An Analytical Study on the Impact of Authentication in Wireless Local Area Network

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

Abstract—**Authentication can provide security by preventing unauthorized usage and negotiating the credentials for secure communications. Nevertheless, it induces heavy overhead to communications, further deteriorating the quality of service (QoS). Therefore, analyzing the QoS and security impact of authentication becomes critical to developing efficient authentication schemes. In this paper, we first introduce a system model for the analysis of challenge/response authentication in wireless networks. Then, we evaluate authentication cost, delay, and call dropping probability for different security levels. By considering traffic and mobility patterns, we show the numerical results to illustrate the impact of authentication on security and system performance.**

I. Introduction

The tremendous emergence of wireless communication technologies such as Wi-Fi and 802.11 in wireless local area network (WLAN) has facilitated the ubiquitous Internet service, whereas inducing more challenges to security due to open medium [1]. In order to provide secure services in wireless networks, *authentication* is used to identify a mobile user (MU) before communication [1]. In the authentication, an MU is required to submit credentials such as certificates and challenge/response values for verification with a security association (SA), which is a trust relationship with parameters such as session keys. With the authentication, the network resource can be maintained by only authorizing legitimate users. The information secrecy and data integrity can also be guaranteed with negotiated keys for encryption. Therefore, authentication has great effects on security.

Meanwhile, authentication also affects the quality of service (QoS) greatly. When public/private-key based authentication is applied, the computation complexity for authentication consumes much time and power [2]. Therefore, secret-key based challenge/response authentication mechanism is widely used in wireless networks. In this mechanism, the credentials of the MU are encrypted and transmitted to the home networks of MUs among authentication servers. The transmission affects many QoS parameters such as authentication cost in terms of signaling and encryption/decryption cost and delay, which affects other parameters such as call dropping probability.

Moreover, the arrival rate of authentication requests is related with the mobility and traffic patterns of MUs, which may greatly affect QoS such as aggregated authentication cost in different scenarios. Thus, the impact of authentication on QoS parameters are far more sophisticated with different mobility and traffic patterns in different scenarios.

Since authentication affects both security and QoS, the design of an authentication scheme should consider security and efficiency, simultaneously. To this end, many authentication protocols are proposed [1], [3]–[5]. However, there is no rigorous method that adapts to the mobility and traffic patterns of MUs, and no quantitative evaluation is provided on authentication efficiency with mobility and traffic patterns. Therefore, they do not meet the requirement of authentication efficiency with concerns of the mobility and traffic patterns.

In this paper, we evaluate the authentication impact on security and efficiency with mobility and traffic patterns based on challenge/response authentication. First, we propose a system model for WLAN, which is consistent with many wireless networks such as Mobile IP networks, to analyze challenge/response based authentication. The consistency guarantees that our analysis has the same impact in various wireless networks with similar system models. Second, we provide completed analysis on authentication cost, delay and call dropping probability *for one authentication request* at different security levels, which are used to represent the security of authentication. Furthermore, we analyze the authentication delay and call dropping probability statistically in combination with *mobility and traffic patterns* in a scenario, which demonstrates potential ways to optimize authentication efficiency in future.

The rest of our paper is organized as follows. In Section II, we introduce the system model, assumptions, and define the metrics used in this paper. We analyze these metrics based on the mobility and traffic patterns of an MU in Section III. Then, in Section IV, we show the numerical results of our analysis on authentication delay and call dropping probability. Finally, we draw conclusions in Section V.

II. System Model and Metrics

In this section, we propose a system model for the basic challenge/response authentication mechanism in wireless networks. Then, we define the security and QoS metrics.

A. General Model and Assumptions

We consider that an MU is roaming within a *foreign network domain* with a number of M subnets of equal size in it. An example of this model is shown in Fig. 1. Each subnet has an access point (AP) in it. A local authentication server

0-7803-8784-8/$20.00 (C) 2004 IEEE

(LAS) is a server that takes charge of the authentication in this network domain, and all of the subnets share security associations with the LAS. A security association (SA) is a trust relationship that provides credentials such as keys for cryptographic operations. In addition, the LAS shares an SA with the authentication architecture, which is composed of many authentication servers.

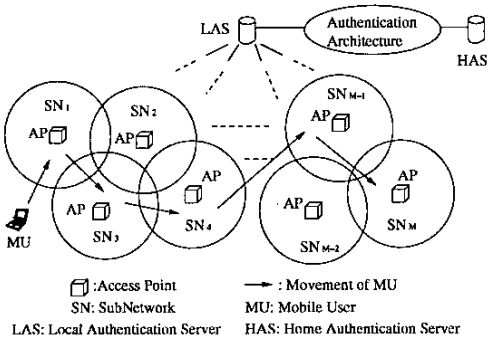

Fig. 1. System Model: Roaming within a Foreign Network.

