

## 무선랜 이동 환경을 위한 선불 과금 연구

김관연\*, 한국민\*, 이진우\*, 정병호\*\*, 김신효\*\*, 박세현\*

\*중앙대학교 전자전기공학부 인터넷세계 보안 연구실

\*\*한국전자통신연구원

### A Study of Prepaid Mechanism for Wireless LAN in Mobile Environment

Gwan Yeon Kim\*, Kuk Min Han\*, Chin U Lee\*, Byung Ho Chung\*\*,  
Sin Hyo Kim\*\*, Se Hyun Park\*

\*School of Electrical and Electronic Engineering, Chung-Ang University,  
Cipher Internet-World Lab.

\*\*Electronics and Telecommunications Research Institute

#### 요 약

과거 사무실과 같은 실내 환경에서 무선을 이용하여 네트워크 접속을 위해 개발된 무선랜 기술이 최근 실외 공중망 서비스와 연계되며 미국을 비롯하여 유럽 등지에서 신규 통신서비스 개발이 활발히 사용되고 있다. 이러한 이동환경에 적합한 선불과금 방안은 선불제 요금제도의 필요성이 대두되면서 중요한 연구과제가 되고 있다. 본 논문에서는 무선랜 이동환경에 적합한 선불과금 모델을 제안하고 검증한다. 제안된 과금 모델은 차세대 이동통신의 이동환경에서 적용이 가능한 인터넷 IP 과금 방안을 연구하는데 기반 기술로 이용될 것이다.

#### I. 서론

과거 사무실과 같은 실내 환경에서 무선을 이용하여 네트워크 접속을 위해 개발된 무선랜 기술이 최근 실외 공중망 서비스와 연계되며 미국을 비롯하여 유럽 등지에서 신규 통신서비스 개발이 활발히 사용되고 있다. 현재 무선랜 기술은 단순한 인터넷 접속 수단이었던 초기 모습과는 달리 공중망 서비스 지원을 위한 인증, 보안, 과금 등에 대한 기술이 개발되어 접목되고 있으며, 3세대 이동통신과의 상호 보완적 서비스 개념의 진보된 초고속 무선 이동 서비스로 발전하고 있다.

이러한 발전 과정에 있어서 이동환경에 적합한 선불과금 방안은 선불제 요금제도의 필요성이 대두되면서 중요한 연구과제가 되고 있다. 그에 따라 무선랜 이동환경에서 적합한 선불 과금 프로토콜을 제안한다.

본 논문에서는 무선랜에서 적용이 가능한 선불

\* 본 논문은 한국과학재단 복직기초(R01-2001-00303) 및 한국전자통신연구원의 지원에 의해 수행되었음.

과금 방안에 대해 비교 분석하고 기존 표준의 내용을 벗어나지 않는 범위 내에서 유선 네트워크와도 잘 연동되도록 구성하였다.

#### II. 연구배경

기존의 논문으로 제안된 과금 방안을 살펴보면 크게 과거 호기반의 전화과금 방안에서부터 차세대 이동통신에 적용하는 과금 방안까지 네트워크 과금에 대한 논문들과 그 네트워크를 통해 전송되는 정보 즉 콘텐츠에 대한 과금을 다룬 논문으로 크게 구분 지어진다.

본문에서 다루고자 하는 무선랜에서 적용 가능한 선불과금 방안은 무선랜 네트워크 과금을 다루며 전송되는 콘텐츠에 대한 고려는 제외한다. 또한 본 논문은 무선랜에 적용되므로 무선랜의 특성에 따른 과금 방안의 필수 요건을 먼저 고려한다.

무선랜은 물리적인 특성상 사용 주파수가 ISM 밴드를 이용하고 있어 간섭에 취약하다. 또한 전파의 도달거리가 대략 100m에서 300m내외로 작

은 편이며 기존의 유선랜에서 링크부분만 무선으로 바뀌었기 때문에 유선랜의 특성을 가지게 된다.

이러한 무선랜의 특징을 살펴보면 기존 전화망의 호기반의 과금방안과는 다음과 같은 부분에서 차이가 발생한다.

사용자의 전송요청을 수락하기 위해서는 인증 및 검증이 필요하다. IEEE 802[1] 방식으로 구성된 네트워크에서는 전화망처럼 1:1로 교환기와 전화기가 연결된 것이 아니므로 단말의 주소정보(MAC 주소)로 사용자를 식별할 경우 불법적인 사용을 막을 수 없다. 그러므로 무선랜에서는 보안적인 인증 및 검증을 통한 상호신뢰 환경이 먼저 보장되어야 한다.

