이동 통신 시스템에서의 키 복구 모델에 관한 연구

황보성[0], 이임영
순천향대학교 정보기술공학부
hbs@ai-cse.sch.ac.kr, imylee@asan.sch.ac.kr

A Study on Key Recovery Model in Mobile Communication Systems

Bo-Sung Hwang[O], Im-Yeong Lee
Division of Information Technology Eng. Soonchunhyang Univ.

요 약

무선이동통신 기술의 발달은 이용자의 수와 데이터 양의 폭발적인 증가를 가져왔다. 이러한 추세에 따라 Cellular, PCS, Radio-paging, Multimedia data, Internet services를 통합하는 제 3세대 무선이동통신이 연구 중에 있다. 모든 서비스들이 무선이동통신으로 이동함에 따라 보안문제들(인증, 키교환, 키복구등)이 중요시되고 있다. 그 중에서도 범법자들의 통신에 대한 국가적 법집행능력 확보를 위한 키 복구 모델은 꼭 필요 할 것이다. 따라서, 본 논문에서는 이동통신시스템에서의 효율적인 키 복구를 위한 모델을 제안하고 이에 따른 데이터 타입을 정의한다.

1. 서론

산업사회에서 정보화사회로 바뀌어 가면서 산업, 교육, 서비스등 모든 분야가 인터넷과 무선 이동 시스템으로 바뀌어가고 있는 추세에 있다. 이러한 이유는 인터넷과 무선 이동 시스템이 편리하기 때문이다. 하지만 이들 시스템의 그 편리함에도 불구하고 개방적인 특성에 의해 사용자의 프라이버시에 큰 피해를 입힐 수 있다는 문제점이 상존하게 된다. 이를 해결해 줄 수 있는 방법이 강력한 암호를 사용하는 것인데, 암호의 사용은 각 사용자들에게 자신의 비밀키에 해당하는 정보를 자신만이 안전하게 보관해야한다는 부담이 따른다. 이러한 부담을 줄이기 위한 방법이 사용자는 미리 자신의 키를 특정기관에게 위탁하고 키 유실시 키를 복구받고 또한 정부는 위탁된 키를 이용해 범법자들의 통신을 감청할 수 있는 시스템이 키 복구 시스템이다. 이동통신시스템의 특징상 사용자의 키복구 요구는 그리 많치 않을 것이다. 키 유실로 인해서 통화를 듣지 못할 경우는 다시 양 사용자 사이에 셋업과정을 거치면 되기 때문이다.

따라서 본 논문에서는 무선이동통신상에서의 범법자들을 정당하게 감청하기 위한 키 복구 모델을 설계하고 그에 따르는 데이터 타입을 정의한다.

* 본 연구는 1999학년도 한국무선관리사업단 연구과제에 의해 수행되었음

2. 제안방식

본 논문에서 제안하는 모델은 GSM(Global System for Mobile Communications)시스템[2][3]을 기본으로 하여 설계되었다. 제안 모델의 구성요소와 시스템 파라메터는 다음과 같다.

2.1 구성요소

- 법기관 : 감청기관의 감청요구를 심사한다.
- LEA(Lawful Interception Agency) : 감청기관으로써 법기관의 허가와 교환국의 도움으로 사용자의 정보를 감청하는 수사기관이다.
- 교환국 : 일반 이동통신의 교환국으로써 이동통신 서비스를 위한 일반적인 Admin과 감청을 위한 Interception Admin으로 구성된다.
- Interception Admin(IA) : 기지국에 속해있으며 DF2, DF3와 사용자의 키정보를 가지고 감청에 관련된 정보와 데이터를 LEA에게 전송한다.
- DF2(Delivery Function 2) : IA에 속해있으며, IRI(Intercept Related Information)를 LEA에 제공한다.
- DF3(Delivery Function 3) : IA에 속해있으며, IR(Intercept Product)을 LEA에 제공한다.
- 사용자 : 키 복구 요구자 또는 감청대상자

2.2 시스템 파라메터

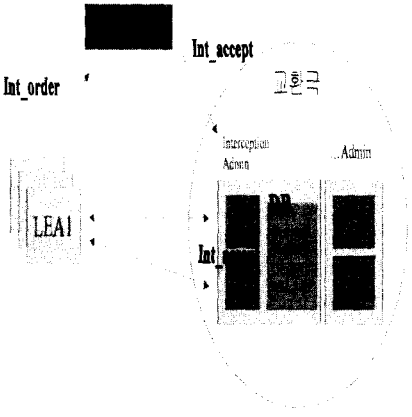
- Id : 감청대상자의 식별자

- Int_id : Interception Admin과 LEA 사이의 통신에서의 식별자
- Call-type : 감청의 종류(통화, 메시지)
- Rea : 감청사유
- Date : Int_order()의 생성날짜
- Lea_add : LEA의 식별 및 주소
- Int_date : 감청기간
- Event_type : 감청대상자의 서비스형태(송신,수신)
- Event_date : 감청대상자의 서비스 이용날짜
- Event_time : 감청대상자의 서비스 이용시간
- Call_result : 통화연결의 결과
- Calloff_rea : 통화종료의 이유
- Dialled_num : 감청대상자와 연결되어 있는 번호
- Loc_area : 감청대상자의 위치정보
- Key_info : 양사용자의 암호화 통신을 복호하기 위한 키정보
- IRI(Intercept related product) : 감청대상자에 관한 정보
- IP(Intercept product) : 사용자에 의해 실제로 생성된 음성 및 데이타

