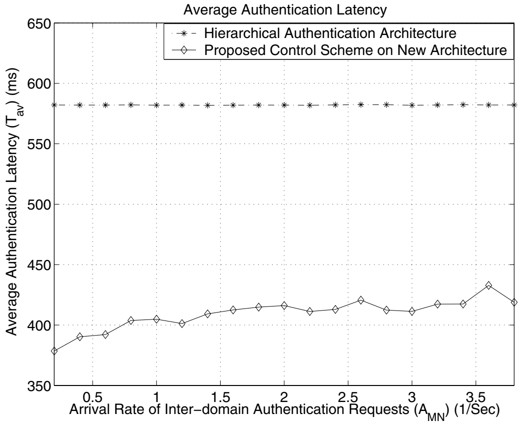


Fig. 4. Authentication Latency vs. Arrival Rate of Authentication Requests.

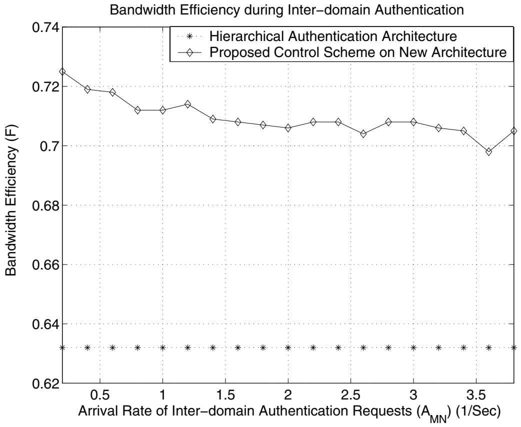


Fig. 5. Bandwidth Efficiency vs. Arrival Rate of Authentication Requests.

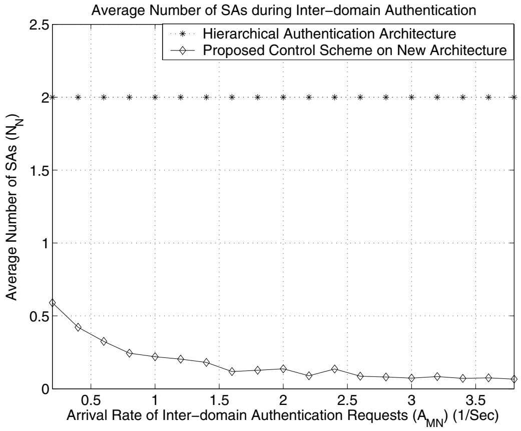


Fig. 6. Average Number of SAs vs. Arrival Rate of Authentication Requests.

Fig. 5 illustrates the improvement of bandwidth efficiency, F, with our scheme on new architecture, which is compared with that in hierarchical architecture without a control scheme. The improvement is up to 14% and comes from the reduction of T_{av}. Increased A_{MN} causes T_{av} to increase, furthermore decreases F, which also depends on T_s, according to our definition of F in (5) because a long service time can utilize the bandwidth efficiently. Although the improvement of F is not very big, it joins with other improvements of average number of SAs and authentication latency. Thus, it is acceptable.

In Fig. 6, the average number of SAs, N_N, is compared between our control scheme on new architecture and the hierarchical architecture without the control scheme. The improvement of N_N is between 70% and 90%, which comes from the small authentication latency and arrival rate of authentication requests between LAC and HAS shown in (2). N_N decreases with the increase of A_{MN} because the increased A_{MN} causes more authentication requests to share a DSA between the LAC and HAS, which reduces N_N compared to the individual authentication in different time.

V. Conclusion

This paper presents a dynamic security association control scheme for authentication to improve system performance. We propose a new architecture with licensed authentication centers (LACs) for authentication. Based on this architecture, security associations (SAs) are created and modified on demand. The optimal threshold time of SAs is determined by a utility function with pricing models, thus maximizing the bandwidth efficiency, reducing the authentication latency, and decreasing the average number of SAs. Therefore, a pioneering effort is conducted to couple the satisfaction of security and quality of service in heterogeneous mobile environments.

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] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," *draft-ietf-aaa-diameter-17.txt*, December 2002.

[3] *IEEE 802.11 Working Group. http://grouper.ieee.org/groups/802/11/index.html.*

[4] 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.

[5] 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.

[6] Y. Lin, S. Mohan, N. Sollenberger, and H. Sherry, "Adaptive Algorithms for Reducing PCS Network Authentication Traffic," *IEEE Transactions on Vehicular Technology*, vol. 46, pp. 588–596, August 1997.

[7] S. Suzuki and K. Nakada, "An Authentication Technique based on Distributed Security Management for the Global Mobility Network," *IEEE JSAC*, vol. 15, pp. 1608 –1617, October 1997.

[8] C. Tseng, G. Lee, and R. Liu, "HMRSVP: A Hierarchical Mobile RSVP Protocol," in *2001 International Conference on Distributed Computing Systems Workshop*, pp. 467–472, April 2001.

[9] I. Akyildiz, J. McNair, J. Ho, H. Uzunalioglu, and W. Wang, "Mobility Management in Next Generation Wireless Systems," *Proceedings of the IEEE*, vol. 87, pp. 1347–1384, August 1999.

[10] B. Aboba and J. Vollbrecht, "Proxy Chaining and Policy Implementation in Roaming," *RFC2607*, June 1999.

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

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

[13] A. Stubblefield, J. Ioannidis, and A. Rubin, "Using the Fluhrer, Martin, and Shamir Attack to Break WEB," *AT&T Labs*, August 21 2001.