行政院國家科學委員會專題研究計畫　期中進度報告

UMTS 全 IP 網路協定及應用(1/3)

計畫類別：個別型計畫
計畫編號：NSC94-2213-E-009-104-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：國立交通大學資訊工程學系(所)

計畫主持人：林一平

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 95 年 5 月 12 日

行政院國家科學委員會專題研究計畫成果報告

UMTS 全 IP 網路協定及應用

UMTS All IP Network Protocols and Applications

計畫編號：94-2213-E-009-104（1/3）
執行期限：94 年 8 月 1 日至 95 年 7 月 31 日

主持人：林一平　　交通大學 資訊工程系

一、中文摘要

本計畫在本年度研究無線網路和行動電話網路整合環境中 802.1X 的認證。在 IEEE 802.1X 的標準裡，EAPOL 協定中定義了幾個超時定時器(Timeout timer)，這些超時定時器的預設值皆相同。我們發現不同的 EAPOL 訊息交換，其延遲變異很大。本計畫用模型研討，調整各別定時器的值，以改良原來用相同超時值的效能。我們的研究提供了為 IEEE 802.1X 操作選擇合適超時值的方針。

關鍵詞: 802.1X、EAPOL、超時定時器

Abstract

This project studies IEEE 802.1X authentication for WLAN and cellular integration. In the IEEE 802.1X standard, several timeout timers are defined for message exchanges in the EAPOL protocol, where the same fixed value is suggested for these timeout timers. We observe that the delays for the EAPOL message exchanges may significantly vary. A modeling study is performed to tune the values of individual timers to yield better performance than that for the identical timeout period setting. Our study provides guidelines to select appropriate timeout values for IEEE 802.1X operation.

Key words: 802.1X, EAPOL, timeout timers

二、前言

The IEEE 802.1X standard specifies authentication and authorization for IEEE 802 LAN [1], which has also been widely adopted for mobile devices to access *Wireless Local Area Network* (WLAN). Furthermore, if WLAN is integrated with cellular network (such as GSM or UMTS [6]), the SIM module (in the mobile device) and the *Authentication Center* (AuC) are utilized together with IEEE 802.1X for authentication. An example of WLAN and cellular integration (in terms of authentication) is illustrated in **Figure 1**.

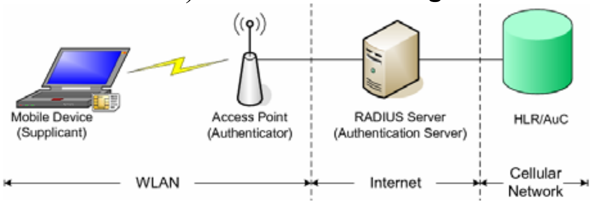


Figure 1: A WLAN and Cellular Integration Environment

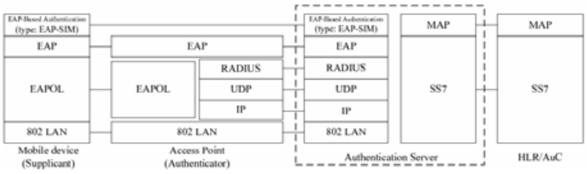


Figure 2: The Protocol Stack for WLAN and Cellular Integration

. **Figure 2** illustrates the protocol stack for the WLAN and cellular integration system. In this figure, the mobile device to be authenticated is called a *supplicant*. The server (typically a RADIUS server) performing authentication is called the *authentication server*. The *authenticator* (e.g., a wireless access point) facilitates authentication between the IEEE 802.1X supplicant and the authentication server.

The integrated system utilizes the *Extensible Authentication Protocol* (EAP) to support multiple authentication mechanisms based on the challenge-response paradigm [4]. The IEEE 802.1X supplicant encapsulates the EAP packets in *EAP over LAN* (EAPOL) frames before they are transmitted to the authenticator. Upon receipt of an EAPOL frame, the authenticator decapsulates the EAP packet from the EAPOL frame. Then the EAP packet is sent to the authentication server using the RADIUS protocol [5]. Implemented on top of UDP, RADIUS provides mechanisms for per-packet authenticity and integrity verification between the authenticator and the authentication server.

