논문 99-24-3B-2 한국통신학회논문지 '99-3 Vol.24 No.3B

CORBA 환경에서 정보보안을 위한 Block Design을 응용한 인증메카니즘의 설계

정회원 이 태 훈*, 정 일 용*

The Design of Authentication Mechanism Employing the Block Design for Information Security in CORBA Environment

Tae-Hoon Lee*, Il-Yong Chung* *Regular Members*

요 약

본 논문은 분산 컴퓨팅을 위한 산업계의 표준인 CORBA 환경에서 block design를 적용하여 인증을 고려한 회의용키 생성 메카니즘을 제안한다. 이를 위해서 block design중의 하나인 (v,k,λ)-configuration 기법을 응용하여 통신키를 생성하고, 참여한 사용자들에 생성된 키를 분배한다. 회의용 키 생성 기술과 ID 정보를 기반으로 하여 수행된 상호 인증을 통하여 통신 프로토콜을 설계한다.

제안된 프로토콜에서 회의용 전송키를 생성하기 위한 메시지 전송 복잡도를 최소화시키며, 특히 $\lambda=1$인 경우에는 복잡도는 $O(v\sqrt{v})$이 된다. 보안 시스템의 구축에 있어서 중요한 문제인 본 프로토콜의 안전도는 소인수 분해와 이산 대수를 계산할 정도의 난이도를 갖고 있으므로 보장할 수 있다.

ABSTRACT

In this paper, we present conference key authentication mechanism by employing the block designs in CORBA environment, which is an industry consensus standard for distributed computing. To accomplish this, (v,k,λ)-configuration method, one class of block designs, is applied for generating the communication key and then this key is distributed to participants. Through this technique for creating a conference key and mutual authentications performed based on identificarion information, the communication protocol is designed.

The protocol presented minimizes the transmission complexity for generating a conference key. Especially, in case of $\lambda=1$, the complexity is $O(v\sqrt{v})$. The security of the mechanism, which is a significant problem in the construction of secure system, can be proved as computationally difficult to calculate as factoring and discrete logarithms.

I. 서 론

보안성 관련 기술은 국가의 안위와 직접 관계되어 기술공개 및 보급등이 제한적으로 이루어지고 있지만 보안 연구 동향 분석[1] 및 핵심 기술 요소 확보를 위한 연구가 꾸준하게 수행되었다. 먼저, 네트워크 시스템의 보안성 제고를 위한 첫단계로 시스템의 취약점을 분석해야하며 그 방법 및 기법, Tool 등을 파악되어 안전한 컴퓨터 시스템에 대한 보안성 평가 기준이 연구되었다. '85년에 미국 NCSC (National Computer Security Center)[2]에서 미국정부표준으로 채택된 컴퓨터 시스템 보안성 평가기준(TCSEC, Trusted Computer System Evaluation Criteria)이 제시되었고, 이 기준은 유럽의 ITSEC(Information Technology Security Evaluation Criteria)에 의해 발전된 형태로 제시되었다. 또한 네트워크 모델에도 적용되어

* 조선대학교 전자정보통신공학과(iyc@mina.chosun.ac.kr)
논문번호 : 98429-0929, 접수일자 : 1998년 9월 29일

TNI(Trusted Network Interpretation)[3]등으로 안전한 컴퓨터시스템 뿐만 아니라 안전한 네트워크, 안전한 기술인 억세스 제어 기술에 대한 모델 분석 및 적용되었다. 그리고 개방형 구조인 ISO에서 네트워크 보안 구조[4]를 설계하였으며, SILS(Standard for Interpretable LAN/WAN Security)[5] 구조 및 미국의 보안성 네트워크 DDN(Defence Data Network)[6]을 구축하였으며 전자 우편 서비스에 디지털 서명[7] 등의 기법을 적용하여 정보 보호 기능을 구현시켰다.

개방형 분산 시스템[8]은 분산 컴퓨팅 환경에서 개방 시스템 특징의 구체화를 통하여 사용자들의 Location, Access, Data Integrity, Security, Network and System Failure등에 대한 완전한 투명성을 제공하는 것이다. 현재까지 개방형 분산 시스템에 관한 연구는 주로 산업체 및 국제 표준을 제정하고, 시스템 및 사용자 서비스 기술을 개발하는 방향으로 진행되고 있다.

CORBA(Common Object Request Broker Architecure)[9]-[11]는 개방 분산 환경에서 어플리케이션들간의 상호 운용성을 제공하고, 이 기종 다중 객체 시스템들에 대한 투명성을 제공하여, 주요 구성 성분들의 재사용을 보장하는 개방형 분산 처리 모델이다. 개방형 분산 객체 처리 기술은 미래의 정보통신 서비스를 효과적으로 지원할 수 있으며, 기존 시스템 환경의 Heterogeneity를 극복할 수 있는 중요한 기술이다 특히 OMG의 CORBA는 분산 객체 컴퓨팅의 표준으로 등장하고 있으며, Digital, IBM, Sunsoft, HP등 다양한 벤더들에 의해 채택되고 있다.

