Journal of Korea Multimedia Society Vol. 8, No. 7, July 2005(pp. 974-987)

Ad Hoc 네트워크에서 신원기반 암호기법을 위한 보안구조 설계

박영호[†], 이경현[††]

요 약

무선 이동 Ad hoc 네트워크는 고정된 기반망의 도움 없이 이동 노드들의 협력에 의해 자율적으로 구성되는 네트워크이다. 최근 상업적인 분야에서도 Ad hoc 네트워크의 응용에 대한 관심이 급증하면서 Ad hoc 네트워크의 보안 문제도 해결되어야 할 기술적 요구사항으로 대두되고 있다. 또한 특정 기반구조가 정립되어 있지 않는 Ad hoc 네트워크상에서 공개키 기반구조(PKI)의 복잡성을 해결하기 위해 ID기반 암호기법(ID-based cryptography)을 이용한 보안 프로토콜도 제안되고 있다. 본 논문에서는 ID기반의 암호기법을 ad hoc 네트워크에 적용하기 위한 보안 구조의 설계에 대해 제안한다. 네트워크에 참여하는 노드들은 초기 시스템 구성단계에서 오프라인 신뢰센터를 통해 해당 노드의 ID에 대한 개인키를 발급 받으며, 공개키로 사용되는 각 노드의 ID에 대한 정보를 제공하기 위해 정당한 노드의 리스트와 취소된 노드의 리스트를 사용한다. 또한 특정 서버에 의존하지 않고 네트워크에 참여한 노드들의 협력에 의해 이러한 리스트를 갱신할 수 있는 분산된 형태의 상태검사 기법에 대해 제안한다. 제안된 구조를 이용하여 Ad hoc 네트워크에서 기존의 PKI와 유사하게 신원기반의 암호시스템을 위한 보안구조를 구성할 수 있다.

A Security Architecture for ID-Based Cryptographic Schemes in Ad Hoc Networks

Young-Ho Park[†], Kyung-Hyune Rhee[††]

ABSTRACT

As the ad hoc networks have been received a great deal of attention to not only the military but also the industry applications, some security mechanisms are required for implementing a practical ad hoc application. In this paper, we propose a security architecture in ad hoc networks for the purpose of supporting ID-based public key cryptosystems because of the advantage that ID-based schemes require less complex infrastructure compared with the traditional public key cryptosystems. We assume a trusted key generation center which only issues a private key derived from IDs of every nodes in the system setup phase, and use NIL(Node ID List) and NRL(Node Revocation List) in order to distribute the information about IDs used as public keys in our system. Furthermore, we propose a collaborative status checking mechanism that is performed by nodes themselves not by a central server in ad-hoc network to check the validity of the IDs.

Key words: Secure Ad Hoc Network, Node Status Checking, ID-Based Security Architecture

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산시 남구 대연3동 599-1번지(608-737), 전화 : 051)620-6395, FAX : 051)626-4887, E-mail : khrhee@pknu.ac.kr
접수일 : 2004년 11월 12일, 완료일 : 2005년 2월 22일
[†]준회원, 부경대학교 대학원 정보보호학과 박사과정 (E-mail : pyhoya@mail1.pknu.ac.kr)
[††]종신회원, 부경대학교 전자컴퓨터정보통신 공학부 부교수
※ 본 연구는 대학 IT 연구센터(ITRC) 육성 지원 사업의 지원으로 수행되었음.

1. 서 론

무선 이동 Ad hoc 네트워크는 고정된 기반구조의 도움 없이 이동 노드들만으로 구성되는 자율적이며 독립적으로 구성되는 네트워크이다[21,23,24]. 이동 ad hoc 네트워크를 구성하는 이동 노드들은 무선 인터페이스를 가지며, 기반구조의 도움 없이 이동 노드들간의 통신을 설정하기 위해 이동 컴퓨팅 능력을 가진 호스트와 라우팅 기능을 가진 라우터의 역할을 동시에 수행하게 된다.

이러한 이동 Ad hoc 네트워크는 기반구조가 존재하지 않거나 기반구조의 구축이 어려운 군사용 작전 지역이나 재난 복구지역에 적합한 네트워크로 인식되어 왔으나, 최근 유비쿼터스(Ubiquitous) 컴퓨팅 기술이 부각되면서 Ad hoc 네트워크가 구성의 융통성을 제공하고 일시적이며 필요에 의한 임시 네트워크 구성이 용이하다는 특성으로 인해 최근 다양한 분야에서의 응용이 논의되고 있다[22].

이동 Ad hoc 네트워크의 가장 큰 특징은 고정된 중재자의 도움 없이 자율적인 네트워크의 구성이 가능하며, 고정된 라우터가 존재하지 않아 이동 노드들이 호스트로서의 기능뿐만 아니라 다른 노드를 대신하여 패킷을 전달할 수 있도록 라우터의 기능도 함께 수행함으로써 네트워크를 유지하기 위한 관리기능들이 노드들의 협력에 의해 자체적으로 해결할 수 있도록 분산 운영되어 진다는 것이다. 또한 이동 Ad hoc 네트워크상에서 보안 기능들이 특정 서버에 의존할 수가 없으므로, 보안 기능들 역시 노드들의 협력에 의해 분산된 형태로 운영될 수 있어야 한다.

최근 상업적인 분야에서 Ad hoc 네트워크에 대한 관심이 급증하면서 Ad hoc 네트워크에서의 보안 문제도 해결되어야 할 기술적인 사항으로 요구되고 있다. Ad hoc 네트워크가 가지는 무선 채널 자체의 보안 취약성과 네트워크 관리를 위한 기반 시스템의 부재로 인해 Ad hoc 네트워크에서의 보안 문제는 기존의 유선 네트워크나 일반적인 무선랜에서의 보안 문제와는 다르게 고려되어야 한다. 또한 네트워크 관리나 접근제어 등을 수행하는 특정 관리서버가 존재하지 않으므로 네트워크 자체적으로 관리 기능을 수행할 수 있는 메커니즘이 요구된다[1].

ID기반 공개키 암호기법은 사용자의 식별정보(Identity)가 바로 공개키로 사용될 수 있기 때문에 PKI(Public Key Infrastructure)기반의 기존의 공개키 암호시스템에서의 인증서 관리보다 복잡성이 적다는 장점을 가지고 있다. 이러한 ID기반 기법의 장점을 활용하여, 특정 기반 구조의 도움이 없는 Ad hoc 네트워크 환경에서 보안 메커니즘을 설계하기 위해 최근 ID기반의 암호시스템을 적용한 보안 기법들이 제안되고 있다[2,3].

그러나 이들 기법들은 원래 ID기반 암호기법이 가지는 시스템 구조적인 측면에서의 성질은 고려하지 않고 단지 ID기반 기법을 이용한 프로토콜의 설계에만 초점을 맞추었다. 실제로 Ad hoc 네트워크에서 ID기반 암호기법을 사용하기 위해 해당 노드의 ID에 대한 키가 미리 발급되는 경우, 기능상이나 의미상의 차이는 있겠지만 기존의 PKI에서와 유사하게 발급된 키의 상태를 관리할 수 있는 보안 관리구조를 필요로 하게 된다. 즉, Ad hoc 네트워크에서 ID 기반의 암호기법을 적용하기 위해 키 생성에 필요한 식별정보의 구성과 발급된 키의 유효기간에 대한 설정 그리고 만료되거나 손상된 키에 대한 키 취소 등에 대한 관리를 수행할 수 있는 메커니즘이 필요하다.

본 논문에서는 Ad hoc 네트워크에서 ID 기반의 암호기법을 위해 요구되는 보안구조에 대해 제안한다. ID 기반의 개인키를 발급하기 위해 시스템의 구성단계와 키 발급에만 관여하는 신뢰센터의 존재를 가정하며, 개인키의 생성을 위해 노드의 식별값에 유효기간을 포함함으로써 함축적 키 취소가 가능하다. 그리고 네트워크에 참여한 노드들의 식별자로 구성되는 리스트를 분배하고 노드들간에 교환하여 공개키로 사용되는 ID에 대한 정보를 Ad hoc 네트워크에서 제공할 수 있다. 또한 사전에 발급된 각 노드의 키가 취소되거나 손상된 경우 노드들의 협력에 의한 상태전달 기법을 이용하여 공개키로 사용되는 ID의 유효성을 검사하도록 함으로써 정당하지 않은 노드가 취소되거나 손상된 키를 도용하여 부당하게 네트워크에 참여할 수 없도록 한다.