2.3 제안 모델

제안 모델의 구성요소는 [그림 1]과 같고 LEA는 감청대상자의 감청을 위해 법기관에게 감청을 요청하고 법기관은 그 요구가 정당하다면 교환국 내의 IA에게 감청대상자의 정보를 전송하고 IA는 그 정보를 저장한다. 데이터타입은 다음과 같다.

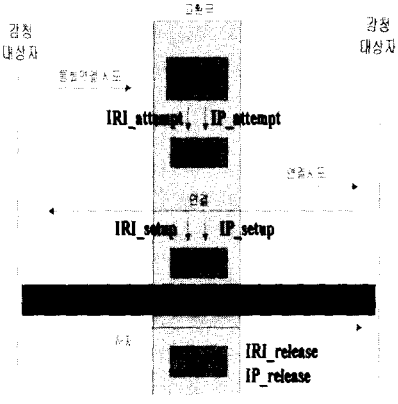
- Int_order(Id, Call_type, Rea, Date, Int_id)
- Int_accept(Id, Int_id, Lea_add, Call_type, Int_date)



[그림 1] 감청 요구 및 설정

사용자가 통화를 위해 셋업과정([그림 2])을 거칠 때 IA는 자신의 DB로 사용자가 감청대상자인지 확인 후, 감청대상자라면 DF2에게 IRI를 IRI_attempt( )를 이용해 전송하고 DF3에게는 LEA와 통신설정을 위해서 IP_attempt를 제공한다. 양쪽 사용자들 사이에 통화가 연결되면 IA는 DF2에게 수신자의 정보와 통화연결의 결과를 제공하고 DF2는 이 정보를 LEA에게 전송한다. 또한, IA는 통화연결의 결과를 제공하고 DF3는 IP_attempt()에게 제공받은 사용자들 사이의 Key_info와 LEA의 주소를 이용해 사용자사이의 세션키를 복구한 후 사용자의 통신내용을 LEA에게 전달함으로써 LEA는 감청대상자를 감청할 수 있다. 통화종료시 IA는 DF2, DF3에게 통화종료의 이유를 제공하고 이 정보는 LEA에게 전송된다. 그리고, LEA의 감청요구에 따라 IRI만을 요구할 수도 있다. 데이터타입은 다음과 같다.

- IRI_attempt(Id, Int_id, Lea_add, Call_type, Event_type, Event_date, Event_time, Dialled_num, Loc_area)
- IP_attempt(Id, Key_info, Int_id, Lea_add, Event_type)
- IRI_setup(Id(수신자), Call_result, Int_id, Loc_area(수신자))
- IP_setup(Call_result, Int_id)
- IRI_release(Id, Id(수신자), Lea_add, Event_type, Event_date, Event_time, Calloff_rea)
- IP_release(Id, Int_id, Event_type, Lea_add)



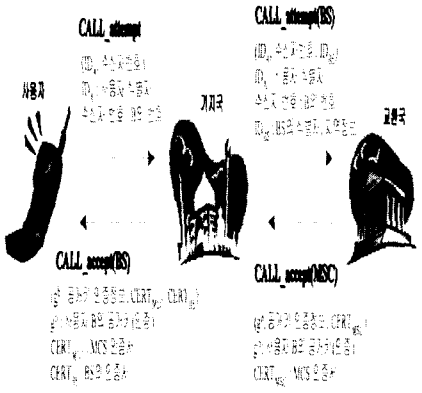
[그림 2] 통화 셋업 과정

3. 제안방식의 이용

본 장에서는 2장에서 제안된 기본 모델과 데이터타입이 실질적으로 어떻게 이용되는지 설명한다. 양쪽 사용자들 사이의 키 설정은 다양한 방법이 있을 수 있지만 본 고에서의 키 설정은 사용자들에 의해 생성되는 것으로 가정한다. 송신자는 수신자와 암호통신을 하기 위해서는 수신자와 세션키를 설정해야 한다. [그림 3]은 키를 설정하기 위해 송신자가 수신자의 공개키를 교환국에서 받는 것을 보여준다. 교환국은 셋업과정에서 송신자와 수신자의 정보를 알 수 있다. 따라서, 교환국은 수신자의 공개키(g^B)를 송신자에게 제공하고 수신자에게는 송신자의 공개키(g^A)를 제공한다. 제공받은 수신자의 공개키를 이용해 송신자는 단말기를 통해서 다음과 같이 ElGamal

