通信情報保護學會論文誌
第 10 券 第 2 號, 2000. 6

이동통신환경에 적합한 상호 인증을 제공하는 키분배 프로토콜의 설계

조 동 욱*, 최 연 이**, 김 희 도***, 원 동 호*

Design of Key Distribution Protocol with Mutual Authentication for Mobile Communication Environments

Dong-wook Cho*, Yeon-yi Choi**, Hee-do Kim***, Dong-ho Won*

요 약

본 논문에서는 이동통신환경의 특징과 기존의 키분배 프로토콜들에서 발생할 수 있는 공격들을 프로토콜 수행전, 수행중, 수행후로 나누어서 살펴보고, 이를 기반으로 이동통신환경에 적합한 키분배 프로토콜 설계에 필요한 요구사항들을 제시한다. 또한, 제시된 요구사항을 기반으로 이동통신환경에 적합한 상호인증을 제공하는 키분배 프로토콜을 제안하고, 제안한 프로토콜을 분석한다.

ABSTRACT

In this paper, We consider the properties of mobile communication environments and the security of key distribution protocols. We analyze various attacks attempted in three stages, that is, pre-stage, run-stage and post-stage and find out required properties of key distribution protocols for mobile communication environments. Based on those proposed properties. We propose a new key distribution protocol and analyze it.

keyword : *Mobile Communication Environments, Key Distribution Protocol, Mobile Computing*

Ⅰ. 서 론

이동 통신망은 언제, 어디서나, 누구와도 어떤 종류의 통신이 가능하도록 구축하는 것을 목적으로 하며, 급속한 기술의 발전에 따라, 그 응용분야도 급속히 확대되고 있는 분야중의 하나이다.

이동통신환경은 아날로그를 사용하는 음성통화위주의 1세대, 디지털을 사용하는 저속의 데이터 통신을 제공하는 음성통신위주의 2세대, 고속의 데이터 통신, 멀티미디어 서비스 및 음성통신을 제공하는 3세대로 나눌 수 있다. 1세대 통신은 아날로그를 방식을 사용함으로써 도청 등에 의한 정보의 유출이 발생하기가 용이하였다. 디지털 방식을 사용하는 2세대 통신에서는 1세대 통신의 채널의 보안성 문제를 해결하고, 사용자 인증 및 키분배를 위하여 주로 대칭암호 시스템을 사용하였다. 그러나, 대칭암호 시스템은 공개키 암호 방식에 비해 계산량이 적다는 장점이 있으나, 인증 및 키분배시 항상 홈 인증 센터를 필요로 하며, 부인불가 서비스를 위한 디지털 서명을 제공하기가 용이하지 않다. 이에 반해 공개

* 성균관대학교 전기 전자 및 컴퓨터 공학부
** 신성대학 컴퓨터계열
*** 영동전문대학 정보통신과

키 암호 방식은 온라인 서버를 필요로 하지 않으며, 이동통신환경에서의 전자 상거래를 위한 서명을 제공하기가 용이하므로 3세대 이동통신환경에서의 암호 시스템으로 사용될 것이다.

본 논문은 이동통신환경의 특징과 기존의 키분배 프로토콜들에 대한 안전성에 대하여 살펴보고 이를 기반으로 제 3세대 이동통신환경에 적합한, 인증서 기반의 공개키 암호방식을 이용하여 상호인증을 제공하는 키분배 프로토콜을 제안하고자 한다. 본 논문의 구성은 2장에서 이동통신환경의 특징과 보안상의 문제점을 살펴보고, 3장에서는 기존의 키분배 프로토콜들에 대한 공격을 분석하고, 4장에서는 이동통신환경에 적합한 키분배 프로토콜 설계시의 요구사항을 제시하고, 5장에서는 이동통신환경에 적합한 상호인증을 제공하는 키분배 프로토콜을 제안 및 분석하고, 6장에선 결론을 내리고자 한다.

Ⅱ. 이동통신환경의 특징

이동통신환경은 사용자 및 이동통신기기의 이동성, 언제 어디서나 누구와도 쉽게 통신을 가능하게 하는 무선 네트워킹 등의 중요한 특성을 가지고 있다.[1] 그러나, 이로 인해 여러 가지 보안 문제들을 발생시킨다.

2.1 사용자의 이동성

이동통신환경에서 사용자들은 다른 도메인(foreign domain)으로 이동하며, 이동한 도메인의 여러 서비스와 자원을 사용하기를 원한다. 따라서, 정당한 사용자만이 서비스와 자원을 사용하도록 하기 위해서는 도메인간 인증정보의 핸드오프를 통한 전역적인 인증(global authentication)이 필요하다.