If we define the residence time of the MU in *one subnet* as T_r , and assume that the probability density function (PDF) of T_r, $f_{T_r}(t)$, is Gamma distribution with mean $1/\mu_r$ and variance V, the Laplace transform of $f_{T_r}(t)$, $F_r(s)$, is:

$$F_r(s) = (\frac{\mu_r\gamma}{s+\mu_r\gamma})^\gamma, \quad \text{where} \quad \gamma = \frac{1}{V\mu_r^2}. \tag{1}$$

Assume that the number of subnets that an MU passes in a network domain is uniformly distributed between 1 and M. The Laplace transform of the PDF of the residence time in a network, $F_M(s)$, and the mean value of the residence time in a network, $\overline{T}_M$, become [6]:

$$F_M(s) = \frac{1}{M}(\frac{\mu_r\gamma}{s+\mu_r\gamma})^\gamma \frac{1-(\frac{\mu_r\gamma}{s+\mu_r\gamma})^{\gamma M}}{1-(\frac{\mu_r\gamma}{s+\mu_r\gamma})^\gamma}, \tag{2}$$

$$\overline{T}_M = -\frac{\partial F_M(s)}{\partial s}|_{s=0} = \frac{M+1}{2\mu_r}. \tag{3}$$

Although some other parameters such as the size of subnets and speed of MUs will affect the residence time of MUs, we do not go further to evaluate these parameters in this paper and will analyze them in our future work.

In this paper, we want to analyze the impact of authentication on voice traffic because it has simple and explicit distribution models. As for other traffic such as data flow, similar analysis can be obtained by replacing the corresponding distribution model in our assumption. Therefore, we assume that the call arrival rate of the MU, which includes the incoming and outcoming calls, is Poisson process with rate λ_u, and a call duration time, T_D, has an exponential distribution with mean value $1/\eta$. The PDFs of the inter-request time, $f_{T_A}(t)$, and call duration time, $f_{T_D}(t)$, are given by:

$$f_{T_A}(t) = \lambda_u e^{-\lambda_u t}, \quad f_{T_D}(t) = \eta e^{-\eta t}. \tag{4}$$

B. Challenge/Response Authentication

In a challenge/response based authentication, a user is identified with a shared SA by an authentication server, which sends a random number to the user for encryption and verifies the returned value with decryption [3]. The challenge/response authentication has three types of signal diagram for three types of authentication requests shown in Fig. 2:

- *Case A: an MU is in intra-domain handoff authentication.* An *intra-domain handoff authentication* is initiated when an MU is crossing the boundaries of subnets in the network domain with an on-going service. In this case, the LAS replies a challenge value, a random value, to the MU. Because there is an on-going session between the MU and the AP, one session SA exists between the MU and the LAS. Thus, the MU encrypts the challenge value with the session SA into a so-called response and replies it. Then, the LAS can authenticate the MU.
- *Case B: an MU is in session authentication in a foreign network.* A *session authentication* is initiated when an MU starts a connection in a subnet. In this case, the LAS does not share an SA with the MU, thus forwarding the challenge and response values to the HAS of the MU. After authentication, the HAS may generate the secret credentials such as keys and send them to the LAS.
- *Case C: an MU is in inter-domain handoff authentication.* An *inter-domain handoff authentication* is initiated when an MU is crossing the boundaries of different networks with an on-going service. In this case, the signaling is similar with that in case B, except that the MU needs registration to its home agent (HA) because we assume that a registration happens during inter-domain roaming.

C. Definitions of Metrics

In this section, we define security levels, authentication cost, delay and call dropping probability for QoS evaluation.