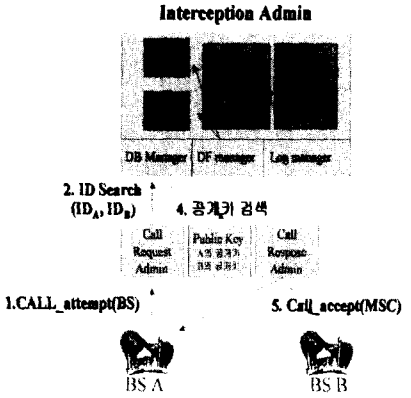
암호를 이용해 통신을 암호화해서 수신자에게 전송함으로써 양쪽 사용자 사이의 안전한 통신이 가능하다.[1]

$g^r \bmod p$, $K*g^{Br}$, $E_K[M]$
(r : 송신자에 의해 생성된 랜덤값, K : 설정된 세션키, M : 메시지, p : 공개 모듈러값)



[그림 3] 사용자사이의 키설정

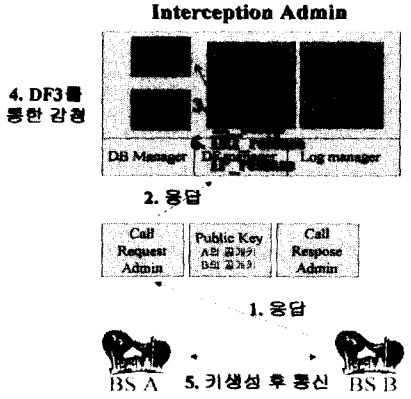
송신자의 CALL_attempt()가 교환국에 전달되면, 교환국은 IA에 문의해 송신자와 수신자 중 감청대상자가 있는지 확인한다. 만약 감청대상자가 있다면 DF manager에 의해 DF2와 DF3에 IR_attempt()와 IRI_attempt()를 전송해 LEA와의 연결을 설정한다. 그 후 각각에게 상대방의 공개키가 전송된다. 만약 감청대상자가 아니라면 상대방의 공개키만이 송수신자에게 전송된다. [그림 4]에서 이용되는 IR_attempt()와 IRI_attempt()의 데이터 타입은 2장에 정의되어 있다.



[그림 4] 감청 과정 1

상대방의 공개키를 전송받은 사용자는 위에서 설명한 것과 같이 둘 사이의 세션키를 생성해 암호화 통신을 시작한다.

셋업과정에 의해서 송수신자의 연결이 설정된다면 DF Manager는 DF2와 DF3에게 IRI_setup()과 IP_setup()을 전송한다. DF3는 IP_attempt()의 Key_info를 이용해 송수신자사이의 세션키를 계산하고 Lea_add를 이용해 이 정보를 안전한 채널을 이용해 LEA에게 전달한다. 통화가 종료되면 DF manager에 의해 IRI_release()와 IP_release()가 DF2와 DF3에게 전달된다. 마찬가지로, [그림 5]에서 이용되는 IRI_setup(), IP_setup(), IRI_release(), IP_release()의 데이터 타입은 2장에 정의되어 있다.



[그림 5] 감청 과정 2

4. 결론

지금까지 무선이동통신상에서의 키 복구 모델과 실질적인 이용을 살펴보았다. 본 논문에서는 키의 생성이 사용자들에 의해서 설정된다고 가정했다. 하지만 키의 생성은 기지국이나 교환국에 의해서 생성될 수도 있고 기지국과 사용자, 교환국과 사용자사이에서도 생성될 수 있다. 사용자사이의 키 생성 또한 공개키 방식을 이용하는 것이 아니라 다른 여러 방법이 제공될 수 있을 것이다. 이러한 다양한 키 생성방법과 일반적인 키복구 요구사항들(신원보호, 감청기한 제한, 공모방지등)을 제안 모델에 포함시키기 위한 연구가 계속 진행되어야 할 것이다. 또한 제 3세대 무선이동통신은 글로벌 로밍을 제공한다. 이러한 시스템을 위해서, 각 나라의 기지국과 교환국사이의 키 복구를 위한 모델의 정립과 정책이 필요할 것이다.

Reference

[1] Juanma Gonzalez, Key Recovery in Third Generation Wireless Communication systems, LNCS 1751, pp 223-237, 2000

[2] 3 GPP TSG SA, Lawful Interception Requirements Version 0.0.2, http://www.3gpp.org

[3] 3 GPP TSG SA, Lawful Interception Version 7.3.0, http://www.3gpp.org