또한, 사용자의 위치가 고정되는 기존의 유선통신과 달리 이동통신환경에서는 사용자의 위치, 움직임 등이 중요한 정보이므로, 이를 보호해야 한다.

2.2 이동통신기기의 이동성

이동통신 사용자들은 이동통신기기를 휴대하고 다니며, 이러한 이동통신기기는 사용자의 휴대성을 높이기 위하여 보다 작고 가벼워야 한다. 따라서, 계산능력과 사용가능한 자원의 제한성이 있다. 또한, 이동통신기기는 물리적인 손상, 분실, 도난 등의 위험이 높아, 저장된 데이터의 분실 위험이 있다.[2]

2.3 무선 네트워킹

무선 네트워킹은 사용자와 이동통신기기의 이동성을 높이기 위한 필수조건이나 전송매체가 대기중의 공기이므로 유선통신망과 같은 물리적인 보안성이 없어 도청자에 의해 도청될 수도 있다. 또한, 사용자 및 이동통신기기가 여러 도메인을 이동하며 서비스 및 자원 이용을 위한 전역적 인증이 필요하고, 이를 위한 도메인사이에 인증정보의 핸드오프가 필요하다.

Ⅲ. 키분배 프로토콜에 대한 공격

프로토콜의 기반이 되는 수학적 문제들의 안전성이 보장되고, 공개 파라미터들의 안전한 선택이 이루어져도 프로토콜의 설계 방식에 따라 다양한 형태의 공격 방법이 존재하게 된다. 즉, 키분배 프로토콜의 안전성은 프로토콜의 설계방식에 크게 의존한다.

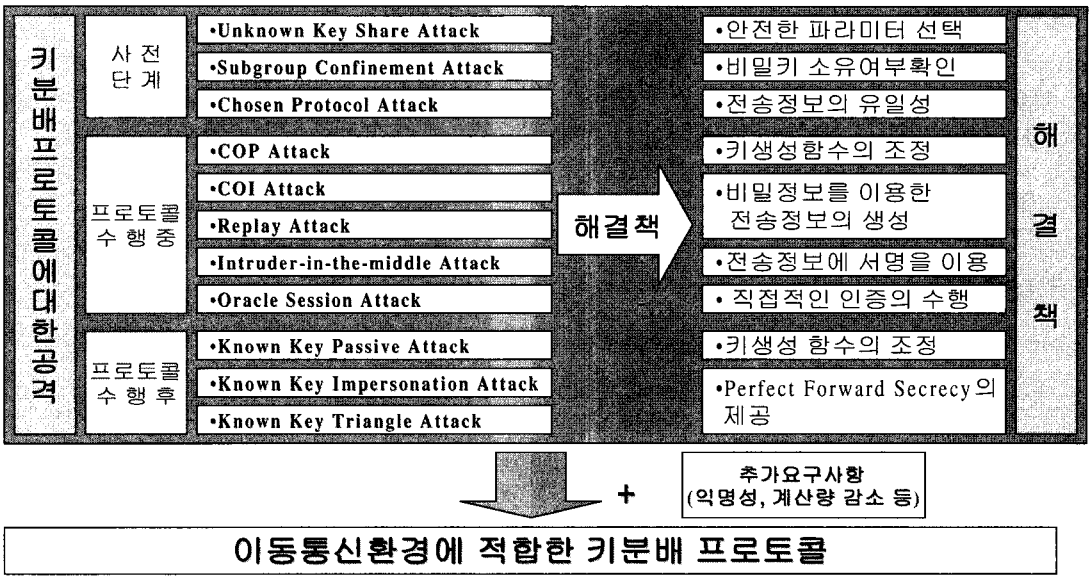
프로토콜에 대한 공격은 공격자들이 취득할 수 있는 정보 및 그들의 공격형태에 따라 다양한 공격이 있다. 그림 1은 키분배 프로토콜들에 대한 공격방법을 공격 시점에 따라, 사전단계, 프로토콜 수행중, 프로토콜 수행후로 분류하고, 각 시점에 따른 해결책을 제시한 것이다.

