임시 핸드오프 키를 이용한 Fast 핸드오프 프로토콜[1]

조성재, 최형기
성균관대학교 정보통신공학부
e-mail : {monocho, hkchoi}@ece.skku.ac.kr

Enhanced Fast Handoff Protocol using Temporary Handoff Key (THK)

Sung-Jae Cho, Hyoung-Kee Choi
Dept. of Information and Communication, Sungkyunkwan University

요 약

최근 무선랜의 이용이 급격하게 증가하고 있는 추세이다. 무선랜은 이동통신에 비해 빠른 데이터 전송이 가능하여 화상통신, VoIP, 동영상 스트리밍 등 멀티미디어 서비스에 적합하다. 하지만 무선랜은 서비스 제공 영역이 작기 때문에 사용자가 자주 이동할 경우 핸드오프가 발생하여 딜레이가 증가한다. 딜레이에 민감한 멀티미디어의 경우 서비스 품질에 영향을 받을 수 있으므로 이에 대한 고려가 필요하다. 본 논문에서는 핸드오프의 인증 과정에서 발생하는 딜레이를 줄이기 위해 핸드오프 할 때 사용되는 임시 키인 THK 의 사용을 제안한다. THK 를 이용할 경우 인증 서버를 이용하지 않고도 인증이 가능하며 사용하는 메시지의 양도 작기 때문에 딜레이 감소가 가능하다. 시뮬레이션 결과는 우리가 제안한 프로토콜을 이용할 경우 현재 사용 중인 프로토콜에 비해 최고 2 배의 성능 향상을 얻을 수 있음을 보여준다.

1. 서론

무선랜 서비스가 이동통신 서비스에서 제공하지 못한 부분을 보완해 주는 역할을 하면서 최근 무선랜의 이용이 증가하고 있다. 무선랜은 핫스팟에서 이동통신 보다 빠른 데이터 전송 속도를 제공하므로 멀티미디어 및 데이터 등 대용량 전송에 적합하다. 하지만 무선랜은 이동통신에 비해 서비스 영역이 작기 때문에 사용자가 자주 이동할 경우 빈번한 핸드오프가 발생하게 된다. 핸드오프는 delay 의 증가를 유발하므로 VoIP, 화상 통화 등과 같이 delay 에 민감한 멀티미디어 서비스는 경우 이용에 어려움이 발생 할 수 있다.

핸드오프로 인한 딜레이는 크게 3 가지로 분류할 수 있다[3]. 첫 번째는 핸드오프가 가능한 채널을 탐색하는 Probe delay, 두 번째는 인증에 소요되는 Authentication delay, 마지막은 재등록에 소요되는 reassociation delay 이다. 현재 핸드오프 시 발생하는 delay 를 줄이기 위한 연구가 활발하게 진행되고 있다 [4][5][6][8][9].

채널 탐색과 재등록도 중요하지만 인증의 경우 서비스 가입자와 제공자가 서로 신뢰하고 안전한 통신을 하기 위해 필수적이므로 중요하다고 할 수 있다. 현재 무선랜은 인증을 위해 IEEE 표준인 802.11i[2]를 사용하고 있다. 802.11i 는 802.1X[1]의 문제점을 해결하고 보다 강한 보안 서비스를 제공한다. 하지만 802.11i 는 이를 위해 메시지들을 추가하였고 이로 인해 delay 도 증가하게 되었다. 따라서 802.11i 와 같은 보안 강도를 유지하면서 delay 를 줄일 수 있는 방법이 필요하다. 본 논문에서는 인증 과정에서 발생하는 delay 를 최소화 하여 멀티미디어 서비스에 적합한 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 fast 핸드오프와 관련되어 진행중인 연구에 대해 설명하며, 3 장에서는 현재 무선랜 인증에 사용중인 802.11i 에 대해 설명한다. 4 장에서는 인증에 소요되는 delay 를 줄이기 위해 우리가 제안한 방법에 대해 설명하고 5 장에서는 제안한 해결책에 대한 분석과 평가를 할 것이다. 마지막으로 6 장에서는 결론과 앞으로의 연구과제에 대해 다루도록 한다.