1) Security Levels: The concept of *security level* here is a value to indicate the level of protection from authentication. We categorize the security according to the protection for integrity, confidentiality and resource availability in Table I:

TABLE I
SECURITY LEVEL CLASSIFICATION

Security Level	Integrity	Confidentiality	Availability Protection
0	No	No	No
1	No	No	Low
2	No	No	Medium
3	Yes	Yes	High

- *Security Level 0*: Any MUs can send data through an AP without authentication. Thus, the integrity, confidentiality, and resource availability cannot be protected.
- *Security Level 1*: Authentication is implemented by verifying MAC address without key generation. The data integrity and confidentiality cannot be protected without the key for communication, but the network resource is slightly protected by identifying the MAC address.
- *Security Level 2*: Authentication is implemented with shared SA without key generation. The network resources can be protected by authorizing legitimate users,while the data integrity and confidentiality are not guaranteed

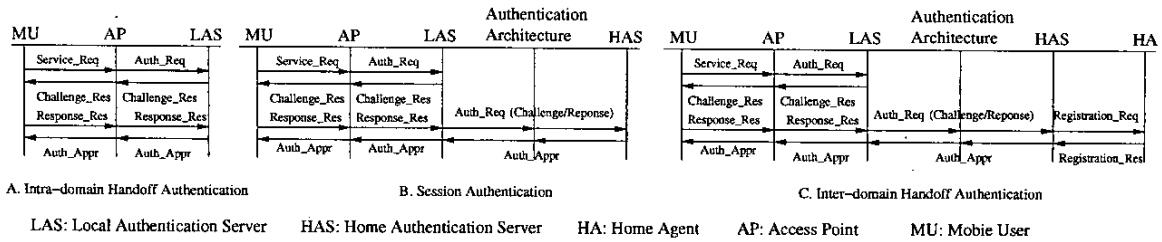

Fig. 2. Challenge/Response Authentication in Wireless Networks.

without the key, which may compromise the availability of the network resources.

- *Security Level 3*: Authentication is implemented with shared SA with key generation. The data integrity and confidentiality can be guaranteed. The network resource is also protected with strong cryptography techniques.

2) Average Authentication Cost, Delay, and Call Dropping Probability: Throughout this paper, the *average authentication cost*, $C(i)$, is defined as follows:

$$C(i) = \sum_{q=1}^{3} \lambda_q [C_q^{(s)}(i) + C_q^{(p)}(i)], \quad q \in \{1,2,3\}, \quad i \in \{0,1,2,3\}, \tag{5}$$

where i is the security level, q is the authentication type. $q = 1$ means an intra-domain handoff authentication, $q = 2$ denotes a session authentication, and $q = 3$ indicates an inter-domain handoff authentication. $C_q^{(s)}(i)$ and $C_q^{(p)}(i)$ are the signaling load and the encryption/decryption cost at security level i for authentication type q, respectively. λ_q is the arrival rate of authentication requests for authentication type q.

The *authentication delay*, $T_q(i)$, is defined as the time from when the MU sends out an authentication request to when the MU receives the authentication reply at security level i. Therefore, we define *average authentication delay*, $T(i)$, as:

$$T(i) = \sum_{q=1}^{3} \lambda_q T_q(i), \quad q \in \{1,2,3\}, \quad i \in \{0,1,2,3\}. \tag{6}$$

In our paper, we consider that the call is dropped when an authentication delay is greater than a threshold time [7], [8]. Then, we define *average call dropping probability*, $P(i)$, as:

$$P(i) = \frac{\sum_{q=1}^{3} \lambda_q P_q(i)}{\sum_{q=1}^{3} \lambda_q}, \quad P_q(i) = P_{T_q(i)}(T_q(i) > T_{th}), \tag{7}$$

where T_{th} is a threshold time, $P_{T_q(i)}(T_q(i) > T_{th})$ is the probability that an authentication delay is greater than the threshold time T_{th} for authentication type q. Next, we evaluate all of the variables to get $C(i)$, $T(i)$, and $P(i)$, respectively.

III. Performance Analysis

In this section, we first analyze $C_q^{(s)}(i)$, $C_q^{(p)}(i)$, $T_q(i)$, and $P_q(i)$, based on the challenge/response authentication shown in Fig. 2. We only provide the analysis while $q = 3$ because the inter-domain handoff authentication, i.e, $q = 3$, is most complicated and we have limited space here. The analysis for $q = 1, 2$ follows the same clue as $q = 3$, and we will provide the numerical results of these cases in Section IV. Then, λ_q, are derived with mobility and traffic patterns of the MU. Finally, $C(i)$, $T(i)$ and $P(i)$ can be obtained.

A. Performance Analysis per Authentication

We analyze $C_q^{(s)}(i)$, $C_q^{(p)}(i)$, $T_q(i)$, and $P_q(i)$ in the case of $q = 3$ at different security levels, which are necessary to obtain $C(i)$, $T(i)$, and $P(i)$. For convenient analysis, we define a set of cost parameters in Table II.

