WAKE-KR을 지원하는 인증서 발행 프로토콜

이용호[†] · 이임영[††]

요 약

정보보호의 중요성이 인식되면서 암호 기술의 사용이 증가하고 있다. 특히, 공개키 암호 기술은 대칭키 암호 기술에 비해 키의 관리가 용이하고, 디지털 서명을 쉽게 구현할 수 있다는 장점을 가지고 있어서 그 사용이 증가하고 있다. 현재 공개키 암호 기술을 효율적이고 안전하게 사용하기 위한 공개키 기반 구조가 구축되어 운영되고 있다. 공개키 기반 구조에서는 사용자가 인증기관에 등록하여 개인키와 공개키 쌍을 생성하고, 인증기관은 생성된 공개키에 대한 인증서를 발행한다. 이러한 인증서를 이용하여 사용자간에 키 설립를 수행하고 암호화 통신을 할 수 있게 된다. 그러나 공개키 기반 구조에서 설립된 세션키에 대한 관리 기능은 제공하고 있지 않다. 본 논문에서는 무선 인증 및 키 설립시 설립된 세션키에 대한 키 복구를 지원하는 인증서 발행 프로토콜을 제안한다.

Certificate Issuing Protocol Supporting WAKE-KR

Yong-Ho Lee[†] and Im-Yeong Lee[††]

ABSTRACT

As the importance of information security gets recognized seriously, ciphers technology gets used more. Particularly, since public key ciphers are easier to control the key than symmetric key ciphers and also digital signature is easily implemented, public key ciphers are increased used. Nowadays, public key infrastructure is established and operated to use efficiently and securely the public key ciphers. In the public key infrastructure, the user registers at the certificate authority to generate the private key and public key pair and the certificate authority issues the certificate on the public key generated. Through this certificate, key establishment between users is implemented and encryption communication becomes possible. But, control function of session key established in the public key infrastructure is not provided. In this thesis, the certificate issuing protocol to support the key recovery of the session key established during the wireless authentication and key establishment is proposed.

Key words: Key Recovery, Certificate Issuing, Wireless Authentication, Public Key Infrastructure, Key Establishment

1. 서 론

컴퓨터 기술의 발전과 인터넷의 확산에 따라 세계에 퍼져있는 다양한 정보가 공유되었고, 쉽게 이용할 수 있게 되었다. 정보의 공유는 우리의 생활에 많은 이점을 가져다 준 반면 개인 정보나 기업 및 국가의 중요 정보가 노출되어 악용되는 문제점을 발생시켰다. 정보의 중요성과 이용 가치가 증가함에 따라 이러한 문제점 또한 증가하게 된다. 현재 안전하고 신뢰성 있는 정보의 교환과 공유를 위해 다양한 정보보안 기술이 개발되고 있다. 특히, 공개키 기반 구조(PKI; Public Key Infrastructure)는 개방 네트워크 상에서 정보의 기밀성, 인증, 무결성, 부인봉쇄 등과 같은 보안 서비스를 제공하기 위해 개발되었다. 공개키 기반 구조에서 사용되는 공개키 암호 알고리즘은 서로 다른 두 개의 키를 사용하게 된다. 이 중 공개키는 인증기관이 안전하게 관리하고 해당하는 인증서를 발행해 소유주는 물

접수일 : 2002년 9월 24일, 완료일 : 2002년 12월 9일
[†] 준회원, TTA SW시험인증센터 전임연구원
[††] 종신회원, 순천향대학교 정보기술공학부 부교수

론이고, 누구나 이용 가능하도록 운영하고 있다. 공개키는 암호화와 서명 검증을 수행하는데 사용된다. 그리고 만약 두 사용자가 암호화 통신을 하려고 할 경우 각각의 인증서를 이용하여 세션키를 설립을 할 수 있으며, 설립된 세션키를 이용하여 대칭키 암호화 통신을 수행할 수 있게 된다. 개인키는 사용자가 안전하게 소유하고 있어야 하며, 이것을 이용하여 메시지 복호화 및 디지털 서명을 수행할 수 있게 된다. 공개키 기반 구조를 이용하게 되면 공개키를 안전하고 효율적으로 관리할 수 있다. 그러나 두 사용자가 암호화 통신 수행 시 설립한 세션키에 대해서는 그 관리가 미흡한 실정이다. 이러한 대칭키들을 안전하게 관리할 수 있는 암호 기술이 키 복구 기술이다. 키 복구란 어떤 특정한 조건이 주어지면 암호문에 사용된 키 또는 복호화된 평문을 복구할 수 있는 기술을 이야기한다. 특정한 조건이란 사용자의 부주의로 인해 키가 분실되거나 자연재해로 인해 키가 유실되는 경우 또는 암호화 통신을 수행하는 송·수신자간에 부정의 소지가 있을 경우 등을 의미한다.[1,6,7,13,18]

무선 기술이 발전하면서 무선 보안 프로토콜 또한 그 중요성이 인식되고 있다. 특히, 무선상 인증 및 키 설립(WAKE; Wireless Authentication and Key Establishment) 프로토콜은 무선 통신상에서 인증, 무결성, 기밀성 등의 보안 서비스를 제공하기 위해 필수적으로 이루어져야 하는 과정으로 그 중요성은 매우 크다고 할 수 있다. 키 복구 기능을 가지는 WAKE (WAKE-KR; WAKE-Key Recovery) 프로토콜은 WAKE 프로토콜에 의해 설립된 세션키에 대해 키 복구 기능을 제공하는 프로토콜로써 ASPeCT 프로젝트에 의해서 처음으로 시도되었다. 이후 다양한 WAKE-KR 프로토콜이 연구되고 있다.[19-21]

본 논문에서는 사용자와 인증기관이 가지고 있는 상이한 요구사항을 모두 만족할 수 있는 인증서 발행 프로토콜과, 상기 프로토콜을 이용하여 인증서를 발행받은 두 개체간에 수행되는 WAKE-KR 프로토콜을 새롭게 구성하였다. 제안하는 인증서 발행 프로토콜은 기존에 제시된 두 가지 인증서 발행 프로토콜의 장점을 모두 가지고 있으며, WAKE-KR 프로토콜은 기존에 제시된 프로토콜의 보안 문제점들을 모두 해결하고 있다. 제안 프로토콜은 다음과 같은 흐름을 가지고 있다. 사용자와 인증기관이 상호 협력하여 사용자의 개인키와 공개키 쌍을 생성하도록 구성하고, 두 사용자간에 무선 인증 및 키 설립 과정을 수행할 경우 특정한 조건이 주어지면 설립된 세션키를 복구할 수 있다.

논문의 구성은 다음과 같다. 2장에서 관련 기술을 소개하고, 3장에서 제안 방식을 소개한다. 4장에서는 제안된 방식의 특징을 설명하고 기존 방식과의 비교 분석을 수행한다. 마지막으로, 5장에서 결론을 맺도록 한다.

2. 관련 기술 소개

본 장에서는 제안하는 프로토콜과 관련된 암호 기술인 공개키 기반 구조와 WAKE-KR 프로토콜에 대해서 소개한다.