본 논문은 CORBA 환경에서 화상회의 시스템에서 필요한 기초 연구로서 오직 회의에 참가하는 사람만이 서로간의 정보를 교환하고 회의를 참석치 않는 사람은 회의의 내용을 알 수 없도록 하는 그룹 상호간의 통신을 가능케 하며 인증[12]까지 고려한 패역 접속 서비스에 관한 것이다.

인증을 고려한 화상회의 시스템에서는 Shamir [13]에 의해 제안되는 Identity를 근거로 하는 공개키 시스템을 이용하는데 각 사용자의 공개키는 사용자의 이름, 주소와 같은 것이다. Shamir와 Fiat[14]는 Discrete Logarithm 방법을 사용하여 서명 방식을 제안하고, 그리고 Okamoto[15]는 공개 키 분배 시스템을 이용하여 Identity-based Scheme를 발표했다.

Diffie와 Hellman[16]이 제안하는 공개키 분배 방식(Public Key Distribution System:PKDS)은 서로간의 통신을 원하는 2개 이상의 그룹이 회의를 개최할 때 서로간에 인식할 수 있는 하나의 공통 통신 회의용 키를 생성하는 방법이다. Ingemarssory, Tang과 Wang[17]이 Ring Network상에서 다자간 회의용 키를 생성하는 방법을 제안하고 Koyama와 Ohta[18]는 인증을 고려한 키분배 방식(Identity-based Conference Key Distribution System:ICKDS)을 Ring Network, 완전 그래프 네트워크와 스타 네트워크 상에서 제안하였다. 하지만 양방향간 위장 공격에 의해서 방어할 수 없음을 Yacobi[19]가 증명하였고, 이에 대한 대응으로 Koyama와 Ohta[20]가 새로운 ICKD를 제안하여 위에서 제시한 공격을 방어하였다. 그리고 Shimbo와 Kawamura[21]는 기 발표된 회의용 키분배 시스템을 분석하였다.

Koyama와 Ohta가 제안한 ICKD가 완전그래프 네트워크 상에서 수행할 때 회의용 키분배를 위해서 N이 가입자의 수라면, N × (N - 1)의 메시지가 필요하다. N이 증대함에 따라 이러한 전송량은 회의의 시작을 지연시키는 요인이 되므로, Ryou[22]가 Finite Projective Plane[23]을 응용하여, 위의 방식보다는 한 단계가 더 요구되지만 O(N$\sqrt{N}$)의 메시지 전송량을 제안하였다. 그러나 이 방식은 Finite Projective Plane의 독특한 점을 적용했기 때문에 특수한 가입자의 수로 제한되는 단점이 있다.

본 논문에서는 Error-correcting Code[24]를 생성하는 기법중의 하나인 block design을 응용하여 CORBA 환경에서 회의용 전송키를 생성하는 메카니즘을 설계한다. 이 방식은 메시지 전송량을 최소화하며 상대적으로 보편적인 가입자의 수를 제시하며 교환하고자 하는 정보가 상호 인증을 고려한 ID-Based를 기반으로 하는 통신 프로토콜하에서 전송하도록 한다.

본 논문의 구성은 제II장에서는 CORBA 구조분석 및 보안연구를 수행하고 제III장에서는 block design에 관하여 고찰하고 이를 응용한 CORBA 기반 인증 메카니즘을 설계하고 마지막으로 결론을 제IV장에서 기술한다.

Ⅱ. CORBA 구조분석 및 보안연구

CORBA는 개방 분산 환경에서 어플리케이션들간의 상호 운용성을 제공하고, 이 기종 다중 객체 시스템들에 대한 투명성을 제공하여, 주요 구성 성분들의 재사용을 보장하는 개방형 분산 처리 모델이다. 개방형 분산 객체 처리 기술은 미래의 정보통신 서비스를 효과적으로 지원할 수 있으며, 기존 시스

템 환경의 Heterogeneity를 극복할 수 있는 중요한 기술이다. CORBA는 ORB(Object Request Broker) 기반 위에 Application Object, common Facility, Object Service로 구성된다. ORB는 객체들 사이의 요청/응답을 전달하는 메커니즘으로, 주요 기능은 모든 객체들 사이에서 발생한 정보들을 처리하는 통로(path)이다. 객체 서비스들은 객체들 위한 기본 서비스들로 Naming Service, Event Service, Life Cycle Service, persistence Service등이 있다. Application Object는 OMG의 기술에 의해 정의된 사용자들의 어플리케션을 말한다. Common Facility는 어플리케이션들에게 공통 요소들을 제공하는 객체 또는 클라이언트의 모임이다.