본 논문은 Ad hoc 네트워크에서 ID기반 암호기법을 적용하기 위해 요구되는 보안 구조의 설계를 목표로 하며, Ad hoc 네트워크에서 PKI 기반의 구조와의 장단점 비교를 대상으로 하지는 않는다. 그러나 공개키 암호기법을 위한 PKI와 ID기반 시스템 자체에 대한 비교는 [4]에 이루어진바 있으며, Ad hoc과 유사한 PAN(Personal Area Network) 환경에서 시스템 구성측면에서 차이점을 [5]에서 간략하게 제시하였다. 2장에서는 Ad hoc 네트워크 보안과 관련한 이전

의 연구와 본 연구에 대한 동기에 대해 언급하고, 3장과 4에서는 보안구조와 노드의 상태전달을 위한 설계 방안에 대해 제안한다. 5장에서는 구현관련 고려사항을 살펴보고 6장에서 향후과제에 대해 살펴보고 결론을 맺도록 한다.

2. 관련연구 및 문제제기

2.1 Ad Hoc 네트워크 보안연구

이동 Ad Hoc 네트워크는 무선 채널을 사용하고 물리적으로 보호되지 못하는 환경에서 네트워크가 구성되거나 노드들간의 통신이 이루어질 수 있으므로 전형적인 유선 네트워크보다 더욱 심각한 보안 문제를 야기하게 된다. 특히, 인증이나 접근제어를 수행할 수 있는 중앙 관리 서버가 존재하지 않기 때문에 외부의 악의적인 공격뿐만 아니라 손상된 내부 노드에 의한 공격도 함께 고려되어야 한다[1].

Ad Hoc 네트워크의 응용에 따라 여러 가지 다양한 보안 요구사항을 필요로 하겠지만, 기밀성, 인증, 무결성, 부인방지 등의 기본적인 보안 서비스는 암호학적인 메커니즘을 이용하여 제공될 수 있다. Ad Hoc 네트워크의 보안을 위한 기존의 대부분 연구들이 암호학적 서비스를 위한 키 관리와 라우팅 프로토콜의 보안에 초점을 맞추어 연구가 되고 있다. 보안 라우팅[6,7]의 경우 전송되는 패킷에 대한 기밀성과 무결성에 초점을 맞추고 있으며, 종단간 인증(End-to-End Authentication)이나 부인방지(Non-repudiation) 기능을 제공하기 위해서는 공개키 암호기법의 사용이 요구되며, 공개키 암호기법은 또한 각 노드의 공개키에 대한 관리를 요구한다.

공개키 관리를 위한[8,9,17]의 연구는 Ad Hoc 네트워크에서 이동 노드들간의 협력을 통한 공개키 인증서의 관리를 위해 비밀분산 기법과 임계 암호기법[11]을 이용하는 분산 CA(Certificate Authority)에 대해 연구하였으며, 인증서의 관리를 위한 CA의 역할을 Ad hoc 네트워크에 참여한 노드들에게 분산시킴으로써 인증서의 관리를 위해 PKI에서 요구되는 기능을 Ad hoc 네트워크에 구현하기 위한 연구이다. 비밀 분산 기법과 임계 암호기법을 Ad hoc에 적용함으로써 시스템의 견고성(Robustness)과 가용성(Availability)을 향상시킬 수 있으나 노드들의 계산에 대한 부담과 통신양의 증가로 인해 시스템의 복잡성은 증가되는 단점을 가진다.

공개키 기법을 적용한 다른 형태의 연구로서, 인증서 관리의 오버헤드를 줄이기 위한 방안으로 ID 기반의 공개키 암호기법을 이용한 기법도 제안되고 있다.[2,3]의 연구는 별도의 공개키 인증서를 요구하지 않는 ID기반의 공개키 기법의 장점을 활용하여 Ad hoc 네트워크에 적용한 연구이다. 두 기법 모두 Ad hoc 네트워크 라우팅 프로토콜에서 종단간 노드의 인증[2]과 비밀 공유키의 안전한 분배를 위해 ID 기반의 기법을 적용하였으며[3], Ad hoc 네트워크에서 개인키 발급을 위한 신뢰기관의 역할을 임계 암호기법을 이용하여 여러 노드들에게 분산시키고 개인키를 미리 발급 받는 형태로 제안하였다. 그러나 두 기법 모두 ID기반 암호기법을 가정하여 보안 프로토콜의 설계에만 초점을 맞추었으며, 실제로 ID기반 시스템이 Ad hoc 네트워크에서 구현되기 위해 필요한 요구사항과 미리 발급된 키의 유효성 검증에 대해서는 고려하지 않고 있다.

2.2 ID 기반 Ad Hoc 보안기법의 문제점

ID기반 암호기법은 Shamir에 의해 처음 제안되었으며[12], Boneh와 Franklin의 ID기반 공개키 암호기법[13]이 제안된 이후로 공개키 암호분야의 주요 연구대상이 되고 있다. ID기반 시스템의 경우 사용자를 식별할 수 있는 신원정보가 공개키의 기능을 대신하게 된다. 그러므로 기존의 공개키 기법에서 임의의적으로 생성된 공개키를 사용자와 연관시키기 위해 요구되는 공개키 인증서의 관리를 필요로 하지 않으며 공개키 인증서의 관리에 대한 부담을 줄일 수 있는 특징을 가지고 있다. 그러나 사용자의 ID에 대한 개인키의 발급을 위해 완전히 신뢰되는 개인키 발급센터(Private Key Generator, PKG)의 존재와 개인키의 안전한 전달을 위한 보안 채널을 가정하게 된다.

기존의 인터넷 환경의 전통적인 공개키 암호기법에 비해 ID기반 기법이 가지는 가장 큰 특징으로, 사용자의 ID정보를 이용하여 해당 ID를 가지는 사용자의 개인키가 공개키가 정해진 시간 이후에 독립적(time independent)으로 생성될 수 있으며 개인키의 생성시점에서 PKG에 의해 해당 사용자의 정당성이 검증되므로 별도의 취소(Revocation) 기법이 요구되지 않을 수도 있다는 것이다[4]. 즉, Alice가 Bob에게 암호화된 메시지를 전달하기 위해 Alice는 자신이 의

도하는 Bob에 대한 ID정보를 공개키로 사용할 수 있고 Bob은 복호화를 위한 자신의 개인키를 PKG의 인증을 통해 자신이 Alice가 요구한 수신자임을 증명한 후 획득해야 한다. 그러므로 공개키에 대한 주체가 명확하게 정의될 수 있고 PKG의 신뢰성을 가정할 때, Alice는 Bob의 공개키 인증서를 필요로 하지 않으며 Bob은 복호화를 위해 자신의 개인키가 필요한 시점에 PKG에 의해 제어가 되므로 별도의 취소 기법이 필요하지 않게 된다.

그러나 대부분 ID기반의 기법을 이용하여 설계된 보안 프로토콜에서는 일반적으로 PKG에 의해 사전에 발급된 개인키를 이용하고 있다. 비록 키 생성을 위한 ID에 키의 유효한 시간정보를 추가하여 하루정도의 짧은 생명주기를 가지는 키(Short-lived key)의 발급이 가능할지라도, 해당 시간주기 동안에 키에 대한 손상이나 노출이 발생하는 경우 이미 발급된 키에 대한 취소 기능을 제공하기 위해 기존의 PKI의 CRL(Certificate Revocation List)[19나 OCSP(Online Certificate Status Check)[20]와 유사한 형태의 메커니즘이 마련되어야 한다.

더욱이 보안 시스템이 열악한 Ad hoc 네트워크에서 각 노드들의 ID에 대한 개인키를 신뢰기관으로부터 미리 발급 받는 형태로 사용할 경우, Ad hoc 네트워크상에서 노드가 공격으로부터 손상되거나 키가 노출될 가능성이 커질 수 있으므로 미리 발급된 키에 대한 취소와 공개키로 사용되는 해당 노드의 ID에 대한 상태정보를 전달할 수 있어야 한다. 그러나 이전에 제안된 관련 기법들은 이에 대해서는 다루지 않고 있다. 비록 Ad hoc 네트워크에서 ID 기반의 보안 프로토콜 자체만은 성공적으로 수행될 수 있을지라도 프로토콜이 수행되기에 앞서 암호학적인 용도로 사용되는 통신 상대방의 키에 대한 유효성 확인이 반드시 선행되어야 한다. 일반적인 네트워크 환경을 가정한 ID기반 시스템의 설계에서도 사용자의 개인키가 사전에 미리 발급되는 형태로 프로토콜의 설계가 이루어지고 있으나, Ad hoc 환경의 경우 노드들은 물리적으로 보호되지 못하는 컴퓨팅 환경에서 네트워크를 구성하게 되고 네트워크 관리를 위한 별도의 부가적인 장치가 마련되어 있지 않으므로 악의적인 공격의 가능성이 더욱 커지게 되므로 노드에 대한 상태검사가 필요하다.