3.1 사전단계에 가능한 공격

이러한 공격은 합법적인 사용자들 사이에 키분배 프로토콜이 수행된 적이 없는 경우에도 가능한 공격으로, 공개키 등록과정에서 인증서 발급기관(CA)의 부주의로 인해 사용자들간에 동일한 공개키가 존재할 경우 공격이 가능한 unknown key share 공격,[3-5] 잘못된 공개 파라미터의 선택에 의해서 발생하는 subgroup confinement 공격,[6] 동일한 키를 여러 프로토콜에 사용함으로써 발생하는 chosen protocol 공격[7] 등이 있다. 이러한 공격들은 적절한 인증서 발급절차와 공개파라미터들을 안전하게 선택함으로써 막을 수 있다.

3.2 키분배 프로토콜 수행중의 공격

이러한 공격은 합법적인 사용자들 사이에 키분배



〔그림 1〕 키분배 프로토콜들에 대한 공격들

프로토콜이 수행되는 중에 가능한 공격으로, 공개정보와 전송정보만을 이용하는 ciphertext-only passive 공격,[8] 공격자가 정당한 사용자인 것처럼 행동하는 impersonation에 의해 발생하는 impersonation 공격[8]이 있다. 또한, 공격자가 합법적인 사용자로 위장하여 정당한 사용자와 세션키를 설정하기 위하여 이전 프로토콜에서 사용된 메시지를 재사용하는 replay 공격이 있으며, 이는 크게 송신자의 메시지가 송신자에게 되돌아가는 reflection 공격[9]과 다른 제 3자에게 사용되는 interleaving 공격[9,10]으로 나눌 수 있다. 또한, 통신 선로상의 중간에 위치한 공격자가 합법적인 사용자들 사이에 전송되는 정보들을 불법으로 도청·변경하여 전송하여 세션키를 구하는 intruder-in-the-middle 공격,[11] 공격자 E가 사용자 B에게 자신을 사용자 A로 위장하기 위해 필요한 전송정보를 A로부터 얻어내는 oracle session 공격[12,13] 등이 있다.

3.3 키분배 프로토콜 수행후의 공격

이러한 공격은 합법적인 사용자들 사이에 한번 이상의 키분배 프로토콜이 수행된 이후, 공격자가 이전 세션에서 얻은 정보를 이용한 공격으로, 기한이 만료되어 공개되거나 부주의로 인해 노출된 이전 세션의 세션키를 이용하여 해당 세션의 세션키를 얻어내는 공격인 known key 공격이 있다. 이 known key 공격은 과거의 키와 현재의 전송정보를 관찰하여 세션키를 획득하려는 known key passive 공격[8]과 과거의 세션키와 현재의 전송정보를 수정하여 세션키를 생성하려는 known key impersonation 공격,[8] known key impersonation 공격을 3자 이상으로 확대한 known key triangle 공격[14]으로 나눌 수 있다.

만일 프로토콜이 known key 공격에 의해서 공격당하기 쉽다면, 현재 및 미래의 세션키의 안전을 위해서는 사용된 모든 세션키를 비밀로 보관해야 한다. 따라서, 보관해야하는 키의 수는 프로토콜을 수행함에 따라 늘어나게 된다. 이러한 공격을 막기 위해서는 서명, 랜덤수 등을 사용하여 공격자가 유효한 전송정보를 생성할 수 없도록 프로토콜을 설계하거나, 과거의 세션키와 현재의 세션키가 상호 연관관계가 없고, 세션키에 고정된 비밀정보로만 이루어지지 않도록 세션키 생성함수를 설계해야한다.

Ⅳ. 이동통신환경에 적합한 키분배 프로토콜 설계시 요구사항

모든 암호 프로토콜은 분배된 키를 사용하므로, 키의 안전한 분배는 매우 중요하다. 특정 분야에 적합한 키분배 프로토콜 설계에는 응용분야에 대한 요구사항을 고려해야 한다. 예를 들어, 본 논문에서의 이동통신을 위한 키분배 프로토콜은 일반적인 키분배 프로토콜의 요구사항뿐만 아니라, 이동통신환경

의 특징인 mobile station의 이동성이나 계산량의 최소화 등의 특징들을 고려해야한다.

본 절에서는 모든 공개 파라미터와 인증서의 발급이 정상적으로 이루어졌다는 가정하에, 앞절에서 언급한 공격들에 안전하고, 이동통신환경의 특성을 만족시키는 키분배 프로토콜의 설계원칙에 대하여 다룬다.

4.1 전송정보의 생성

키분배 프로토콜에서의 공격은 일반적으로 공격자에 의한 impersonation, 전송정보의 변경, 전송정보의 재전송 등에 의해서 일어난다. 이러한 공격들은 다음과 같은 요구사항을 만족시킴으로써 쉽게 막을 수 있다.

