효율적인 이동통신 보안을 위한 키 분배 프로토콜

심현정*, 김문기, 염흥열
순천향대학교 전자상거래학과*, 정보보호학과

An Efficient Key Distribution Protocols for Secure Mobile Communication

Hyunjung Sim*, Moonki Kim, Heungyoul Youm
Dept. of Electronic Commerce*, Dept. of Information Security Eng., Soonchunhyang Univ.,

요 약

이동 통신망은 여러 다른 전송 특성을 갖는 구간들로 구성된 통신 채널을 갖고 있으며, 사용자의 위치 정보가 다른 공격자에 의하여 밝혀지지 않아야 하는 사용자 위치 익명성 제공이 되어야 하며, 이동국에서의 계산량과 저장량이 작도록 구성되어야 한다. 본 논문에서는 이동 통신망의 환경을 분석하고, 기존의 이동 통신망을 위한 보안 요구사항을 도출하며, 이를 바탕으로 이동통신망을 위한 키 분배 방식들을 분석하며, 또한 기존의 키 분배 방식을 제시한다. 그리고 이를 바탕으로 4가지 키 분배 방식을 제안하고, 제안된 키 분배 방식들의 특징을 제시한다.

제1장 서론

최근 이동 통신망을 통한 인터넷이 일반화되면서 이동 통신망에서 보안의 중요성이 크게 대두되고 있다. 이동 통신에서의 보안은 종단간(End-to-end) 보안과 무선 링크간의 링크간(Link-by-link) 보안이 있다. 이동 통신을 위한 보안 서비스는 기밀성(Confidentiality) 서비스, 무결성(Integrity) 서비스, 인증(Authentication) 서비스, 부인방지(Non-Repudiation) 서비스 등이 있다. 이동 통신은 사용자가 여러 셀들을 이동하면서 기지국으로부터 서비스(일명 로밍 서비스)를 제공받으므로 이동국의 신원이 기지국 이외의 다른 개체에게는 익명성을 유지해야 한다. 따라서 이동 통신에서는 사용자가 위치를 이동할 때 사용자를 인증하고, 세션 키를 교환하는 상호인증 및 세션키 공유를 위한 키 분배 프로토콜이 요구된다. 이동 통신 보안은 다음과 같은 이동 통신 환경의 특성을 고려하여 설계되어야 한다.

- **복합적인 통신 채널 구성**: 종단간 통신 채널이 보안 측면에서 취약성이 있는 무선 링크를 포함하는 다양한 복합적인 통신 채널로 구성된다. 따라서 이동 통신을 위한 보안 시스템은 이중 가장 취약성이 높은 링크에 보안 목표치를 맞추면서 설계되어야 한다.
- **사용자 위치에 대한 프라이버시 요구사항**: 이동 단말이 여러 셀을 이동하면서 서비스를 제공받으므로, 사용자 위치 정보가

공격자에게 알려져서는 안되도록 설계되어야 한다.

- **계산과 메모리의 제한**: 이동 단말은 메모리 용량이 제한되어 있고, 계산 능력이 기존의 통신 장치보다 떨어진다.
- **저속의 통신 채널**: 기지국과 이동국의 통신 채널의 속도가 일반적으로 작다.

기지국은 이동 사용자에게 서비스를 제공할 때 우선 이동 단말기의 신분을 확인하고, 이동 링크의 데이터를 보호하기 위하여 사용되는 세션 키를 안전하게 분배해야 한다. 따라서 사용자 신원 확인 방식과 키 분배 프로토콜이 요구된다. 본 논문에서는 기존의 무선통신을 위한 키 분배 프로토콜을 분석하고, 각 방식의 장단점을 분석하며, 이를 바탕으로 무선 통신망을 위한 새로운 키 분배 프로토콜을 제안한다. 본 논문의 2장에서는 이동통신 보안을 위한 요구사항을 도출하고, 3장에서는 지금까지 알려진 인증 및 키 분배 프로토콜을 분석하며, 4장에서는 기존의 프로토콜을 이용한 새로운 키 분배 프로토콜을 제안한다.

제2장 이동통신 보안을 위한 보안 기본 요구사항

본 장에서는 지금까지 알려진 이동통신을 위한 요구사항과 기존 키 분배 프로토콜의 일반적인 특성을 기술한다.

2.1 이동통신에서 보안 시스템 설계를 위한 일반적인 요구사항

이동 통신망에서 보안은 최종 사용자간의 보안을 제공하는 종단간 보안(end-to-end) 보안과 무선 인터페이스에서의 사용자 단말과 기지국간의 보안을 제공하는 링크 보안(Lnk-by-link) 으로 분리 또는 통합되어 제공되어야 한다. 따라서 이동 통신 보안을 위한 프로토콜은 제시된 프로토콜이 안전한지를 나타내는 보안성(Security), 제시된 프로토콜이 무선 환경을 위한 요구사항을 만족한 지를 나타내는 적합성(Suitability), 그리고 제시된 프로토콜이 성능이 우수하고, 효율이 우수한지를 살펴보는 최적성(Optimization) 측면에서 설계되어야 한다. 이동 통신망에서 종단간 보안과 링크간 보안을 위한 요구사항은 다음과 같다. 종단간 보안은 기밀성, 사용자의 데이터 무결성, 부인방지 서비스를 요구한다. 일반적으로 기밀성은 대칭형 암호 알고리듬을 이용한다. 대칭형 알고리듬을 사용하면, 각 사용자의 비밀정보가 서로 다른 이동 영역에 안전하게 전달되어야 한다. 그러나 공개키를 사용하면 비밀키의 이동이 요구되지 않지만 복잡도를 크게 한다. 따라서 대칭형 알고리듬을 이용하는 경우보다 키 관리를 간단히 할 수 있다. 부인 방지 서비스는 제2세대 이동 통신망에서는 대부분 제공되지 않지만, 대부분의 공개키 알고리듬을 이용하며, 제3세대 이동 통신망에서 요구되는 서비스이다. 링크 보안을 위한 요구사항은 다음과 같다.

- 이동 단말기와 기지국 사이의 무선 링크에 대한 기밀성 유지
- 이동 단말기와 기지국 사이의 상호 인증
- 이동 단말기 사용자의 신원의 익명성 제공
- 이동 단말기에서의 프로토콜 계산의 복잡도의 간단화

2.2 기존 키 분배 프로토콜의 일반적인 특성

키 분배 프로토콜은 사용자 A와 사용자 B 간의 수행되는 프로토콜이다. 추후의 암호 통신을 위한 대칭키 암호을 위한 세션키를 공유하는 방법으로 일반적으로 공개키 알고리듬을 이용하여 수행된다. 기존의 키 분배 프로토콜은 다음과 같은 특성을 갖는다.