2. 관련연구

무선랜에서 빠른 핸드오프를 제공하기 위해 다음과 같은 연구들이 진행되고 있다.

먼저 [4][5][6] 에서 저자들은 probe delay 를 줄이기 위해 neighbor graph (NG), channel mask, 그리고 syncscan 과 같은 방법을 이용하고 있다.

다음으로 [8][9]의 저자들은 빠른 핸드오프를 위해 사용자의 이동을 예측하여 사용자 Context 를 전달하는 방법들에 대해 연구하고 있다.

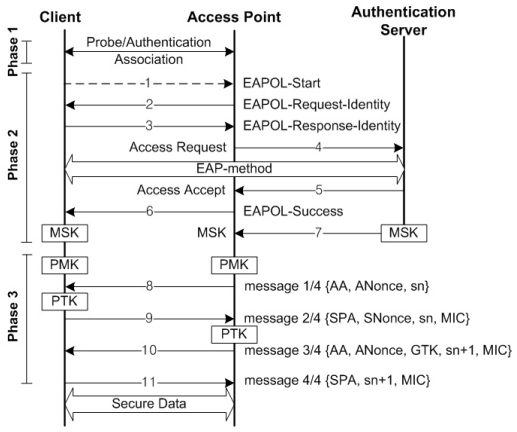
다음 장에서는 무선랜 인증에 대한 이해를 위해 현재 사용중인 802.11i 에 대하여 설명한다.

[1] 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음

3. 현재 무선랜 인증 : 802.11i

(그림 1) 은 802.11i 에서 인증에 필요한 메세지들의 흐름을 세 개의 인증요소 관점에서 보여주고 있다. 인증 요소는 (그림 1) 과 같이 인증을 요청하는 사용자인 Client, 서비스를 제공하는 AP, 그리고 DIAMETER 나 RADIUS 와 같은 인증프로토콜을 이용하여 실제적인 인증을 하는 인증서버로 구성된다.

.



(그림 1) 802.11i 인증과정

802.11i 인증절차는 크게 세 단계로 나눌 수 있는데 그림 1 에서는 첫 번째 단계를 제외하고 두 번째, 세 번째 단계만을 나타내고 있다.

1 단계는 단말과 AP 간 암호화 방식 탐지 및 인증방식을 협상하는 단계로 총 7 개의 메세지로 구성된다. 첫 번째 부분의 자세한 설명은 [10]에서 찾을 수 있다. 1 단계를 통해 단말과 AP 사이의 인증 방식 및 암호화 방식이 결정된다. 1 단계가 완료되면 단말과 AP 는 초기 인증 및 결합 상태가 되지만, 신뢰할 수 있는 보안 상태가 성립되지는 않는다.

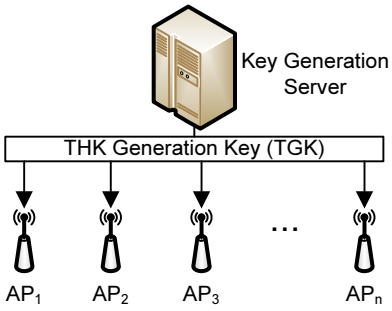
2 단계에서는 사용자 인증 및 마스터 세션 Key 분배를 하고, (그림 1) 의 메시지 1 로부터 메시지 7 까지를 포함한다. 802.11i 는 자체적으로 새로운 인증방법과 Key 분배 보단 기존에 표준으로 나와있는 인증방법들을 사용하기를 권하고 있다. 자체의 인증방법을 사용할 경우에는 인증방법에 취약점이 발견되거나 더 나은 인증방법이 나타났을 경우에 새로운 인증방법으로 변경할 수 있는 확장성이 떨어지기 때문이다. 대신에 802.11i 에서는 기존의 다양한 인증방법을 지원하기 위해 Extensible Authentication Protocol (EAP) [11]를 사용한다. EAP 자체는 인증방식이 아니라 여러 인증방식은 802.11 프로토콜에 사용할 수 있게 하는 프레임워크이다. EAP 를 사용하여 802.11i 에서 사용할 수 있는 인증방식은 EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), Protected EAP (PEAP) 등이 있다[12]. 메시지 1 부터 메시지 7 까지, 그리고 선택한 인증방식에 해당하는 메시지를 교환하고 인증결과가 성공으로 확인이 되면 단말과 인증서버가 상호인증을 하게 된다. 단, EAP 를 통한 상호 인증은 단말과 인증서버간에 이루어 지기 때문에 단말과 AP 사이의 완전한 상호 신뢰 관계를 보장할 수 없다.