三、研究目的及文獻探討

IEEE 802.1X authentication for the WLAN and cellular integration network has been investigated in [10], [11] and [12]. These studies focused on the design of the network integration architectures, and proposed IEEE 802.1X authentication procedures for the integration network. In [9], we proposed an integration solution for *Third Generation* (3G) and WALN services, called the *WLAN-based GPRS Support Node* (WGSN). WGSN re-uses 3G mechanisms for WLAN user authentication and network access without introducing new procedure and without modifying the existing 3G network components. In WGSN, the mobile device must obtain an IP address before it is authenticated by the HLR/AuC. This paper describes IEEE 802.1X authentication that enhances the WGSN security by allowing a mobile device to be authenticated before it is assigned an IP address.

In our solution, the WLAN and cellular integration network in **Figure 1** employs EAP-SIM authentication, which is an EAP-based authentication protocol utilizing the GSM *Subscriber Identity Module* (SIM) [3]. In GSM, a secret key *Ki* is stored in the HLR/AuC as well as in the SIM. The authentication server communicates with the HLR/AuC to obtain the GSM authentication information through the *Mobile Application Part* (MAP) implemented on top of the *Signaling System Number 7* (SS7) protocol [6]. In the EAP-SIM authentication, the MAP is responsible for retrieving the GSM authentication information in the HLR/AuC.

In the implementation of IEEE 802.1X authentication for WGSN, we observe that the elapsed times for authentication message pairs exchanged between the mobile device and the network are different. In IEEE 802.1X specification, the message pairs are associated with fixed timeout timers. We analyze the timeout timers used in IEEE 802.1X authentication and improve the performance of IEEE 802.1X authentication by selecting appropriate timer values.

四、研究方法

Figure 3 illustrates the authentication message flow of the SIM-based IEEE 802.1X authentication procedure.

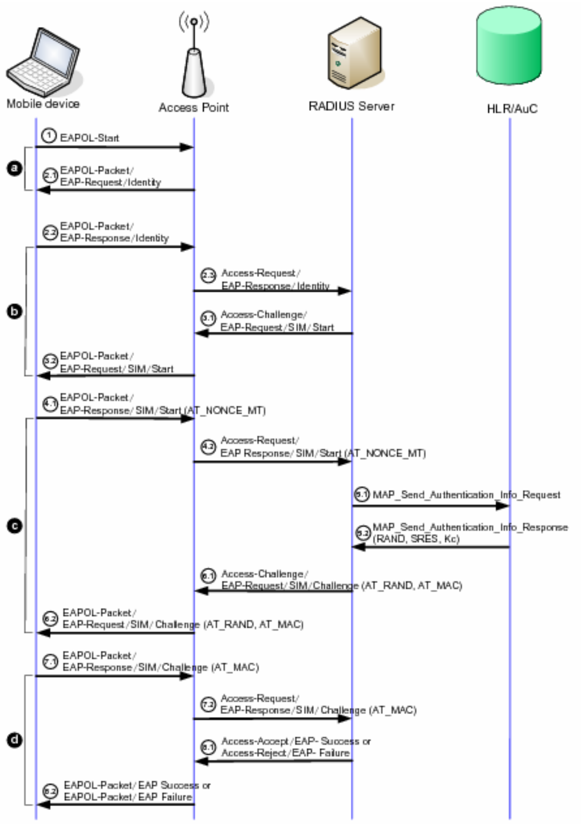


Figure 3: SIM-based IEEE 802.1X Authentication Message Flow

In the IEEE 802.1X supplicant (mobile device), three EAPOL timers are defined:

1. *startWhen* (associated with message pair ⓐ in **Figure 3**): When the IEEE 802.1X supplicant initiates the authentication, it sends EAPOL-Start to the authenticator and starts the *startWhen* timer. If the supplicant has not received any response from the authenticator after this timer expires, it resends EAPOL-Start. The supplicant gives up when it sends EAPOL-Start for n_1 times. In the IEEE 802.1X specification [1], the default n_1 value is 3. The default value of the *startWhen* timer is 30 seconds.
2. *authWhile* (associated with message pairs ⓑ, ⓒ, and ⓓ in **Figure 3**): Every time the supplicant sends an authentication message (Steps 2.2, 4.1, and 7.1 in **Figure 3**), it starts the *authWhile* timer. If the supplicant does not receive any response from the authenticator after this timer has expired, the supplicant sends an EAPOL-Start message to re-start the authentication procedure. The supplicant gives up after it has consecutively sent EAPOL-Start for n_2 times. The default n_2 value is 3. The default value of the *authWhile* timer is 30 seconds.
3. *heldWhile* (associated with Step 8.2 message in **Figure 3** if the client fails the authentication): If the IEEE 802.1X authentication fails, the supplicant has to wait for a period *heldWhile* before it re-starts the authentication procedure. The default value of the *heldWhile* timer is 60 seconds.