- **함축적인 키 인증(IKA : Implicit Key Authentication)** : 만약 사용자 A가 확인된 사용자 B 이외의 어떤 다른 사용자도 자신들이 공유하는 세션키를 알 수 없다고 확신한다면, 이 키 분배 프로토콜은 함축적인 키 인증을 제공한다고 말할 수 있다. 이는 사용자 B의 개인키를 모르는 어떤 사용자도

공유된 세션키를 계산할 수 없을 때 사용된다.

- **분명한 키 인증(EKA : Explicit Key Authentication)** : 만약 사용자 A가 현재 사용자 B가 실제로 공유된 키를 가지고 있다고 확신한다면, 이 키 분배 프로토콜은 분명한 키 확신(EKC:Explicit Key Confirmation) 특성을 가지고 있다고 말해진다. 이는 사용자가 B가 공유된 세션키의 해쉬 값을 사용자 A에게 보냄으로써 제공된다. 만약 사용자 A가 사용자 B가 분배키를 계산할 수 있다고 보장하면, 이 키 분배 프로토콜은 함축적인 키 확신(IKC: Implicit Key Confirmation) 기능을 제공한다고 말해진다. 이 특성은 개인키를 소지한 사용자 B만이 공유된 세션키를 계산할 수 있다고 확신할 수 있는 키 분배 프로토콜에서 사용된다. EKC 특성은 IKC 특성보다 훨씬더 강력한 키 확신 기능을 사용자 A에게 제공한다. 일반적으로 분명한 키 확신은 함축적인 키 확신을 포함한다. 키를 계산했다는 것과 키를 계산할 수 있다는 것의 차이는 공유된 키의 증거를 분명히 보여주는냐 보여주지 않는냐의 차이에 있다. 사용자 B가 한번 공유키를 계산했다고 해서 이를 키를 구축하고 이를 사용하는 사이에 공유된 키를 잃어버리지 않을 것이라고 확신할 수 없다. 따라서 본 논문에서는 키 확신을 구별하지 않는다. 키 분배 프로토콜이 두 당사자 이외에 누구도 세션키를 계산할 수 없는 IKA 특성과 사용자 B가 공유된 키를 계산할 수 있다는 키 확신(Key Confirmation) 기능을 갖는다면 이 키 분배 프로토콜은 분명한 키 인증 특성을 갖는다고 말해진다.

두 사용자 A와 B 상호간에 함축적인 키 인증을 제공하는 키 분배 프로토콜은 인증된 키 분배(AKE : Authenticated Key Agreement) 프로토콜이라고 정의한다. 또한 분명한 키 인증을 두 사용자 상호간에 제공하는 키 분배 프로토콜은 키확신 기능을 갖는 인증된 키 분배(AKC:Authenticated Key Agreement Protocol with Key Confirmation)이라고 정의한다.

키 분배 프로토콜을 위한 또 다른 특성은 다음과 같다.

- **KKS(Known-key Security)** : 각 키 분배 프로토콜을 수행할 때 마다 사용자 A와 사용자 B가 서로다른 유일한 비밀키(Unique Secret Key)를 생성한다. 이러한 키를 세션 키(Session Key)라고 한다. 이 세션키는 암호학적 공격에 유용하게 사용되는 정보의 량을 줄일 수 있기 위하여 매우 중요하다. 따라서 한번 키가 알려지면 그후의 모든 암호문이 복호되는 것을 막기 위하여 키 분배 프로토콜은 KKS 특성을 가져야 한다. KKS는 이미 알려진 키를 추후의 암호문을 복호하는데 사용할 수 없도록 하는 것이다.
- **FS(Forward Secrecy)** : 만약 장기간 개인키가 손상되었다고 하드래도 개인키 손상 이전의 모든 암호문을 복호할 수 없다면, 이 키 분배 알고리듬은 전진 보안(Forward Sercrecy) 를 만족한다고 할 수 있다.
- **KCI(Key-compromise Impersonation)**: 만약 공격자가 사용자 A의 장기간 개인키를 알고 있다면, 공격자는 사용자 A를 흉내 낼 수 있다. 그러나 사용자 B의 개인키 손상이 사용자 A에게 사용자 B를 흉내내지 못하도록 하는 것이 바람직할 경우가 있다.
- **UKS(Unkonown Key-share)**: 사용자 B는 사용자 B가 사용자 A라는 확신이 없을 때 사용자 A와 키 공유 절차를 수행하지 않는다.

제3장 이동 통신을 위한 기존의 키 분배 프로토콜

키 분배 프로토콜은 사용자의 신원을 확인/검증하고, 세션 보안을 위한 암호 알고리즘을 위하여

사용하는 세션 키를 생성한다. 일반적으로 세션키가 적용될 암호 방식은 공개키 암호 방식과 대칭키 암호 방식이 존재하나, 공개키 암호는 암호문 계산을 위한 복잡도가 크고 대칭키 암호는 암복호 속도가 빠르나 키관리 문제가 복잡한 특징이 있다. 일반적으로 키 분배는 공개키 알고리듬을 사용하고, 데이터를 암호하기 위해서는 대칭형 알고리듬을 결합한 혼합형 프로토콜이 많이 사용된다. 참고로 본 논문에서는 사용될 기호는 다음과 같다.

- k : 세션 키
- B : 기지국 B의 신분 정보
- M : 이동 사용자 M의 신분 정보
- b : B의 고정 개인 키
- m : M의 고정 개인 키
- x : B의 임시 개인 키
- y : M의 임시 개인 키
- N_{user}: 이동국 또는 기지국이 랜덤하게 생성한 난수값
- PK_{user}: g^b 또는 g^m를 만족하는 사용자의 고정 공개키
- R_{user}: g^x를 만족하는 사용자의 임시 공개키
- SC_{user}: 사용자의 비밀 인증서, 이 인증서는 비밀스럽게 이동 단말이 간직해야 하고 이 인증서 소유로 사용자의 신원이 확인된다. 따라서 무선 링크에서 이 인증서는 암호화한 형태로 전달되어야 한다.
- $Cert(user)$: 기지국 또는 이동국의 공개키 인증서
- $E\{\}, D\{\}$: 공개키/대칭키 암호화 및 복호화 과정

본 장에서는 기존의 이동 통신을 위한 대표적인 키 분배 알고리듬들을 분석한다. Beller,Chang,Yacobi등은 논문 [1]에서 MSR(Modulo Square Root) 키 분배 프로토콜을 제안했다. MSR 프로토콜은 여러 가지 변형 방식으로 발전될 수 있다. 무선 통신망을 위한 기존의 대표적인 키 분배 방식은 기본 MSR 프로토콜, 개선된 IMSR(Improved MSR) 프로토콜, Diffie-Hellman 기법이 추가된 MSR+DH 프로토콜, Beller와 Yacobi(BY)가 IMSR 프로토콜을 변형한 BY 프로토콜, 그리고 개선된 BY 프로토콜 등이 있다.