또한 일시적인 필요에 따라 노드들에 의해 자율적으로 구성되고 중앙관리 서버가 존재하지 않는 Ad hoc 네트워크에서, 공개키를 위한 각 노드의 ID정보를 어떻게 구성할 것인가에 대한 합의가 이루어져야 하며, 새로운 노드가 네트워크에 추가되는 경우에 새로 추가되는 노드의 식별정보를 어떻게 알려줄 것인가에 대한 문제도 고려되어야 할 것이다. 비록 공개키 관리에 대한 구조적 복잡성이 적은 ID기반 암호기법의 특징이 Ad hoc 네트워크의 특성과 잘 부합된다고 할 지라도, 키가 미리 발급되는 환경에서 사용되기 위해서는 발급된 키에 대한 상태검사 메커니즘에 대한 연구도 필요하다. 특히 Ad hoc 네트워크처럼 기반구조가 미비한 환경에서는 키의 취소나 상태를 검증하기 위해 일반적인 네트워크 환경과는 다른 새로운 형태의 접근법이 요구된다.

3. ID 기반 암호시스템을 위한 Ad Hoc 보안구조

전형적인 인터넷 환경에서의 보안구조는 전적으로 PKI라는 잘 정의된 기반구조에 의존하고 있다. 이때 PKI 구조는 인증기관을 통한 공개키 인증서의 발급과 인증서의 분배를 위한 저장소와 발급된 인증서를 취소하고 인증서의 유효성을 판단하기 위한 인증서 상태검증 등의 기능을 제공하기 위한 물리적, 기능적 구조를 모두 포함한다. 그러나 물리적 기반구조가 미흡하고 필요에 의해 일시적으로 구성되는 Ad hoc 네트워크에서 PKI와 같이 잘 정형화되었지만 복잡한 보안구조를 구성하는 것은 어렵다. 그러므로 본 장에서는 기존의 PKI보다는 구조적인 복잡성을 덜 요구하는 신원기반의 암호시스템을 물리적 기반구조가 미흡한 Ad hoc 네트워크에 적용하기 위한 보안구조에 대해 제안한다.

3.1 시스템 개요 및 표기

본 장에서는 Ad hoc 네트워크에 ID기반 암호기법을 적용하기 위한 보안 구조에 대해 제안하며, 시스템을 구성함에 있어서 세부적인 구현 관련 요소는 생략하고 구조적인 관점에서 설계를 위한 프로시져를 중심으로 구성하도록 한다. Ad hoc 네트워크는 기반 네트워크의 도움 없이 네트워크를 구성하는 노드들의 협력에 의해 구성되고, 접근제어를 수행할 수 있는 온라인 상태의 중앙관리 개체가 가능하지 않으므로 보안기능도 네트워크에 참여한 노드들의 협력

에 의해 수행될 수 있어야 한다. 그리고 새로 네트워크에 추가되는 노드는 기존의 다른 노드들과 신뢰관계를 형성하고 있다고 볼 수도 없으므로 보안 프로토콜을 수행하기에 앞서 각 노드의 정당성을 확인할 수 있는 메커니즘이 제공되어야 한다. 본 논문에서는 신원기반의 보안구조를 설계하기 위한 요구사항을 다음과 같이 정의한다.

1) 키 발급을 위한 신뢰기관은 시스템 구성을 위한 초기 단계에만 관여.
2) 네트워크에 참여한 노드들의 공개키를 계산하기 위한 식별정보를 알 수 있어야 함.
3) 노드들의 공개키의 유효성에 대한 상태정보가 제공될 수 있어야 함.

본 논문은 네트워크에 참여하는 노드들의 식별자에 대한 키를 발급하기 위해 신뢰기관 PKG의 존재를 가정하며 신뢰기관은 오직 키 발급을 위한 시스템 구성단계에만 관여하게 된다. PKG는 시스템 구성단계에서 보안 프로토콜에 필요한 시스템 파라미터들을 생성하고 네트워크에 참여하는 노드들의 ID를 식별하고 해당 ID에 대한 개인키를 발급한다. 네트워크에 참여한 노드들의 공개키로 사용되는 ID에 대한 정보를 제공하기 위해 정당한 노드들의 ID 리스트인 NIL(Node ID List)와 취소된 노드의 ID 리스트인 NRL(Node Revocation List)을 제공한다. 그리고 PKG에 의해 발급된 키에 대응되는 ID의 유효성을 검사하기 위해 네트워크에 참여한 노드들의 협력에 의해 분산된 형태로 운영되는 상태전달 기법을 적용한다. PKG로부터 허가된 정당한 노드가 참여하는 경우 해당 노드의 ID를 NIL에 추가하며, 상태전달 기법을 통해 부정한 노드나 손상된 노드의 ID를 네트워크의 다른 노드에게 제공하도록 한다. 또한 노드들의 협력에 의한 상태정보 전달에 임계값 t를 지정하여 손상된 내부노드에 의한 부정이나 단일 노드의 오류에 대한 영향을 줄이고 t개의 상태 메시지를 효율적으로 검증할 수 있도록 한다.

그림 1과 그림 2는 시스템의 구성과 프로시져의 구성을 간단히 도식화하여 보여준다. Ad hoc 네트워크를 구성하기 위해 노드들은 PKG와 별도의 통신채널을 통해 자신의 ID를 등록하여 ID에 대한 개인키를 안전하게 발급 받고 네트워크에 참여하게 된다. 발급받은 개인키를 이용하여 네트워크상에서 각각의 노드들은 안전한 통신을 위해 필요한 보안 프로토콜을 수행할 수 있게되며, 필요한 경우 노드들의 협력을 통해 특정 노드의 공개키의 유효성을 판단하기 위한 상태검사를 수행할 수도 있다.

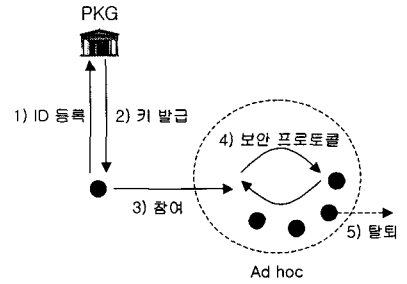

그림 1. 보안 Ad hoc 개요

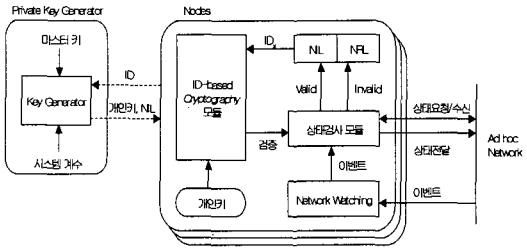

그림 2. 보안 프로시저 구성

다음은 ID기반 시스템을 설계하기 위한 표기들을 나타내며 ID기반의 암호기법으로 [13]의 신원기반 공개키 암호기법과 [14]의 신원기반 서명기법을 가정하고, 안전성을 위한 시스템 파라미터들은 [13]과 [14]의 시스템 구성을 따르도록 한다.

- PKG : 키 발급을 담당하는 신뢰기관.
- SK_0, PK_0 : PKG의 마스터 비밀키와 공개키.
- N_i : 네트워크 노드.
- ID_i : 노드 N_i의 식별정보.
- SK_i : PKG가 발급한 노드 N_i의 ID_i에 대한 개인키 ($i \neq 0$).
- NIL(Node ID List) : 정당한 노드들의 ID 리스트.
- NRL(Node Revocation List) : 취소된 노드들의 ID 리스트.
- $Gen\_ID\_Key(SK_0, id)$: PKG에 의한 id의 개인키 생성 프로시저.
- $IBE\_Enc(m, id)$: 메시지 m에 대한 id의 신원기반 암호화(encryption) 프로시저.

· $IBE\_Dec(c, SK_{id})$: 암호문 c에 대한 개인키 SK_{id}를 이용한 복호화(decryption) 프로시저.

· $IBS\_Sig(m, SK_{id})$: 메시지 m에 대한 개인키 SK_{id}를 이용한 서명(Signing) 프로시저.