2.1 공개키 기반 구조

본 절에서는 공개키 기반 구조의 정의와 구성요소 그리고 인증서 발행 과정에 대해 알아본다.[2,8,14,15]

2.1.1 공개키 기반 구조의 정의와 구성요소

인터넷과 같은 개방형 네트워크 환경에서 안전하고 효율적인 통신을 수행하기 위해서는 공개키 암호 기술과 인증서의 사용이 필수적이라 할 수 있다. 이러한 것들을 편리하게 이용할 수 있는 기반 구조를 공개키 기반 구조(PKI : Public Key Infrastructure)라고 한다. 공개키 기반 구조는 다음과 같은 보안 서비스를 제공할 수 있다.

- 기밀성(confidentiality) 서비스 : 정보가 네트워크를 통해 전송되는 과정에서 제 3자에게 노출되지 않도록 하는 서비스
- 무결성(integrity) 서비스 : 네트워크를 통해 전송되는 정보의 위·변조 여부를 검증할 수 있는 서비스
- 인증(authentication) 서비스 : 통신을 하는 송·수신자에 대한 신원을 확인할 수 있는 서비스
- 부인방지(non-repudiation) 서비스 : 통신을 하는 송·수신자에 대해 각각 송·수신 사실의 부인을 방지할 수 있는 서비스

다음은 공개키 기반 구조를 구성하는 최소 객체들을 소개한다.

- 인증기관(CA; Certification Authority) : 등록된 사용자의 공개키가 올바르게 생성되었는지를 검증하고 이상이 없을 경우 해당 공개키에 대한 인증서를 발행하는 기능을 수행한다.

• 등록기관(RA; Registration Authority) : 인증기관과 멀리 떨어져 있는 사용자들을 위해서 인증기관 대신 인증서 신청을 받고, 인증기관에게 이 사실을 통보하는 역할을 수행한다.

• 디렉토리(Directory) : 사용자 정보나 인증서 등을 저장하는 장소로써 임의의 사용자들에게 검색할 수 있는 기능을 제공한다. 이것은 인증기관이 관리하게 된다.

• 사용자(User) : 공개키 기반 구조를 이용하는 객체로써 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

2.1.2 공개키 기반 구조에서의 인증서 발행 과정

사용자가 공개키 기반 구조를 이용하여 인증서를 발행 받고자 할 경우 수행되는 과정은 다음과 같다.

• 등록 : 사용자가 인증서를 발급 받고자 할 경우, 인증기관으로부터 사용자 식별 이름, 사용자 속성 정보 등을 제공받고 이들의 유효성을 인증기관으로부터 검증 받는 과정이다.

• 초기화 : 인증기관이 사용자에게 자신의 인증서를 안전하게 제공하는 과정이다.

• 키 생성 : 사용자가 자신의 공개키와 개인키를 생성하는 과정이다. 사용자의 개인키와 공개키는 사용자 측에서 키 생성 프로그램을 이용하여 생성하거나 인증기관에 의해서 생성된다.

• 인증서 발행 : 인증기관이 인증서를 발행하고 공표한 후 사용자에게 생성된 인증서를 전달하는 과정으로 사용자가 생성된 공개키와 인증서 발행 요청을 인증기관에게 전송할 경우 수행된다.

상기와 같은 과정을 수행하는 방법은 두 가지가 있다. 하나는 최종 개체(사용자)의 개인키와 공개키 쌍이 인증기관에 의하여 생성되는 집중화된 방식이고, 다른 하나는 개인키와 공개키 쌍이 최종개체에 의하여 생성되는 기본 인증 방식이다.

1) 집중화된 방식

이 방식은 등록 및 인증 과정이 인증기관에서 시작된다. 이것은 정보의 전송 방향을 보면, 인증기관에서 최종 개체로만 전송된다는 것을 의미한다. 최종 개체의 인증서를 발행하는 과정은 다음과 같다.

① 최종 개체와 인증기관은 사전에 안전한 방법으로 키를 공유한다.

② 인증기관은 최종 개체의 개인키와 공개키 쌍을 생성한다.

③ 인증기관은 생성된 공개키에 대해서 공개키 인증서를 생성한다.

④ 인증기관은 생성된 개인키와 공개키 쌍, 인증서 그리고 자신의 공개키를 ①번에서 공유한 키를 이용하여 암호화하여 최종 개체에게 전달한다.

⑤ 최종 개체는 인증기관에서 전송된 암호문에 대해 ①번에서 공유한 키를 이용하여 정보를 획득한다.

2) 기본 인증 방식

이 방식에서는 다음과 같은 절차를 통해 수행된다.

① 최종 개체와 인증기관은 사전에 안전한 방법으로 키를 공유한다.

② 최종 개체는 자신의 개인키와 공개키 쌍을 생성한다.

③ 최종 개체는 ①번에서 공유한 키를 이용해 공개키와 인증서 요청 메시지를 암호화한다. 그리고 생성된 암호문을 인증기관에서 전송한다.

④ 인증기관은 최종 개체로부터 전송된 암호문을 ①번에서 공유한 키를 이용해 복호화하고, 최종 개체가 요청한 공개키 인증서를 생성한다. 그리고 인증서와 응답 메시지를 ①번에서 공유한 키로 암호화해서 최종 개체에게 전송한다.

⑤ 최종 개체는 전송된 인증서에 포함된 공개키에 대응하는 개인키를 소유하고 있음을 인증기관에게 증명하기 위한 개인키 소유 증명 메시지를 생성해서 인증기관에 전송한다.

⑥ 인증기관은 최종 개체로부터 전송된 개인키 소유 증명 메시지를 검증한다. 검증이 성공적으로 완료되면 최종 개체의 인증서를 공표한다.

만약 최종 개체가 개인키와 공개키 쌍을 생성했다면, 최종 개체는 자신의 인증서에 포함된 공개키에 대응되는 개인키를 소유하고 있음을 인증기관에게 증명할 수 있어야 한다. 최종 개체는 개인키 소유 증명이 인증기관을 통해서 올바르게 검증되어야 인증서를 발급 받을 수 있게 된다.

2.2 WAKE-KR 프로토콜

무선 통신 기술이 발전하면서 통신하고자하는 개체간에 인증, 무결성, 기밀성 등의 보안 서비스를 제공하면서 키 설립을 수행하는 WAKE 프로토콜에 대한 연

구가 활발히 진행되고 있다. 이와 더불어, 설립된 세션 키의 분실 및 유실로 인해 암호화된 중요 데이터에 접근할 수 없게 되는 문제점을 해결하기 위해 키 복구 기능을 제공하고자 하는 연구가 시도되었다. WAKE-KR 프로토콜은 키 복구 기능을 가지는 무선 인증 및 키 설립 프로토콜이다. 이 프로토콜은 1999년도에 처음으로 ASPeCT(European Commision ACTS Project)에 의해서 개발되었다. 그 이후 현재까지 계속적으로 연구되고 있다. WAKE-KR 프로토콜은 무선 환경에서 두 사용자간에 안전하게 암호화 통신에 사용되는 키를 설립하고 설립된 키에 대한 관리를 할 수 있는 기술로써 그 중요성이 매우 크다고 할 수 있다. 이 절에서는 WAKE-KR 프로토콜의 요구사항과 기존에 제안되었던 방식들을 소개한다.