3.1 기본 MSR 프로토콜

기본 MSR 프로토콜은 그림 1과 같이 공개키 암호 방식에 바탕을 두고 구현된 세션키 설정 방식이다. 그림에서 굵은 박스 안의 기호는 각 참여자 및 각 참여자가 프로토콜을 개시하기 이전에 가지고 있는 데이터이다.

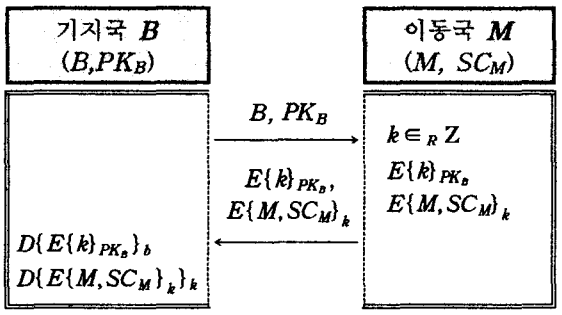

그림 1 기본 MSR 프로토콜

기지국 B는 자신의 신분정보(B), 공개키(PK_B)를 이동 단말에 전송한다. M은 세션키 k를 임의로 생성하고, 세션키(k)를 기지국의 공개키로 암호화한 $\{k\}_{PK_B}$ 를 기지국으로 전달한다. SC_M 은 비밀 인증서 이다. 그리고 동시에 이동 단말은 자신이 생성한 세션키(k)의 암호값, 이동국의 신분정보(M), 그리고 비밀 인증서(SC_M)을 세션키 k 로 암호화하여 기지국으로 전송한다. 세션키 k로 자신의 신분정보와 비밀인증서를 암호화하여 전송함으로써, 무선 링크를 감시하는 제삼자에게 이동국 위치에 대한 익명성을 제공한다. 기지국은 자신의 개인키로 암호문을 복호하여, M의 신원확인을 확인하고, 이동 단말의 비밀 인증서를 구한다. 이 이

동 단말의 인증서를 이용하여 추후의 암호 서비스를 제공한다. 이 프로토콜의 목적은 이동국이 기지국에게 자신의 인증서와 신분 정보를 기지국의 공개키를 이용하여 전달하되, 될 수 있는 한 공개키의 사용을 줄이기 위하여 비밀키 k 만을 공개키로 암호화하고, 나머지 이동국 신분정보와 비밀 인증서는 세션키로 암호화하는 절차로 구성된다. 이 비밀 인증서는 이동국의 신원을 확인하기 위하여 사용된다. 즉 비밀 인증서 내에 포함된 신분 정보를 인증기관의 공개키를 이용하여 유효성을 검증할 수 있다. 이 방식에서 기지국은 이동국의 신원을 확인할 수 있는 반면 이동국은 기지국의 신원을 확인할 수 없으며, 또한 Man in the middle 공격이 가능하여, 세션키가 노출될 수 있다. 또한 재생 공격도 가능하여 침입자가 B에게 M인척 할 수 있음이 알려져 있다. 따라서 기본 MSR 프로토콜은 기밀성과, 상호 인증이 제공되지 않는 단점을 지니고 있다.

3.2 개선된 MSR (IMSR) 프로토콜

Beller, Chang, 그리고 Yacobi는 [1]에서 개선된 MSR 프로토콜을 제안하였다. 기존 MSR 방식의 취약점을 개선하기 위해 최초 통신 개시에 기지국 B의 인증서(Certificate)를 포함하여 전달한다. 이와 같은 방법을 통하여 이동국 M은 기지국 B의 신원을 확신할 수 있게 되며, 또한 난수의 사용을 통해 재생공격(Replay Attack)을 막을 수 있게 되었다. 그림 2는 Improved MSR(IMSR) 프로토콜을 나타낸다.

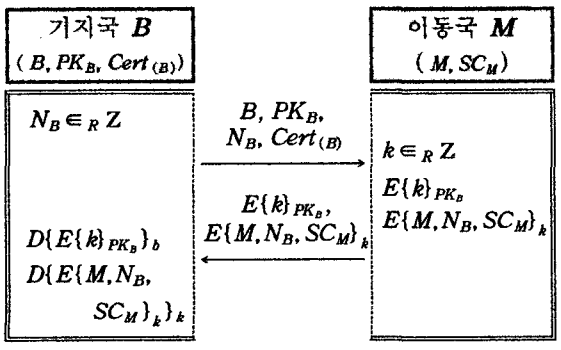

그림 2 IMSR 프로토콜

IMSR 프로토콜은 도전-응답(Challenge-Response) 메커니즘을 포함한다. IMSR 프로토콜은 다음과 같은 절차로 수행된다. 기지국 B는 자신의 난수 N_B와 B의 인증서를 같이 이동국 M에게 전달한다. M은 B의 공개키로 자신이 랜덤하게 생성한 세션키 k를 암호화하고, 또한 자신의 신원정보 M, N_B, 그리고 자신의 비밀 인증서 SC_M 를 세션키 k로 암호화하여 B에게 전달한다. 이동국 M으로부터 암호화된 메세지를 전달받은 B는 자신의 개인키 b로 첫 번째 메시지 k값을 복호화한 다음, 구해진 세션키 k로 두 번째 메시지를 복호화한다. 이때 M에게 받은 N_B와 자신이 초기에 생성한 N_B가 일치하는지 확인하여 재생 공격에 대비하고, 결론적으로 M이 동일한 세션에서 암호화하여 주었는지를 확인한다. 그러나 개선된 방법도 [5]에 언급된 것과 같이 "impersonation attack"이 가능하기 때문에 세션키 k 가 타협될 수 있다. 따라서 이동 사용자과 기지국 사이에 기밀성 유지가 불가능할 수도 있다.

3.3 MSR+DH 키 분배 프로토콜

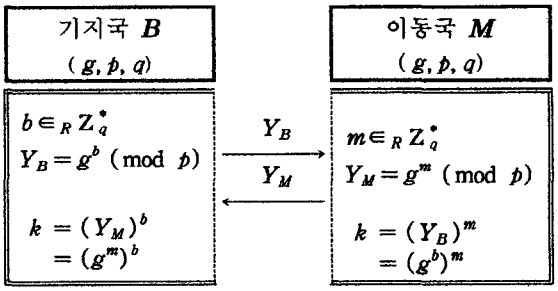

그림 3 Diffie-Hellman 키교환 프로토콜

Diffie-Hellman 키교환 프로토콜은 그림 3과 같이 전통적인 키 교환 프로토콜로서 특히 man in the middle attack 에 약점이 있다. B는 자신의 비밀키(b)를 생성하여 공개키(Y_B)를 계산하고 공개키를 M에게 보내준다. M도 자신의 비밀키를 생성하여 공개키를 계산하고 공개키를 B에게 보내준

다. B와 M은 상대방에게서 받은 공개키로부터 K 값을 계산한다. 이러한 방식으로 서로는 동일한 값을 갖는 K를 공유하게 된다.

