자바 카드를 이용한 Ad-hoc망의 노드 인증에 관한 연구

이철승* · 신명숙* · 이준**

*조선대학교 대학원 컴퓨터공학과

**조선대학교 전자정보공과대학 컴퓨터공학과

A Study of node Authentication in Ad-hoc Network using Java Card

Cheol-seung Lee* · Myeong-sook Shin* · Joon Lee**

*Dept. of Computer Engineering Graduate School. Chosun University

**Dept. of Computer Engineering. Chosun University

E-mail : cheolseung@hotmail.com

요 약

본 논문은 Ad-hoc망 환경에서 자바카드 인증 프로토콜을 이용한 이동 노드 인증 문제를 해결하고자 한다. Ad-hoc망은 기존의 무선망과는 달리 고정 노드가 없이 망 전체가 이동 노드들로 구성된 망이며, Ad-hoc망의 DSR 라우팅 프로토콜을 이용하여 경로 설정 및 경로 유지 문제를 해결한다.

무선망에서 정의한 보안 구조 및 요소, 기존 인증 시스템과 관련된 각종 암호 기술을 살펴본 후, Ad-hoc 기반 구조와 전송 계층 보안등을 이용하여 응용 계층에서의 이동 노드 인증을 위해 서버 클라이언트가 지니는 설계상의 문제점과 이동 노드간의 보안상 취약점을 찾아 대안을 제공한다.

이동 노드의 자바카드 인증은 무선 상거래, 무선 보안, 그리고 유비쿼터스 컴퓨팅 환경 등에 널리 사용 될 수 있다.

ABSTRACT

In this paper we challenge the mobile node Authentication using Java Card authentication protocol in Ad-hoc network environment. Ad-hoc network is a collection of wireless mobile nodes without the support of a stationary infrastructure. and DSR routing protocol, which is one of famous mobile ad-hoc routing protocols, has the following network path problem. this paper is the security structure that defined in a mobile network and security and watches all kinds of password related technology related to the existing authentication system. It looks up weakness point on security with a problem on the design that uses Ad-hoc based structure and transmission hierarchical security back of a mobile network, and a server-client holds for user authentication of an application level all and all, and it provides one counterproposal.

Java Card Authentication of mobile node can possibly be applied to the area of M-Commerce, Wireless Security, and Ubiquitous Computing and so on.

키워드

Ad-hoc, Authentication, Java Card, Routing

Ⅰ. 서 론

인터넷의 급속한 성장으로 무선망 사용에 대한 요구가 다양해 졌으며, 시간과 공간의 제한을 받지 않는 새로운 차원의 인터넷 기술인 Ad-hoc망이 필요하게 되었다. Ad-hoc망은 기지국 중심의 통신을 하지 않으며, 망에 포함된 각 이동 노드들이 서로 중계국 역할을 하여 통신한다.

본 논문은 Ad-hoc망에서 신뢰성 있고, 적법한 이동 노드 인증 문제를 해결하기 위해, 기존의 무선망과는 달리 DSR 라우팅 프로토콜을 이용하여 경로설정 및 경로유지를 하며, 무선망의 보안 구조 및 요소, 인증 시스템과 관련된 각종 암호 관련 기술을 살펴본 후, Ad-hoc망과 자바카드 인증 프로토콜을 이용하여 USIM(Universal Subscriber Identification Module) 카드 기반 인증 프로토콜

을 보완하고 적용 가능성을 검증하기 위하여 자바카드 기반 인증프로토콜 연구 및 설계 방법을 제안한다. 본 논문의 구성은 다음과 같다. Ⅱ인증 시스템 기반기술, ⅢAd-hoc망의 인증 메커니즘, Ⅳ제안 메커니즘, 그리고 Ⅴ결론 및 향후 연구 방향을 제시한다.

Ⅱ. 인증 시스템 기반 기술

2.1 Ad-hoc

Ad-hoc망은 데이터전송에 필요한 고정된 네트워크 기반 시설이나, 중앙 통제 요소가 없이 동적으로 구성된 이동 노드들이 라우터로서의 기능을 제공하는 네트워크를 말한다.