2.2.1 WAKE-KR 프로토콜의 요구사항

WAKE-KR 프로토콜이 가져야 하는 요구사항은 WAKE 프로토콜이 가져야 하는 요구사항과 키 복구 기능이 추가되면서 가져야 하는 요구사항으로 나눌 수 있다. 다음은 WAKE 프로토콜이 가져야 하는 요구사항이다.[3-5,11,12,16,17]

• 인증 : 인증이란 통신을 수행하는 두 개체 사이에 신뢰성을 보장하는 요구사항이다. 인증 기능을 제공함으로써 송·수신자간에 신뢰성을 확보할 수 있다.

• 기밀성 : 기밀성이란 전송 정보에 대한 도청이나 감시와 같은 소극적 공격으로부터 전송 정보를 보호하는 요구사항이다.

• 무결성 : 무결성이란 전송 정보가 전송되는 과정에서 제 3자에 의해 불법적으로 수정 또는 위조되지 않고 수신됐음을 보장하는 요구사항이다.

• 무선 환경을 고려한 멱승 연산량 : 유선에서 무선으로 환경이 변화함에 따라 사용자가 이용하는 통신 장비 또한 많이 변화되었다. 이동성이나 편재성과 같은 고려사항을 만족하기 위해서는 무선 단말기를 이용해야 한다. 무선 단말기의 연산량을 고려하여 연산량을 최소화하여야 한다.

• 위장 공격 방지 : 위장 공격 방지란 제 3자가 사용자 또는 서비스 제공자로 위장하여 통신 상대방에게 피해를 주는 행위를 방지하기 위한 요구사항이다. 따라서 이 요구사항은 모든 무선 통신에서 필수적으로 보장되어야 한다.

다음은 키 복구 기능이 추가되면서 가져야 하는 요구사항이다.

• 복구 공개 검증성 : WAKE-KR 프로토콜을 수행하게 되면 통신을 수행하는 두 개체 사이에 비밀키가 설립된다. 이러한 비밀키에 대하여 유사시 키 복구가 가능하다는 것을 공개적으로 검증 가능해야 한다. 그리고 검증하는 주체는 프로토콜 참여 개체 누구나 가능해야 한다. 복구 공개 검증성은 전체 프로토콜의 신뢰성 향상을 위하여 필수적으로 이루어져야 하는 요구사항이다.

• 적은 통신량 : WAKE 프로토콜에 키 복구 기능을 추가하기 위해서 사용되는 자원은 최소화되어야 한다. 이 요구사항은 무선 환경을 고려한 멱승 연산량과도 깊은 관계를 가지고 있으며 전체 시스템의 효율성에 큰 영향을 미친다.

• 도메인 확장성 : 이것은 동일 도메인에 속한 두 개체간에 WAKE-KR 프로토콜을 수행하다가 한 개체가 다른 도메인으로 변경되는 경우나 서로 다른 도메인에 속한 사용자들간에 WAKE-KR 프로토콜을 수행하고자 할 경우를 대비한 요구사항이다. 즉, 이 프로토콜에서 키 복구 기관이 두 개로 분리되는 경우 두 개의 키 복구 기관 모두에게 해당하는 사용자의 키 복구 기능을 제공해야 한다는 것이다.

• 불법적인 키 복구 방지 : WAKE 프로토콜에 키 복구 기능을 추가하기 위해서는 통신 당사자를 제외한 다른 개체가 필요하게 된다. 그리고 이 개체에게 통신 당사자간에 설립되는 키에 대한 관련 정보를 위탁하게 되므로, 불법적인 키 복구에 대한 위험이 존재한다. 불법적인 키 복구 방지는 전체 시스템의 안전성 향상을 위하여 필수적으로 이루어져야 하는 요구사항이다.

2.2.2 기존 WAKE-KR 프로토콜 소개

여기서는 기존에 제시된 3개의 WAKE-KR 프로토콜에 대해 설명한다.

1) R-M WAKE-KR 프로토콜

이 프로토콜은 ASPeCT 프로젝트에 의해 개발된 것으로써 1999년 Rantos와 Mitchell이 소개하였다.[10] 이것은 UMTS(Universal Mobile Telecommunications System) 환경하에서 사용자와 서비스 제공자 사이에 인증 및 키 설립을 수행하고, 설립된 세션 키에 대해서 키 복구를 수행할 수 있다.

(1) 시스템 계수

다음은 R-M WAKE-KR 프로토콜에서 사용하는 시스템 계수에 대하여 설명한다.

- idCAV : 인증기관의 ID
- g^v : VASP(Value Added Service Provider)의 공개키
- g^w : TTP의 공개키
- h1, h2, h3 : 해쉬함수 1, 2, 3
- TV : 타임스탬프
- certV : VASP의 인증서

(2) 프로토콜

이 프로토콜은 사전 준비 단계와 WAKE 단계 그리고 키 복구 단계로 나누어진다.

a) 사전 준비 단계

① 사용자는 TTP에게 초기값 k_u를 위탁한다.

② 사용자는 랜덤값 s를 선택하고 다음과 같이 u를 생성하여 L을 계산한다.

- $u = f(k_u, s)$, (f는 임의의 일방향 함수)
- $L = (g^w)^u$

b) WAKE 단계

사용자 U		VASP V
g^u 계산	g^u, idCAV, $(idU, s)_L$ →	
		랜덤수 r 생성
랜덤수 IV 생성 세션키 K 생성 후 $h2(K, r, idV)$ 비교	r, $h2(K, r, idV)$, TV, certV ←	세션키 $K = h1((g^u)^v, r)$
	$(Sig_u(h3(g^u, g^v, r, idV, ch\_data, TV, IV)), certU, IV)_K$ →	$h3(\ )$ 비교

그림 1. R-M WAKE-KR의 WAKE 단계

c) 키 복구 단계

① 키 복구 기관은 통신 데이터 감청시, 전송 정보들 중에서 g^u, $(idU, s)_L$을 획득한다. 그리고 L과 s를 차례대로 계산한다.

- $L = (g^u)^w$
- $s = ((idU, s)_L)_L$

② 사용자가 위탁한 k_u와 s를 이용하여 u를 계산한다.

- $u = f(k_u, s)$

③ u를 이용하여 세션키를 복구한다.

- $K = h1((g^v)^u, r)$

(3) 요구사항 만족도 분석

다음은 R-M WAKE-KR 프로토콜의 요구사항 만족도를 분석한다. 만족하는 요구사항은 기술하지 않는다.