요구사항 1 (상대방에 대한 명시적인 인증(explicit authentication)) :

사용자는 상대방으로부터의 전송정보의 유효성을 검사하기 위하여 통신상대방이 자신이 프로토콜을 수행하고자 하는 사람인지를 확인하는 명시적 인증이 필요하다.

일반적으로 공격자의 impersonation을 이용한 공격을 막기 위해 통신상대방에 대한 명시적인 인증을 수행한다. 이는 전송정보에 대해 디지털 서명을 사용하여 수행되거나, 키분배를 하는 두 객체가 상호 정당한 사람만이 키를 생성할 수 있다는 확신을 갖는 묵시적 인증(implicit authentication)과 세션키가 올바르게 생성되었는지를 확인하는 키확인(key confirmation)을 결합하여 수행된다.

요구사항 2 (전송정보에 대한 메시지인증) :

메시지 인증으로 전송정보의 변경을 막는다.

전송정보에 대한 디지털 서명, MAC 등을 사용하여 메시지 인증을 제공함으로써 공격자의 전송정보에 대한 내용변경, 순서변경, 삭제여부 등을 확인하여 메시지의 변경에 의한 공격을 막는다.

요구사항 3 (재전송 방지) :

각각의 전송정보에 유일성을 부여하고, 상호연관관계를 맺어 다른 프로토콜에 사용되거나 프로토콜 수행후에 재전송되는 것을 막는다.

키분배 프로토콜들에서의 대부분의 공격들은 전송정보를 기록하고 그 전송정보나 일부분을 다른 세션에 재사용하는 경우에 발생한다. 따라서, 이러한 공격들을 막기 위해서는 전송정보의 재사용을 막을 수 있는 방법이 필요하다. 이는 주로 각 라운드의 전송정보들이 다른 구조를 갖도록 하거나, 각 라운드들의 메시지들이 연관성을 갖게 함으로써 이 요구사항을 만족시킬 수 있다.

요구사항 4 (키확인의 제공) :

두 사용자간에 동일한 세션키를 가지고 있는지를 확인하는 키확인을 수행한다.

Unknown key share 공격과 같은 경우는 키분배 프로토콜 수행단계에서 사용자간에 동일한 세션키를 생성했는지를 확인하여 쉽게 막을 수 있다. 또한, 묵시적 인증을 수행한 경우, 키확인을 수행하여 명시적 인증을 수행할 수 있다.

4.2 키생성 함수의 구성

키분배 프로토콜에 대한 공격중에서 known key 공격류는 사용자들의 키 토큰을 결합하여 세션키를 생성하는 키생성 함수가 적절하게 선택되지 못한 경우에 발생한다. 따라서, 적절한 키생성 함수의 선택도 중요하다.

요구사항 5 (키생성 함수의 선택) :

세션키의 생성에 항상 값이 고정되는 항이나 다른 항과 별도로 분리되는 항이 존재하지 않도록 함으로써 known key 공격에 안전할 수 있다.

Known key 공격은 키생성 함수에 사용자들의 비밀키로만 이루어진 항이 존재하는 경우 비밀키에 해당하는 세션의 세션키가 노출될 때 발생한다. 따라서, 키생성 함수에 다른 항과 분리되거나 세션에 상관없이 항상 고정된 항이 존재하지 않도록 세션키 생성함수를 선택해야만 한다. 일반적으로 해쉬함수를 이용한 세션키를 생성하여 known key 공격을 막을 수 있다.

4.3 이동통신환경의 특성을 고려한 설계사항

특정 환경에 적합한 키분배 프로토콜의 설계시에는 일반적인 키분배 프로토콜에서의 요구사항뿐만 아니라 환경에 적합한 추가요구사항을 추가하여 프로토콜을 설계한다. 따라서, 이동통신환경에서는 다음과 같은 요구사항들을 고려해서 설계한다.

요구사항 6 (전송정보의 량 및 패스의 수 최소화) :
이동통신에서의 프로토콜은 전송정보의 량 및 프로토콜의 패스의 수를 최소화시킨다.

일반적으로 이동통신환경의 특징인 무선통신은 유선통신에 비하여 낮은 대역폭과 높은 에러율을 나타낸다. 따라서, 이동통신환경의 무선통신 환경에서의 프로토콜들은 메시지의 량과 패스의 수가 최소화되도록 설계한다.[1]

요구사항 7 (mobile station 계산량의 최소화) :
일반적으로 mobile station의 계산능력은 base station에 비해 낮으므로 mobile station의 계산량을 최소화하도록 프로토콜을 설계해야 한다.