CORBA는 이 기종의 분산 환경에서 분리되어 있는 객체들간의 투명한(transparent) 실행 시간의 요구와 응답을 제공하며, 객체지향 개념을 이용하여 개발된 Object Request Broker를 사용하는 객체 관리 시스템으로, 객체에 대한 바인딩을 위해 사용자 프로그램이 요구하는 기능과 이 요구를 제공하는 객체에 전달하는 기능을 요구하며, ORB에 서비스를 요구할 수 있는 서비스 인터페이스를 제공한다. ORB는 객체 바인딩을 위해 IDL(Interface Definition Language)과 이것을 컴파일할 수 있는 컴파일러를 제공하여 동적으로 연결하기 위한 Interface Repository Service를 제공한다.

CORBA에서는 또한 객체간의 원활한 통신을 위해 다양한 서비스를 제공한다. 예를 들어서 객체 서로간에 원하는 객체를 찾을 수 있어야 하고, 이벤트 서비스, 객체의 생성 이동 삭제에 대한 서비스, 객체를 저장시키는 방법등 객체를 위한 유용한 서비스가 필요하다. OMG에서는 이들 중 일부를 선택하여 표준화된 인터페이스로 정의한다. 이들에는 Naming Service, Event Service, Life Cycle Service, Persistence Service, 다른 객체 서비스로의 관계 서비스, 트랜잭션 서비스, 외부 접근 서비스 등등이 있다.

안전한 통신을 위해 CORBA 환경에서는 보안 요구사항은 사용자와 객체에게 적용되는데 사용자의 접근제어뿐만 아니라 객체의 접근제어도 보장되어야 한다. 동시에 ORB S/W를 설계하는데 있어서 분산처리 환경이므로 시스템에 대한 보안의 영향력을 최소화한다. 그러므로 성공적인 보안구조는 이들 두 가지의 요구조건을 만족시켜야 하며 OMG White Paper에서 제시하고 있는 보안절차는 다음과 같다. 먼저 사용자는 로그인하고 지역 시스템에서 인증되고, 다음은 사용자는 객체를 호출하기 위해서 클라이언트 어플리케션을 활성화시킨다. 이때 사용자의 인증서(credential)는 클라이언트에게 사용가능하게 되고, 클라이언트는 객체를 호출하여 클라이언트와 객체는 서로간의 신뢰를 구축하고, 상호간의 보안 콘텍스트를 구축하여 객체를 활성화시킨다. 그리고 객체 구현은 사용자의 인증서에 대한 액세스 제어를 수행한다. 마지막으로 만약 객체 구현이 다른 객체를 요청된 일을 수행하기 위해서 필요한 다른 객체를 호출하게 되면, 객체 구현은 자신의 인증서를 사용하여 다시 인증 과정을 거쳐서 객체를 호출한다.

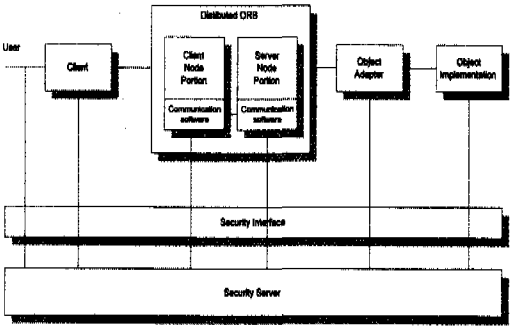

그림 1. OMG White Paper Security Architecture

CORBA에서 보안은 거의 모든 단계에서 적용되어야 하는데 사용자뿐만 아니라 모든 객체들에게도 적용되어야 한다. (그림 1)는 OMG 보안구조에 대한 White Paper Architecture 구조를 보여주는데 White Paper Architecture는 다양한 보안 서비스 기능들을 위해 필요한 네 가지의 가능한 인터페이스 단계들을 보여주고 있는데 이는 보안 파라메터를 IDL에 첨부하는 Application level, ORB가 보안 콘텍스트를 관리하는 GSS-API-like한 단계, Security Service 단계와 Security service provider 단계이다.

본 논문에서는 CORBA 환경에서 신뢰성있는 화상회의 시스템을 구축하기 위해서 필요한 키관리, 통신 프로토콜등 인증 메카니즘의 설계를 Security Server에 실현하고 있는데 Client side에서 stub나 dynamic invocation이 ORB로 진행하기 전에 authentication filter를 사용하여 인증정보(물리적 위치, 이름, 활성화 정책, 사용프로토콜등)를 받아서 적법한 사용자인 가를 확인하고 추가적인 모듈을 첨가하여 정보보안 서비스를 제공하고자 한다. 메카니즘을 설계하기 위해서 대수학의 모델인 block design 방식을 응용하여 진행하고자 한다.