TABLE II
Authentication Cost Parameters

Symbol	Description
c_s	Transmission cost on one hop
c_p	Encryption/decryption cost on one hop
c_v	Verification cost at an authentication server
c_{us}	Encryption/decryption cost for a session key
c_g	Key generation cost
c_{ts}	Transmission cost for a session key to other communication identities
c_{rg}	Registration cost

1) Authentication Cost per Operation: $C_q(i)$, is composed of $C_q^{(s)}(i)$ and $C_q^{(p)}(i)$, which depend on the authentication type q and security level i. The signaling costs, $C_3^{(s)}(i)$, can be derived from the signaling diagrams in Fig. 2.C as follows:

$$C_3^{(s)}(i) = \begin{cases} 2(N_h+1)c_s, & i = 0 \\ 2(N_h+2)c_s, & i = 1 \\ 2(N_h+3)c_s, & i = 2,3 \end{cases}, \tag{8}$$

where N_h is the number of hops between the MU and its HAS. The coefficients before c_s denote the number of hops by which the whole authentication process passes. Similarly, $C_3^{(p)}(i)$, can be written as:

$$C_3^{(p)}(i) = \begin{cases} c_{rg}, & i = 0 \\ 2N_h c_p + c_v + c_{rg}, & i = 1 \\ 2(N_h+1)c_p + c_{us} + c_v + c_{rg}, & i = 2 \\ 2(N_h+1)c_p + 2c_{us} + c_v + c_g + c_{ts} + c_{rg}, & i = 3 \end{cases}, \tag{9}$$

where the coefficients before c_p denote the number of hops, on which we should consider the encryption/decryption cost during one authentication. At security level 0, no cost is needed for encryption/decryption. At security levels 1, 2, and 3, the credentials needed to be verified at an authentication server, thus the cost is c_v. At security level 2 and 3, challenge/response values are encrypted for authentication, thus one cost variable c_{us} is needed. In addition, at security level 3, keys are encrypted and transmitted to the MU at the HAS, thus additional cost c_{us} and c_{ts} are required.

2) Delay per Authentication: We define a set of time parameters shown in Table III for convenient description. Then, we use the signaling diagram in Fig. 2.C to derive $T_3(i)$ as shown in (10). The coefficients before T_{tr} and T_{pr} denote

$$T_3(i) = \begin{cases} 2T_a + 2(N_h+1)(T_{pr}+T_{tr}) + 2(N_h-1)T_{sq} + T_{rg}, & i=0 \\ 2(N_h+2)(T_{tr}+T_{pr}) + 3T_a + 2T_v + 2(N_h-2)T_{sq} + 2N_hT_{ed} + T_{rg}, & i=1 \\ 2(N_h+3)(T_{tr}+T_{pr}) + 4T_a + 2T_v + T_{us} + 2(N_h+1)T_{ed} + 2(N_h-2)T_{sq} + T_{rg}, & i=2 \\ 2(N_h+3)(T_{tr}+T_{pr}) + 4T_a + 2T_v + 2T_{us} + 2(N_h+1)T_{ed} + 2(N_h-2)T_{sq} + T_g + T_{ts} + T_{rg}, & i=3 \end{cases} \quad (10)$$

the number of hops by which the authentication messages pass, while the factors before T_{ed} are the number of hops on which the encryption/decryption exist. The numbers before T_a, T_{sq} and T_v are the number of times to access the AP, intermediate authentication servers and HAS, respectively, during one authentication. At security level 2, a pair of challenge/response values is used for verification. Therefore, time T_{su} is needed. At security level 3, another T_{us} is needed to encrypt and decrypt the key generated with time T_g and transmitted to the MU. In order to protect the data communication between the communication partners, T_{ts} is needed to transfer the credentials such as keys to the other communication partners.

TABLE III
AUTHENTICATION COST PARAMETERS

Symbol	Description
T_{pr}	Message propagation time on one hop
T_{tr}	Message transmission time on one hop
T_{ed}	Message encryption/decryption time on one hop
T_a	Authentication request service & waiting time at the AP
T_{sg}	Authentication request service & waiting time at the proxy authentication server
T_v	Authentication request service & waiting time at the HAS
T_{us}	Key encryption & decryption time
T_g	Key generation time at the HAS
T_{ts}	Transmission time for the session key to the other communication identities such as HA
T_{rg}	Registration request service & waiting time at the HA