Selection of the EAPOL timer values is not trivial. If the timer value is too large, it will take long time before the mobile device detects the failure of the network (e.g., RADIUS server failure). If the timer value is too small, the timer may expire before the mobile device receives the response message. In this case, the mobile device needs to re-start the authentication process due to *false failure detection*.

Table 1 shows the *expected Round-Trip Times* (RTTs) of message exchanges that measured from the WGSN implemented in National Chiao Tung University. These measurements do not experience waiting delays due to queuing at the network nodes (i.e., AP, RADIUS server and HLR/AuC).

Table 1: Expected Round-Trip Times for EAP-SIM Authentication Messages (Without Queuing Delays)

Events occurring at the mobile device	Associated timer	RTT (sec.) (no queueing)
ⓐ in Figure 3	*startWhen*	0.005
ⓑ in Figure 3	*authWhile*	0.013
ⓒ in Figure 3	*authWhile*	1.087
ⓓ in Figure 3	*authWhile*	0.013

In our measurement, the mobile device and the AP are located in one subnet. The RADIUS server and the HLR are located in another subnet. The data rate of the fixed network is 100Mbps. It is observed that the RTT of a message exchange between the mobile device and the RADIUS server are much shorter than that of a message exchange between the mobile device and the HLR/AuC. This significant RTT discrepancy is due to the fact that accessing the HLR/AuC is much more time-consuming than accessing the RADIUS server. This phenomenon is especially true when the HLR/AuC is fully loaded by cellular user accesses and when the RADIUS server and the HLR/AuC are located at different cities or different countries. To reduce the false failure detection probability without non-necessary timer timeout delay, the values of the *startWhen* timer and *authWhile* timers should not be identical for all message exchanges in the IEEE 802.1X authentication. For example, the *authWhile* timer for ⓒ in Table 1 should be different from that for ⓑ and ⓓ.

We propose an analytic model to investigate the *false failure detection probability* p_f of the IEEE 802.1X authentication procedure and the expected elapsed (response) time $E[\tau]$ for executing the IEEE 802.1X authentication procedure. Input parameters and output measures used in the model are listed in **Table 2**.

Table 2: Input Parameters and Output Measures

Input Parameters				
message pair	associated timeout period	service time of message exchange	response time of message exchange	timeout probability
ⓐ	T_s	t_s	τ_s	p_s $= \Pr[\tau_s \geq \mathrm{T}_s]$
ⓑ	T_{a1}	t_{a1}	τ_{a1}	p_{a1} $= \Pr[\tau_{a1} \geq \mathrm{T}_{a1}]$
ⓒ	T_{a2}	t_{a2}	τ_{a2}	p_{a2} $= \Pr[\tau_{a2} \geq \mathrm{T}_{a2}]$
ⓓ	T_{a3}	t_{a3}	τ_{a3}	p_{a3} $= \Pr[\tau_{a3} \geq \mathrm{T}_{a3}]$
Output Measures				
p_f	the false failure detection probability of the IEEE 802.1X authentication procedure; p_f = Pr[the mobile device has consecutively sent the EAPOL-Start frame for three times]			
$\mathrm{E}[\tau]$	the expected response time of the IEEE 802.1X authentication procedure			

In **Table 2**, t_X is the RTT of the message exchange without waiting delay (i.e., the queueing at a network node) where $X = s$, a_1, a_2, or a_3. This RTT is called "service time" in the queueing model. For our measurement in Table 1, $\mathrm{E}[t_s]$ =0.05 seconds, $\mathrm{E}[t_{a1}]$ = 0.013 seconds, $\mathrm{E}[t_{a2}]$ = 1.087 seconds, and $\mathrm{E}[t_{a3}]$ = 0.013 seconds. The response time τ_X of the message exchange is the RTT of the message exchange including the queuing delay. Since we cannot conduct large-scale service trial in our IEEE 802.1X prototype, τ_X are derived from the service times using the M/G/1 queuing model. Let EAPOL message arrivals to the AP be a Poisson stream with rate λ. The service time t_X of the message exchange has an arbitrary distribution. The response time of the message exchange is represented by the random variable τ_X, the density function $f_X(\cdot)$.