이동통신기기는 사용자의 휴대성을 높이기 위하여 소형화 및 경량화되고 있다. 따라서, 이동통신기기는 낮은 계산능력과 적은 자원을 가지므로, 상대적으로 높은 계산량과 많은 자원을 가진 base station이 보다 많은 계산을 수행하고 mobile station은 최소의 계산을 수행하도록 프로토콜을 설계해야한다. 예를 들어 Park의 프로토콜[15]에서는 mobile station의 계산을 최대한 base station으로 이동시킴으로써, mobile station의 계산량을 최소화하고자 했다.

요구사항 8 (익명성 보장) :
이동통신환경에서는 사용자의 위치정보가 알려질 경우 개인의 프라이버시가 침해될 여지가 있으므로 익명성을 보장해야한다.

사용자의 위치가 항상 고정된 유선통신과는 달리, 이동통신환경에서는 개인의 전송정보의 보호도 중요하지만, 개인의 위치정보가 노출되는 경우 개인의 프라이버시의 침해를 가져올 수 있다. 따라서, 의도된 상대만이 통신하고 있는 상대가 누구인지를 알 수 있는 사용자에 대한 익명성을 보장해야하며, 이러한 익명성 보장은 base station의 공개키로 mobile station의 인증정보를 암호화하여 보내거나, 둘 사이에 세션키 생성후 mobile station의 인증정보를 암호화시켜 보냄으로써 수행할 수 있다.

요구사항 9 (인증정보의 핸드오프) :
mobile station의 이동성 및 유용성을 높이기 위하여 인증정보의 핸드오프를 제공해야 한다.

이동통신환경에서 이동통신기기는 여러 도메인을 이동하며, 다른 도메인(foreign domain)에서 서비스를 받기 위해서는 홈 도메인(home domain)에서 다른 도메인으로 인증정보를 제공해야만 한다. 따라서, 프로토콜 설계시에는 인증정보의 핸드오프를 고려하여 설계해야한다. 주로 X.509 형식의 인증서를 사용하여 온라인 인증서버의 도움 없이 인증정보의 핸드오프를 해결할 수 있다.

요구사항 10 (송신정보의 부인불가) :
mobile station은 자신이 전송한 정보에 대하여 차후에 부인할 수 없어야 한다.

현재진행중인 ASPeCT 등의 제 3세대 이동통신을 위한 프로젝트에서는 이동통신을 활용한 전자상거래를 고려하여 프로젝트를 수행하고 있다.[16] 따라서, 소비자가 판매자로부터 물건을 구입하는 경우나 어떠한 서비스를 사용한 경우, 나중에 이를 부인할 수 없어야 한다. 이러한 부인불가 서비스는 디지털 서명을 사용하여 구현되고 있다.

V. 제안하는 키분배 프로토콜

이 절에서는 현재까지 제시한 요구사항들을 고려하여, 이동통신환경에 적합한 새로운 키분배 프로토콜을 제안하고 이를 분석한다.

5.1 약어 및 기호

본 절에서 사용되는 약어 및 기호는 표 1과 같다.

〔표 1〕 본 논문에 사용된 약어 및 기호

기 호	설 명
P_X	사용자 X의 공개키
$ES_Y(\cdot)$	키 Y를 사용한 대칭키 암호화
$E_{P_X}(\cdot)$	사용자 X의 공개키를 사용한 공개키 암호화
SK	두 객체 사이에 생성된 세션키
$h(\cdot)$	일방향 해쉬함수
r_X	사용자 X가 생성한 난수
$Sig_X(\cdot)$	사용자 X의 서명,
$Cert_X$	CA에 의해 발급된 사용자 X의 인증서
pay	지불 데이터
chd	청구 데이터

5.2 제안하는 프로토콜

제안하는 하는 프로토콜에서는 base station B는 항상 자신의 인증서를 전송하고 있으며, mobile station M은 해당하는 셀에 들어갈 때마다 수신한 base station B의 인증서의 유효성을 검증한다고 가정하며, 키분배 프로토콜은 다음과 같다.

① mobile station M은 난수 r_M을 선택한다.