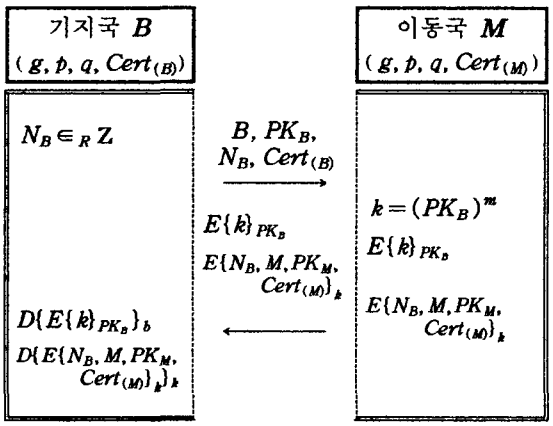

그림 4 MSR+DH 프로토콜

이 프로토콜은 IMSR 프로토콜과 잘 알려진 Diffie-Hellman 키교환을[3] 통합하여 확장한 버전이다. 이 프로토콜에서 가장 크게 개선된 점은, 두 참여자가 각각 고정 공개키를 가지고 있기 때문에 더 이상 비밀스럽게 수행할 필요가 없다는 것이다. 이 프로토콜의 수행 과정은 다음과 같다. M은 B로부터 받은 공개키로 자신이 생성한 고정 개인키로 세션키 k를 계산한다. M은 B의 공개키로 M이 생성한 세션키를 B의 공개키로 암호한다. M은 이동국의 신분 정보, B에게서 받은 N_B 값, M의 공개키, M의 인증서를 세션키로 암호하여 B에게 보낸다. B는 자신의 개인키로 세션키를 복호, B로부터 받은 암호 메세지를 복호 한다. B에게서 받은 B의 공개키를 이용하여 세션키를 계산 한 후 자신이 받은 값과 비교한다. M은 M 단독으로 세션키를 생성하지 않고, B도 M에게서 받은 정보를 가지고 세션키를 생성하기 때문에 Man in the middle attack을 방지할 수 있다. B와 M은 둘다 비밀 공개키를 공유하고 있으므로 이동사용자는 기지국을 위하여 비밀적으로 수행할 필요가 없다, 이는 비밀 인증서 SC_M을 전송할 필요가 없다. 이 방법은 서로간의 키 확신 기능도 제공한다. 그러나 이러한 과정을 수행하면서, 계산 복잡도가 증가하게 되는 점이 발생한다.

3.4 Beller와 Yacobi 프로토콜

Beller와 Yacobi는 IMSR 프로토콜을 변형하여 새로운 키 분배 방식을 제안하였다[2]. 이들이 제안한 프로토콜은 B에서 사용되었던 것과 같이 M

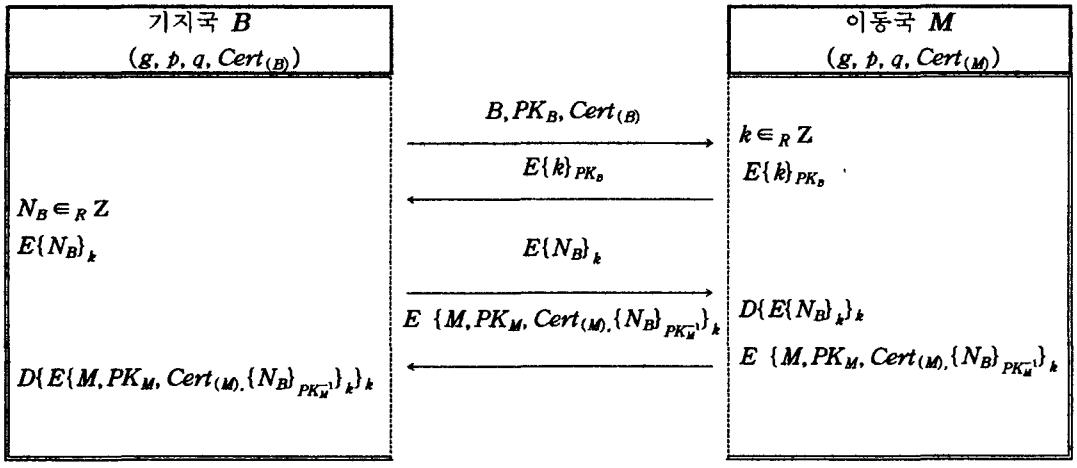

그림 5 Beller와 Yacobi 키 분배 프로토콜

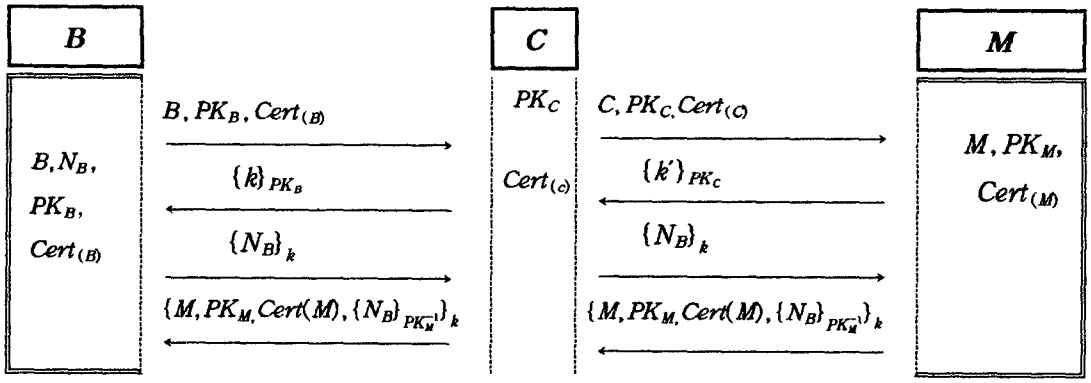

그림 6 Beller와 Yacobi의 프로토콜의 공격 예

에서도 공개키를 사용하도록 한 것이다. M의 개인키는 ElGamal 알고리즘[4]을 이용한 전자서명을 수행하는데 사용된다. 이 프로토콜에서 M은 자신의 개인키로 ElGamal 알고리즘을 이용한 전자서명을 하여 전송함으로써, B는 M에게 송신 부인방지 기능을 제공한다. 그러나 전자서명을 사용하는데 있어서 가장 중요하게 봐야할 점은 메시지에 서명을 함으로써 계산이 복잡해지는 것이다.

또, 이 프로토콜에서는 다음과 같이 중간에 있는 공격자에 의한 공격이 가능하다.