· $IBS\_Ver(m, sig, id)$: 메시지 m의 서명문 sig에 대해 id를 이용한 서명 검증(Verification) 프로시저.

· $N_i \rightarrow *$: 노드 N_i의 브로드캐스트 전송.

3.2 시스템 초기화

제안방안은 각 노드의 ID에 대한 개인키를 발급하기 위해 신뢰기관인 PKG의 존재를 가정하며, PKG는 네트워크의 구성단계와 키 발급에만 관여할 뿐 실질적인 Ad hoc 네트워크에서는 PKG의 관여를 가정하지 않는다. 키 발급을 위해 사용될 각 개체의 ID는 네트워크 계층의 IP 주소나 사용자 이름 또는 노드의 장비(Device) 이름과 키의 사용기간을 정의한 유효기간을 결합한 문자열로 구성된다. 3.1절의 요구사항 1)과 관련하여, 오프라인 신뢰기관의 존재를 가정하지 않고, 비밀 분산(Secret sharing)과 임계암호(Threshold cryptography) 기법을 이용하여 키 발급의 기능을 네트워크에 존재하는 각 노드에게 분담시킴으로써 시스템의 키 발급 업무의 가용성(Availability)과 견고성(Robustness)을 향상시킬 수도 있다. 그러나 본 논문에서는 시스템 구성 관점에서 단일의 오프라인 PKG로 가정하여 설명하도록 한다.

각 노드는 PKG를 신뢰하며 네트워크에 참여한 노드들간에는 네트워크를 구성하기 이전에 통신을 위한 어떠한 접촉도 없었다고 가정한다. 따라서 Ad hoc에 참여한 노드들이 모두 상대방의 공개키로 사용되는 식별값 ID에 대한 정보를 알고 있다고 볼 수는 없으므로, PKG가 현재 네트워크에 참여하는 정당한 노드들의 공개키로 이용될 ID 리스트인 NIL (Node ID List)를 생성하여 각 노드의 개인키와 함께 제공하도록 한다. 이때 PKG는 각 노드에 대한 인증을 수행하고 개인키는 별도의 인증과 기밀성이 보장되는 보안 채널을 통해 해당 노드에게 안전하게 전달된다고 가정한다. 만약 Ad hoc 네트워크의 구성을 위해 키 발급을 담당하는 개체와 노드가 물리적으로 근접한 위치에 존재할 수 있다면 MANA(Manual Authentication) 프로토콜이나 패스워드 기반의 보안 프로토콜 등을 이용하여 개인키를 안전하게 전달할 수도 있다[5].

PKG로부터 개인키를 발급 받은 후 노드들은 Ad hoc 네트워크를 형성하게 되며, NIL은 현재 네트워크에서 사용 가능한 노드들의 ID를 포함한다. NIL에 등록되어 있는 ID를 이용하여 참여한 노드 또는 사용자들은 공개키 암호화(IBE_Enc)와 전자서명의 검증(IBS_Ver)에 이용하게 되고, 해당 ID에 대해 PKG로부터 발급 받은 개인키를 이용하여 암호문의 복호(IBE_Dec) 및 전자서명의 생성(IBS_Sig)에 이용할 수 있다.

Procedure 1 : 시스템 초기화(Setup)

1. PKG는 시스템 파라미터를 생성.
2. PKG는 자신의 마스터 비밀키 SK_0를 선택하고 해당 공개키 PK_0를 계산.
3. PKG는 시스템 파라미터와 PK_0를 공개.
4. 각 노드 N_i $(i=1,...,n)$는 자신의 식별값 ID_i를 PKG에게 등록;
   $N_i \rightarrow KGC$: ID_i.
5. PKG는 노드 N_i의 개인키 SK_i를 계산;
   PKG : $SK_i = Gen\_ID\_Key(SK_0, ID_i)$.
6. PKG는 각 N_i의 개인키를 안전한 채널을 통해 분배;
   $KGC \rightarrow N_i$: SK_i , $NIL = ID_1,...,ID_n$.

3.3 노드의 참여(Join)

Ad hoc 네트워크가 구성되고 난 후 새로운 노드 N_j가 네트워크에 참여하기 위해, 새로 참여하는 노드는 우선 PKG를 통해 네트워크 참여에 대한 허가(Admission)를 거치고 시스템 구성단계에서와 유사하게 자신의 ID에 대한 키를 발급 받아야 한다. PKG의 승인을 거친 노드는 네트워크에 참여하기 위해 자신의 ID를 포함하는 참여 요청 메시지를 브로드캐스트 한다. 이때 요청 메시지는 참여 노드에 의해 서명되어지고 이를 수신한 노드들은 서명 검증이 올바른 경우 해당 노드의 ID를 NIL에 추가하도록 한다. 그림 3은 새로운 노드의 추가에 대한 개요를 나타내며, Procedure 1은 노드 참여 처리에 대한 과정을 나타낸다.

참여 메시지에 대한 서명의 사용은 참여 노드가 PKG의 승인을 통해 자신의 식별값 ID_j에 대한 올바른 개인키 SK_j를 획득하였음을 네트워크의 다른 노

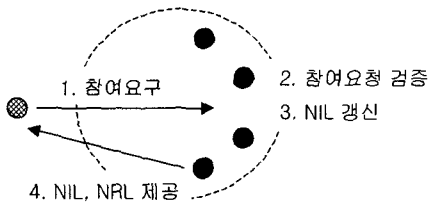

그림 3. 새로운 노드의 참여과정

드들에게 증명하기 위함이다. 그러나 네트워크에서 취소된 노드나 부정한 노드가 도용된 키로 위장하여 네트워크에 참여하려는 시도가 가능하므로 참여요청 메시지의 검증시 해당 노드의 ID가 취소목록 NRL에 등록된 ID인지 여부도 함께 검사한다.

Procedure 2 : 노드의 참여(Join)

1. PKG는 새로운 노드 N_j에게 개인키를 제공;
   $KGC \rightarrow N_j : SK_j = Gen\_ID\_Key(SK_0, ID_j)$.
2. N_j는 네트워크 참여 요구를 브로드캐스트.
   $N_j \rightarrow *$: $Join\_Req$, ID_j ,
   $Sig_j = IBS\_Sig(\text{Join\_Req}, \text{ID}_j, \text{SK}_j)$.
3. N_i $(i \neq j)$:
   if ($ID_j \notin NRL$ &&
   $IBS\_Ver(\text{Join}_{\text{Req}}, \text{ID}_j, \text{Sig}_j, \text{ID}_j) = \text{true}$)
   ID_j를 N_i의 NIL에 추가.
   else
   abort $Join\_Req$.
4. N_j 에 근접한 어떤 노드 N_k가 NIL과NRL을 N_j에게 제공;
   $N_k \rightarrow N_j$: NIL, NRL,
   $IBS\_Sig(\text{NIL}, \text{NRL}, \text{SK}_k)$.

새로 참여하는 노드 N_j의 경우, 기존 네트워크에 존재하는 노드들의 정보를 가지고 있지 않으므로 자신의 주변에 있는 노드를 통해 NIL리스트를 수신하도록 한다. 시스템 구성이후로 PKG는 Ad hoc 네트워크와 분리되어 지므로, PKG의 N_j에 대한 키 발급 과정에서 PKG가 NIL을 발급하는 경우 네트워크의 탈퇴나 손상으로 인해 네트워크에서 제거된 노드의 정보가 갱신되지 않을 수도 있으므로 Ad hoc 네트워크에 존재하는 노드로부터 최신의 NIL과 네트워크에서 손상되거나 취소된 노드들의 리스트인 NRL을 획득하도록 한다. NRL에 포함된 노드의 ID는 악의적인 노드나 손상된 노드뿐만 아니라 자발적으로 네트워크의 탈퇴를 통보한 노드의 ID도 포함한다. NIL과 NRL의 갱신에 대한 내용은 4장에서 다루도록 한다.

시스템의 구성과 노드의 참여가 성공적으로 이루어지면, 현재 네트워크에 참여한 노드들은 ID기반 암호기법들을 적용하여 기밀성, 무결성, 인증, 부인방지 등을 위한 기법뿐만 아니라 비밀키 또는 그룹키를 설정하기 위한 키 분배(Key distribution) 프로토콜이나 키 합의(Key agreement) 등 ID기반의 다양한 기법[25]을 사용할 수 있게 될 것이다. 그러나 사전에 어떠한 신뢰관계도 가지고 있지 않는 두 노드가 통신을 설정하기에 앞서 각각 상대방을 식별하기 위한 단계가 필요할 것이며, 이러한 식별 프로토콜은 자신들의 ID에 대한 개인키를 이용하여 시도/응답(Challenge/Response) 기법 또는 ID 기반의 전자서명이나 식별 프로토콜[20] 등을 통해 수행 될 수 있다.