단말과 인증서버는 상호인증 과정에서 사전에 공유하고 있던 정보를 통해 각각 동일한 Master Session Key (MSK) 를 생성한다. 반면에, AP 는 인증 과정에 직접 참여하지 않고 프록시 역할만 하기 때문에 스스로 MSK 를 유도할 수 없다. 메시지 7 에서 인증서버는 해당 MSK 를 AP 에게 안전하게 분배한다. 안전한 분배를 위해서는 AP 와 인증서버 사이에는 사전에 비밀을 공유하고 있어야 한다. 이후에, 단말과 AP 는 MSK 로 부터 Pairwise Master Key (PMK) 를 생성한다. 3 단계의 주요 역할은 단말과 AP 간에 동일한 PMK 를 생성하였음을 확인하고 4-Way Handshake 를 이용하여 Pairwise Transient Key (PTK) 를 생성하는 것이다. 4-Way Handshake 가 완료되면 Client 와 AP 사이에 안전한 채널 형성된다.

4. Temporary Handoff Key (THK)

802.11i 를 이용할 경우 핸드오프가 발생하면 Client 와 AP 는 (그림 1) 에서와 같이 전체 인증 과정을 다시 진행해야 한다. 하지만 무선랜의 경우 이동통신에 비해 서비스 반경이 작기 때문에 핸드오프가 자주 발생하게 되고 잦은 핸드오프는 delay 를 유발하여 seamless 한 서비스를 제공할 수 없게 된다.

인증과정에서 발생하는 delay 를 줄이고 멀티미디어 환경에 적합한 프로토콜을 위해 우리는 임시 핸드오프 키의 사용을 제안한다. Temporary Handoff Key (THK)의 기본적인 개념은 다음과 같다. 만약 Client 가 이전 AP 에서 인증 받았음을 새로운 AP 에게 증명할 수 있는 방법이 있다면 AS 를 거치지 않고도 인증이 가능할 것이다. 따라서 우리는 Client 가 새로운 AP 에게 자신이 인증 여부를 증명할 수 있는 방법으로 THK 를 제안한다. Client 는 THK 를 이용하여 새로운 AP 에게 자신의 인증 여부를 증명하게 되며 AS 를 거치지 않고도 인증이 가능하므로 인증과정에서의 delay 를 줄일 수 있게 된다.



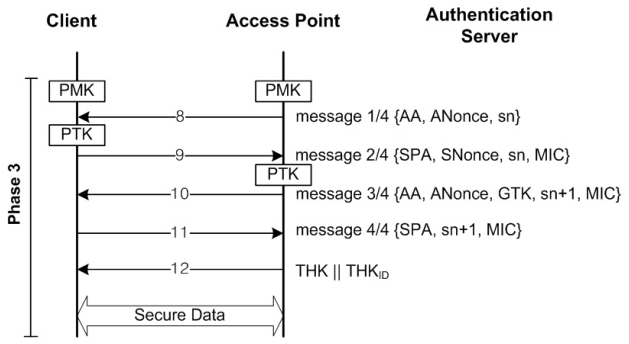
(그림 2) THK Generation Key (TGK) 분배 방식

먼저 THK 생성을 위해서 (그림 2) 에서와 같이 AP 들은 THK 생성을 위한 키(THK Generation Key)를 공유해야 한다. THK Generation Key (TGK)는 THK 의 생성과 검증에 이용되므로 모든 AP 들은 TGK 를 공유하고 있어야 한다. AP 들 사이에는 키를 공유할 수 있는 방법이 없으므로 Key Generation Server (KGS) 가

THK Generation Key (TGK)를 생성하여 AP 들에게 전달한다. 이 때 KGS 와 AP 사이는 안전한 채널이어야 한다.