유선 망에서는 Link-State, Distance-Vector와 같은 효율적인 라우팅 프로토콜을 많이 사용하지만, 빈번하게 변화하는 Ad-hoc망에서는 적용하기가 힘들다. 또한 이동 노드의 제한된 대역폭과 저전력을 효율적으로 사용하기 위해서 라우팅 오버헤드를 줄여야 하는 제약 조건을 가진다. Ad-hoc망에서의 라우팅 프로토콜은 크게 Tablen-driven 방식과 On-demand 방식으로 분류할 수 있다. 전자는 각각의 이동 노드가 망 전체 이동 노드에 대한 라우팅 정보를 유지하고 이용하여, 라우팅을 수행하며, 후자는 망 내의 모든 이동 노드에 대한 전체 경로를 항상 유지하는 것이 아니라 전송할 데이터가 발생했을 때에 경로를 획득하고 실제 경로에 대한 정보만을 유지하는 방식이다[1].

2.2 DSR

DSR(Dynamic source Routing)은 Ad-hoc망의 노드들 사이의 다중 홉을 지원하는 간단하고 효율적인 프로토콜로써, 실제 네트워크 관리나 어떤 기반시설에 대한 요구 없이도 스스로 조직화되며, 경로 발견과 경로 유지는 완전한 On-demand에 의해서 구성되어 질 수 있다[2]. 그러므로 라우팅 정보 교환으로 인해 발생된 불필요한 네트워크 대역폭 내의 부하를 줄일 수 있고, 이동 노드 자체의 전력에 관한 문제, 네트워크 내에서 다양한 패킷의 충돌로 발생되는 문제 등을 감소시킬 수 있다. 따라서 빠르게 변화하는 이동 네트워크의 적응을 원할 히 할 수 있는 여러 장점을 가질 수 있다.

2.3 Java Card

자바카드란 스마트카드 기술을 기반으로 하여 자바의 기술을 접목시킨 것으로 COS(Card Operating System) 위에 JCVM(Java Card Virtual Machine)이 랩핑 되어 있는 IC 카드를 말한다. 자바카드 API는 스마트카드와 같은 작은 메모리를 가진 임베디드 장치를 위한 프로그래밍에 필요한 패키지와 클래스만을 정의하고 있으며, 플랫폼 독립성, 복수의 응용프로그램, 응용프로그램 갱신, 융통성, 호환성 자바카드의 특징을 가지고 있다.

자바카드 상에서 실행될 수 있는 자바애플릿은 APDU(Application Program Data Unit) 교환을 통해 JCRE(Java Card Run-time Environment)와 통신을 하며, AID(Application IDentifier)에 의해 식별된다. JCRE는 애플릿과 호스트간에 교환되는 APDU의 관리와 감독을 수행하며, APDU는 카드상의 통신에서 사용되는 전송메시지 형태로 ISO 7816에 구성되어 있다[3].

2.4 인증 시스템 문제점

무선 인터넷 환경 및 Ad-hoc 망에서 대부분의 인증 프로토콜은 비밀키 기반을 사용하기 때문에 방대한 규모의 네트워크에서 효과적으로 키를 관리하기가 불가능하며, Ad-hoc 망의 동적으로 변화되는 대역폭과, 낮은 전송률 이동 노드의 열악성 때문에 공개키 암호화 기법은 무선 환경에 맞지 않으며, 또한 Ad-hoc망의 경로 설정 요청시 네트워크 부하 및 프로토콜 변환을 위한 라우팅 기술이 불가피 하는 문제점이 발생하였다[1]. 또한 신속한 재경로 설정을 위한 다중 경로를 고려해야 하며, 이동 노드간의 호환성과, 신뢰할 수 있는 보안 및 적법한 이동 노드 인증 문제가 시급한 실정이다.

Ⅲ. Ad-hoc망의 이동노드 인증

3.1 인증 메커니즘

본 장에서는 자바카드 인증 프로토콜을 이용하여 Ad-hoc망의 이동 노드간 인증 메커니즘을 설계한다. 기존 인증 기술 및 인증 시스템의 문제점과 제안한 인증 메커니즘의 요구 사항과 구성 요소들을 고려한 후, Ad-hoc망의 적합성 여부를 평가 및 분석하여, Ad-hoc망의 보안 인프라를 구축한다. 제안메커니즘에서는 이동 노드간의 상호 인증(Mutual Authentication)을 실시하며, 각 이동 노드는 USIM과 AuC(Authentication Center)가 공유한 비밀키 지식을 보유함으로써, 이루어진다. RAND(RANDom number), XRES(eXpected RESponse), CK(Cipher Key), IK(Integrity Key), 그리고 AUTN(Authentication Token)으로 이루어진 각 이동노의 인증벡터는 Ad-hoc망에 연결된 AuC에서 생성되고 인증 및 키 일치 정보 유도과정은 USIM에서 이루어진다.