기존의 호기반의 전화망과는 다르게 사용자가 전송을 예약하지 않는다. 전화망은 교환방식이 어찌되었건 사용자의 전송영역을 호가 시작함과 동시에 예약되지만 무선랜에서는 사용자의 전송요청이 있는 동안에만 네트워크 자원을 분배한다. 또한 선불 과금이기 때문에 사용자가 실제 네트워크를 이용해 송수신할 때마다 실시간으로 과금해야 한다.

무선랜의 이동환경에서 짧은 전파환경과 간섭에 의해 단말은 접속환경이 좋은 AP쪽으로 이동하게 된다. 이러한 잦은 이동 때마다 과금 서버와 AP, 단말간의 트랜잭션을 통해 세션을 생성하는 방법은 네트워크 자원의 낭비를 초래한다. 따라서 이동하기 전의 과금세션을 연속적으로 이용할 수 있는 방안이 필요하다.

이렇게 이동환경에서의 무선랜 과금은 상호신뢰성 보장, 실시간 과금, 과금 세션의 연계라는 세 가지 요건을 가지게 된다. 이러한 요건들을 모두 충족시키며 선불 과금을 수행할 수 있는 과금 프로토콜을 제안한다.

### III. 선불 과금 프로토콜 제안

프로토콜을 제안하기 위해 필요한 요건으로 결정한 세 가지 요건을 충족시키기 위해 각 요건에 참조할 수 있는 논문이나 이론을 접목하고 이를 통합하여 하나의 과금 프로토콜로 정립하고자 한다.

#### 1. 상호 신뢰성 보장 방안

이동 통신시스템에서의 티켓을 이용한 인증 및 과금 프로토콜을 다룬 논문[2]에 보면 결국 상호 신뢰성 보장을 위해 PKI[3]를 가져와서 티켓 서버에서 인증서 검증과 동시에 과금을 위한 티켓을 사용하도록 하는 내용이다.

무선랜을 구성하는 3가지 구성요소로 AAA(Authentication, Authorization, Accounting) 서

버, AP, 단말이 있고 서로를 신뢰할 수 있도록 하려면 결국 모든 구성요소들을 인증해줄 수 있는 인증서버가 있어야 하며 이 인증서버를 통한 구성요소들의 검증을 거쳐 신뢰관계가 형성된다. 하지만 현재 과금체계에서는 과금을 수행하고 전달하는 개체는 AP와 AAA 서버뿐이므로 단말은 AP를 통해 사용자 인증이 끝나면 AP를 신뢰하게 되도록 되어 있다. 우선적으로 AP가 동작시에 AAA 서버와의 상호 신뢰관계를 맺기 때문이다.

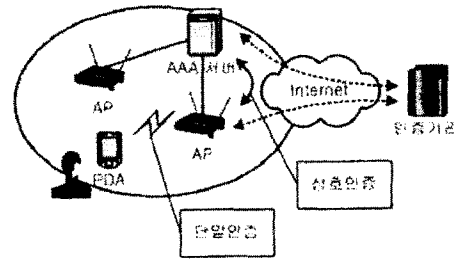


그림 1: 무선랜 구성요소간의 인증관계

그림 1에서 보면 AP와 AAA 서버사이의 인증기관에 의해 상호 인증이 되어 있음을 알 수 있다. 단말과 AP사이의 단말의 AP종속적인 인증이지만 모든 구성요소들간 신뢰관계가 형성되어 패킷기반의 IEEE 802 랜 환경에서도 안전한 과금이 가능하다.

#### 2. 실시간 과금 방안

앞 절에서 알아본 바대로 무선랜 선불 과금을 위해서 실시간 과금이 필요하다. 현재 사용되고

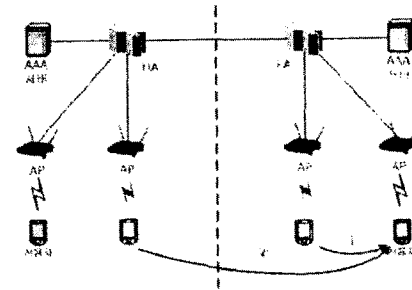


그림 2: 무선랜 과금 모델

있는 대부분의 과금방안에서 채용하고 있어 개념적으로는 거의 동일하다. 즉 매 전송이 발생할 때마다 AP는 전송된 데이터의 양을 측정하고 전송한 사용자의 과금 데이터를 과금서버로 전송하는 것이다. 그런데 과금데이터를 전송할 때의 방식에 따라 두 가지로 구분할 수 있다.