TGK 는 정해진 *lifetime* 동안만 사용할 수 있으며 *lifetime* 이 끝나게 되면 KGS 에서 다시 생성되어야 한다. 또한 AP 는 THK 의 최소 사용 시간을 보장하기 위해 n 개의 TGK 저장한다. 이는 THK 의 lifetime 은 TGK 의 lifetime 을 따르므로 만약 하나의 TGK 만 이용할 경우 TGK 의 유효기간이 끝날 무렵에 생성된 THK 는 TGK 의 유효기간이 끝남과 동시에 사용할 수 없게 되기 때문이다. 이 경우 Client 는 다시 full authentication 을 수행해야 하므로 효율성의 저하를 가져온다. 이를 보완하기 위해 AP 가 n 개의 TGK 를 저장하게 되고, THK 는 생성 시간과 관계 없이 최소한 $(n-1)\times lifetime$ 동안 사용할 수 있게 된다.

초기에 Client 는 THK 가 없기 때문에 (그림 3)에서와 같이 수정된 802.11i full authentication 을 수행해야 한다. (그림 3)을 보면 4-way handshake 가 완료된 후 AP 는 THK 와 THK_{ID} 를 생성하여 Client 에게 전달 하는 것을 확인 할 수 있다. 이 때 THK 와 THK_{ID} 역시 Client 와 AP 사이의 세션 key 로 암호화 하여 안전하게 전송된다.



(그림 3) THK full authentication

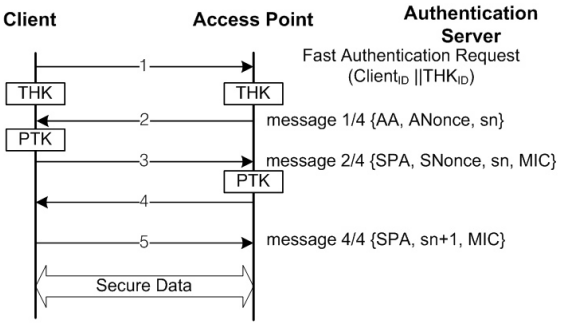
THK 와 THK_{ID} 의 구성은 다음과 같다.

$$THK = f^{1}_{TGK}(Client_{ID}, RAND) \quad (1)$$

$$THK_{ID} = TGK_{ID} \quad RAND \quad f^{2}_{TGK}(TGK_{ID} \quad Client_{ID} \quad RAND) \quad (2)$$

식(1)에서 볼 수 있듯이 THK 는 f^{1} 함수로 구성된다. f^{1} 함수는 TGK 를 key 로 사용하며 Client 의 ID 와 RAND 를 입력으로 사용한다. ClientID 를 이용하므로 Client 마다 고유한 THK 가 생성되며 RAND 를 사용하므로 매번 새로운 THK 가 생성된다. 따라서 같은 키를 반복적으로 사용하여 생기는 보안적 취약성을 방지할 수 있다. 식 (2)의 THK_{ID} 에는 THK 생성에 사용된 TGK 의 ID 인 TGK_{ID} 와 RAND, 그리고 메시지 인증 코드가 포함되어 있다. TGK_{ID} 와 RAND 는 새로운 AP 가 THK 를 생성하는데 이용된다. 메시지 인증코드는 f^{2} 를 이용 하여 생성되고 TGK_{ID} 와 RAND, 그리고 Client 의 ID 인 $Client_{ID}$ 의 변경 여부를 확인하기 위해 사용된다. 메시지 인증 코드도 TGK 를 key 로 이용한다.