- 무선 환경을 고려한 멱승 연산량 : 사용자는 3번의 멱승 연산을 하게 되고, VASP는 1번의 멱승 연산을 하게 된다.
- 위장 공격 방지 : 이 프로토콜은 위장 공격이 가능하다. 만약 사용자가 TTP에게 위탁한 초기값 k_u가 공격자에게 노출된다면 공격자는 k_u를 이용하여 VASP로 위장할 수 있게 된다. 공격자는 k_u를 이용하여 u를 계산하고, u와 자신이 생성한 랜덤수 r'를 이용하여 K'_{AB}를 계산할 수 있기 때문이다.
- 복구 공개 검증성 : 이 프로토콜은 복구 공개 검증성을 가지고 있지 않다.
- 적은 통신량 : 이 프로토콜은 이후 모든 프로토콜의 비교 대상이 될 것이다. 따라서 키 복구 기능을 추가함으로써 부가되는 통신량은 없다고 가정한다.
- 도메인 확장성 : 이 프로토콜은 사용자와 VASP가 서로 다른 도메인을 가정하고 있지만 도메인 확장에 따른 키 복구 기능은 제공하지 않고 있다.
- 불법적인 키 복구 방지 : 이 프로토콜에서 사용자나 VASP는 키 복구 기관을 무조건적으로 신뢰한다는 것을 가정하고 있다. 따라서 키 복구 기관이 부정을 저지른다면 해결할 수 있는 방법이 존재하지 않는다.

2) N-P-B-E WAKE-KR 프로토콜

이 프로토콜은 Nieto 등이 R-M WAKE-KR 프로토콜에서 VASP 위장 공격이 가능하다는 문제점을 제기하고 이를 해결하고자 제안한 프로토콜이다.[9]

(1) 시스템 계수

다음은 N-P-B-E WAKE-KR 프로토콜에서 사용하는 시스템 계수에 대하여 설명한다.

- v : VASP의 개인키
- g^v : VASP의 공개키
- h1, h2, h3 : 해쉬함수 1, 2, 3
- f : 일방향 함수
- w_V : VASP와 자신이 신뢰하는 키 복구 기관간에 공유된 비밀값
- s_V : 랜덤수
- w_U : 사용자와 자신이 신뢰하는 키 복구 기관간에

공유된 비밀값

• s_U : 랜덤수

(2) 프로토콜

이 프로토콜은 사전 준비 단계, 키 복구 정보 생성 단계, 키 복구 정보 공개 검증 단계, WAKE 단계 그리고 키 복구 단계로 나누어진다.

a) 사전 준비 단계

① 사용자는 자신이 신뢰하는 키 복구 기관과 비밀값 w_U를 공유한다.

② VASP는 자신이 신뢰하는 키 복구 기관과 비밀값 w_V를 공유한다.

b) 키 복구 정보 생성 단계

① 키 복구 기관은 키복구 키 w를 생성하고 ψ를 계산하여 공개한다.

- $\psi = g^w \bmod q$

② 사용자는 랜덤수 u를 선택하고 U를 계산하여 공개한다.

- $U = g^u \bmod q$

③ 사용자는 c를 계산한다.

- $c = h(U) \bmod q$

④ 사용자는 s를 계산하여 공개한다.

- $s = w*c + u \bmod q$

c) 키 복구 정보 공개 검증 단계

① 키 복구 정보를 공개적으로 검증하고자 하는 사용자는 c′를 계산한다.

- $c' = h(U) \bmod q$

② 공개된 값들을 이용하여 gs와 $\psi c'*U$를 계산하고 이 것이 같은지 비교한다. 만약 같다면 키 복구 정보가 올바르게 생성되었다는 것이 증명된다.

- $g^s \stackrel{?}{=} \psi c'*U$

d) WAKE 단계

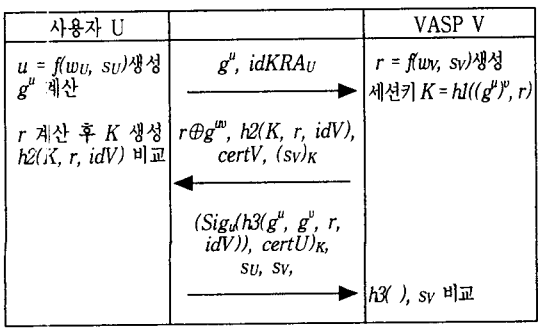

그림 2. N-P-B-E WAKE-KR의 WAKE 단계

e) 키 복구 단계

① 공개되어 있는 U를 이용하여 c를 계산한다.

- $c = h(U) \bmod q$

② 소유하고 있는 c와 w 그리고 공개된 s를 이용하여 u를 계산한다.

- $u = s - w*c \bmod q$

③ 계산된 u와 r을 이용하여 세션키 K를 복구한다.

- $K = h1((g^v)^u, r)$

(3) 요구사항 만족도 분석

다음은 N-P-B-E WAKE-KR 프로토콜의 요구사항 만족도를 분석한다. 인증과 기밀성, 무결성 그리고 불법적인 키 복구 방지 요구사항은 R-M WAKE-KR 프로토콜과 동일하므로 언급하지 않는다.

• 무선 환경을 고려한 멱승 연산량 : 사용자는 2번의 멱승 연산을 하게 되고, VASP는 1번의 멱승 연산을 하게 된다.

• 위장 공격 방지 : 이 프로토콜에서는 세션키를 먼저 만들고 관련 정보를 나중에 줌으로써 공격자의 위장 공격을 방지하고 있다.

• 복구 공개 검증성 : 이 프로토콜에서는 복구 공개 검증성을 만족시키기 위하여 키 복구 정보 생성 단계와 키 복구 정보 공개 검증 단계를 추가하였다.

• 적은 통신량 : WAKE 프로토콜이 진행되는 상황에서 키 복구 기능을 추가함으로써 부가되는 통신량은 s_V 이다.

• 도메인 확장성 : 이 프로토콜은 사용자와 VASP가 서로 다른 도메인을 가정하고 있지만 도메인 확장에 따른 키 복구 기능은 언급하고 있지 않다.

3) K-L WAKE-KR 프로토콜

이 프로토콜은 N-P-B-E WAKE-KR 프로토콜에

(1) K-L WAKE-KR 프로토콜의 WAKE 단계

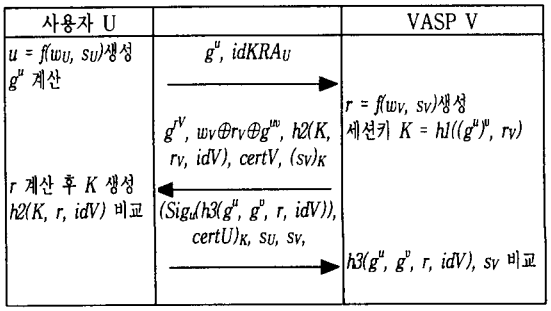

그림 3. K-L WAKE-KR 프로토콜의 WAKE 단계

서 VASP가 속한 도메인에서는 키 복구 정보 생성과 공개 검증 그리고 키 복구가 수행되지 않는다는 문제점을 제시하고 이를 해결하고자 제안한 프로토콜이다.[4] 상기 2)에서 소개한 N-P-B-E WAKE-KR 프로토콜과 진행 과정은 동일하다. 따라서 여기서는 차이점에 대해서만 설명한다.

(2) 추가 부분

• VASP가 속한 도메인에 사용자측과 동일하게 키 복구 정보 생성 과정과 키 복구 정보 공개 검증 과정을 그대로 추가하였다.