Ad-hoc망에서 유효기간 내에 직접 인증이 가능하도록 해주며, 각 이동노드에 내장된 자바카드는 내부 패스워드, 암호키 등을 안전하게 저장할 수 있어 보안성 및 휴대성에 유리하게 하였다. 그리고 Ad-hoc망의 DSR 프로토콜을 이용하여 경로 설정 과정 및 경로 유지를 하며 자바카드 프로토콜 절차를 응용하여 소스노드(SN : Source node)가 접근하려는 목적지노드(DN : Destination node)에 보안성을 강화하였다.

3.2 DSR의 경로 설정

DSR 프로토콜은 어떤 SN가 DN로 패킷을 보내려고 할 때 모든 라우터들에 대한 정보를 알고 있지 않는 관계로 SN에서 DN의 경로에 대한 정보를 알아내어야 한다. SN은 패킷 전송을 위한 경로가 필요할 때 경로 요구(RREQ : Route Request) 패킷을 인접한 이동 노드로 브로드캐스팅 하여, 중간 이동 노드에서 DN까지의 경로를 얻거나, DN을 찾을 때까지 계속 브로드캐스팅 된다]. DN이나 DN까지의 경로를 가지고 중간노드들이 RREP 패킷을 SN으로 응답하여 경로 발견 과정을 마치게 된다[2].

DN에서는 경로에러가 발견되었을 때 사용하기 위한 다중 경로를 응답한다. SN에서는 응답받은 다중경로중 최선의 경로를 선택하여 패킷 전송을 시작하고, 다른 경로들은 라우트 캐쉬에 저장해 둔다.

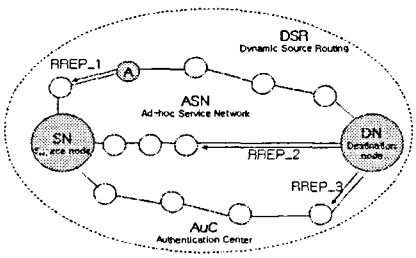

그림 1. 다중 경로의 응답

그림 1은 SN에서 DN로의 다중경로를 응답 받는 경우를 보여주고 있다. SN은 경로 발견을 위해 RREQ 패킷을 생성하여 브로드캐스팅 한 후, 일정 시간 동안 RREP의 응답을 기다린다. SN은 일정 시간 동안 도착한 RREP중 최적의 경로를 선택하고 2개의 후보 경로를 더 선택한다. SN에서 최적 경로 선택 후, 다른 RREP가 도착 할 경우에는 경로의 홉 수를 계산하여 현재 사용 중인 경로보다, 최적이라면 사용하던 이동노드는 후보 경로로 만들고, 도착한 경로를 사용한다. 만일 현재 사용 경로보다 최적의 경로는 아니지만 보관하고 있는 후보 경로보다 최적이라면 후보 경로를 대신하여 도착한 경로를 사용한다. 결국 SN은 경로의 최적 정도에 따라 3개의 다중 경로를 보관한다. 이때, 보관할 필요가 없는 다중 경로는 라우트 캐쉬의 타이머 동작에 의해 자동으로 삭제된다.

3.3 DSR의 경로 유지

경로 유지 단계(Route Maintenance)는 앞에서 획득한 경로를 보관/유지하는 알고리즘이다. SN상에 있는 어떤 연결이 실패하여 DN까지의 경로가 더 이상 사용하지 못한다면, SN은 경로 에러(RERR : Route Error)패킷을 발생시켜 SN 캐쉬로부터 실패한 경로를 삭제하게 된다. 만일 SN의 라우트 캐쉬에 다른 우회 경로가 존재하면, 패킷을 전송하고, 이러한 경로가 없을 때에는 다시 경로 설정 단계를 시작하게 된다.