THK 가 생성되면 Client 는 핸드오프 시 full authentication 과 fast authentication 중 선택할 수 있다. 만약 Client 가 fast authentication 을 선택할 경우 (그림 4)에서 보는 것과 같이 Client 는 EAPOL-Start 메시지 대신 Fast Authentication Request 에 $Client_{ID}$ 와 THK_{ID} 를 함께 전달한다. THK_{ID} 를 수신한 AP 는 먼저 저장되어 있는 TGK 들과 비교하여 TGK_{ID} 의 유효성을 확인하고 TGK_{ID} 의 유효성이 확인 되면 f^{2} 함수를 이용하여 TGK_{ID}, RAND, ID_{Client} 의 무결성을 확인한다. THK_{ID} 의 무결성까지 확인이 완료되면 AP 는 식(1)을 이용하여 THK 를 생성한다. THK 가 생성된 이후의 과정은 4-way handshake 와 동일하다. 단 full authentication 의 경우와는 달리 새로운 THK 와 THK_{ID} 는 전달하지 않는다. Fast authentication 시 THK 를 생성하지 않는데, 이는 THK 를 이용하여 새로운 THK 를 생성하게 되면 AS 가 Client 에 대한 제어를 할 수 없게 되기 때문이다. 따라서 THK 의 유효 기간이 지나면 다시 full authentication 를 수행해야 하고 이를 통해 AS 는 Client 에 대한 제어를 할 수 있게 된다.



(그림 4) THK fast authentication

5. 평가

우리는 THK 를 이용하여 현재 사용되고 있는 인증 프로토콜인 802.11i 보다 delay 를 줄일 수 있도록 하였다.

<표 1> EAP-TLS 와 THK 와의 비교

Message	EAP-TLS	*Our mechanism*	
		Fast	***Full***
between Client and AP	13	***5***	***14***
between AP and AS	8	***0***	***8***
Total	21	***5***	***22***

<표 1>은 EAP-TLS 와 THK 의 full authentication, 그리고 fast authentication 의 메시지를 비교하고 있다. 먼저 EAP-TLS 를 이용할 경우 Client 와 AP 사이에서 13 개의 메시지가 사용되고 AP 와 AS 사이에서 8 개의 메시지가 사용되어 총 21 개의 메시지가 사용된다. 이에 비해 THK 를 이용할 경우 full authentication 은 22 개의 메시지를 사용하여 EAP-TLS 에 비해 메시지가 1 개 더 많게 된다. 하지만

THK 의 fast authentication 의 경우 5 개의 메시지만 사용하므로 EAP-TLS 에 비해 16 개 적은 메시지를 사용하는 것을 확인 할 수 있다.

우리는 EAP-TLS 와 THK 의 비교를 위해 각각의 인증에 소요되는 비용을 분석 할 것이다. 각 인증에 사용되는 비용 계산을 위해 EAP-TLS 인증에 소요되는 비용을 C1, THK 인증에 소요되는 비용을 C2 라 정의 한다. 그리고 Client 와 AP 사이의 메시지 전달 비용을 α, THK 를 이용한 fast authentication 을 수행할 확률을 P 라 할 때 C1 과 C2 는 다음과 같이 계산할 수 있다.

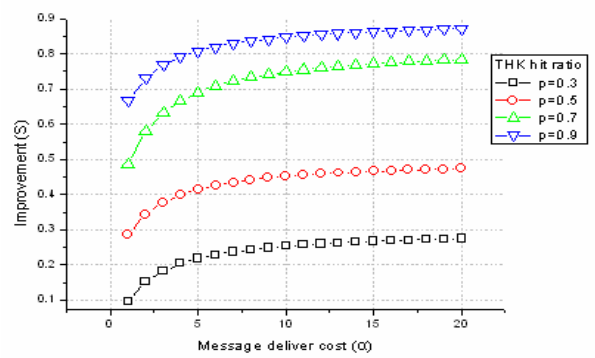
$$C_1 = 13 + 8\alpha \quad (3)$$

$$C_2 = P2 + (1-P)(14 + 8\alpha) \quad (4)$$

다음은 식 (3)과 식 (4)를 이용하여 EAP-TLS 대비 THK 의 성능 향상을 측정한다. 성능 향상의 척도를 위해 우리는 S 를 다음과 같이 정의한다.

$$S = (C_1 - C_2) / C_1 \quad (5)$$

식 (5)를 통해 S 를 구하면 α 와 P 의 변화에 따른 THK 의 성능 향상을 확인 할 수 있다.