3.5 개선된 Beller와 Yacobi의 프로토콜

이 프로토콜에서 바뀐점은 N_B 가 처음 세션이 시작할 때 전송된다는 것이 Beller and Yacobi's 프로토콜과의 다른 점이다. 세션이 시작할 때 난수 N_B를 전달함으로써 위에서 예를 들은 공격방법을 차단할 수 있다. 이 방식은 제한된 계산능력을 가지는 경우 적합한 방식이다. 그리고 이 기법은 원래의 BY기법과 동일한 계산량과 통신량을 요구한다. 즉 계산상의 복잡도가 동일하다. BY 프로토콜의 공격을 피하기 위한(man in the middle attack) 변경된 프로토콜 방법. 전자서명에 해쉬함수를 사용하여, 해쉬함수의 one-way 에 의해 기밀성을 제공한다.

3.6 KEA(Key Exchange Algorithm)

KEA 프로토콜은 NSA(National Security Agency)에서 고안하였고, 1998년 5월에 공개되었다. 이것은 1994년에 NSA에 의해 고안된 암호학 알고리즘들 중의 하나인 FORTEZZA에 있는 키관리 프로토콜이다. 이 프로토콜과 매우 비슷한 프로토콜로서는 Goss [10]와 MTI/A0 [11]프로토콜이 있다.

참여자 B와 참여자 M은 서로 다른 당사자의 공개키 PK_M과 PK_B를 각각 가지고 있다고 가정한다. 참여자 M은 임의의 난수 $x \in_R Z_q^*$를 선택한 후, 임시 공개키 $R_B = g^x$ 를 계산한다. 그리고 참여자 B의 임시 공개키를 참여자 M에게 전달한다. 참여자 B는 임의의 난수 $y \in_R Z_q^*$를 선택한 후, 임시 공개키 $R_M = g^y$ 를 계산한다. 참여자 B는 다음 두 가지 등식(i)$1 < R_B < P$, ii)$(R_B)^q \equiv 1 (\mathrm{mod} P)$ 을 검증한다. 그리고 참여자 M의 임시 공개키를 참여자 B에게 전달한다. 참여자 M은 세션키 k를 $k=(R_B)^m+(PK_B)^y$를 이용하여 계산한다. 참여자 B는 다음 두 가지 등식(i)$1 < R_B < P$, ii)$(R_B)^q \equiv 1 (\mathrm{mod} P)$ 을 검증한다. 참여자 B는 세션키 k를 $k=(R_B)^m+(PK_B)^y$ 를 이용하여 계산한다. 이 프로

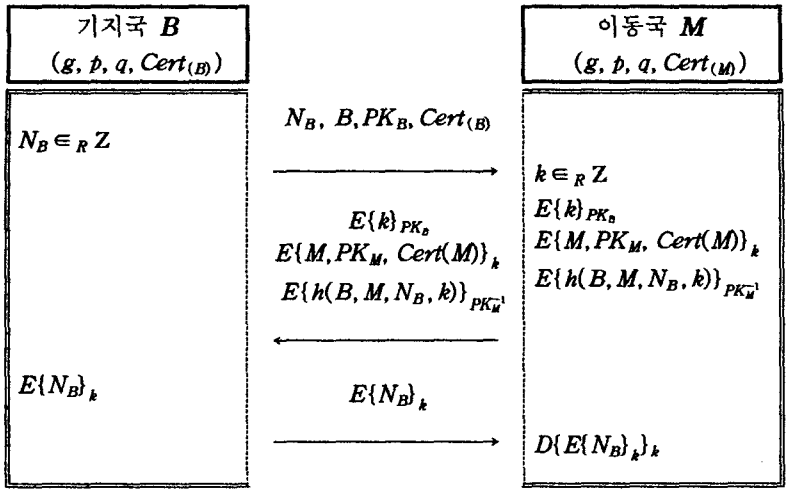

그림 7 개선된 Beller와 Yacobi의 프로토콜

토콜을 이용하여 참여자 M과 참여자 B는 서로 동일한 세션 키를 계산할 수 있다.

3.7 통합된 인증된 키 분배 프로토콜

통합된 키 분배 프로토콜은 Ankney, Johnson and Matyas[6] 의해 제안된 프로토콜로써, 이 프로토콜은 드래프트문서인 ANSI X9.42 [7], ANSI X9.63 [8], 그리고 IEEE P1363 [9]에 표준화되어 있는 키 분배 프로토콜이다. 이 프로토콜의 장점은 개념적으로 간단하고, 그 결과로서 분석이 쉽

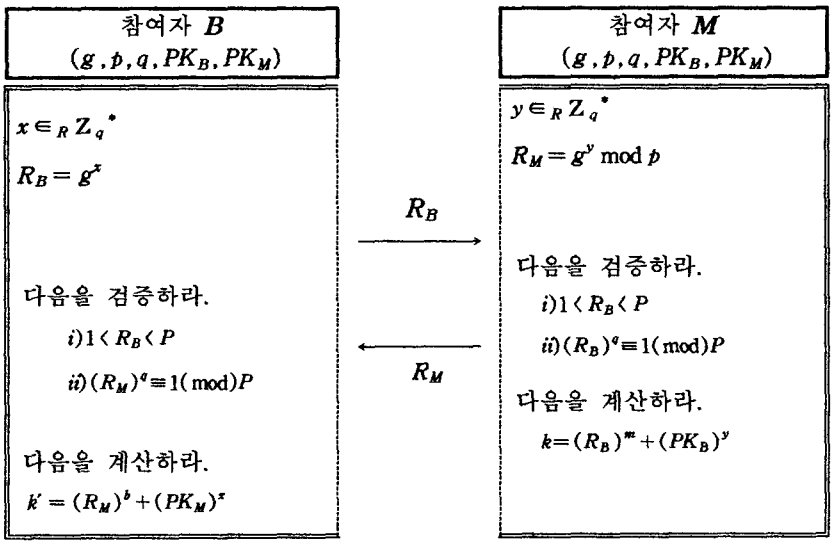

그림 8 KEA

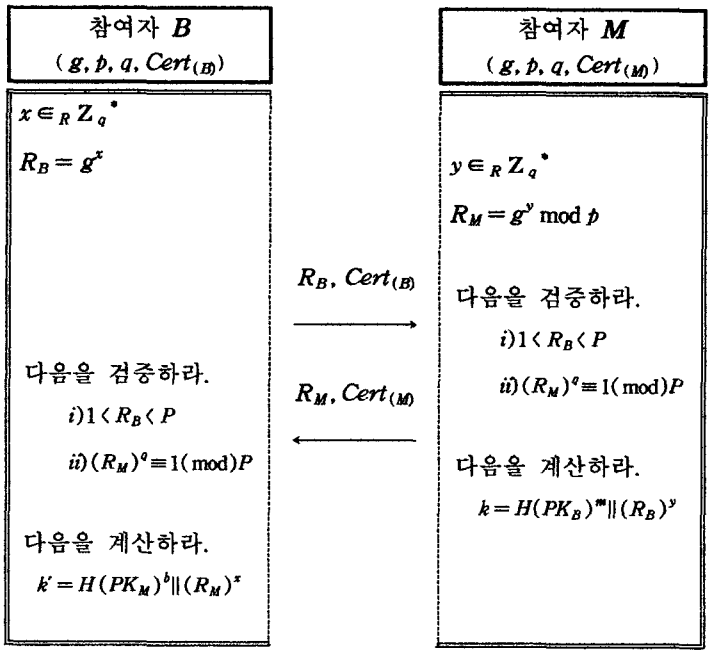

그림 9 통합화된 키 분배 모델

다는 것이다. 이 방식은 KEA 방식과 유사하나 세션키를 계산할 때 해쉬 함수가 개입된다.