• VASP가 속한 도메인에서도 키 복구를 가능하게 하기 위해서 WAKE 프로토콜 과정에서 다음과 같은 정보를 추가하였다. VASP가 속한 도메인의 키 복구 기관은 w_v와 r_v를 알 수 있으므로 g^{uv}를 계산하여, 세션키를 복구할 수 있다.

- $w_v \oplus r_v \oplus g^{uv}$

(3) K-L WAKE-KR 프로토콜의 요구사항 만족도

다음은 K-L WAKE-KR 프로토콜의 요구사항 만족도를 분석한다. 인증, 기밀성, 무결성, 위장 공격 방지, 복구 공개 검증성 그리고 불법적인 키 복구 방지 요구사항은 N-P-B-E WAKE-KR 프로토콜과 동일하므로 언급하지 않는다.

• 무선 환경을 고려한 멱승 연산량 : 두 개체는 모두 2번의 멱승 연산을 하게된다.

• 적은 통신량 : WAKE 프로토콜이 진행되는 상황에서 키 복구 기능을 추가함으로써 부가되는 통신량은 s_v와 g^{rv}이다.

• 도메인 확장성 : 이 프로토콜은 사용자와 VASP가 서로 다른 도메인을 가정하고 있고 도메인 확장에 따라 키 복구 기능을 추가하였다.

3. 제안 방식

본 장에서는 제안하는 프로토콜에 대해 설명한다. 제안하는 프로토콜은 사용자와 인증기관간에 인증서를 발행하는 과정에서 발생할 수 있는 개인키의 누출과 참여 개체들의 부정을 방지할 수 있다. 그리고 제안하는 프로토콜을 이용하여 인증서를 발급 받은 사용자들 간에 무선 환경에서 세션키를 설립하는 기능과 유사시 암호화 통신에 사용된 세션키를 복구하는 기능을 지원한다.

3.1 시스템 계수

제안하는 프로토콜에서 사용되는 시스템 계수는 다음과 같다.

• p : 임의의 소수

• g : GF(p)의 원시원소

• Sig_list : CA의 서명이 붙은 K_i들의 리스트

• Part_key_list(= (k_i, K_i)) : CA에서 생성하여 사용자에게 제공하는 임시 개인키 및 공개키 리스트

• h : 안전한 일방향 해쉬함수

• α: 참여개체(키복구기관(KRA; Key Recovery Agency), 위탁기관(EA; Escrow Agent), 인증기관(CA; Certification Authority), 사용자(Alice 또는 Bob))를 가리키는 지시자

• β : 암호 알고리즘에 사용되는 키(공개키, 개인키, 대칭키)를 가리키는 지시자

• ID_α : α의 식별자

• R_α : α가 생성한 임의의 난수

• t_α, d_α : α의 개인키를 구성하는 비밀 난수

• Cert(α) : α의 인증서

• (X_α, Y_α) : 최종적인 참여개체 α의 개인키 및 공개키 쌍

• Sig_β( ) : 공개키 암호 알고리즘에서 β를 키로 사용해서 생성한 서명문

• AE_β( ) : 공개키 암호 알고리즘에서 β를 키로 사용해서 생성한 암호문

• SE_β( ) : 대칭키 암호 알고리즘에서 β를 키로 사용해서 생성한 암호문

3.2 프로토콜

제안하는 프로토콜은 초기 설정 단계, 인증서 신청 및 발행 단계, 무선 인증 및 키 설립 단계, 키 복구 단계로 구성된다. 여기서 CA와 EA는 이미 개인키와 공개키 쌍을 가지고 있다고 가정한다.

1) 초기 설정 단계

이 단계는 CA가 인증서를 발행하기 위해 수행하는 단계로써 사용자들의 임시 개인키와 공개키를 생성하고 공표하는 단계이다. 임시 개인키와 공개키는 사용자와 인증기관이 동시에 사용자의 개인키와 공개키를

생성하기 위해 생성된다.

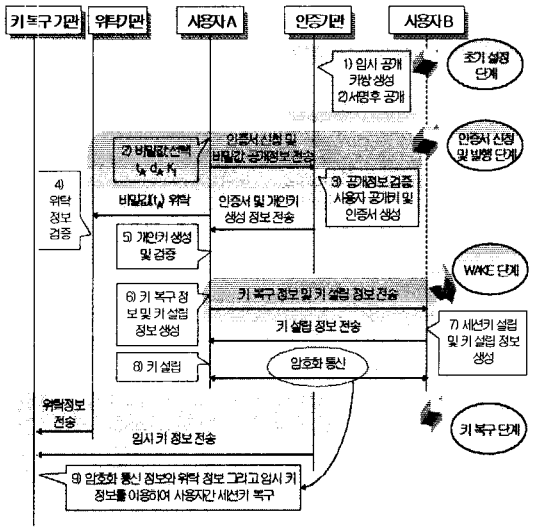

그림 4. 제안 방식 전체 흐름도

① CA는 m개의 임시 개인키와 공개키 쌍 리스트를 생성한다.

Part_key_list = (k_i, K_i)

$K_i = g^{ki} \bmod p$ (단, $1 \le i \le m$) (식 1)

② CA는 임시 개인키와 공개키 쌍 중 K_i에 서명을 수행하여 공표한다.

$Sig\_list = Sig_{X\_CA}(K_i)$ (단, $1 \le i \le m$) (식 2)

2) 인증서 신청 및 발행 단계

이 단계는 Alice와 EA그리고 CA가 수행하는 단계이다. 최종적으로 Alice는 자신의 개인키와 공개키 쌍을 획득하게 되고, CA는 Alice의 공개키에 대하여 인증서를 발행하게 된다. 이러한 진행 과정 중에서 Alice는 EA에게 자신의 부분 개인키 정보를 위탁하게 된다. 위탁된 정보는 제안하는 프로토콜의 키 복구 단계에서 사용자가 생성한 세션키에 대한 키 복구를 수행하는데 사용된다.

① Alice는 비밀값 t_A와 d_A를 생성하고 아래와 같이 T_A와 D_A를 계산한다. 계산이 완료된 후에 T_A를 CA의 공개 디렉토리에 등록한다.

$T_A = g^{t_A} \bmod p$, $D_A = g^{d_A} \bmod p$ (식 3)

② Alice는 CA가 공표한 Sig_list 중에서 임의의 t번째 K_t를 획득하고, CA와 EA의 공개키를 이용하여 다음을 계산한다. 계산된 값을 각각 CA와 EA에게 전송한다.

$AE_{Y\_CA}(ID_A \| K_t \| D_A \| T_A)$, $AE_{Y\_EA}(t_A)$ (식 4)

③ CA는 전송된 값을 복호화하고 안전하게 저장한다. CA는 전송된 T_A와 사용자가 이전에 공개한 T_A와 같은지 비교한다. 만약 같지 않으면 인증서 신청 및 발행 단계를 다시 시작한다.

④ EA는 전송된 값을 복호화하고 안전하게 저장한다. EA는 전송된 t_A와 CA에 공개된 값을 이용하여 다음을 검증한다. 만약 같지 않으면 인증기관에 통보하고 인증서 신청 및 발행 단계를 다시 시작한다.