② mobile station M은 난수 r_M과 자신의 식별자 ID_M을 base station B의 공개키로 암호화하여 base station B에게 전송한다.

$$E_{P_B}(r_M, ID_M)$$

③ base station B는 난수 r_B를 선택하고 청구 데이터 chd를 암호화하여 mobile station M에게 전송한다.

$$ES_{r_M}(r_B, chd, h(SK, chd))$$

④ mobile station M은 청구 데이터 chd에 대한 지불데이터 pay에 서명하여, 인증서 $Cert_M$와 함께 암호화하여 base station B에게 전송한다.

$$ES_{SK}(Cert_M, pay, Sig_M(h(ID_B, pay, chd, r_B, r_M)))$$

5.3 제안한 프로토콜에 대한 분석

5.3.1 Mobile station M의 키확인 및 인증

Mobile station M은 세 번째 전송정보에 지불데이터에 대한 서명을 전송하고, base station B는 서명을 검증함으로써 mobile station M에 대한 명시적인 인증을 수행한다. 또한, mobile station M은 전송정보를 세션키 SK로 암호화하여 전송함으로써 세션키 확인을 수행한다.

5.3.2 Base station B의 키확인 및 인증

Mobile station M이 보낸 첫 번째 전송정보는 base station B의 공개키 P_B로 암호화하여 전송된다. 따라서, base station B만이 r_M를 복호화하여 세션키 SK 및 두 번째 전송정보를 생성할 수 있다는 묵시적 인증(implicit authentication)을 제공하며, r_M과 chd에 대한 해쉬값을 생성하여 키확인 및 명시적인 인증을 한다.

5.3.3 Key freshness

세션키의 생성에 mobile station M과 base station B가 생성한 난수 r_M과 r_B를 이용하므로 상호 key freshness를 제공한다.

5.3.4 지불정보에 대한 부인불가

Mobile station M이 어떤 서비스를 이용하거나, 물품을 구입하는 경우, base station B는 그에 대한 지불을 요구하는 청구 데이터 chd를 mobile station M에게 전송하고, 그에 대한 지불 데이터 pay에 대하여 디지털 서명을 요구함으로써 부인불가 서비스를 제공하여 전자 상거래로의 확장을 용이하게 하였다.

5.3.5 Mobile station M에 대한 익명성 제공

Mobile station M은 첫 번째와 세 번째 메시지에 있는 자신의 식별자, 인증서, 서명 등을 암호화하여 전송한다. 따라서, base station B만이

mobile station M		base station B
	$E_{P_B}(r_M, ID_M)$ →	
	← $ES_{r_M}(r_B, chd, h(SK, chd))$	$SK = h(r_M \| r_B)$
$SK = h(r_M \| r_B)$	$ES_{SK}(Cert_M, pay, Sig_M(h(ID_B, pay, chd, r_B, r_M)))$ →	

〔그림 2〕 제안하는 키분배 프로토콜

mobile station M이 누구인지를 알 뿐, 다른 사용자들은 알 수 없다. 이는 사용자에 대한 익명성을 제공한다.

5.3.6 Mobile station의 계산량 감소

[17]에서 제시된 ASPeCT 프로토콜[16]에 대한 공격 시나리오는 사용자에 대한 정보를 프로토콜의 첫 번째 메시지에 보냄으로써 막을 수 있다. 만일, Boyd-Park 프로토콜[17]처럼 인증서를 공개키 암호 방식을 사용하여 암호화하여 전송할 경우, 많은 공개키 암호 계산이 필요하다. 이를 막기 위해서 64bit인 사용자 식별자를 공개키로 암호화하여 전송하고, 세션키의 생성후 인증서를 세션키로 암호화하여 전송한다. 위와 같은 과정은, mobile station M의 공개키 암호연산을 대칭키 암호연산으로 바꿈으로써 mobile station M의 계산량을 감소시킨다.

5.3.7 인증정보의 핸드오프

인증서 기반의 공개키 암호방식을 사용하는 다른 키분배 프로토콜[15-17,20]과 같이 프로토콜의 세 번째 전송정보 생성에 X.509 형식의 인증서를 사용한다. Base station B가 mobile station M의 인증을 위해 교차인증, 인증서 체인 등을 사용하여 mobile station M의 인증서를 검사한 후, 서명을 검증함으로써 mobile station M을 인증할 수 있다.

5.3.8 전송정보의 최소화

이동통신환경은 유선통신에 비하여 대역폭이 낮다. 따라서, 전송정보의 량이 최소화되도록 설계해야 한다. X.509 대신 [18]에서 제시한 간략화된 인증서를 사용하여 전송량을 줄일 수 있다.