3) Call Dropping Probability per Authentication: In order to evaluate $P_3(i)$, we consider the authentication delay in (10). We only consider the time variables, T_{sq}, T_a, T_v, and T_{rg}, as random variables because the variance of the other time variables are relatively small. Thus, $P_3(i)$ can be written as $P_3(i) = P_{T_3(i)}\{T_3(i) > T_{th}\}$ with $T_3(i)$ shown in (10). The problem now is changed to find the PDF of $T_3(i)$. If we assume that two conditions exist: (1)$M/M/1$ queues are applied at APs, authentication servers, and HAs; (2)The PDFs of T_{sq}, T_a, T_v, and T_{rg} are independent identical distribution (IID), the PDF of T_{sq}, T_a, T_v, and T_{rg}, $w(t)$, can be shown as [9]:

$$w(t) = (\mu_s - \lambda_s)e^{-(\mu_s-\lambda_s)t}, \quad (11)$$

where μ_s and λ_s are the service and arrival rate of requests, respectively. The PDF of $T_3(i)$ can be determined by:

$$f_{T_3(i)}(t) = \begin{cases} \frac{\xi(\xi t)^{2N_h}e^{-\xi t}}{\Gamma(2N_h+1)}, & i=0 \\ \frac{\xi(\xi t)^{2N_h+1}e^{-\xi t}}{\Gamma(2N_h+2)}, & i=1 \\ \frac{\xi(\xi t)^{2N_h+2}e^{-\xi t}}{\Gamma(2N_h+3)}, & i=2,3 \end{cases}, \quad (12)$$

where $f_{T_3(i)}(t)$ is the PDF of $T_3(i)$, $\Gamma(x) \triangleq \int_0^\infty s^{x-1}e^{-s}ds$, and $\xi = \mu_s - \lambda_s$. $P_3(i)$ can be obtained with (12).

B. Arrival Rates of Authentication Requests

Since the authentication requests are categorized into three types, we analyze the arrival rates of different types of authentication requests, i.e., $\lambda_q, (q = 1, 2, 3)$ next.

1) Arrival Rate of Intra-domain Handoff Authentication Requests, λ_1: The intra-domain handoff authentication happens whenever an MU crosses the boundaries inside a network domain with an on-going service. In order to calculate the arrival rate of intra-domain handoff authentication requests, we categorize the calls into four events shown in Fig. 3:(1) Y_1 is the event that one call starts before entering a network and ends in the network; (2) Y_2 is the event that one call starts and ends in the same network; (3) Y_3 is the event that one call starts in a network and ends after leaving the network; (4) Y_4 is the event that one call is held on throughout the residence time of an MU in a network. Then, λ_1 can be written as:

$$\lambda_1 = \lambda_u Pr_1(\overline{N}_{a1} - 1) + \lambda_u Pr_2(\overline{N}_{a2} - 1) + \lambda_u Pr_3(\overline{N}_{a3} - 1) + \lambda_u Pr_4(\overline{N}_{a4} - 1), \quad (13)$$

where Pr_j, $(j = 1, 2, 3, 4)$, is the probability that event Y_j happens, and $\overline{N}_{aj}$, is the average number of subnets passed by an MU in current network in event Y_j. Pr_j can be derived from Fig. 3 in (17) at next page. In (17), T_D's PDF is shown in (4), T_{Dr} is the residual time of T_D with the same PDF as T_D in (4), T_M's Laplace transform of PDF is shown in (2), and T_{Mr} is the residual time of T_M with Laplace transform of PDF, $F_{Mr}(s)$, as:

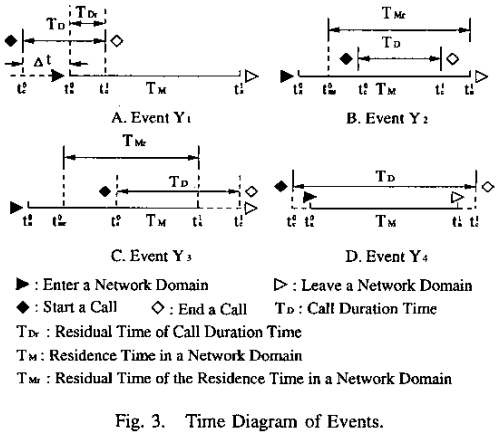

Fig. 3. Time Diagram of Events.