$T_A \stackrel{?}{=} g^{t_A}$ (식 5)

⑤ CA는 Alice가 선택한 K_t에 대응하는 k_t를 검색한다. 그리고 전송된 D_A와 T_A 그리고 검색된 k_t를 이용하여 아래와 같이 Alice의 최종 공개키 Y_A를 생성하고, 인증서 Cert(A)를 발행한다.

$Y\_A = T_A * D_A^{kt} \bmod p$ (식 6)

⑥ CA는 D_A를 키로 이용하여 k_t를 암호화하고, Alice의 인증서와 함께 Alice에게 전송한다.

$Cert(A) \| AE_{DA}(k_t)$ (식 7)

⑦ Alice는 전송된 암호문을 복호화해서 k_t를 획득한다. k_t와 d_A 그리고 t_A를 이용하여 아래와 같이 자신의 최종 개인키 X_A를 생성한다.

$X\_A = t_A + d_A * k_t \bmod p$ (식 8)

⑧ Alice는 생성된 개인키를 이용하여 아래와 같이 계산하여 Cert(A)에 있는 공개키 Y_A와 비교한다. 만약 같으면 Y_A를 공개키로 인정한다.

$Y\_A \stackrel{?}{=} g^{X\_A} \bmod p$ (식 9)

이러한 과정을 통하여 Alice는 안전하게 개인키와 공개키 인증서를 획득할 수 있게 된다.

3) 무선 인증 및 키 설립 단계

이 단계는 제안된 인증서 발행 프로토콜에 의해 인증서를 발행 받은 Alice와 Bob이 수행하는 단계이다. 두 사용자는 이전에 생성한 비밀값을 이용하여 무선 환경에서 인증 및 키 설립을 수행하게 된다.

① Alice는 자신이 가지고 있는 K_t와 T_A를 이용하여 c_A와 s_A를 계산하고, s_A를 인증기관의 공개 디렉토리에 등록한다.

$$c_A = h(K_t \oplus T_A)$$
$$s_A = t_A + c_A * k_t \bmod p \quad \text{(식 10)}$$

이러한 과정을 통하여 키 복구 정당성 공개 검증이 가능하게 된다. 키 복구 정당성을 공개 검증하고자 하는 참여 개체는 사용자가 등록한 s_A를 이용하여 (식 11)의 좌변과 같이 계산하고, 인증기관과 위탁기관이 각각 공개한 K_t와 T_A를 이용하여 (식 11)의 우변과 같이 계산한다. 계산된 결과를 비교하여 같으면 키 복구 정당성을 만족하게 된다.

$$g^{s_A} \bmod p \stackrel{?}{=} K_t^{c_A} * T_A \bmod p \quad \text{(식 11)}$$

위 식은 다음과 같이 유도된다.

$$K_t^{c_A} * T_A \bmod p$$
$$= g^{k_t * c_A} * g^{t_A} \bmod p$$
$$= g^{k_t * c_A + t_A} \bmod p$$
$$= g^{s_A} \bmod p$$

② Alice는 비밀값 k_t와 t_A 그리고 R_A를 이용하여 키 복구 정보 KRI_A와 인증 정보 RK_A를 다음과 같이 계산한다.

$$KRI_A = k_t \oplus t_A$$
$$K_A = KRI_A \oplus R_A$$
$$RK_A = g^{K_A} \bmod p \quad \text{(식 12)}$$

③ Alice는 인증 정보 RK_A와 R_A 그리고 자신의 인증서 Cert(A)를 사용자 B에게 전송한다.

$$Cert(A) \| RK_A \| R_A \quad \text{(식 13)}$$

④ Bob은 전송된 RK_A와 자신의 개인키 X_B를 이용하여 중간 세션키 SK_B를 계산한다.

$$SK_B = RK_A^{X\_B} \bmod p$$
$$= g^{K_A * X\_B} \bmod p \quad \text{(식 14)}$$

⑤ Bob은 전송된 R_A와 자신이 생성한 SK_B 그리고 R_B를 이용하여 다음과 같이 세션키 K_{AB}를 계산한다.

$$K_{AB} = h(SK_B \| R_A \| R_B) \quad \text{(식 15)}$$

⑥ Bob은 무결성을 위한 검증값 hm(=$h(R_A \| R_B \| K_{AB})$)과 자신의 개인키를 생성할 때 선택한 k_j를 이용하여 다음 정보를 구성한다. 그리고 이들 정보를 Alice에게 전송한다.

$$SE_{KAB}(hm) \| Cert(B) \| R_B \oplus SK_B \| c_B * k_j \oplus t_B \oplus SK_B \quad \text{(식 16)}$$

⑦ Alice는 전송된 Bob의 공개키 Y_B(=$g^{X\_B} \bmod p$)와 자신이 생성한 K_A를 이용하여 SK_A를 계산한다.

$$SK_A = Y\_B^{K_A} \bmod p$$
$$= g^{X\_B * K_A} \bmod p \ (=SK_B) \quad \text{(식 17)}$$

⑧ Alice는 계산한 SK_A와 전송된 $R_B \oplus SK_B$를 이용하여 R_B를 계산하고, SK_A와 R_A를 이용하여 세션키 K_{AB}를 계산한다.

$$R_B = R_B \oplus SK_B \oplus SK_A$$
$$K_{AB} = h(SK_A \| R_A \| R_B) \quad \text{(식 18)}$$

⑨ Alice는 hm'를 구성하여 전송된 $SE_{KAB}(hm)$을 K_{AB}로 복호화한 값 hm과 비교한다. 만약 같다면 사용자 B를 인증하고 키 K_{AB}를 설립하게 된다.

$$hm' = h(R_A \| R_B \| K_{AB})$$
$$hm' \stackrel{?}{=} hm \quad \text{(식 19)}$$

4) 키 복구 단계

이 단계는 Alice와 Bob간에 이루어지는 무선 인증 및 키 설립 프로토콜 과정에서 설립된 세션키를 복구하는 단계로써 사용자가 속한 인증기관에서 각각 수행될 수 있다. 즉, 여기서는 Alice와 Bob은 서로 다른 인증기관에 속해있으며 Alice가 속한 인증기관을 CA_A, Bob이 속한 인증기관을 CA_B로 가정한다.