제4장 새로운 이동 통신망을 위한 키 분배 프로토콜

본 장에서는 기존의 무선 통신망을 위한 키 분배 방식과 기존의 키 교환 알고리듬을 결합하여 구한 키 분배 프로토콜을 제안한다.

4.1 방식 1 프로토콜

방식 1 프로토콜은 기본적으로 기존의 MSR + DH 프로토콜에 KEA 알고리듬을 적용한 프로토콜이다. 이 프로토콜의 수행 과정은 다음과 같다. 참여자 B는 난수 N_B를 생성하고 자신의 임시 개인키 x를 생성하여 임시 공개키 R_B를 계산한 후, $B, PK_B, R_B, N_B, Cert_{(B)}$ 을 이동국에게 보낸다. M은 자신의 임시 개인키 y를 생성하여 임시 공개키 R_M을 계산하고 기지국으로부터 받은 정보 R_B를 검증하고, M의 정보와 B의 정보를 사용하여 세션키 k를 계산한다. 그리고 이동국은 $E\{k\}_{PK_B}, E\{N_B, M, PK_M, Cert_{(M)}\}_k, R_M$을 기지국으로 전송한다. B는 M에게서 받은 정보 R_M을 검증하고 B의 정보와 M의 정보를 사용하여 세션키 k'를 계산하고, $k = k'$ 인지를 검증한다. 이 프로토콜에서 난수 N_B를 생성하여 사용함으로써 재생공격을 방지할 수 있고 인증서를 주고받음으로써 Man in the middle attack을 방지할 수 있다. 또한 임시 대칭키 쌍을 생성하여 사용함으로써 매 세션마다 세션키를 변경할 수 있게 되어 암호 시스템의 보안 강도를 높여준다. 임시의 비대칭키 쌍을 사용함으로써, 매 세션마다 세션키 변경이 가능하고, 인증서를 주고받음으로써 "man in the middle" 공격을 방지하였다. 동시에 난수을 생성하여 사용함으로써 재생공격을 방지하였다.

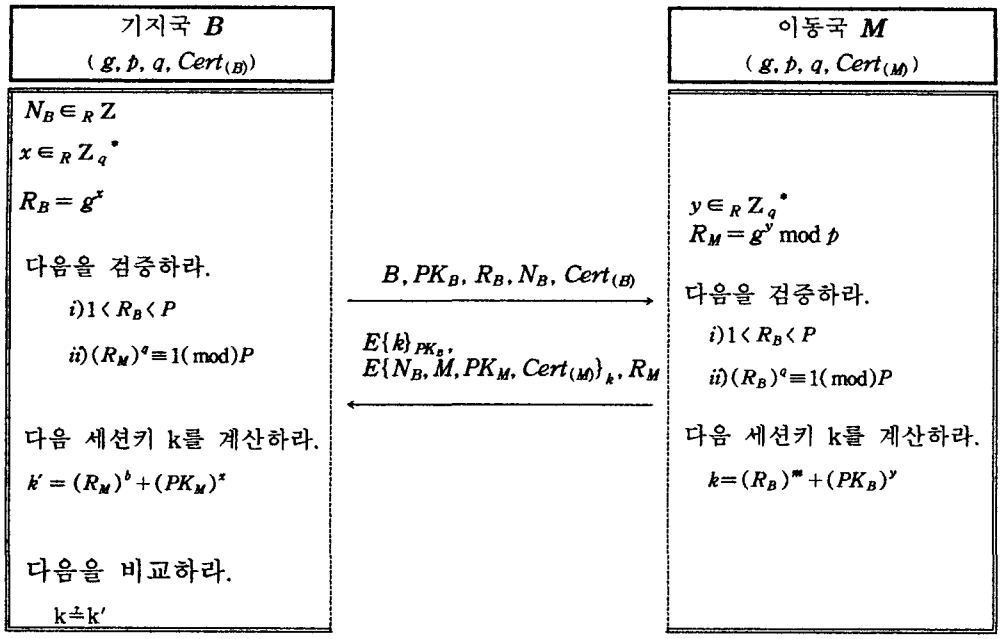

그림 10 방법 1 키 분배 프로토콜

4.2 방식 2 프로토콜

방법 2 프로토콜은 MSR + DH 프로토콜에 통합된 키 분배 모델을 적용한 프로토콜이다. 이 프로토콜의 수행과정은 다음과 같다. 참여자 B는 난수 N_B를 생성하고 자신의 임시 개인키 x를 생성하여 임시 공개키 R_B를 계산한 후, $B, PK_B, R_B, N_B, Cert_{(B)}$ 을 M에게 보낸다. M은 자신의 임시 개인키 y를 생성하여 임시 공개키 R_M을 계산하고 B에게서 받은 정보 R_B를 검증하고, M의 정보와 B의 정보를 사용하여 세션키 k를 계산한다. 그리고 $E\{k\}_{PK_B}, E\{N_B, M, PK_M, Cert_{(M)}\}_k, R_M$을 B에게 보낸다. B는 M에게서 받은 정보 R_M을 검증하고 B의 정보와 M의 정보를 사용하여 세션키 k'를 계산하고, $k = k'$ 인지를 검증한다. 이 프로토콜에서 난수 N_B를 생성하여 사용함으로써 재생공격을 방지할 수 있고 인증서를 주고받음으로써 "man in the middle" 공격을 방지할 수 있다. 또 세션 키에 해쉬 함수를 사용하여 고정된 키 길이를 생성한다. 또한 임시 공개키 쌍을 생성하여 사용함으로써 매 세션마다 세션키를 변경할 수 있게 되어 상호인증의 강도를 증가한다.