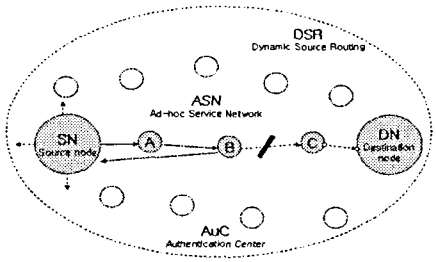

그림 2. 경로 유지

그림 2는 SN에서 DN으로 패킷을 전송할 때 패킷에는 A, B, C 노드를 거쳐서 전송되는 경로에 대한 정보가 포함되어 있다. 최초 SN에서 A로 패킷이 전달되면, A는 SN에게 응답 신호를 보내며, B, C 노드들도 같은 방법으로 응답 신호를 보낸다. 그러나 그림 3처럼 경로가 파손되었을 경우 C는 B에게 응답 신호를 보내지 못하게 되고, B가 경로 파손을 감지하여 경로 유지 알고리즘을 사용한다. B가 C로부터 응답 신호를 받지 못하거나 제한 시간이 지나서 패킷을 재 전송할 경우 B는 DN으로 가는 다른 경로를 라우트 캐쉬에 검색한다. 만일 B에 DN으로 가는 다른 경로가 있으면 이동노드는 전달해야 할 데이터 패킷의 헤더를 지우고 라우트 캐쉬에서 검색된 새로운 경로를 패킷의 헤더로 바꾼다. 그러나 B가 DN으로 가는 다른 경로를 라우트 캐쉬에 가지고 있지 않으면 B는 데이터 패킷을 버린다. 또한 SN로의 RREP도 생성하지 않는다. 대신에 B는 SN로 Route Error메시지를 보낸다. SN가 노드 B로부터 Route Error 메시지를 받으면 SN의 라우트 캐쉬에 저장되어 있는 DN으로 가는 경로를 지우고 Route Error 메시지를 이웃 노드에게 전파하여 패킷이 전달되지 않았음을 알린다.

이와 같이 라우팅프로토콜을 이용하여 SN에서 DN로 연결이 이루어지면, SN와 DN사이에 신뢰성 있는 인증절차가 수행된다.

3.4 Java Card 인증 데이터베이스

AuC로부터 부여받은 SN과 DN의 자바카드는 이동노드에서 보유해야 하는 IMSI(International Mobile Subscriber Identity), K(Security Key), PIN(Personal Identification Number), 그리고 TMSI(Temporary Mobile Subscriber Identity) 정보를 저장하여 SN와 DN의 상호인증을 위해 정보를 할당 분배한다.[4]

3.5 인증 수행 절차

Ad-hoc망의 자바카드기반 이동 노드 인증절차는

SN와 ASN(Ad-hoc Service Network)사이의 SM (Securing Message) 와 ASN과 DN 사이의 SSL (Secure Socket Layer)에 의해 보호된다.

ASN은 SN의 인증을 위해 DN에게 인증데이터를 요구하면, DN은 ASN의 인증데이터 요구에 대한 SN의 인증인자를 생성한다. DN은 생성한 인증인자 및 데이터를 ASN에게 전달하며, ASN은 DN으로부터 받은 인증인자를 자신의 DB에 저장한다. ASN은 n개의 AUTN중에서 하나를 선택하여 SN에게 전달한다.

SN은 ASN으로부터 전달받은 AUTN안의 DN에서 생성한 인증정보를 계산한다. SN은 자바카드내에서 생성한 인증정보를 ASN으로 전송한며, ASN은 수신한 SN의 자바카드 인증정보와 DN에서 생성한 인증정보가 동일한지를 검사하여 인증 유·무를 결정한다.

SN은 DN의 자바카드 공유 세션 키와 DN의 자바카드 초기 공유키를 가지고 인증 절차를 수행한다.