4. 키 취소와 상태검사 기법

앞서 2장에서 언급했듯이, ID기반 암호기법이 Ad hoc 네트워크에서 개인키가 미리 발급된 형태로 사용되는 경우 키의 손상이나 노출에 대한 부정적인 영향을 피하기 위해 발급된 키에 대한 취소기법과 상태검사가 요구된다. 전통적인 PKI에서는 CRL의 분배서버를 통해 취소된 인증서의 목록을 제공하고 OCSP 서버를 통해 사용자가 원하는 인증서의 유효상태를 실시간으로 검증할 수 있다. 그러나 Ad hoc 네트워크는 CRL 분배서버나 OCSP 서버와 같은 특정 온라인 서버가 항상 가능하지는 않으므로, 상태정보가 네트워크에 참여한 노드들의 자체적인 협력에 의해 전달될 수 있어야 한다.

ID기반 기법에서는 사용자의 식별정보로 사용되는 ID 자체가 공개키의 역할을 하므로, Ad hoc 네트워크에서 키의 상태검사 기능은 요구되는 식별정보 또는 해당 ID를 가진 노드의 유효성이나 존재여부를 검사하는 것으로 구현될 수 있을 것이다. 본 장에서는 키의 유효기간에 의한 함축적 취소와 네트워크에 참여한 노드들의 협력을 통해 특정 ID를 가지는 노드의 상태를 주변의 다른 노드들에게 요청하여 해당 노드의 유효성을 검사하고 NIL과 NRL를 갱신하기 위한 상태전달 기법에 대해 설명한다.

4.1 함축적 키 취소(Implicit key revocation)

ID기반 시스템에서는 ID정보가 바로 공개키이므

로 키의 취소는 곧 ID정보의 취소를 의미하고 새로운 ID의 생성을 요구하게 되므로 PKI에서의 인증서 자체를 취소하고 새로 발급하는 메커니즘과는 다르게 적용되어야 한다. 일반적으로 ID기반 시스템에서는 개인키의 발급시 키의 수명(lifetime)을 하루, 한달 또는 일년으로 제한하기 위해 시간 정보를 사용자의 식별정보와 결합하여 공개키 값으로 사용함으로써 해당 키에 대한 함축적 취소가 가능하도록 하였다[13]. 예를 들어 Alice에 대한 ID기반의 키를 하루동안 사용하도록 하기 위해 키 생성을 위한 Alice의 식별자로 "Alice || 2004.11.1"를 사용하여 PKG로부터 발급되는 키의 사용기간을 제한하도록 하는 것이다. 날짜는 누구나 알 수 있는 정보이므로 Alice에 대한 공개키가 요구되는 시점에서 쉽게 구성 가능하고, 지정된 시간 이후로는 사용될 수 없다. 즉, 신원기반 공개키의 취소는 "Alice"라는 ID 자체의 취소가 아니라 "Alice || 2004.11.1"라는 식별값의 취소를 의미한다.

Ad hoc 네트워크는 필요에 따라 일시적으로 구성되어 질 수 있으므로, 해당 Ad hoc 네트워크의 생존기간(life-time)에 따라 시간 정보를 ID와 결합하여 키의 사용을 네트워크의 수명과 연관시킴으로써 일시적인 키의 사용이 가능하게 할 수 있다. 이때, 키의 수명을 짧게 하는 경우 매 시간 주기마다 키를 새로 발급 받아야 하므로 키의 발급에 대한 오버헤드가 증가하게 되며, 키의 수명을 길게 하는 경우 키의 노출이나 손상에 대한 가능성이 증가하게 된다. 그리고 만일 키가 손상되었다면 해당 시간이 만료되어 새로운 키를 발급 받기 전까지 해당 노드는 보안 프로토콜을 수행할 수 없는 단점을 가지며, 이를 해결할 수 있는 키의 갱신에 대한 문제는 ID기반 기법에서 지속적인 연구를 요구하는 분야로 남아있다[15].

4.2 노드 상태정보 전달

키 생성을 위한 ID로 키의 사용을 위한 시간 정보를 결합하여 키의 함축적 취소가 가능하다 할지라도 적절한 보안 장비가 갖추어져 있지 않는 Ad hoc 환경에서는 악의적인 공격 등으로 인해 미리 발급된 키가 만료되기 이전에 노출이나 손상에 대한 위협의 가능성이 높으므로 PKI의 OCSP와 유사하게 어떤 형태로든 이미 발급된 키에 대한 상태를 요구되는 시점에 전달 할 수 있는 메커니즘이 요구되며, 중앙집중형의 OCSP 서버와 달리 Ad hoc 네트워크에서는 분산된 형태로 운영될 수 있어야 한다. 그림 4는 NIL과 NRL의 갱신을 위한 상태검사 프로시져를 도식화하여 보여준다.

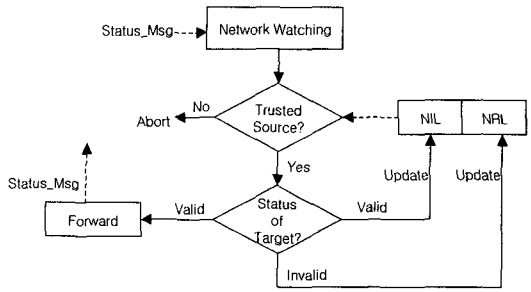

그림 4. 노드 상태검사 프로시져

본 절에서는 Ad hoc 노드들에 의한 상태정보를 제공하기 위해 두 가지 형태의 상태전달 기법과 메시지를 다음과 같이 정의한다. 아래의 기법1과 기법2는 Ad hoc 네트워크에서 경로발견(Routing)을 위해 라우팅 정보를 교환하는 형태(Topology)를 적용하여 암호학적인 용도의 상태정보를 전달하기 위한 방안이다. Status_Request는 특정 노드의 상태를 파악하기 위해 주변의 다른 노드들에게 대상 노드(Target node)의 상태를 질의하기 위한 메시지로서 대상 노드의 식별자와 요청 노드의 식별자를 포함한다. 그리고 Status_Msg 메시지는 어떤 특정노드의 상태를 다른 노드들에게 알려주기 위한 메시지로서, 메시지 송신 노드의 식별자와 상태에 대한 대상 노드의 식별자와 대상 노드의 상태정보를 포함한다. Status_Msg 메시지의 경우 메시지의 무결성과 송신 노드의 부인을 방지하기 위해 송신자의 서명도 부가하도록 한다.

$Status\_Request$: Requster_ID, Target_ID // 상태 요청 메시지

- Requester_ID : 상태 요청 노드.
- Target_ID : 해당 상태의 대상 노드.

$Status\_Msg$: $msg =< \text{Responder\_ID}, \text{Target\_ID}, \text{Status} >, Sig_R$ // 상태 메시지

- Responder_ID : 메시지 응답 노드.
- Target_ID : 해당 상태의 대상 노드.
- $Status = \{Valid | Invalid\}$: 대상 노드의 상태.
- $Sig_R = IBS\_Sig(msg, SK_R)$: 상태 메시지에 대한 응답노드(Responder)의 서명.

(1) 기법 1 : Detect & Forward

기법 1은 Ad hoc 네트워크상에서 모든 노드들이 자신의 주변 노드들의 상태를 감시하면서 특정 노드의 부정이나 공격으로 인한 손상이 발생하는 경우뿐만 아니라 어떤 노드가 자의적으로 네트워크에서 탈퇴하거나 자신의 키에 대한 손상을 감지하였을 경우, 이러한 상태를 알리기 위한 *Status_Msg*를 해당 네트워크로 브로드캐스트하여 노드의 상태를 알려주도록 하기 위한 방법이다.