Ⅲ. block design을 응용한 인증 메카니즘의 연구

3.1 block design 분석

만일 ζ 가 코드일 때 최단거리 d(ζ) = min d(ci, cj)이고 이는 코드를 평가하는데 중요한 기준이 된다. 일반적으로 좋은 코드는 codeword가 최단거리 내에 많이 분산되는 것이다. 아래의 정리는 최단거리가 중요한 파라메터임을 보여주고 있으며 [26]에서 증명하고 있다.

정리 1 : 만일 코드가 최단거리 d를 갖는다면, 최단거리 디코딩 방법은 (d-1)/2까지의 에러를 수정할 수 있다.

증명 : e = ⌊(d-1)/2⌋이고 x를 둘러싸고 있는 영역을 e-sphere라고 하고 set Se(x)로 표현된다;Se(x) = {y: d(x,y) ≤ e}. 최단거리 가설에 의해서 만일 x와 z가 서로 다른 codeword일 때, Se(x)∩Se(x)는 공집합이 된다. 그러므로 최단거리 디코딩은 e까지의 에러를 수정할 수 있다.

코드가 길이 n의 M개 codeword와 최단거리 d를 가질 때 (n,M,d)-code라고 하며 고정된 n에 대하여 파라메터 M과 d는 서로간에 반작용을 한다. Aq(n, d)는 q-ary(n, M, d)가 가질 수있는 최대갯수 M을 나타낸다. 예를 들면 Aq(n, 1) = qn.

정리 2 : 만일 d가 홀수일 때, Aq(n, d)에 있는 sphere-packing upper bound는 다음의 식으로 생성된다. [proven in p. 52 of [26]]

$$A_q(n,d)\sum_{k=0}^{e}\binom{n}{k}(q-1)^k \le q^n$$

다시 말해서 d = 2e + 1이면, 위의 정리로부터 두 codeword인 x와 y($x \neq y$)는 만일 Se(X)가 x를 둘러싸고 있는 e-sphere를 의미할 때 우리는 Se(x)의 영역과 Se(y)의 영역으로부터 아래와 같은 새로운 바운드를 구해낼 수가 있다.

$$A_q(n,d)\sum_{k=0}^{e-1}\binom{u}{i}(q-1)^i \le q^n,$$

where $S_e(x)\bigcap S_e(y)=\varnothing$ and

$$|S_e(x)| = \sum_{k=0}^{e}\binom{n}{k}(q-1)^k$$

본 연구에서는 error-correcting Code를 생성하는 기법중에서 block design을 이용하여 Code를 생성하는 방법을 고찰하도록 한다. block design은 주어진 set에서 특정한 조건을 만족하는 subset을 선택하는 방법으로서 이 논문에서는 Balanced Incomplete block design을 적용하고 있으며 먼저 이 block design을 정의하도록 한다.

정의 1 : Let X = {x1,x2,...,xv} be a set of v objects. A Balanced Incomplete block design of X is a collection of b k-subsets of X such that the following conditions are satisfied:

1. Each object appears in exactly r of the b blocks.
2. Every two objects appears simultaneously in exactly λ of the b blocks.
3. k < v.

$$Q = \begin{bmatrix} 1&1&1&0&0&0&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ 0&0&0&0&0&0&1&1&1\\ 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1\\ 1&0&0&0&1&0&0&0&1\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&1&0&0&0&1&0\\ 1&0&0&0&0&1&0&1&0\\ 0&1&0&1&0&0&0&0&1\\ 0&0&1&0&1&0&1&0&0 \end{bmatrix}$$

그림 2. (12×9) incidence matrix

예를 들어 B1={x1,x2,x3}, B2={x4,x5,x6}, B3={x7,x8,x9}, B4={x1,x4,x7}, B5={x2,x5,x8}, B6={x3,x6,x9}, B7={x1,x5,x9}, B8={x2,x6,x7}, B9={x3,x4,x8}, B10={x1,x6,x8}, B11={x2,x4,x9} ,B12={x3,x5,x7}일 때 X= {x1,x2,...,x9}, b=12, v=9, r=4, k=3, λ =1가 되고 이것은 다섯 개의 파라메터 b,v,r,k,λ 를 사용하여 (12,9,4,3,1)-configuration로 표현되며 Balanced Incomplete block design을 만족하는 이들 파라메터들의 관계는 다음과 같으며 증명은 [25]에 있다.