(1) Alice의 키 복구 요청에 의해 CA_A가 키 복구를 수행하는 과정

① Alice는 키 복구 요청과 함께 다음 정보를 CA_A에게 전송한다.

$$AE_{Y\_CAA}(Cert(A), R_A, Y\_B, R_B \oplus SK_B) \quad \text{(식 20)}$$

② CA_A는 전송된 정보를 복호화하여 저장한 후 위탁기관에 저장되어 있는 Alice의 비밀값 t_A를 획득한다. 그리고 자신이 가지고 있는 Alice의 비밀값 k_t를 이용하여 키 복구 정보 KRI_A를 계산한다.

$$KRI_A = w_A \oplus j_A \quad \text{(식 21)}$$

③ CA_A는 키 복구 정보를 이용하여 K_A와 SK_A를 차례로 계산한다.

$$K_A = KRI_A \oplus R_A$$
$$SK_A = Y_B^{KA} \bmod p = g^{XB * KA} \bmod p \quad (식\ 22)$$

④ CA_A는 저장된 정보와 계산된 정보를 이용하여 R_B를 계산한 후 세션키 K_{AB}를 복구한다.

$$R_B = R_B \oplus SK_B \oplus SK_A$$
$$K_{AB} = h(SK_A \| R_A \| R_B) \quad (식\ 23)$$

(2) Bob의 키 복구 요청에 의해 CA_B가 키 복구를 수행하는 과정

① Bob은 키 복구 요청과 함께 다음 정보를 CA_B에게 전송한다.

$$AE_{Y\_CAB}(Cert(B), R_A, R_B \oplus SK_B, c_B * k_j \oplus t_B \oplus SK_B) \quad (식\ 20')$$

② CA_B는 전송된 정보를 복호화하여 저장하고 Bob의 공개 정보를 이용하여 c_B를 계산한다.

$$c_B = h(J_B \oplus W_B) \quad (식\ 21')$$

③ CA_B는 위탁기관에 저장되어 있는 Bob의 비밀값 t_B를 획득하고, 자신이 가지고 있는 Bob의 비밀값 k_j와 계산된 c_B를 이용하여 SK_B를 계산한다.

$$SK_B = c_B * k_j \oplus t_B \oplus SK_B \oplus c_B * k_j \oplus t_B \quad (식\ 22')$$

④ CA_B는 저장된 정보와 계산된 정보를 이용하여 R_B를 계산한 후 세션키 K_{AB}를 복구한다.

$$R_B = R_B \oplus SK_B \oplus SK_B$$
$$K_{AB} = h(SK_B \| R_A \| R_B) \quad (식\ 23')$$

4. 비교 분석

이 장에서는 제안하는 프로토콜을 인증서 발행 프로토콜과 WAKE-KR 프로토콜로 나누어 각각 기존에 제시된 프로토콜들과 비교 분석한다.

4.1 인증서 발행 프로토콜

기존 인증서 발행 프로토콜은 집중화된 방식과 기본 인증 방식이 있다. 이 두 방식은 다음과 같은 특징을 가지고 있다.

- 집중화된 방식의 경우, 인증기관 내에서 직접 사용자의 개인키와 공개키 쌍을 생성하기 때문에 제 3자로부터 좀 더 안전하게 키쌍을 생성하고 인증서를 발행할 수 있지만 사용자의 개인키가 인증기관에 무방비 상태로 노출될 수 있다.
- 기본 인증 방식의 경우, 사용자가 직접 자신의 개인키와 공개키를 생성함으로써 개인키에 대한 비밀을 유지하기 쉽지만, 인증기관에 비해 안전하지 않은 사용자 환경이나 악의적인 사용자에 대해서 항상 주의해야 한다.

제안 방식은 공개키 기반 구조하에서 기존에 인증서를 발행하는 과정을 새롭게 구성하였다. 사용자의 개인키는 자신이 생성한 3개의 비밀 정보로 구성된다. 이 중 2개는 각각 인증기관과 위탁기관에게 위탁되고 나머지 1개는 사용자만이 알 수 있도록 구성하였다. 이 비밀 정보를 이용하여 사용자는 자신의 개인키를 유일하게 생성 및 소유할 수 있게 되고, 인증기관은 사용자의 개인키와 관계없이 공개키를 직접 생성할 수 있다.

4.2 WAKE-KR 프로토콜

다음은 2장에서 기술한 기존 프로토콜과 비교하여 제안 방식이 각 요구사항을 어떻게 해결하고 있는지를 알아보고, 기존 방식과 비교 분석한다.

- 인증 : 통신 당사자가 각각 생성하는 랜덤수와 비밀 검증값 그리고 공개키 인증서를 이용하여 개체 인증을 수행하고, 변형된 Diffie-Hellman 키 교환 기법을 이용하여 묵시적인 키 인증을 제공한다.
- 기밀성 : 대칭키 암호화와 XOR 연산자를 이용하여 전송되는 정보에 대하여 기밀성을 제공하고 있다.
- 무결성 : 제안 프로토콜에서는 검증이 필요한 정보들에 대하여 메시지 다이제스트를 구성하고 이를 중간 세션키로 암호화함으로써 전송 메시지나 설립되는 키에 대한 무결성을 제공하고 있다.
- 무선 환경을 고려한 멱승 연산량 : 제안 프로토콜에서 사용자 A는 2번의 멱승(RK_A와 SK_A를 계산할 때 각각 1번씩)을 연산하게 되고, 사용자 B는 1번의 멱승(SK_B를 계산할 때 1번)을 연산하게 된다.
- 위장 공격 방지 : 제안 프로토콜은 키 복구 기관과

위탁 기관이 가지고 있는 사용자의 정보가 모두 노출되지 않는 한 위장 공격은 불가능하다. 왜냐하면, 위장 공격을 시도하기 위해서는 키 복구 기관과 위탁 기관이 나누어 가지고 있는 사용자의 비밀 정보를 모두 가지고 있어야 가능하기 때문이다.

• 복구 공개 검증성 : 기존 프로토콜은 키 복구 정보를 생성하고 이를 이용하여 공개 검증과 키 복구 기능을 모두 수행한다. 그러나 제안 프로토콜은 키 복구 공개 검증 과정이 독립적으로 수행될 수 있도록 구성하였다. 키 복구 공개 검증을 수행하기 위해서는 키 복구 기관과 위탁 기관 그리고 사용자가 각각 공개한 정보를 모두 이용한다는 특징을 가지고 있다.

• 적은 통신량 : WAKE 프로토콜이 진행되는 상황에서 키 복구 기능을 추가함으로써 부가되는 통신량은 $c_B*k_j \oplus t_B \oplus SK_B$이다.

• 도메인 확장성 : 제안 프로토콜은 동일한 도메인에 속해있는 두 사용자를 가정하고 있다. 그러나 하나의 도메인에서 멀티 도메인으로 도메인이 확장된 경우에는 추가적인 정보($c_B*k_j \oplus t_B \oplus SK_B$)를 이용하여 해결한다.

• 불법적인 키 복구 방지 : 제안 프로토콜은 두 개의 키 복구 정보를 각각 키 복구 기관과 위탁 기관에게 위탁한다. 따라서 두 기관이 단합하여 부정을 저지르지 않는 한 불법적인 키 복구를 방지할 수 있다. 물론 n개의 위탁 기관을 고려해 볼 수 있다. 그러나 본 논문에서 키 복구 정보를 두 개로 나누는 것은 키 복구 기관과 위탁 기관의 역할이 다르다는 것을 강조하기 위해서다.

다음 표 1은 기존 WAKE-KR 방식과 제안된 WAKE-KR 방식의 비교 분석표이다.

5. 결 론

우리는 서론에서 개방 네트워크 환경에서 안전한 통신과 공유을 위해서는 암호 기술이 반드시 필요하다는 것을 기술했다. 암호 기술 중에서 가장 큰 비중을 차지하고 있는 것이 공개키 암호 기술을 기반으로 하는 공개키 기반 구조이다.