과금데이터의 가공을 AP에서 하는지 아니면 서

버에서 하는지에 따라 구분된다. 실제 요금을 계산하는 빌링을 위해서는 하위 데이터가 아니라 가공된 데이터가 필요하다. 또한 과금서버로의 잦은 전송은 네트워크 자원을 소모하게 하기 때문에 AP에서 일차적인 가공을 하는 경우 네트워크 자원의 낭비를 막을 수 있지만 실시간 과금과는 거리가 있게 되므로 Interim Accounting이라고 하여 정해진 시간을 두고 일차적인 가공을 하여 과금 서버로 전송한다.

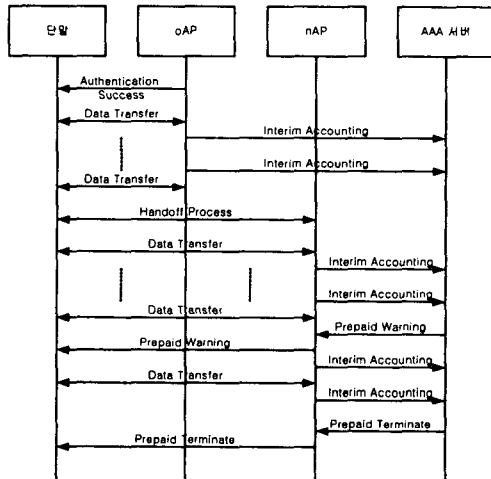


그림 3: 제안된 선불과금 프로토콜

### 3. 과금 세션의 연계 방안

무선랜 서비스 사업자의 입장으로는 사용되는 네트워크 자원에서 네트워크의 관리로 사용되는 부분은 과금할 수 없기 때문에 경제적인 이유로 관리목적의 네트워크 트래픽을 줄여야 한다. 또한 서버의 요청빈도가 많아지면 가입자의 증가에 따라 서버의 증설도 고려해야 하기 때문에 다음과 같은 두 가지 방법을 고려해볼 수 있다.

첫 번째로는 AP와 AAA 서버사이의 완벽한 보안적인 터널이 구성된다고 가정하고 예를 들어 이메일 주소처럼 유일한 사용자 ID를 이용하여 실제 정보의 전송은 AP와 서버지만 서버에서 사용자의 ID로 과금데이터를 관리하도록 한다. 그러면 단말이 이동하여 새로운 AP로 이동하더라도 과금세션이 없기 때문에 발생한 과금데이터를 해당 과금서버로 전송할 수 있게 된다.

두 번째 방법은 서버에서 AP와의 인증세션을 Chain형태로 관리하는 방법이다. 즉 단말이 이동해서 새로운 AP로 접속한 다음 사용자 인증을 하게 되면 AP는 AAA 서버로 사용자 인증을 요청하게 되는데 이때 AAA 서버는 과거 과금세션이 존재하기 때문에 이를 이용하여 동일한 세션 ID 밑으로 다중 세션 ID를 등록하여 이용한다. 이런 방식을 이용하면 과금서버와 AP간 트랜잭션을 감소시켜 서버의 부하를 줄일 수 있다.

### 4. 프로토콜의 제안

그림 2는 과금 프로토콜을 위한 네트워크 모델이다. 그림에서 보듯이, 홈 도메인은 AAA 서버, 홈 에이전트(HA), AP들로 구성되고, 다른 도메인에서도 홈 도메인과 마찬가지로 구성된다. 단말은 같은 도메인 안에서의 핸드오프(①)와 다른 도메인으로의 핸드오프(②)를 할 수 있다.

이에 따른 시나리오는 핸드오프를 하지 않는 경우, 같은 도메인에서 핸드오프 하는 경우, 그리고 다른 도메인으로 핸드오프 하는 경우의 3가지로 나눌 수 있다. 그러나 제안하는 선불과금 프로토콜에서는 다른 도메인에 있는 AAA 서버 사이에서 일어나는 트랜잭션에 대해선 고려하지 않겠다. 따라서 제안하는 선불 과금 프로토콜은 같은 도메인 안에서든 다른 도메인으로의 핸드오프든 따로 구분하지 않는 핸드오프에 대한 것만을 제시한다.

그림 3은 제안하는 선불과금 프로토콜이다. 이 프로토콜은 IETF AAA 워킹그룹의 Diameter[3]를 기반으로 한다.