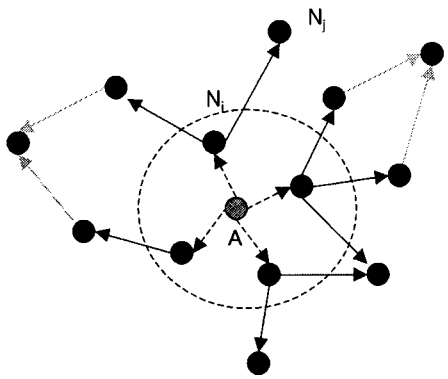

그림 5. 상태발견 및 전달 모델

그러나 모든 노드들이 항상 자의적으로 자신의 상태를 다른 노드들에게 알려준다고 보장할 수 없으므로 노드들간에 서로서로 주변을 감시하여 이벤트가 발생한 특정 노드의 상태를 전달하는 방법이 필요하다. 모든 노드들이 Ad hoc 네트워크에서 주변의 노드들을 관찰하거나 부정한 노드를 감지하기 위한 네트워크 감시(Neighbourhood watch)[18] 등의 기능을 갖추고 있다고 가정하고, 만일 어떤 노드의 손상이 발견되는 경우, 그림 5와 Procedure 3에 나타낸 것처럼, 이를 발견한 노드 A가 앞에서 정의한 상태 응답 메시지에 해당 노드의 상태와 자신의 서명을 포함하여 주변의 다른 노드들에게 브로드캐스트하게 되고, 이 메시지를 수신한 노드들은 다시 주변의 다른 노드들에게 상태 메시지를 전달(Forward)하도록 한다. 상태 메시지를 수신한 노드들은 상태 메시지의 송신 노드의 ID가 *NIL*에 등록되어 있는 유효한 ID이고 서명 검증이 성공하면 상태 메시지에 포함되어 있는 대상 노드(Target node)의 ID를 *NRL*에 추가하고 해당 상태 정보를 이웃한 다른 노드들에게 다시 전달한다.

Procedure 3 : 상태발견과 전달(Status Detecting & Forwarding)

1. 노드 A가 노드 B의 부정이나 공격을 감지.
2. A가 B에 대한 상태 메시지를 네트워크로 브로드캐스트;

   $A \rightarrow * :$

   $Status\_Msg = \{<\mathrm{A,B,Invalid}>, \mathrm{Sig_A}\}$.
3. 메시지를 수신한 각각의 N_i는 수신한 상태 메시지를 처리;

   if ($ID_A \in NIL$ && IBS_Ver(Sig_A,ID_A)=true)

   B를 *NIL*에서 삭제하고, *NRL*에 추가.

   $N_i \rightarrow N_j.(j^* \neq i)$: *Status_Msg*.

   else

   abort *Status_Msg*.

(2) 기법 2 : Request & Response

기법 1의 경우 Ad Hoc 네트워크내에서 노드들간(Node-by-Node)의 전달을 통해 특정 노드의 상태를 다른 노드들에게 알리기 위한 방법이다. 그러나 무선 채널의 비신뢰성(Unreliability)과 노드의 이동성(Mobility)으로 인해 모든 노드들이 어떤 특정시점에서의 상태 메시지를 모두 올바로 수신했다고 보장할 수는 없을 것이다.

기법 2는 이를 보완하기 위해 특정 노드의 상태가 요구되는 경우, 해당 노드의 상태를 주변의 다른 노드들에게 요청하여 이에 대한 응답을 수신하도록 하는 방법이다. 그림 6과 Procedure4에서처럼, 노드 A는 상태정보가 요구되는 대상 노드의 ID를 포함하는 상태요구 메시지를 자신의 주변 노드들에게 브로드캐스트하고, 이를 수신한 노드들 중에서 요청된 노드의 상태를 인지하고 있는 노드들이 Status_Msg 메시지를 노드 A에게 제공하도록 하는 방법이다.

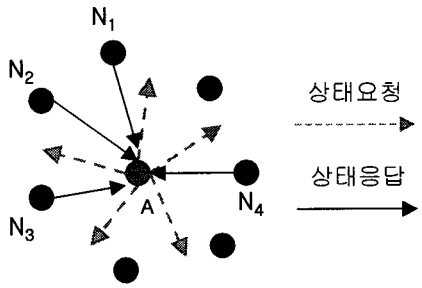

그림 6. 상태요청과 응답 모델

Procedure 4 : 상태요청과 응답(Status Request & Response)

1. 노드 A가 노드 B의 상태를 네트워크상에 요청.
   $A \rightarrow *$: $Status\_Request = \{A, B\}$.
2. 노드 B의 상태를 인지하는 노드들이 A에게 응답.
   $N_j \rightarrow A$:
   $Status\_Msg = \{< N_j, B, Status >, Sig_{N_j}\}$.
3. 노드 A는 상태 메시지를 검증;
   if ($N_j \notin NIL$ || IBS_Ver($Status\_Msg$, Sig_{N_j}, ID_{N_j}) $\neq$ true)
   abort $Status\_Msg$.
   상태 메시지 확인;
   if ($Status\_Msg.Status = Invalid$)
   NIL에서 B의 ID를 삭제하고 NRL에 추가.

4.3 일괄 서명검증(Batch Signature Verification) 적용

상태 응답 메시지는 네트워크상에 존재하는 모든 노드들에게 알려질 수 있어야 하므로 메시지에 대한 기밀성은 중요하지 않겠지만 메시지에 대한 신뢰성을 위해 인증과 무결성을 위한 응답 노드의 서명을 포함하도록 하였다. 그러나 Ad hoc 네트워크상에서 노드들의 자율적인 참여와 협력을 통해 상태 검증 서비스를 제공하는 경우, 내부 노드의 부정이나 오류에 대해서도 고려되어야 한다. 예를 들어, 내부의 부정한 노드 A′가 어떤 특정 노드 B가 손상되지 않았음에도 불구하고 A′의 주변노드들에게 B노드가 손상되었다는 잘못된 메시지를 제공하게 되는 문제가 발생할 수 있을 것이다.

이를 해결하기 위한 대안으로, 어떤 노드의 상태를 검사하기 위해 임계값 t를 지정하여 단일 노드가 아닌 t개의 노드들로부터 상태 메시지를 수집하여 검증함으로써 상태 메시지에 대한 신뢰성을 증가시킬 수 있을 것이다. 그러나, 예를 들어, t개의 메시지를 검증하는 경우 t번의 서명 검증이 요구되며 이는 많은 계산량을 요구하게 된다. 그러므로 제안방안에서는 ID기반의 서명 검증을 일괄 서명 검증[18]으로 변환하여 t개의 메시지에 대한 서명 검증을 단일 서명 검증과 유사한 계산량으로 해결하도록 한다. Bilinear Pairing을 이용한 ID기반의 서명 기법을 일괄 서명 검증에 적용하는 경우, 다중 메시지의 서명을 효율적으로 검증할 수 있다.

다음은 [14]의 ID기반 서명기법과 일괄 서명 검증 과정으로의 변환을 나타내며, 구현을 위한 파라미터들의 생성과 서명 검증식의 정확성(Correctness)은 [14,18]을 참조하도록 한다.

- IBS_Sig : $(m,\ SK_s)$ /* 서명생성 */
  1. 임의의 큰 난수 r을 선택하고 다음을 계산,
     1.1 $U = r \cdot H_1(id_s) \in G_1$
     1.2 $V = (r+h) \cdot SK_s \in G_1$
     ; 이때 $SK_s = k \cdot H_1(id_s)$, $h = H_2(m, U) \in Z_q^*$.
  2. 서명 $Sig_s = < U, V >$

- IBS_Ver : $(m,\ Sig_s = < U, V >,\ id_s)$ /* 서명검증 */
  1. $Q = H_1(id_s)$ 와 $h = H_2(m, U)$를 계산하고,
  2. 검증 if $e(P, V) \stackrel{?}{=} e(P_0, U + h \cdot Q)$

- IBS_Batch_Ver $(m_i,\ Sig_{s_i} = < U_i, V_i >,\ id_{s_i})$ /* $i = 1, \ldots, t$ 일괄 서명 검증 */
  1. $Q_i = H_1(id_{s_i})$ 와 $h_i = H_2(m_i, U_i)$ 를 계산하고,
  2. 검증 $\prod_{i=1}^{t} e(P, V_i) \stackrel{?}{=} \prod_{i=1}^{t} e(P_0, U_i + h_i \cdot Q_i)$ (1)

     $= e(P, \sum_{i=1}^{t} V_i) \stackrel{?}{=} e(P_0, \sum_{i=1}^{t} (U_i + h_i \cdot Q_i))$ (2)

- m : 메시지
- G_1 : q를 차수(order)로 가지는 타원곡선상의 덧셈군(additive cyclic group)
- G_2 : q를 차수로 가지는 유한체상의 곱셈군(multiplicative cyclic group)
- $e : G_1 \times G_1 \rightarrow G_2$: Bilinear pairing 연산
- $H_1 : 0,1^* \rightarrow G_1$: 일방향 해시 함수
- $H_2 : 0,1^* \times G_1 \rightarrow Z_q^*$: 일방향 해시 함수
- SK_s : 신뢰기관이 발급한 id_s에 대한 개인키; $SK_s \in G_1$
- id_s : 서명자 s의 식별값
- k : 신뢰기관의 마스터 비밀키; $k \in Z_q^*$.
- P, P_0: 신뢰기관의 공개키; P, $P_0 = k \cdot P \in G_1$
- 공개 파라미터 : $< G_1, G_2, q, e, P, P_0, H_1, H_2 >$

ID기반의 암호기법에서는 Pairing이 연산의 대부분을 차지하게 된다. 일괄 서명 검증에서 t개의 서명

문이 결합된 형태인 식(1)의 검증식은 Pairing의 Bilinearity[13] 성질에 의해 식(2)로 변환될 수 있다. 따라서 서명 검증을 위한 Pairing 연산의 횟수를 $O(2t)$번에서 $O(2)$번으로 줄일 수 있으므로, 일괄서명 검증기법을 사용하여 동일한 프로토콜을 수행함에 있어 거의 단일 서명의 검증과 비슷한 효율성으로 상태메시지 검증을 수행할 수 있다.