Let T_X be the timeout period associated with the timer for the message pair X and p_X be the timeout probability of the message exchange.

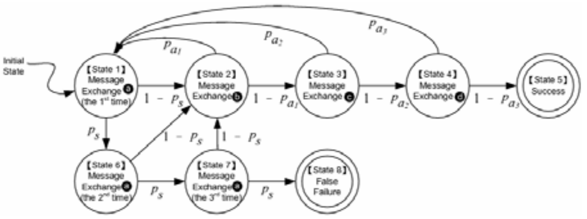
$$p_X = \Pr[\ \tau_X \geq \mathrm{T}_X\ ] = \int_{\mathrm{T}_X}^{\infty} f_X(\,t\,)\,\mathrm{d}\,t \qquad (1)$$

The expected response time $\mathrm{E}[\tau_X]$ of the message exchange can be obtained by differentiating the Laplace Transform.

$$\mathrm{E}[\tau_X] = p_X\,\mathrm{T}_X + (1 - p_X)\int_0^{\mathrm{T}_X} t\,f_X(\,t\,)\,\mathrm{d}\,t \qquad (2)$$

The probability transition diagram of the mobile device is illustrated in **Figure 4**. In IEEE 802.1X, the AP can also control the number of retransmissions for EAPOL-Start (① in **Figure 3**) sent from the mobile device to the AP. To simplify our discussion, we assume that the number of retransmissions is sufficiently large, so that the state diagram in **Figure 4** is not affected.

During IEEE 802.1X authentication, the mobile device restarts the procedure (i.e., come back to state ① again) whenever the *authWhile* timer (associated with message exchanges ⓑ, ⓒ, and ⓓ) expires. The authentication exits and is considered failed if the *startWhen* timer (associated with message exchange ⓐ) has consecutively expired for three times (i.e., the *finite state machine* (FSM) moves from state ①, ⑥, ⑦, to state ⑧).



Initial State
【State 1】 Message Exchange ⓐ (the 1st time)
【State 2】 Message Exchange ⓑ
【State 3】 Message Exchange ⓒ
【State 4】 Message Exchange ⓓ
【State 5】 Success
【State 6】 Message Exchange ⓐ (the 2nd time)
【State 7】 Message Exchange ⓐ (the 3rd time)
【State 8】 False Failure
p_{a_1}
p_{a_2}
p_{a_3}
$1 - p_s$
$1 - p_{a_1}$
$1 - p_{a_2}$
$1 - p_{a_3}$
p_s
$1 - p_s$
$1 - p_s$
p_s
p_s

Figure 4: The Probability Transition Diagram of the IEEE 802.1X Authentication Message Exchange

Let x be the probability that the FSM starts from state ① and eventually comes back to state ① (i.e., state ① may be revisited zero or more times). All possible scenarios for the probability transitions in **Figure 4** are described as follows:

Scenario I: From state ① (i.e., state ① may have been visited zero or more times), the *startWhen* timer consecutively expires for three times (i.e., the last transitions are ①

→⑥→⑦→⑧). The probability for Scenario I is xp_S^3.

Scenario II: From state ①, the *startWhen* timer consecutively expires for two times, and the procedure successes at the third try (i.e., the last transitions are ①→⑥→⑦→②→③→④→⑤). The probability for Scenario II is $x\,p_S^2(1-p_S)(1-p_{a1})(1-p_{a2})(1-p_{a3})$.

Scenario III: From state ①, the *startWhen* timer expires once, and the procedure successes at the second try (i.e., the last transitions are ①→⑥→②→③→④→⑤). The probability for Scenario III is $xp_S(1-p_S)(1-p_{a1})(1-p_{a2})(1-p_{a3})$.

Scenario IV: From state ①, the procedure successes without incurring any timer expiration (i.e., the last transitions are ①→②→③→④→⑤). The probability for Scenario IV is $x(1-p_S)(1-p_{a1})(1-p_{a2})(1-p_{a3})$.

It is apparent that the false failure probability p_f is the probability that Scenario I occurs. The success probability $(1-p_f)$ is the probability that either Scenarios II, III, or IV occur. That is,

$$p_f=\frac{p_S^3}{p_S^3+(1-p_S^3)(1-p_S)(1-p_{a1})(1-p_{a2})(1-p_{a3})} \quad (3)$$

By using (1) and (9), the value of p_f can be computed from λ, f_S, f_{a1}, f_{a2}, and f_{a3}.