정리 3 : In a Balanced Incomplete block design, bk=vr, and r(k-1)=λ (v-1).

k-subset 대신에 Balanced Incomplete block design은 element가 0과 1로 구성된 (b x v) incidence matrix Q로 표현할 수 있는데 matrix의 열은 x1,x2,..,x9으로, matrix의 행은 B1,B2,...,B12으로 대응되어 아래에 나타난다. 만일 xj가 Bi에 있다면 Qi,j=1이고 아니면 Qi,j=0으로 표시된다. 위의 예를 incidence matrix로 나타내면 아래와 같다.

3.2 block design을 응용한 인증 메카니즘의 설계

n개의 시스템이 서로 정보 교환하기 위해서 서로간의 공통의 키를 각 사이트의 키를 이용하여 통신키를 빠른 시간안에 생성하여야 하고 이 키의 생성에 필요한 time complexity와 space complexity는 최대한 보장이 되어야 한다. 본 논문에서는 error-correcting code가 갖는 이온적인 특징을 이용하여 회의용 키를 생성하기 위한 메시지 전송량을 최소화하는 일반적인 형태를 구성하고자 한다. 이 코딩 기법은 최적의 코드워드가 주어졌을 때 어떤 특정 codeword가 속한 coset를 찾아가서, 만일 codeword에 에러가 발생했다고 하더라도 원래의 데이터 값을 갖는 것이다. 이것을 메시지의 경로 설정에 적용한다면 원래의 데이터 값을 갖는 것이다. 이것을 메세지의 경로 설정에 적용한다면 대단히 효율적인 decentralized routing방법을 선택할 수 있을 것이다.

CORBA 환경에서 보안 메카니즘을 설계하기 위해서 White Paper 보안구조에서 제안하고 있는 Security Server에 설계하는데 시스템에서 제공하고 있는 인증 필터의 기능을 이용하여 ORB를 통과하는 시점에서 인증을 수행할 수 있으리라 사료된다.

인증 메카니즘에서 사용되는 키는 Symmetric Balanced Incomplete block design를 적용하는데 여기에서 Bi는 objecti로, xi는 keyi로 대응되어 Block의 개수와 |X|의 값은 동일해야 한다. block design에서 b=v인 특별한 class는 아래에 정의되어 있다.

정의 2 : A Balanced Incomplete block design is said to be a Symmetric Balanced Incomplete block design if b=v and r=k

Symmetric Balanced Incomplete block design에서는 어떤 두 block은 공통으로 λ 개가 들어있다는 것을 알 수 있고, 이는 (v,k,λ)-configuration로 표현하며 정리 3을 만족하고 있다. 예를 들어서 B1={x1,x2,x4,x7,x11}, B2={x1,x2,x3,x5,x8}, B3={x2,x3,x4,x6,x9}, B4={x3,x4,x5,x7,x10}, B5={x4,x5,x6,x8,x11}, B6={x5,x6,x7,x9,x1}, B7={x6,x7,x8,x10,x2}, B8={x7,x8,x9,x11,x3}, B9={x8,x9,x10,x1,x4}, B10={x9,x10,x11,x2,x5}, B11={x10,x11,x1,x3,x6}일 때 b=v=11, r=k=5, λ=2이 되어 (11,5,2)-configuration이 된다. 또한 이들 block design으로부터 교집합(B1-Bi)이나 차집합(B1 ∩Bi) 과정을 통하여 Balanced Incomplete block design을 쉽게 얻을 수 있다.[25]

통신에 참여하는 각 사용자는 (v,k,λ)-configuration를 이용하여 효율적인 메시지 전송량을 가지고 통신 키를 얻을 수가 있다. 예를 들어서 7명의 사용자가 화상회의를 할 때 (7,4,2)-configuration을 사용하고 각 사용자는 비밀키 ri를 가지고 있다. 먼저 incidence matrix를 아래와 같이 구한다.

$$Q = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

그림 3. (7×7) incidence matriz

각 사용자는 상대방으로부터 키를 받아서 통신키를 생성하는데 본 논문에서는 두단계를 이용하여 계산한다. 먼저 사용자 i는 i번째의 행에서 element의 값이 1인 사용자 j로부터 키값 rj을 받고 다음에는 k번째의 행(i≠k)에서 키값을 받아 통신키를 계산한다. 위의 matrix에서는 사용자 1은 1번째의 행에서 element의 값이 1인 사용자 2,4,7로부터 키값을, 2,5,7행에서 키값을 받아 계산한다. Block 1에서는 k11=r2*r4*r7, k12=r1*r4*r7, k14=r1*r2*r7, k17=r1*r2*r4을 계산한다. Block 2에서 k21=r2*r3*r5, Block 5에서 k51=r5*r6*r4, Block 7에서 k71=r7*r3*r6를 받아 통신키 K를 얻는다; K = r12 * (k11*k21*k51*k71).