5.4 기존의 프로토콜과의 비교 분석

[표 2]는 앞 절에서 언급한 특성들에 대하여 제안한 프로토콜과 기존의 이동통신을 위한 프로토콜들을 비교한 것이다. 공개키를 이용한 서명과 암호화에는 512bit 암호 시스템을 사용하며, 그 결과 또한 512bit로 가정하며, 대칭키 암호시스템은 64bit를 사용한 것으로 가정하였다. 각 프로토콜들에서 사용된 모듈러 $n(=p \cdot q)$, 비밀키 s_X는 512bit로 가정하였다. 또한, BCY 프로토콜을 제외한 모든 프로토콜들은 약 1,024Byte 길이의 X.509 형식의 인증서를 사용하고 있으며, 전송정보량의 계산을 위해서, pay와 chd를 제외한 r_X, ID_X, COUNT[17], TS[16], alg_list[20], sel_alg[20] 등의 파라미터는 64bit로, 프로토콜들에서 사용된 해쉬함수의 출력값은 128 bit로 가정하였다.

[표 2] 프로토콜들의 중요특성 비교

프로토콜	명시적 객체인증	묵시적 키 인증	전자상거래 이용가능성	사용자 익명성	Mobile station 공개키 연산 횟수	전송 정보량	공격/결함
BCY 프로토콜[19]	None	Mutual	No	No	검 증 : 1회 암 호 화 : 1번 멱승연산 : 1회	2,240 bit	[16]
Aziz-Diffie 프로토콜[20]	Mutual	Mutual	No	No	서 명 : 1회 검 증 : 2회 암 호 화 : 1회 복 호 화 : 1회	18,624 bit	[21]
Park의 프로토콜[15]	Mobile station	Mobile station	No	No	검 증 : 1회 멱승연산 : 1회	17,728 bit	[16, 17]
ASPeCT 프로토콜[16]	Mutual	Mutual	Yes	Yes	서 명 : 1회 검 증 : 1회 멱승연산 : (1)+1회	17,728 + Z bit	[17]
Boyd-Park 프로토콜[17]	Mutual	Mutual	No	Yes	서 명 : 1회 검 증 : (1)회 암 호 화 : (17)회	9,408 bit	-
제안한 프로토콜	Mutual	Mutual	Yes	Yes	서 명 : 1회 검 증 : (1)회 암 호 화 : (1)회	9,408 + Z bit	-

( ) : 오프-라인 계산, Z : |pay+chd|, [ ] : 참고문헌

[표 2]에서 보는 것과 같이 제안하는 프로토콜은 다른 프로토콜들에 비해서 전송정보량 및 계산량 등이 효율적이며, 사용자의 익명성과 객체들간의 상호 인증을 제공하고 있다. 또한, 청구 데이터 chd와 지불 데이터 pay를 추가함으로써 마이크로 지불 시스템을 구현하여 전자 상거래로의 확장성이 용이하다. 그러나, X.509 형식의 인증서를 사용한 인증정보의 핸드오프를 위해서는 공개키 기반구조(PKI : public key infra-structure)의 구축이 필요하다.

Ⅵ. 결 론

본 논문에서는 이동통신 환경의 특징에 의해서 발생하는 문제점과 키분배 프로토콜들의 각 과정에서 생길 수 있는 공격들에 대하여 살펴보았으며, 이를 기초로 이동통신환경에서 키분배 프로토콜에서 필요한 특징에 대하여 논하고, 새로운 키분배 프로토콜을 제시하였다. 제안한 프로토콜은 기존의 프로토콜에 비하여 계산량을 감소시켜 효율성을 높였고, 향후 3세대 이동통신환경에서의 정보보호기술 활용에 이용가능하다. 또한, 이 논문은 차후 이동통신환경에서의 안전한 키분배 프로토콜의 설계에 사용될 수 있다.

참 고 문 헌

[1] N. Asokan, "Security Issues in Mobile Computing", *CS 690B-Research Proposal*, April 1995. Available on-line as http://www.semper.org/sirene/people/asokan /research/proposal.ps.gz

[2] George H. Forman and John Zahorjan, "The Challenges of Mobile Computing", *Technical Report* 93-11-03, Depart-ment of Computer Science and Engineering, University of Washington, December 1993.

[3] W. Diffie, P. C. Oorschot, M. J. Wiener, "Authentication and Authenticated Key Exchange", *Designs, Codes and Cryptography*, 2, pp. 107-125, 1992.

[4] A. Menezes, M. Qu, S. Vanstone, "Some new key agreement protocols providing mutual implicit authentication", *Workshop on Selected Area in Cryptography (SAC '95)*, pp. 22-32, 1995.