$$F_{Mr}(s) = \frac{1 - F_M(s)}{s\overline{T}_M}, \quad (14)$$

where $\overline{T}_M$ and $F_M(s)$ are defined in (3) and (2), respectively. In (17), $X_1 \triangleq T_M - T_{Dr}$, $X_2 \triangleq T_{Mr} - T_D$, and $X_3 \triangleq T_D - T_{Mr}$. Thus, $f_{X_j}(t), (j = 1, 2, 3)$ can be computed as:

$$f_{X_j}(t) = \begin{cases} \mathscr{L}^{-1}\left\{\frac{(\eta+s)F_M(s)}{\eta}\right\}, & j=1 \\ \mathscr{L}^{-1}\left\{F_{Mr}(s)\frac{\eta+s}{\eta}\right\}, & j=2 \\ \mathscr{L}^{-1}\left\{\frac{\eta}{(\eta+s)F_{Mr}(s)}\right\}, & j=3 \end{cases}, \quad (15)$$

where $F_{Mr}(s)$ and $F_M(s)$ are shown in (14) and (2), respectively, $\frac{\eta}{\eta+s}$ is the Laplace transform of the PDF of T_D shown in (4). Note that $f_M(t)$ and $f_{Mr}(t)$ can be obtained by:

$$f_M(t) = \mathscr{L}^{-1}\{F_M(s)\}, \quad f_{Mr}(t)dt = \mathscr{L}^{-1}\{F_{Mr}(s)\}, \quad (16)$$

$$Pr_j = \begin{cases} \int_0^\infty \lambda_u \Delta t e^{-\lambda_u \Delta t} \cdot Pr(T_D > \Delta t) d(\Delta t) \cdot Pr(T_{Dr} \le T_M) = \frac{\lambda_u}{(\lambda_u+\eta)^2} \int_0^\infty f_{X_1}(t)dt, & j=1 \\ Pr(T_D < T_{Mr}) \cdot Pr(t_{mr}^0 \le t_c^0 < t_{mr}^0 + T_{Mr}) = \int_0^\infty f_{X_2}(t)dt \int_0^\infty \lambda_u t e^{-\lambda_u t} f_{Mr}(t)dt, & j=2 \\ Pr(T_D > T_{Mr}) \cdot Pr(t_{mr}^0 \le t_c^0 < t_{mr}^0 + T_{Mr}) = \int_0^\infty f_{X_3}(t)dt \int_0^\infty \lambda_u t e^{-\lambda_u t} f_{Mr}(t)dt, & j=3 \\ \int_0^\infty \lambda_u \Delta t e^{-\lambda_u \Delta t} \cdot Pr(T_D > \Delta t) d(\Delta t) \cdot Pr(T_{Dr} > T_M) = \frac{\lambda_u}{(\lambda_u+\eta)^2}[1 - \int_0^\infty f_{X_1}(t)dt], & j=4 \end{cases}, \quad (17)$$

Therefore, $Pr_j, (j = 1, 2, 3, 4)$ are determined.

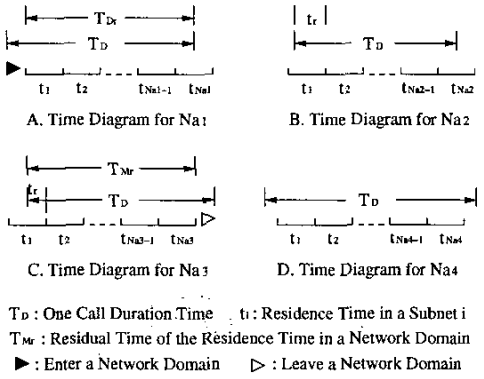

Fig. 4. Time Diagram for Number of Subnets Passed by in One Call.

Next, we need to evaluate $\overline{N}_{aj}$ in the event Y_j according to the time diagrams shown in Fig. 4. In order to evaluate $\overline{N}_{a1}$ and $\overline{N}_{a2}$, we consider a theorem in [10], which says that given call holding time and subnet residence time with Gamma distribution, the average number of subnets passed by an MU within a call can be obtained. In event Y_1 and Y_2, the call duration time in the network domain are T_{Dr} and T_D, respectively, which are exponential distribution, one special case of Gamma distributions. Therefore, $\overline{N}_{a1}$ and $\overline{N}_{a2}$ can be obtained with a theorem in [10] as:

$$\overline{N}_{a1} = \overline{N}_{a2} = \frac{\mu_r}{\eta}. \quad (18)$$

On the other hand, note that the call duration time in events Y_3 and Y_4, i.e., T_{Mr} and T_M are not Gamma distributions, thus we cannot obtain $\overline{N}_{a3}$ and $\overline{N}_{a4}$ with the theorem in [10]. Therefore, we need to derive $\overline{N}_{a3}$ and $\overline{N}_{a4}$ next.