정리 4 : (v,k,λ)-configuration에서 (v x v) incidence matrix를 이용하여 통신키 K는 다음과 같이 계산된다.

$$K = r_i \times \left(\prod_{j \in B_i} k_{ji}\right)^{\lambda-1}$$

증명 : (v,k,λ)-configuration의 정의에 의해서 (v x v) incidence matrix의 각 행과 열에는 k개의 1이 존재한다. 각 사용자는 화상회의를 위해서 통신키가 만들어져야 하는데 값은 r1*r2*...*rv이다. 통신키는 두단계를 거쳐서 얻어지는데 첫 번째 단계에서 (k-1)개의 키의 곱이 주어지고 두 번째 단계에서 (k-1)행에서 (k-1)개의 키의 곱이 주어지므로 이를 계산하면 (k-1)+(k-1)*(k-1)=k2-k가 된다. 정리 3을 적용하면 k(k-1)=λ (v-1)가 되어 k(k-1)개의 곱에는 자신의 비밀키를 제외한 상이한 (v-1)개의 비밀키가 λ 개씩 들어있음을 알 수 있다. 그러므로 각 사용자는 (k2-k)개의 곱을 λ -1승하여서 얻은 값과 자신의 비밀키를 곱하면 위의 식이 계산된다.

각 사용자들이 (7,4,2)-configuration에서 정리 3을 사용하여 동일한 통신키를 구하는데 일련의 과정이 (표 1)에서 표현된다.

표 1. (7,4,2)-configuration에서 통신키 생성단계

사용자 ID	단계 1	단계 2
1	$k_{11}=r_2*r_4*r_7$, $k_{12}=r_1*r_4*r_7$, $k_{14}=r_1*r_2*r_7$, $k_{17}=r_1*r_2*r_4$	$r_1^2 * (k_{11}*k_{21}*k_{51}*k_{71})$
2	$k_{22}=r_1*r_3*r_5$, $k_{21}=r_2*r_3*r_5$, $k_{23}=r_2*r_5*r_1$, $k_{25}=r_2*r_3*r_1$	$r_2^2 * (k_{22}*k_{12}*k_{32}*k_{62})$
3	$k_{33}=r_2*r_4*r_6$, $k_{34}=r_2*r_3*r_6$, $k_{36}=r_2*r_4*r_3$, $k_{32}=r_3*r_4*r_6$	$r_3^2 * (k_{33}*k_{23}*k_{43}*k_{73})$
4	$k_{44}=r_3*r_5*r_7$, $k_{45}=r_3*r_4*r_7$, $k_{47}=r_3*r_5*r_4$, $k_{43}=r_4*r_5*r_7$	$r_4^2 * (k_{44}*k_{14}*k_{34}*k_{54})$
5	$k_{55}=r_4*r_6*r_1$, $k_{56}=r_4*r_5*r_1$, $k_{51}=r_4*r_6*r_5$, $k_{54}=r_5*r_6*r_1$	$r_5^2 * (k_{55}*k_{25}*k_{45}*k_{65})$
6	$k_{66}=r_2*r_5*r_7$, $k_{67}=r_2*r_5*r_6$, $k_{62}=r_6*r_5*r_7$, $k_{65}=r_2*r_6*r_7$	$r_6^2 * (k_{66}*k_{36}*k_{56}*k_{76})$
7	$k_{77}=r_1*r_3*r_6$, $k_{71}=r_7*r_3*r_6$, $k_{73}=r_1*r_7*r_6$, $k_{76}=r_1*r_3*r_7$,	$r_7^2 * (k_{77}*k_{17}*k_{47}*k_{67})$

위의 방법은 회의를 참여하는 사용자가 메시지를 전송하기 위한 공통의 통신키를 생성하는 과정을 살펴보았지만 이 과정에서는 통신키를 생성하기 위해 필요한 전송된 상대방의 키가 적법한 가에 대한 확신은 없다. 이를 위해 우리는 인증을 위해서 사용자의 ID 정보를 활용하는데 시스템내의 각 서버는 사용자에게 ID정보의 개념을 이용하여 통신망에서 다음과 같이 비밀정보를 생성한다.

(1) 서버는 256비트이상의 자리수를 가진 p,q를 생성하고 n=p*q를 계산한다.

(2) 조건을 만족하는 e와 d를 계산한다.

e.d = 1 mod (p-1)*(q-1)

(3) GF(p)와 GF(q)를 만족하는 g를 얻는다.

(4) 각 사용자에게 비밀정보 Si를 계산하다.

$$S_i = ID_i^d$$

각 사용자는 e,g,n,IDi,Si와 같은 정보를 갖고 있으며 공개정보로는 e,g,n이 있다. 이제 사용자를 효율적으로 인증하고 메시지 전송을 위한 통신키 생성 프로토콜은 다음과 같다.