5. 제안구조 분석

본 장에서는 제안된 시스템 구조를 3.1에서 언급한 요구사항에 맞추어 분석하도록 하고, 실제 구현과정에서 고려될 수 있는 몇 가지 사항에 대해 설명한다.

5.1 보안성

신원기반의 암호시스템을 위한 제안구조의 보안성은 전적으로 적용되는 암호기법들[13,14]과 신뢰센터에 의존하게 된다. 제안 시스템에의 신뢰기관인 PKG의 마스터 비밀키가 노출되지 않았다고 가정할 때, 각 노드의 ID로부터 개인키를 직접 계산할 수 없으며 PKG의 인증을 통해서만 정당한 개인키를 발급받을 수 있다. 사용되는 신원기반의 암호기법들이 안전하다고 가정할 때, 새로운 노드가 네트워크에 참여시에 참여 요청 메시지에 PKG로부터 발급 받은 개인키에 대한 서명을 생성할 수 있어야 하므로 PKG로부터 정당한 개인키를 발급 받지 못한 노드는 참여 요청 메시지에 대한 정당한 서명을 생성할 수 없으므로 네트워크에 참여할 수 없다.

그러나 이전에 네트워크에서 탈퇴한 노드나 악의적인 노드가 손상된 키를 도용하여 네트워크에 참여를 시도할 수 있으므로 정당한 노드의 정보와 취소된 노드의 정보를 포함하는 *NIL*과 *NRL*을 이용하여 노드에 대한 유효성을 검사할 수 있도록 하였다. 그리고 특정 서버에 의존하지 않고 네트워크에 참여한 노드들의 협력을 통해 노드들의 상태정보를 제공함으로써 노드의 상태가 변경되는 경우 *NIL*과 *NRL*을 갱신하도록 하여 기존의 PKI에서 사용되는 CRL이나 OCSP와 비슷한 효과를 제공하도록 하였다. 따라서 네트워크 노드들에 의한 상태전달 기법이 올바로 진행된다면 *NRL*에 등록된 ID를 가지는 노드는 자신의 ID와 관련된 정보를 더 이상 키로 사용할 수 없으며, 어떤 공격자가 해당 ID로 위장하여 네트워크에 참여할 수도 없다. 그리고 기반이 되는 신원기반 서명기법이 안전하다고 가정할 때 상태전달 메시지에 송신 노드의 서명을 부가함으로써 악의적인 노드가 중간에 이를 변조하거나 위조할 수 없으며, 송신 노드는 자신의 메시지 전달에 대한 사실을 부인할 수도 없다.

그러나 네트워크 관리를 위한 중앙관리 서버의 부재로 인해 Ad hoc 네트워크에서는 공격으로부터의 손상이나 오류로 인한 네트워크 내부 노드의 부정도 가능하다. 대부분 Ad hoc 네트워크 관리 기법에서는 내부 노드의 부정이나 오류에 대한 영향을 최소화하기 위해 단일 노드가 아닌 여러 노드로부터 네트워크나 노드의 상태에 대한 응답을 수신하여 처리하는 방법을 사용하고 있다. 본 논문에서는 상태검사 메시지에 대한 임계값 t를 지정하여 단일 노드의 부정이나 오류에 대한 영향을 줄이도록 하였으며, 일괄서명 검증 기법을 이용하여 t개의 메시지를 효율적으로 검증할 수 있다.

5.2 기능분석

특정 관리개체의 존재를 가정하지 않는 Ad hoc 네트워크 환경에서 ID기반 암호기법을 사용하는 경우 일반적으로 신뢰기관으로부터 ID에 대한 개인키를 미리 발급 받는 형태로 운용된다. 그러므로 어떠한 사전 접촉도 없이 Ad hoc 네트워크에 참여하는 노드에 대해 해당 노드의 공개키로 사용될 ID를 다른 노드들에게 알려줄 수 있는 방법이 요구된다. 본 논문에서는 이를 위해 시스템 초기단계에서는 신뢰기관이 등록된 ID에 대한 리스트 *NIL*을 분배하고, 네트워크에 새로 참여하는 노드는 참여 요청 메시지에 자신의 ID를 포함하여 네트워크에 존재하는 다른 노드들에게 알려줄 수 있도록 하였다. 이때 새로 참여하는 노드는 신뢰기관으로부터 발급된 개인키를 이용하여 서명함으로써 신뢰기관의 승인을 얻은 정당한 노드임을 증명할 수 있고, 자신과 인접한 노드로부터 *NIL*을 수신함으로써 현재 네트워크에 존재하는 노드들의 리스트를 획득할 수 있다. 만일 Ad hoc 응용에 따라 키를 도출하기 위한 노드의 식별자의 구성이나 명명법 등이 사전에 합의될 수 있다면 별도의 NIL의 필요 없이 합의된 규칙에 따라 통신을 원하는 노드나 사용자의 ID를 이용하여 공개키를 계산할

수 있다. 그리고 손상되거나 네트워크에서 탈퇴한 노드에 대한 *NRL*을 관리하여 *NRL*에 등록된 노드의 ID는 더 이상 암호학적인 용도로 사용될 수 없도록 하였다.

그리고 신뢰기관은 네트워크 구성단계에서 각각의 노드들에게 키를 발급하는 과정에만 관여하게 되며 Ad hoc 네트워크상에서는 신뢰기관의 참여를 가정하지 않는다. 비록 ID기반의 암호기법이 신뢰기관의 공개키를 필요로 하지만, 암호학적 프로토콜을 위한 신뢰기관의 공개키와 파라미터들은 키의 발급과정에서 함께 제공될 수 있으므로 실제 Ad hoc 네트워크상에서의 프로토콜은 신뢰기관의 참여 없이 수행될 수 있다. 또한 노드의 유효성을 검사하기 위한 상태검사 기법도 신뢰기관에 의존하지 않고 노드들의 직접적인 협력에 의해 수행되어진다. 일반적인 공개키 기법을 사용하는 유선 네트워크 환경에서는 공개키 인증서의 상태를 검사하기 위해 CRL이나 OCSP 서버를 이용할 수 있지만, ID기반 암호기법에서는 각 노드의 식별을 위한 ID 자체가 공개키로 사용될 수 있으며 제안 구조에서는 Ad hoc 네트워크 환경에서 특정 ID를 가지는 노드의 상태를 검사하기 위해 특정 관리서버에 의존하지 않고 현재 네트워크에 참여한 노드들간에 상태메시지를 요청하고 제공함으로써 상태검사를 수행할 수 있다. 네트워크에 참여한 노드들이 자신의 주변 노드의 상태를 관찰하여 부정이 발생하거나 탈퇴한 노드의 정보를 다른 노드들에게 알려주거나, 필요한 경우 특정 노드의 상태를 주변의 다른 노드들에게 요청하여 다른 노드에 대한 정보를 획득할 수 있다.

표 1은 기능적인 측면에서 신원기반의 기법을 위한 제안구조와 기존의 공개키 기법을 위한 PKI구조를 간략히 비교하여 나타내고 있다. 서론에서도 언급했듯이 제안구조와 PKI의 장단점을 비교하기 위함은 아니며 Ad hoc 네트워크의 보안구조로서 신원기반 암호기법을 적용하는 경우 PKI에서와 유사한 기능상의 구조를 제시하기 위함이다.