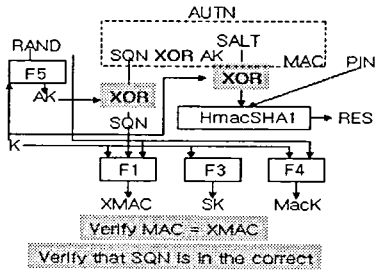

그림 3. 자바카드 인증절차

IV. 제안 메커니즘

ⓐ MAC(i) = f1{K(l) : SQN(i) : RAND(i)}
ⓑ SK(1) = f3{K(i) : RAND(i)}
ⓒ MacK(i) = f4{K(i) : RAND(i)}
ⓓ AK(1) = f5{K(i) : RAND(l)}
ⓔ AUTN = [SQN(i)⊕AK(i)||SALT(i)||MAC(l) ||RAND(i)]
ⓕ XRES = HmacSHA1(PIN_I)
ⓖ Secure SMS Type AUTN(i), XRES(i)
ⓗ General Type : SK(i), MacK(i), CAF(l)
ⓘ Secure SMS Type : AUTN(i)
ⓙ AK(i) = f5{K(i) : RAND(l)}
ⓚ XMAC(i) = f1{K(i) : SQN(i)[(SQN⊕AK) ⊕AK] : RAND(i)}
ⓛ SK(i) = f3{K(l) : RAND(i)}
ⓜ MacK(i) = f4{K(i) : RAND(i)}
ⓝ RES(i) = HmacSHA1([SALT⊕K], PIN_I)
ⓞ Secure SMS Type RES(l)
ⓟ if RES(i) = XRES(l) Execution
ⓠ if RES(i) = XRES(l), CAF++ { if CAF <= 5, repeat else account interception }

본 논문에서 제안한 인증 메커니즘은 Ad-hoc망의 DSR라우팅 프로토콜 및 자바카드 프로토콜을 이용한 이동노드간의 상호 인증 서비스를 위해 정보보호 모델의 설계와 각 프로토콜별 사용되는 표준화된 암호화 알고리즘, 메시지 인증코드, 해쉬함수 및 SM과 SSL 메커니즘을 사용하여 설계되었다.

자바카드 발급 및 이동노드의 정보를 등록하는 JCIC(Java Card Issue Center)와 이동노드의 인증 서비스를 지원하는 AuC, 그리고 자바카드를 탑재한 이동노드의 역할을 수행하는 에뮬레이터로 구성되어 있다. 제안 메커니즘은 자바카드 인증 프로토콜, Ad-hoc망의 DSR라우팅 프로토콜을 기본으로 하고 있으며, SN와 DN 사이의 인증 정보가 교환시 보안에 대한 취약성을 방지하는 대안을 제시한다.

V. 결론 및 향후 연구 과제

최근 몇 년 동안 Ad-hoc망에서의 다양한 라우팅 프로토콜 및 무선 네트워크의 보안, 인증 방법에 대한 연구가 활발히 진행 중에 있지만, 무선인터넷 및 Ad-hoc망에서의 보안, 인증은 미비한 실정이다.

본 논문에서는 USIM 카드에 인증 및 키일치 기술 적용 가능성을 고려한 자바카드와 Ad-hoc망의 DSR 라우팅 프로토콜을 이용하여 이동노드간의 안전한 인증 메커니즘을 제안하였다.

자바카드 프로토콜과 DSR 라우팅 프로토콜을 사용하여 Ad-hoc망의 인증 문제는 제안해 보았지만, 다른 라우팅 프로토콜을 이용한 인증 및 Ad-hoc망의 보안은 아직 미비한 실정이다.

향후 무선 인터넷 시장의 성장을 감안한다면, 모바일 자바카드 및 USIM 카드의 하드웨어 제약성이 극복될 것이 예상되기 때문에 자바카드 기반의 좀더 안전하고, 효율적인 무선 인터넷 환경을 위해 보안성 및 효율성이 강화된 강력한 무선 인터넷 환경을 위해 지속적인 연구 및 논문이 필요할 것이다.

참고문헌

[1] R. Comerford, "State of the Internet : Roundtable 4.0", IEEE Spectrum, Oct. 1998.
[2] D. B. Johnson and D. A. Maltz. "Dynamic source routing in ad hoc wireless networks." Mobile Computing, vol 353, 1996. 9.
[3] Sung-Jun Kim, .. "Design and Implementation of Arbitrary Precision Class for Public Key Crypto API based on Java Card", KIPS Transactions, Vol. 9-C, No2.
[4] Sun Microsystems. Java Card 22 Development Kit User's guide specification 2002.
[5] http://www.3gpp.org/spec/specs.htm. SMS Packet Specification.