[1단계] i → j : $X_i = g^{e \cdot r_i} \bmod n$,

$Y_i = S_i \times g^{C_1 \cdot r_i} \bmod n$,

where $C_i = h(X_i, time)$ and $j \in B_i$

제 1 단계에서는 Block j에 속한 사용자 i는 인증을 위한 두가지 정보 Xi와 Yi를 생성하여 사용자 j에게 (IDi, Xi, Yi, time)을 보내며 이때 h는 모든 사용자가 공통으로 가지고 있는 해쉬 함수이다.

[2단계] j : $ID_i = Y_i^e / X_i^{C1}$,

where $C1 = h(X_i, time)$

제 2 단계에서는 사용자 j는 전송된 정보와 보유하고 있는 해쉬 함수를 이용하여 사용자 i를 인증하는데 만일 $ID_i = Y_i^e / X_i^{C1}$ 이라면 사용자 i의 인증을 성공한다.

[3단계] j → p : $X_{jp} = X_{p_1} \cdot X_{p_2} \cdots \cdot X_{p_{(k-1)}}$,

where $p \neq p_i$ and $p, p_i \in B_j$

$Y_{jp} = S_i \times g^{C_2 \cdot r_i} \bmod n$,

where $C_2 = h(X_{jp}, time)$ 제 3 단계에서 사용자 j는 Block j에 속한 사용자들이 전송한 정보들로부터 Xjp와 Yjp를 계산하여 사용자 p에게 (IDj, Xjp, Yjp, time)를 보낸다.

[4단계] p :

$ID_j = Y_{jp}^e / X_{jp}^{C2}$, *where* $C2 = h(X_{jp}, time)$

제 4 단계에서는 사용자 p는 사용자 j로부터 받은 정보를 이용하여 사용자 j를 인증하는데 만일 $ID_j = Y_{jp}^e / X_{jp}^{C2}$ 이라면 메시지가 사용자 j로부터 전송되었음을 확인하고 이 정보들을 이용하여 통신키를 생성한다.

정리 5 : 사용자 j는 IDi가 만일 Y_i^e / X_i^{C1} 이라면

통신키를 생성하기 위한 정보가 사용자 i로부터 전송된 것임을 인증한다.

증명 : $Y_i^e / X_i^{c1} = (S_i \cdot g^{c1 \cdot r_i})^e / (g^{e \cdot r_i})^{c2} = S_i^e$, if $c1 = c2$ 이 되어 Si는 IDid이므로 (IDid)e는 Euler의 정리에 의해 IDi가 된다.

위의 프로토콜에서 회의용 통신키 생성을 위해 사용자 p는 Xjp1, Xjp2,...,Xjp(k-1)과 자신의 비밀키를 이용하여 얻을 수 있는데 Xjp1, Xjp2, ...,Xjp(k-1)에는 각 사용자의 비밀키가 λ 번씩, e는 λ (v-1)번이 멱승으로 되어 있으므로 모든 사용자가 동일한 통신키를 갖기위해 사용자 p는 자신의 비밀키와 e를 λ로 각각 멱승하여 아래와 같이 계산한다.

$$K = (X_{jp_1} \cdot X_{jp_2} \cdots \cdot X_{jp_{(k-1)}}) \cdot g^{e^{\lambda} \cdot r_p^{\lambda}}$$

3.3 인증 메카니즘의 분석

제안된 프로토콜에서 통신키 생성을 위한 전송 복잡도를 고찰하도록 한다. 이 방식은 (v,k,λ)-configuration을 응용하여 설계된 것으로 정리 4에서 증명하는 과정과 같이 1단계에서 v*(k-1)의 전송이 발생하고 2단계에서도 동일하게 v*(k-1)의 전송량이 필요하게 되어 전체 복잡도는 O(v*k)이 된다. 정리 3을 통하여 알 수 있듯이 k는 v와λ 의 값에 의해서 결정되며 λ =1인 특별한 경우에는 k가 $\sqrt{v}$의 근사값으로 되어 복잡도는 O(v$\sqrt{v}$)이다.

프로토콜의 안전도 측면에서는 비밀 정보 Si를 알아내기 위해서는 공개정보 e와 n을 가지고 d를 구해야 하는데 이를 위해 n을 소인수 분해를 수행해야 하는데 265bit 이상의 p,q를 선택하므로 이는 불가능하다. 그리고 인증과 통신키 생성을 위한 메시지인 Xi로부터 비밀키 ri를 계산해야 하는데 이는 GF(r)상의 이산 대수(discrete logarithm) 문제의 어려움 때문에 비밀키를 찾아낼 수 없어 안전성을 보장받는다.