From Fig. 4.C, we have:

$$T_{Mr} = t_r + \sum_{i=2}^{N_{a3}} t_i, \quad (19)$$

where t_i is the residence time of an MU in a subnet i, and T_{Mr} has a PDF in (16). Therefore, by taking Laplace transform on both sides of (19), we have:

$$F_{Mr}(s) = F_{t_r}(s) G_{N_{a3}-1}(z)|_{z=F_r(s)}, \quad (20)$$

where $F_r(s)$ is defined in (1), $G_{N_{a3}-1}(z)$ is the generating function of the PDF of $N_{a3} - 1$. Thus,

$$\begin{aligned} \overline{N}_{a3} &= \frac{\frac{\partial [G_{N_{a3}-1}(z)|_{z=F_T(s)}]}{\partial s}|_{s=0} + 1}{} \\ &= \frac{2M^2-M-1}{12T_M\mu_r} + \frac{(M+1)}{4}\frac{(\gamma+1)}{\gamma} + 1. \end{aligned} \quad (21)$$

As for $\overline{N}_{a4}$, according to Fig.4.D, $\overline{N}_{a4}$ is equal to the average number of subnets that an MU passes in the network. Because we assume that the number of subnets that an MU passes in a network domain is uniformly distributed between 1 and M in the system model [6], we have:

$$\overline{N}_{a4} = \frac{M+1}{2}. \quad (22)$$

Since the variables Pr_j and $\overline{N}_{aj}$ $(j = 1, 2, 3, 4)$ are obtained, λ_1 can be evaluated here.

2) Arrival Rate of Session Authentication, λ_2: After an MU has moved into a network domain, a session authentication is initiated whenever a call arrives. Therefore,

$$\lambda_2 = \lambda_u. \quad (23)$$

3) Arrival Rate of Inter-Domain Handoff Authentication, λ_3: The inter-domain handoff authentication requests happen when an MU enters the network domain with an on-going service. Therefore, λ_3 can be obtained by:

$$\lambda_3 = \lambda_u(Pr_1 + Pr_4), \quad (24)$$

where Pr_1 and Pr_4 can be found in 17.

Thus, we obtain all the variables needed to evaluate $C(i)$, $T(i)$ and $P(i)$. By substituting these variables into (5), (6), and (7), $C(i)$, $T(i)$, and $P(i)$ can be determined.

IV. Numerical Results

In this section, we evaluate the effects of mobility and traffic patterns on $C(i)$, $T(i)$, and $P(i)$ at different security levels. We only provide the analysis results in our paper without comparison because of lack of similar study in authentication before. The parameters for evaluation are shown in Table IV. For the values of authentication costs, we assume that $c_p = 1$, and weight the other costs with the ratio of the time needed to finish the operation. The values of the authentication time in Table IV come from [11] with the assumption that APs and LASs are connected with links of 10Mbps.

TABLE IV
Parameters for Evaluation on QoS Metrics

Parameters for Authentication Cost					
c_s	c_p	c_v	c_g	c_{ts}	N_h
10	1	20	1	110	10
Parameters for Authentication Delay					
T_{th}	T_{pr}	T_{tr}	T_{ed}	T_g	M
3s	20 μ s	4ms	2ms	2ms	120
Parameters for Random Variables					
λ_u	η	γ	μ_r	ξ	
0.1 min^{-1}	0.3 min^{-1}	225	1/15 min^{-1}	15 sec^{-1}	

The effects of residence time of an MU in a subnet are shown in Fig. 5, 6, and 7. In Fig. 5, $C(i)$ decreases with the increase of the residence time of an MU in a subnet because less intra-domain handoff authentication requests happen in this case. In Fig. 6, $T(i)$ decreases with the increase of the residence time of an MU in a subnet. This trend is also due to the decrease of the intra-domain handoff authentication requests. In Fig. 7, $P(i)$ increases with the increase of the residence time of an MU in a subnet. Because the increased residence time means less intra-domain handoff authentication, the major part of the call dropping probability approximates that of session authentication according to (7). Since the call

dropping probability for session authentication is far more than that in intra-domain handoff authentication, $P(i)$ will increase and approximate the call dropping probability in session authentication with the increase of the residence time. As we can see, the higher the security levels will cause more authentication cost, delay, and dropping probabilities.