4.3 방식 3 키 분배 프로토콜

방법 3 프로토콜은 MSR 프로토콜을 변경한 개선된 Beller와 Yacobi의 프로토콜에 KEA 알고리즘을 적용한 프로토콜이다. 이 프로토콜의 수행과정은 다음과 같다. 참여자 B는 난수 N_B를 생성하고 자신의 임시 개인키 x를 생성하여 임시 공개키 R_B를 계산한 후, $B, PK_B, R_B, N_B, Cert_{(B)}$을 M에게 보낸다. M은 자신의 임시개인키 y를 생성하여 임시공개키 R_M을 계산하고 B에게서 받은 정보 R_B를 검증하고, M의 정보와 B의 정보를 사용하여 세션키 k를 계산하고, B, M, N_B, k 에 해쉬를 취하고 M의 개인키로 암호화(서명)한다. 그리

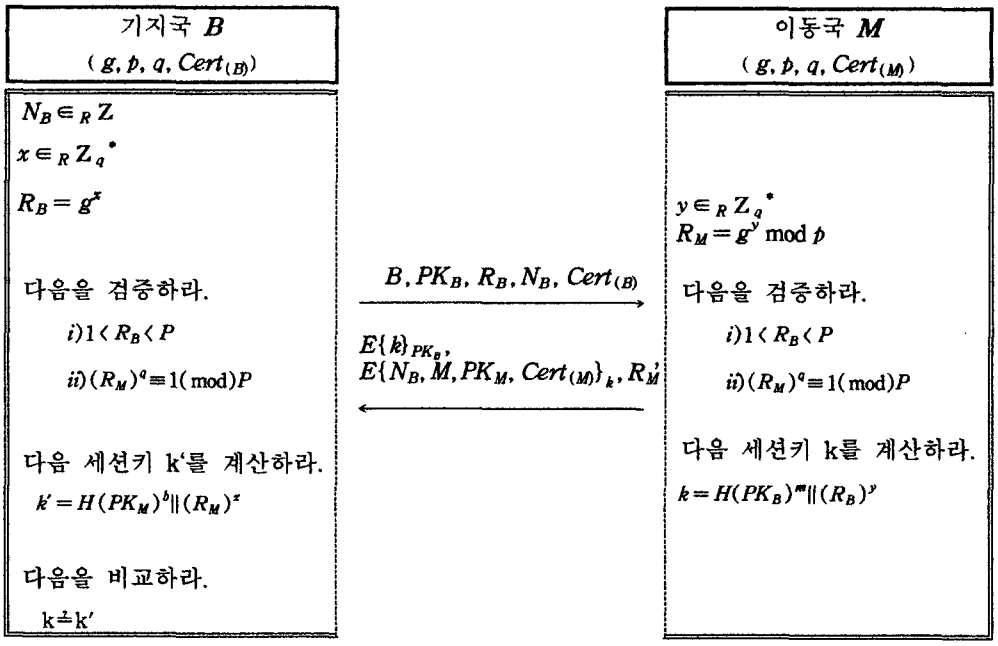

그림 11 방식 2 키 분배 프로토콜

$, R_M, E\{h(B, M, N_B, k)\}_{PK_M^{-1}}$을 B에게 보낸다. B는 M에게서 받은 정보 R_M을 검증하고 B의 정보와 M의 정보를 사용하여 세션키 k'를 계산하고, $k = k'$ 인지를 검증한다. 마지막으로 B는 M의 서명문을 확인한다. 이 프로토콜에서 난수 N_B를 생성하여 사용함으로써 재생공격을 방지할 수 있고 인증서를 주고받음으로써 "man in the middle" 공격을 방지할 수 있다. 또 임시 대칭키 쌍을 생성하여 사용함으로써 매 세션마다 세션키를 변경할 수 있게 되어 상호 인증의 강도를 높여준다.

4.4 방식 4 키 분배 프로토콜

방법 4 키 분배 프로토콜은 Beller와 Yacobi의 프로토콜에 통합된 키 분배 보델을 적용한 프로토콜이다. 이 프로토콜의 수행 과정은 다음과 같다. 참여자 B는 난수 N_B를 생성하고 자신의 임시 개인키 x를 생성하여 임시 공개키 R_B를 계산한 후, $B, PK_B, R_B, N_B, Cert_{(B)}$ 을 M에게 보낸다. M은 자신의 임시 개인키 y를 생성하여 임시 공개키 R_M을 계산하고 B에게서 받은 정보 R_B를 검증하고, M의 정보와 B의 정보를 사용하여 세션키 k를 계산하고, B, M, N_B, k 에 해쉬를 취하고 M의 개인키로 암호화(서명)한다. 그리고 $E\{k\}_{PK_B}, E\{N_B, M, PK_M, Cert_{(M)}\}_k$ $, R_M, E\{h(B, M, N_B, k)\}_{PK_M^{-1}}$을 B에게 보낸다. B는 M에게서 받은 정보 R_M을 검증하고 B의 정보와 M의 정보를 사용하여 세션키 k'를 계산하고, $k = k'$ 인지를 검증한다. 마지막으로 B는 M의 서명문을 확인한다. 이 프로토콜에서 난수 N_B를 생성하여 사용함으로써 재생 공격을 방지할 수 있고 인증서를 주고 받음으로써 "man in the middle" 공격을 방지할 수 있다. 또 세션키에 해쉬 함수를 사용하여 고정된 키 길이를 생성하여 계산속도가 빨라졌다. 여기에 임시 세션 키 쌍을 생성하여 사용함으로써 매 세션마다 세션키를 변경할 수 있게 되어 암호 시스템의 보안 강도가 증가한다.