(그림 5) THK 이용 시 EAP-TLS 대비 향상

(그림 5)는 EAP-TLS 대비 THK 의 성능 향상 그래프를 보여준다. THK 를 이용한 fast authentication 의 경우 인증 과정에서 AS 와 AP 사이의 메시지 전달이 없으므로 α 값이 커질수록, 즉 AP 와 AS 사이의 메시지 전달 비용이 커질수록 EAP-TLS 에 비해 성능이 향상함을 알 수 있다.

또한 THK 를 이용한 fast 핸드오버의 확률이 증가할수록 성능 향상의 정도가 커지는 것도 확인할 수 있다. Fast authentication 의 성공 빈도는 Client 의 이동성과 TGK 의 lifetime, 그리고 AP 가 저장하는 TGK 의 개수와 관련이 있다. 먼저 Client 가 자주 이동하여 핸드오프가 빈번하게 발생하면 P 가 증가하므로 S 가 커지게 된다. 또한 TGK 의 lifetime 이 길어지거나 AP 가 저장하는 TGK 의 개수가 많아지면 THK 의 유효시간이 길어지게 되므로 이 경우 역시 S 가 증가하게 된다.

6. 결론

본 논문에서는 핸드오프의 인증과정에서 발생하는 delay 를 줄이기 위한 방법을 제안하였다. 802.11i 는 802.1X 에 비해 보안 강도는 증가시켰지만 하지만 보안 강도를 높이기 위해 메시지가 추가되어 delay 가 증가하게 되었다.

우리는 인증과정에서의 delay 를 줄이기 위해 THK 를 제안하였다. THK 는 802.11i 에 비해 최고 2 배의 성능 향상을 가져 올 수 있으므로 delay 에 민감한 멀티미디어 서비스 사용에 적합하다. 또한 THK 의 lifetime 에 대해 최소 사용 시간을 보장하므로 key 에 유효기간만 설정하는 경우보다 효율적이다.

이번 연구를 통해 TGK 의 lifetime 과 AP 의 TGK 저장 개수가 성능 향상에 영향을 주는 것을 확인 할 수 있었다. 본 논문에서는 이에 대한 고려하지 않았지만 THK 의 최적화를 위해서 TGK 의 lifetime 과 저장 개수에 대한 연구가 필요하다.

참고문헌

[1] IEEE Standard 802.1X, “IEEE standard for local and metropolitan area networks, port-based network access control”, October 2001

[2] IEEE Standard 802.11i, “Wireless medium access control (MAC) and physical layer (PHY) specification: Medium access control (MAC) security enhancements”, July 2003

[3] Sangheon Park, Jaeyoung Choi, Taekyoung Kwon, and Yanghee Choi, “Fast-Handoff Support in IEEE 802.11 Wireless Networks”, IEEE Communications Surveys, 1st Qurter 2007, Vol 9, No.1

[4] M. Shin, A. Mishar, and W. Arbaugh, “Improving the Latency of 802.11 Hand-offs using Neighbor Graphs”, Proc. ACM MobiSys 2004, June 2004

[5] S. Shin et al., “Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs”, Proc. ACM MobiWac 2004, Oct.2004

[6] I. Ramani and S. Savage, “SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks.” Proc. IEEE Infocom 2005

[7] J.C. Chen and Y.P. Wang, “Extensible Authentication Protocol (EAP) and IEEE 802.1X: Tutorial and empirical experience”, IEEE communication magazine, December 2005

[8] S. Park and Y.Choi, “Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN systems,” IEEE proc. Communication, Vol. 151, no. 5, Oct. 2004, pp. 489-95

[9] S. Pack et al., “SNC: A Selective Neighbor Caching Scheme for Fast Handoff in IEEE 802.11 Wireless Networks.” ACM Mobile Computing and Communication. Review, vol. 9, no.4, Oct. 2005, pp. 39-49

[10] IEEE Std 802.11i/D4.1, “Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements,” July 2003

[11] B. Aboba et al., “Extensible Authentication Protocol(EAP),” RFC 3748, Jun. 2004.

[12] Jyh-Cheng Chen and Yu-Ping Wang, “Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience”, IEEE Communications Magazine, Dec. 2005.