먼저, 단말은 oAP에 접속하여 모든 인증과정을 완료한다(Authentication Success). 이때 단말은 AAA 서버로부터 자신에게 남아 있는 요금에 대한 정보를 받는다. 이 정보는 사용할 수 있는 패킷의 양 혹은 사용할 수 있는 시간이 될 수 있다.

모든 인증과정을 완료한 사용자는 과금서버와 과금세션을 맺고 실시간 과금의 원칙에 따라 사용한 리소스의 양(Data Transfer)에 따른 Interim Account 정보를 과금서버에서 정한 주기마다 전송한다.(Interim Accounting) 과금서버는 주기적으로 전송되는 Interim Account 정보에 따라 해당 사용자의 남아 있는 요금을 검사하고 감산한다.

이 때 단말이 nAP로 이동한다면(Handoff Process), 다시 사용자 인증과정을 수행하게 되는데, 이때 과금서버에는 기존의 과금세션이 남아 있기 때문에 과금세션의 유지를 위해 기존 세션 ID이외에 다중 세션 ID를 할당한다. 이 부분의 추가로 인해 추가 과금세션을 생성하는 부분만큼 네트워크 자원을 사용자들이 사용할 수 있다.

그리고 nAP에서 사용자 인증을 완료한 후, 단말의 네트워크 리소스 사용량에 따라 주기적으로 Interim Account 정보가 전송되는데 이때 사용자는 선불세션 종료를 요청하여 서비스를 중지시킬 수 있고, 남아 있는 요금이 다할 때까지 사용할 수도 있다.

먼저, 중간에 서비스 요청을 중지시킬 경우에 과금세션이 종료되는데, 이때 과금의 단위에 따라 발생할 수 있는 부분과금(Partial Accounting)은 과금서버에서 정하는 정책에 따라 반올림 혹은 버림을 할 수 있다.

그 다음으로 남아 있는 요금의 다할 때까지 사용하는 경우에는, 사용자가 사용할 수 있는 요금의 양이 과금서버에서 정하는 첫 번째 한계점에 다다랐을 때 1차 경고 메시지(Prepaid Warning)를 보내어 사용자가 적절히 대처할 수 있도록 한다. 이 경고 메시지는 과금서버 임의로 2, 3차 경고 메시지를 보낼 수 있다. 남아 있는 요금이 0이 되었을 때, 과금서버는 해당 사용자에 대한 과금세션을 종료(Prepaid Terminate)한다.

제안된 선불 과금 프로토콜에서 설명이 생략된 부분으로 AP와 AAA 서버사이의 신뢰성 있는 통신으로 위해 초기 AP 기동 시에 소속 AAA 서버와 인증서 교환을 통한 상호인증을 수행하는 과정이 있다.

이렇게 제안된 선불과금 프로토콜은 무선랜 이동환경에서 선불과금을 수행하고 과금세션의 연계를 통해 네트워크 자원의 낭비를 최소화하며 초기 AP와 AAA 서버사이의 상호 인증을 통해 신뢰성 있는 방법이며 차세대 이동통신망에서 ALL-IP[4]기반의 네트워크에서 패킷 과금 프로토콜로 확장이 가능하다.

#### IV. 결론

본 논문에서는 무선랜 환경의 선불과금을 위해 필요한 요구조건을 제시하였고, 이에 따른 선불과금 네트워크 모델과 선불과금 프로토콜을 제시하였다.

제안된 프로토콜을 통해 무선랜 이동환경에서 실시간 선불 과금을 실현할 수 있는 기반 기술이 될 수 있을 것으로 기대되며 제안된 모델과 프로토콜을 이용하여 공중 무선랜의 과금 방안을 구현한다면 서비스 제공자와 사용자 모두에게 이익을 주고 무선랜이 차세대 이동통신망의 중요한 축으로 발전할 수 있을 것이다.

#### 참고문헌

- [1] ISO/IEC, "8802-11 Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications"
- [2] Byung-Rae Lee and Tai-Yun Kim, "Ticket based authentication and payment protocol for mobile telecommunications systems", Dependable Computing, 2001. pp. 218-221
- [3] ITU-T, "X.509 The directory: public-key and attribute certificate frameworks", 03/00
- [4] "Diameter Base Protocol", IETF Internet Draft, draft-ietf-aaa-diameter-13.txt,
- [5] 3GPP2 TSG-P, "Wireless IP Architecture Based on IETF protocols", P.R0001