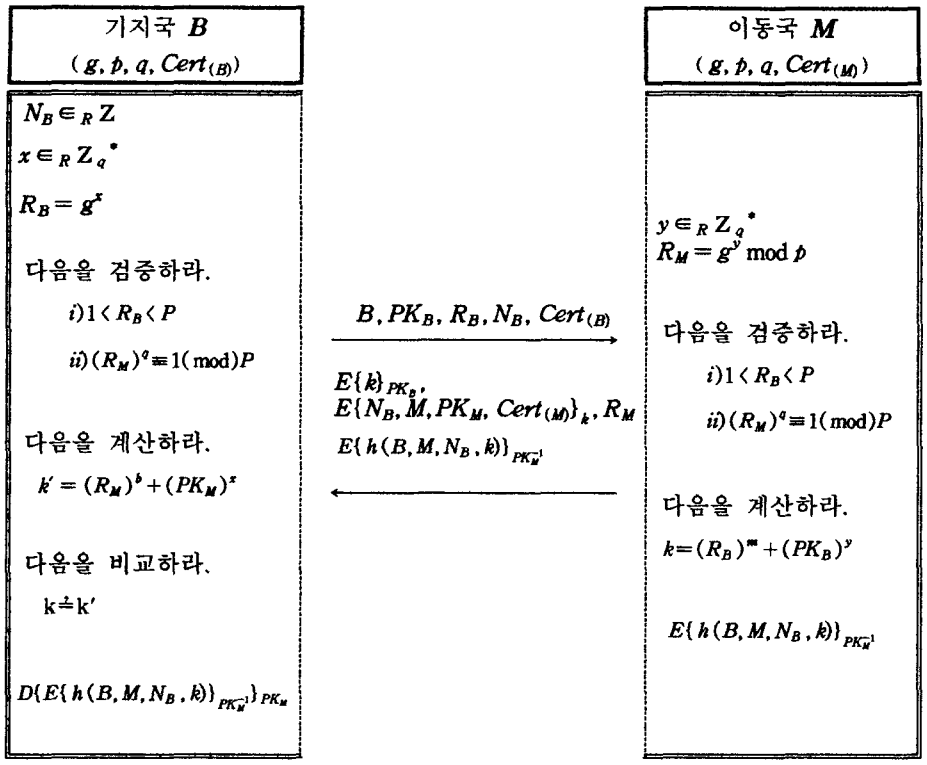

그림 12 방법 3 키 분배 프로토콜

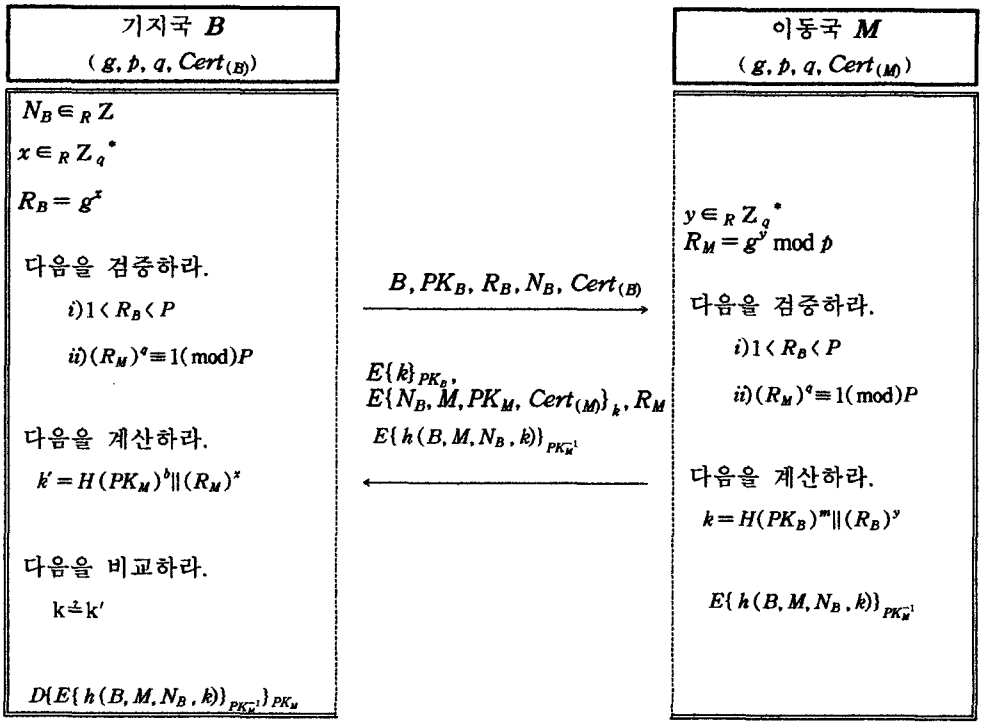

그림 13 방법 4 프로토콜

4.5 각 방식의 특징 비교 분석

본 절에서는 기존의 키 분배 프로토콜과 제안된 키 분배 프로토콜에 대한 특징을 비교 분석한다.

제5장 결 론

무선망을 통한 인터넷 통신이 일반화되면서 이동 통신망 보안을 위한 인증 및 키 분배 프로토콜을 비롯한 암호 방식에 대한 연구가 매우 중요하게 요구되고 있다.

본 논문에서는 기존의 무선 통신망 보안을 위한 환경을 분석하고, 보안 서비스 제공을 위한 요구 사항을 도출하였으며, 무선 통신망과 기존의 유선 통신망을 위한 기존의 키 분배 방식들을 분석하였다. 그리고 이를 근거로 네 가지 방식의 새로운 키 분배 프로토콜을 제안하고 각 방식의 특징을 비교 분석하였다. 이동 통신 보안 환경은 무선 링크를 포함하므로, 가장 보안상의 취약 지점으로 예측되는 무선 링크에서의 보안을 제공하기 위한 여러 가지 방법이 제시되었다. 또한 기존의 대표적인 이동 통신을 위한 키 분배 방식들을 분석했으며, 각 방식의 장단점을 도출하였다. 각 방식의 특징을 분석하기 위하여 비교 항목을 도출하였다.

제안된 네 가지 방식은 재생 공격이 불가능하며, 중간에 공격자가 존재하여 시스템을 공격하는 "man in the middle" 공격을 예방하며, 세션마다 새로운 세션키가 갱신되며, 인증서의 사용으로 공개키의 신뢰성을 보장할 수 있다. 여기서 제안된 방식은 상당한 계산 능력과 저장 능력을 보유하게 될 제삼세대 이동 통신 단말에 유용하게 활용될 것으로 예측된다. 따라서 본 논문의 결과는 이동 통신망의 인증 및 키 분배 시스템 설계 시 유용하게 활용될 수 있을 것으로 예측된다.

표 1 키 분배 프로토콜 특성 분석

	IKA	EKA	KKS	FS	KCI	UKS
MSR	×	×	×	×	×	×
IMSR	×	×	×	×	×	×
DH	✓	×	×	×	×	✓
MSR+DH	✓					✓
BY	×	×	×	×	×	×
BY의 향상된 프로토콜	✓	✓	✓	×	✓	×
KEA	✓	×	✓	×	✓	✓
UM	✓	×	✓?	✓?	×	✓
제안 방식 1	✓	×	✓	×	✓	✓
제안 방식 2	✓		✓	×?		✓
제안 방식 3	✓	✓	✓		✓	✓
제안 방식 4	✓	✓	✓	✓?	✓	✓

참고문헌

[1] M. J. Beller, L, -F. Chang, and Y. Yacobi, "Security for Personal Communication Services: Public-Key vs. Private Key Approaches," in *Proceedings of Third IEEE* Press, 1991.

[2] M. J. Beller and Y. Yacobi, "Fully-Fledged two-way Public Key Authentication and Key Agreement for Low-Cost Terminals," *Electronic Letters*, 29, pp. 999-1001, May 1993.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644-654, 1976.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469-472, 1985.

[5] V. Varadharajan and Y. Mu, "On the Design of Security Protocols for Mobile Communications," *ACISP'96 Conference*, Springer-Verlag, 1996, pp. 134-145

[6] R. Ankney, D. Johson and M. Matyas, "The Unified Model," contribution to X9F1, October 1995.

[7] ANSI X9.42, *Agreement of Symmetric Algorithm Keys Using Diffie-Hellman*, working draft, May 1998.

[8] ANSI X9.63, *Elliptic Curve Key Agreement and Key Transport Protocols*, working draft, July 1998.

[9] IEEE P1363, *Standard Specification for Public-Key Cryptography*, working draft, July 1998.

[10] K. C. Goss, "Cryptographic method and apparatus for public key exchange with authentication," U.S. patent 4,956,865, September 11 1990.

[11] T. Matsumoto, Y. Takashima and H. Imai, "ON seeking smart public-key distribution systems," *The Transactions of the IECE of Japan*, E69, pp. 99-106, 1986.