본 논문에서는 공개키 기반 구조의 정의, 구성요소, 인증서 발행 방식들과 기존에 제안되었던 3가지 WAKE-KR 프로토콜을 자세히 소개하였고 이들의 문제점들을 알아보았고, 기존 방식들의 문제점을 해결하는 새로운 프로토콜을 제안하였다. 제안 방식 중 인증서 발행 프로토콜은 기존에 인증기관이 인증서를 발행하는 과정에서 발생할 수 있는 문제점들을 해결할 수 있도록 새롭게 구성하였으며, WAKE-KR 프로토콜 부분에서는 기존에 제시되었던 WAKE-KR 프로토콜들의 단점들을 개선하였고, 키 복구를 제공하기 위해 필요한 추가적인 연산을 최소화하였다. 사용자는 최대 2번의 지수승을 통하여 무선 인증 및 키 설립을 수행할 수 있으며, 설립된 키에 대하여 키 복구 기능을 지원하게 된다. 또한 WAKE-KR 프로토콜을 공개키 기반 구조에 적용함으로써 보다 신뢰할 수 있는 정보 보호 서비스를 제공할 수 있게 되었다.

제안 방식은 사용자와 인증기관간에 개인키 및 공개키 쌍을 생성하여 인증서를 발생하고, 발행된 인증서를 이용하여 무선 인증 및 키 설립 과정을 수행하며, 설립된 세션키에 대한 키 복구 기능을 제공하는 일련의 프로토콜을 제시함으로써 사용자가 공개키 기반 구

표 1. WAKE-KR 프로토콜 비교 분석표 ○ : 제공, × : 제공하지 않음

요구사항 \ 프로토콜	R-M 프로토콜	N-P-B-E 프로토콜	K-L 프로토콜	제안 프로토콜
인증	○	○	○	○
기밀성	○	○	○	○
무결성	○	○	○	○
복구 공개 검증성	×	○	○	○
위장 공격 방지	×	○	○	○
도메인 확장성	×	×	○	○
불법적인 키 복구 방지	×	×	×	○
멱승 연산량(User, VASP)	(3, 1)	(2, 1)	(2, 2)	(2, 1)
적은 통신량	-	s_1	s_1, g^{r_1}	$c_B*k_j \oplus t_B \oplus SK_B$

조하에서 안전하게 암호화 통신을 수행할 수 있는 모델과 이 모델을 기반으로 다양한 응용 프로토콜을 연계할 수 있는 가능성을 제시하였다.

향후 실생활에 적용하기 위해서 좀 더 효율적이고 통합적인 서비스를 제공할 수 있는 프로토콜을 연구해야 할 것이다.

참 고 문 헌

[1] A. Levi and M. Caglayan, "An Efficient, Dynamic and Trust Preserving Public Key Infrastructure," Proceedings of 2000 IEEE Symposium on Security and Privacy, pp. 203-214, 2000.

[2] A. Levi and M. Caglayan, "NPKI: Nested Certificate Based Public Key Infrastructure," Advances in Computer and Information Sciences '98, ISCIS XIII, IOS Press, Concurrent Systems Engineering Series, vol. 53, pp. 397-404, 1998.

[3] A. Perrig and D. Song, "Looking for diamonds in the desert: Extending automatic protocol generation to three-party authentication and key agreement protocols." In Proceedings of the 13th IEEE Computer Security Foundations Workshop. IEEE Computer Society Press, 2000.

[4] ChongHee Kim and PilJoong Lee, "New Key Recovery in WAKE Protocol," PKC2001, Springer-Verlag, pp.325-338, 2001.

[5] G. Ateniese, M. Steiner, and G. Tsudik, "New multi-party authentication services and key agreement protocols," IEEE Journal of Selected Areas in Communication, vol. 18, 2000.

[6] J. Kilian and T. Leighton, "Fair Cryptosystems, Revisited," CRYPTO 95, 1995.

[7] J. Menezes, C. Oorschot, and A. Vanstone, *Handbook of applied cryptography*, CRC Press LLC, 1997.

[8] J. Ines, M. Verdier, N. Ganivet, D. Maillot and J. Skretting, "Public Key Infrastructure and Certification Policy for Inter-domain Management," IS&N '98 Conference Proceedings, 1998.

[9] J. Nieto, D. Park, C. Boyd, and E. Dawson, "Key Recovery in Third Generation Wireless Communication System," PKC2000, Springer-Verlag, pp.223-237, 2000.

[10] K. Rantos and C. Mitchell, "Key Recovery in ASPeCT Authentication and Initialization of Payment protocol," ACTS Mobile Summit, 1999.

[11] L. Harn and H. Y. Lin, "An Authenticated Key Agreement Protocol Without Using One-way Functions," National Conference on Information Security, pp.155-160, 1998.

[12] M. Basyouni and E. Tavares, "Public Key versus Private Key in Wireless Authentication Protocols," Proceedings of the Canadian Workshop on Information Theory, pp.41-44, 1997.

[13] M. Bellare and S. Goldwasser, "Verifiable Partial Key Escrow," Annual Conference on Computer and Communications Security, ACM, 1996.

[14] M. Blaze, J. Feigenbaum and A. Keromytis, "Keynote: Trust management for public-key infrastructure," In Proceedings Cambridge 1998 Security Protocols International Workshop, 1998.

[15] P. McDaniel and S. Jamin, "Windowed Key Revocation in Public Key Infrastructure," Tech. Rep. CSE-TR-376-98, EECS, University of Michigan, Ann Arbor, 1998.

[16] R. Gennaro, "Theory and Practice of Verifiable Secret Sharing," Ph.D. thesis, MIT, 1996.

[17] S. Hirose and S. Yoshida, "An authenticated Diffie-Hellman key agreement protocol secure against active attacks." PKC '98, Springer-Verlag, pp.135-149, 1998.

[18] 최용락, 소우영, 이재광, 이임영, *컴퓨터 통신 보안*, 도서출판 그린, 2001.

[19] 이용호, 이임영, 김주한, 문기영, "WAKE 키 복구 프로토콜에 관한 연구," 한국멀티미디어학회 춘계학술발표논문집, pp.912-915, 2002.

[20] 김건우, 류회수, "키 복구 기능을 가지는 ASPeCT 프로토콜에 관한 분석," 한국정보보호학회 충청지부 학술발표회논문집, pp.153-166, 2002.

[21] 이용호, 이임영, "인증서 기반 WAKE 키 복구 프로토콜을 지원하는 인증서 발급 메커니즘," 한국정보보호학회 충청지부 학술발표회논문집, pp. 167-180, 2002.

이 용 호

2001년 2월 순천향대학교 컴퓨터공학과 졸업
2003년 2월 순천향대학교 대학원 전산학전공 석사
2003년 3월~현재 한국정보통신기술협회 SW시험인증센터 전임연구원
관심분야 : SW시험인증, 정보보호, 암호 프로토콜

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학 전공 석사
1989년 3월 오사카대학 통신공학전공 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안

교 신 저 자

이 용 호 463-824 경기도 성남시 분당구 서현동 267-2 한국정보통신기술협회 IT시험연구소 S/W시험인증센터