[5] Simon Blake Wilson, Alfred Menezeds, "Unknown Key-share Attacks on the station-to-station(STS) Protocol", University of Waterloo Dept. of Combinatorics and Optimization, *research report*, CORR 98-42, 1998.

[6] C. H. Lim, P. J. Lee, "A Key Recovery Attack on discrete log-based schemes using a prime order subgroup", *Advances in Cryptology-Crypto 97*, Springer-verlag, LNCS 1294, pp. 249-263, 1997.

[7] J. Kelsey, B. Schneier, D. Wagner, "Protocol Interactions and the Chosen Protocol Attack", *Proceedings of Security Protocols, 5th International Workshop*, pp. 233-246, April 1998.

[8] 이필중, 임채훈, "일반화된 Diffie-Hellman 키이 분배 방식의 안전성 분석", *한국정보통신학회논문지* '97-7 Vol. 16 No. 7, pp. 575-597, 1997.

[9] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, pp. 103-113

[10] R. Anderson, S. Vaudenay, "Minding your p's and q's", *Advances in Cryptology-Asiacrypt* '96, Springer-verlag, LNCS 1163, pp. 15-25, 1996.

[11] R. L. Rivest, A. Shamir, "How to expose an eavesdropper", *Communi-cations of the ACM*, 27, pp. 393-395, 1984.

[12] 임채훈, 이필중, "상호 신분 인증 및 디지털 서명기법에 관한 연구", *통신정보보호학회논문지*, 제 2권/제1호, pp. 16-33, 1992.

[13] B. Bird, I. Goa, A. Herzberg, P. Janson, S. Kutte, R. Molva, M. Yung, "Systematic design of a family of Attack-resistant authentication protocols", *IEEE Journal on Selected Areas in Communications*, 1993.

[14] M. Burmester, "On the risk of opening distribution keys", *Advances in Cryptology-Crypto* '94, Springer-verlag, LNCS 839, 1994.

[15] C. S. Park, "On Certificate-Based Security Protocol for Wireless Mobile Communication Systems", *IEEE Network, September/October*, pp. 50-55, 1997.

[16] Keith Martin and Chris Mitchell, "Evaluation of Authentication Protocols for Mobile Environment Value-Added Services", *Draft*, Available on-line as http://isg.rhbnc.ac.uk/cjm/EOAPFM.ZIP, 1998.

[17] C. Boyd, D. G. Park, "Public Key Protocols for Wireless Communi-cations", *Proceedings of ICISC '98*, pp. 47-57, 1998.

[18] G. Horn, B. Preneel, "Authentication and Payment in Future Mobile Systems", *Proceedings of ESORICS* '98, Springer-Verla, 1998.

[19] V. Varadharajan and Y. Mu, "On the Design of Security Protocols for Mobile Communica tions",*ACISP'96 Conference, Springer-Verlag*, pp. 134-146, 1996.

[20] A. Aziz and W. Diffie, "Privacy and Authentication for Wireless Local Area Networks", *IEEE Personal Communications*, Vol. 1, pp. 25-31, 1994.

[21] C. J. Mitchell, "Security in future mobile networks", *Proc. of Second International Workshop on Mobile Multi-Media Communications* (MoMuC-2), 1995.

〈著者紹介〉

조 동 욱 (Dong-wook Cho)
1998년 2월 : 성균관대학교 정보공학과 졸업
2000년 2월 : 성균관대학교 전기 전자 및 컴퓨터 공학부 석사
〈관심분야〉 부호이론, 암호이론, 통신이론

최 연 이 (Yeon-yi Choi)
1993년 2월 : 한림대학교 화학과 졸업
1995년 8월 : 성균관대학교 산업과학대학원 석사
1996년 3월~현재 성균관대학교 전기 전자 및 컴퓨터 공학부(박사수료)
1997년 3월~현재 신성대학 컴퓨터계열 전임강사
〈관심분야〉 부호이론, 암호이론, 통신이론

김 희 도 (Hee-do Kim)
1985년 2월 : 서울산업대학교 전자공학과 졸업
1988년 2월 : 한양대학교 전자통신과 석사
1998년~현재 : 성균관대학교 전기 전자 및 컴퓨터 공학부(박사수료)
1993년~현재 : 영동전문대학 정보통신과 조교수
〈관심분야〉 통신망 정보보호, 암호인증

원 동 호 (Dong-ho Won)
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학과 박사
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1990년~1999년 : 한국통신정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부장
(겸) 정보통신대학원장, 한국통신정보보호학회 부회장
〈관심분야〉 암호이론, 부호이론