본 논문에서는 상태메시지에 대한 인증과 신뢰성을 효율적으로 처리하기 위한 일괄서명 검증기법[18]에 대해서도 고려하였다. 일괄서명 검증은 n개의 서명문이 주어진 경우 한꺼번에 검증함으로써 n개를 각각 개별적으로 검증하는 것보다 효율적으로 처리할 수 있는 장점을 가진다. Ad hoc 네트워크 보안을 위한 일부 기법에서 멤버십 관리에 내부 노드의 부정으로부터 시스템의 견고성을 높이기 위해 임계암호 기법을 이용하여 제안 기법과 유사한 모형을 제안하였다. 그러나 임계암호 기법을 적용하기 위해서는 비밀 분산과 부분 서명의 결합을 위한 별도의 시스템 구성단계와 여러 번의 통신과 계산량을 요구하는 복잡한 프로토콜의 수행이 요구된다. 그러나 제안 기법은 Pairing을 이용한 ID기반의 일반적인 서명기법을 일괄 서명 검증에 바로 적용할 수 있으므로 임계암호 기법과 같은 사전 프로토콜의 수행을 요구하지 않으며, 일반적인 서명의 생성이나 검증 연산과 동일하게 적용될 수 있다.

6. 결론 및 향후과제

최근 Ad hoc 네트워크의 보안을 위해 ID기반 암호기법을 적용한 연구들이 제안되고 있다. 그러나 ID기반 암호기법을 적용하여 이전에 제안된 기법들은 보안 프로토콜의 설계에만 초점을 맞추었으며 Ad hoc 네트워크에서 이러한 프로토콜을 지원하기 위한 시스템 구조에 대해서는 고려를 하지 않고 있다. 본 논문은 모든 노드들이 신뢰할 수 있는 신뢰기관의 존재를 가정하여 ID기반의 기법을 지원하기 위한 보안 구조에 대해 제안하였다. 각 노드의 공개키로

표 1. 제안구조와 PKI의 기능비교

구분	PKI	제안구조
신뢰기관	CA(Certificate Authority)	PKG(Private Key Generator)
	인증서 발급	개인키 발급
공개키 분배	공개키 디렉토리, 직접교환	NIL, 직접교환
키 취소목록	CRL	NRL
상태정보	OCSP(중앙형)	상태검사 기법1, 2 (분산형)
유효기간	인증서에 명시	식별자 문자열에 포함

사용되는 ID정보를 제공하기 위해 *NIL*과 *NRL*을 네트워크에 참여한 노드들에 의해 관리하도록 하였다. 그리고 네트워크상에서 특정 노드의 유효성을 검증하기 위한 방안을 제안하고, 상태 검증 메시지의 신뢰성을 일괄 서명 검증을 이용하여 효율적으로 검증할 수 있도록 하였다.

본 논문에서는 ID기반 암호기법을 적용하기 위해 Ad hoc 네트워크의 구조적 특성을 고려한 보안 시스템의 설계에 초점을 맞추었으며, 상태 메시지의 전달을 위해 Ad hoc 네트워크에서의 경로 발견을 위한 라우팅 프로토콜이나 CONFIDANT 프로토콜과 결합되는 형태로 구현될 수 있을 것으로 판단된다. 또한 실질적인 보안 구조의 설계를 위해 향후 다양한 Ad hoc 네트워크 기반의 응용환경을 고려한 시스템의 평가와 분석이 요구된다.

참 고 문 헌

[1] L. Buttyan and J. Hubaux, "Report on a Working Session on Security in Wireless Adhoc Networks," in *Mobile Computing and Communications Review*, Vol. 6. No. 4, 2002.

[2] H. Deng and D. P. Argawal, "TIDS: threshold and identity-based security scheme for wireless ad hoc networks," *Ad Hoc Network*(2), Elsevier, pp. 291-307, 2004.

[3] M. Bohio and A. Miri, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Network*(2), Elsevier, pp. 309-317, 2004.

[4] K. G. Paterson and G. Price, "A comparison between traditional public key infrastructure and identity-based cryptography," *Information Security Technical Report*, Elsevier, Vol. 8, Issue 3, pp. 57-72, 2003.

[5] IST-2000-25350-SHAMMAN, "Security for heterogeneous access in mobile applications and networks," Technical Report, pp. 56, 2002.

[6] Y. Hu, D. B. Johnson, and A. Perrig. "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless ad hoc Networks," *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications* (WMCSA 2002), pp. 3-13, Jun. 2002.

[7] Y. Hu, A. Perrig, and D. B. Johnson. "Ariadne: A secure On-Demand Routing Protocol for ad hoc Networks," *In Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking* (MobiCom 2002), pp. 12-23, 2002.

[8] H. Luo, P. Zerfos, J. Kong, S. Ju, and L. Zhang, "Self-securing ad hoc Wireless Networks," *In 7th IEEE Symposium on Cmputers and Communications*, pp. 567-574, 2002.

[9] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile ad hoc Networks," *9th International Conference on Network Protocol* (ICNP '01), pp. 251-260, 2001.

[10] S. Capkun, L. Buttyan, and J-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE transactions on mobile computing*, Vol. 2, No. 1, 2003.

[11] A. Shamir, "How to share a secret", *Communications of the ACM* (22), pp. 612-613. 1979.

[12] A. Shamir, "ID-based Cryptosystems and Signature Schemes," *in Advances in Cryptology-CRYPO '84*, LNCS 196, pp. 47-53, 1984.

[13] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *In Advances in Cryptology-CRYPTO 01*, LNCS 2139, pp. 213-229, 2001.

[14] J. Cha and J. Cheon, "An Identity Based Signature Scheme from Gap Diffie-Hellman Groups," *International Workshop on Practice and Theory in Public Key Cryptography - PKC 2003*, LNCS 2567, pp. 18-30, 2003.

[15] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Limitation of Immediate Key Revocation in Identity-Based Schemes," *in Pre-Proceeding of The 3rd International Workshop for Applied PKI*(IWAP2004), pp. 26-37,

2004.

[16] H. Yoon, J. Cheon, and Y. Kim, "Batch Verifications with ID-based Signatures," *Pre-Proceedings of the 7th International Conference on Information Security and Cryptology*, pp. 171-186, 2004.

[17] J. Kong, H. Luo, K. Xu, D. Gu, M. Gerla, and S. Lu, "Adaptive Security for Multi-layer Ad-hoc Networks," *Wireless Communications and Mobile Computing, Special Issue on Mobile Ad Hoc Networking*, Vol. 2, pp. 533-547, 2002.

[18] S. Buchegger and J-Y Le Boudec, "Performance Analysis of the CONFIDANT Protocol(Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks)," *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 226-236, 2002.

[19] R. Housley, W. Polk, W. Ford, and D. Solo, "Certificate and Certificate Revocation List (CRL) Profile," IETF RFC 3280, 2002.

[20] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP," IETF RFC 2560, 1999.

[21] 권혜연, 신재욱, 이병복, 최지혁, 남상우, 임선배, "이동 ad hoc 네트워크 기술 동향", *전자통신동향분석서*, 제18권, 제2호, 2003년 4월.

[22] 권혜연, 신재욱, 이병복, 최지혁, 남상우, "이동 ad hoc 네트워크 서비스," *전자통신동향분석서*, 제18권, 제4호, 2003년 8월.

[23] Mohammad Ilyas, "*The Handbook of ad hoc Wireless Networks*," CRC Press, 2003.

[24] C. E. Perkins, *Ad hoc Networking*, Addison-Wesley, 2001.

[25] The Pairing-based Crypto Lounge, http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html

박 영 호

2000년 2월 부경대학교 전자계산학과 이학사.
2002년 2월 부경대학교 대학원 전자계산학과 이학석사.
2002년 3월 ~ 현재 부경대학교 대학원 정보보호학과 박사과정.
관심분야 : 암호프로토콜, Ad-hoc 네트워크, 네트워크 보안.

이 경 현

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 이학석사.
1992년 한국과학기술원 수학과 이학박사.
1982년 ~ 1993년 3월 한국전자통신연구소 선임연구원.
1993년 3월 ~ 현재 부경대학교 전자컴퓨터정보통신 공학부 교수.
1997년 12월 ~ 현재 한국멀티미디어학회, 학술이사, (현) 재무이사, 논문지 편집위원
관심분야 : 암호이론, 멀티미디어 정보보호, 네트워크 보안, 암호프로토콜.