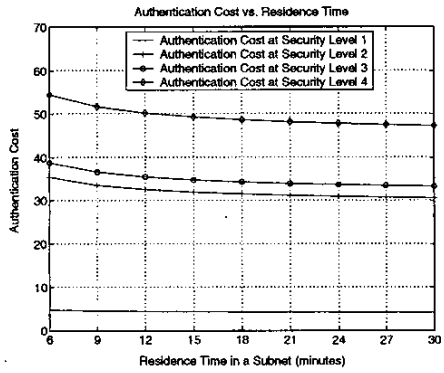

Fig. 5. Authentication Cost vs. Residence Time in a Subnet.

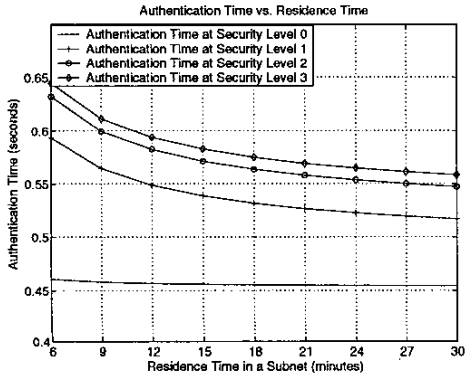

Fig. 6. Authentication Time vs. Residence Time in a Subnet.

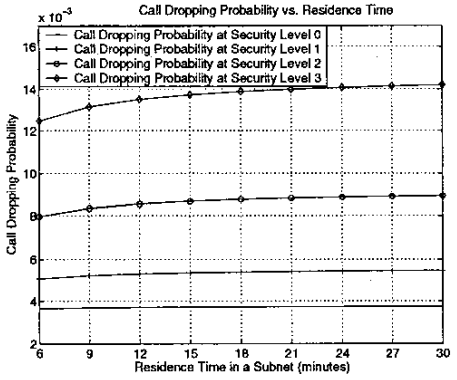

Fig. 7. Call Dropping Probability vs. Residence Time in a Subnet.

For the effects of traffic load in terms of call arrival rate, λ_u, we only show the relationship between $T(i)$ and λ_u in Fig. 8 due to limited space. However, λ_u has the same effect on $C(i)$ and $T(i)$, in which $C(i)$ and $T(i)$ are proportional to λ_u. On the other hand, λ_u has no effect on $P(i)$. As we can see in (7), λ_u is a factor of λ_1, λ_2, and λ_3, and will be removed in (7). Thus, λ_u cannot change the value of $P(i)$.

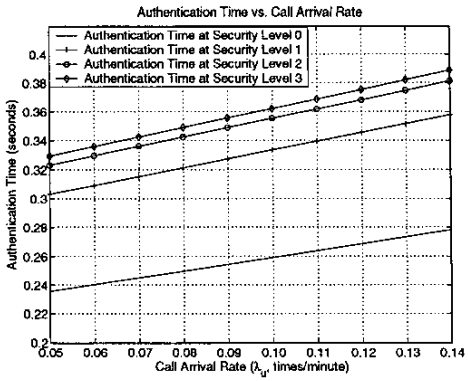

Fig. 8. Authentication Time vs. Call Arrival Rate.

V. Conclusions

In this paper, we address the impact of authentication on security and quality of service (QoS), which is critical to deliver secure and efficient services in public wireless networks such as wireless local area network (WLAN). We analyze the authentication cost, delay, and call dropping probability at different security levels in wireless networks based on the system model with challenge/response mechanism. In the analysis, the mobility and traffic patterns are taken into account for the QoS at different security levels. Therefore, this work provides a solid ground for deep understanding of authentication impact, and demonstrates a framework for future design of efficient authentication scheme in various 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] 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] C. Perkins and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions," *RFC3012*, November 2000.

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

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

[6] 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.

[7] F. Hu and N. Sharma, "Priority-Determined Multiclass Handoff Scheme With Guaranteed Mobile QoS in Wireless Multimedia Networks," *IEEE Transactions on Vehicular Technology*, vol. 53, pp. 118–135, January 2004.

[8] W. Wang and I. Akyildiz, "A New Signaling Protocol for Intersystem Roaming in Next-Generation Wireless Systems," *IEEE Journal on Selected Areas in Communications*, vol. 19, pp. 2040–2052, October 2001.

[9] D. Gross and C. Harris in *Fundamentals of Queueing Theory*, 1974.

[10] Y. Fang, I. Chlamtac, and Y. Lin;, "Channel Occupancy Times and Handoff Rate for Mobile Computing and PCS Networks," *IEEE Transactions on Computer*, vol. 47, pp. 679–692, June 1998.

[11] 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.