Table 3: The p_X Values: Analysis Versus Simulation (T_X = 10×E[t_X], var[t_X] = E[t_X]^2,and X = s, a_1, a_2, or a_3).

λ (Unit: $\frac{1}{E[t_X]}$)	0.2	0.4	0.6	0.8
Simulation	0.0003	0.0025	0.0183	0.1353
Analytic	0.0004	0.0027	0.0196	0.1271
Error	0.0001	0.0002	0.0013	0.0082

The above analytic model is validated against simulation experiments. The simulation model follows the discrete event approach [7], and the details are omitted. **Table 3** indicates that the analytic and the simulation results are consistent (the errors are within 1%). Therefore, both the analytic model and the simulation implementation are validated.

五、結果與討論

This paper described IEEE 802.1X authentication for WLAN and Cellular integration. We presented the protocol stack and the authentication message flow, and measured the response times of all EAPOL message exchanges in the IEEE 802.1X authentication for the integrated system implemented in NCTU.

In the IEEE 802.1X standard, a fixed-value timer is used in all authentication message exchanges, which does not reflect the real network operation. A modeling study was presented in this paper to tune the values of individual timers, which yields better performance than the fixed timeout period setting.

Our study provides guidelines to select appropriate timeout periods for corresponding authentication message exchanges. For example, comparing with the fixed timeout periods setting where T_X are set to 10 seconds, the suggested setting for the timeout periods (i.e., T_S = 10 seconds, T_{a1} = 10 seconds, T_{a2} = 5 seconds, and T_{a3} = 30 seconds) decreases the false failure detection probability p_f and significantly improves the expected response time E[τ] of the IEEE 802.1X authentication procedure.

六、成果自評

(一) 對於學術研究、國家發展及其他應用方面預期之貢獻:

1. 本計畫之引申成果亦用在和工研院合作之 WLAN/Cellular 整合網路研究，以本計畫名義發表論文 1 篇，參見 [14]。
2. 本計畫之最新學術成果已投稿於 IEEE Transactions on Wireless Communications。

3. 效能評估：提出超時定時器的建議超時值來比較 IEEE 802.1X 標準中預設相同超時值的系統效能，並定量指出所提出的建議超時值有較優異的效能表現。

(二) 對於參與之工作人員，預期可獲之訓練。

1. 設計電腦模擬模型
2. 效能分析與比較

七、參考文獻

[1] LAN/MAN Standards Committee of the IEEE Computer Societ, IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control. IEEE Std 802.1X-2001, 2001.

[2] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture. 3G TS 33.102, v6.2.0, 2004.

[3] IETF. Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM). IETF Internet Draft draft-haverinen-pppext-eap-sim-05, June 2002.

[4] IETF. Extensible Authentication Protocol (EAP). IETF RFC 3748, 2004.

[5] IETF. Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865, 2000.

[6] Lin, Y.-B., and Chlamtac, I. *Wireless and Mobile Network Architectures*. John Wiley & Sons, Inc., 2001.

[7] Jerry Banks, John S. Carson, Barry L. Nelson, and David M. Nicol. *Discrete-Event System Simulation*. Prentice Hall, 2001.

[8] Lin, Y.-B., and Chen, Y.-K. Reducing Authentication Signaling Traffic in Third Generation Mobile Network. *IEEE Trans. on Wireless Commun.*, 2002.

[9] Lin, Y.-B., and Pang, A.-C. *Wireless and Mobile All-IP Networks*. John Wiley & Sons, Inc., 2005.

[10] Salkintzis, A. K., Fors, C., and Pazhyannur, R. WLAN-GPRS Integration for Next-generation Mobile Data Networks. *IEEE Wireless Communications*, 2002.

[11] Ahmavaara, K., Haverinen, H., and Pichna, R. Interworking architecture between 3GPP and WLAN systems. *IEEE Communications Magazine*, 2003.

[12] Salkintzis, A.K. Interworking techniques and Architectures for WLAN/3G Integration toward 4G Mobile Data Networks. *IEEE Wireless Communications*, 2004.

[13] Klenrock, L., *Queueing Systems; Volume I: Theory*. John Wiley & Sons, Inc., 1976.

[14] Chang, M.-F., Wu, L.-Y., and Lin, Y.-B. Lin. Performance Evaluation of a Push Mechanism for WLAN and Mobile Network Integration. Accepted and to appear in *IEEE Trans. on Vehicular Technology*.