Ⅳ. 결 론

정보통신망에서 적법한 사용자를 인증하는 것은 중요한 과제이며 본 논문에서는 분산 컴퓨팅을 위한 facility를 정의하고 있는 산업계의 표준인 CORBA 환경에서 설계한다. block design를 적용하여 인증을 고려한 통신키 생성 메카니즘을 설계하는데 먼저 CORBA 시스템의 구조를 분석하여 서비스를 실현하는 과정에 대하여 살펴보고 OMG White Paper에서 제안하고 있는 보안 기법을 분석하였다. 인증 메카니즘을 설계하기 위해서 block design중의 하나인 (v,k,λ)-configuration 기법을 응용하여 통신키를 생성하여 참여한 사용자들이 키를 분배한다. 이런 키 생성 기술과 ID 정보를 기반으로 하여 수행된 상호 인증을 통하여 통신 프로토콜은 설계한다.

제안된 프로토콜에서 프로토콜의 효율성 측면에서는 회의용 전송키를 생성하기 위한 메시지 전송 복잡도를 최소화시키고, 특히 λ =1인 경우에는 복잡도는 O(v$\sqrt{v}$)이 된다. 보안 시스템의 구축에 있어서 중요한 문제인 프로토콜의 안전도 측면에서는 비밀 정보 생성과 인증과정에서 소인수 분해와 이산 대수 문제를 적용하고 있어 이들 문제들의 계산학적 난해도에 근거하고 있어 보장된다.

참 고 문 헌

[1] 한국전자통신연구소, 컴퓨터 네트워크 보안기술 연구, 1991. 2.

[2] "Department of Defence Trusted Computer System Evaluation Criteria" DoD5200.28-STD, Department of Defence, Dec. 1985. Supercedes CSC-STD-001-83

[3] National Computer Security Center, Trusted Network interpretation, NCSC-TO-005 Version-l, July 1987.

[4] ISO/IEC 7498-2: Information Technology - Open Systems Interconnection - Basic Reference Model.

[5] IEEE Std 802.10: Interoperable LAN/MAN Security(SILS), 1992

[6] C. Weissman, "BLACKER: Security for the DDN Examples of A1 Security Engineering Trades," Proceedings of 1992 IEEE Symposium on Research in Security and Privacy, pp.286-292, 1992.

[7] J.Seberry and J.Pieprzyk, Cryptography: An Introduction of Computer Security. Prentice-Hall, NewYork, 1988.

[8] G. Coulouris, J. Dollimore, T. Kindberg, Distributed Systems Concepts and Design, Addison-Welsey, New York, 1994

[9] T. Mowbray, R. Zahavi, The Essential CORBA:Systems Intergration Using Distributed Objects, John Wiley & Sons Inc., New York, 1995

[10] Distributed Object Computing with CORBA, NETWORLD+INTEROP, Chappell & Associates, 1994

[11] A. Vogel, K. Duddy, JAVA Programming with CORBA, John Wiley & Sons, New York, 1998

[12] W. Stallings, Network and Internetwork Security Principles and Practice, Prentice Hall, New Jergey, 1995

[13] A. Shamir "Identity-based cryptossystems and signature schemes", Proc. of Crypto'84, Lecture Notes in Computer Science no. 196, Springer-Verlag, pp.47~53, 1985

[14] A.Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature schemes", Proc. of Crypto'86, Lecture Notes in Computer Science no. 263, Springer-Verlag, pp. 186~194, 1987

[15] T. Okamoto, "Proposal for identity-based key distribution system", Electron. Lett., N0. 22, pp. 1283~1284, 1986

[16] W. Diffie and M.E.Hellman, "New Directions In Cryptography", IEEE Trans., IT-22, pp.644~654, 1976

[17] I. Ingemarsson, D. T. Tang and C. K. Wong, "A Conference Key Distribution system", IEEE Trans., IT-28, pp.714~720, 1982

[18] K. Koyama and K. Ohta, "Identity-Based Conference Key Distribution System", Proceeedings of Crypto'87, Lecture Notes In Computer Science No. 293, Springer-Verlag, pp.175~184, 1988

[19] Y. Yacobi, "Attack On The Koyama-Ohta Identity-Based key Distribution System", Proceedings of Crypto'87, Springer-Verlag, pp.429~433, 1986

[20] K. Koyama andd K. Ohta, "Security of Improved Identity-Based Conference Key Distribution system", EUROCRYPT88, pp.11~19, 1988

[21] A. Shimbo and S. I. Kawamura, "Cryptanalysis of Several Conference Key Distribution Schemes", Preceeedings of Asiacrypt91, pp.115~160, 1991

[22] 김수진, 류재철, "효율적인 회의용 키 분배 방식에 관한 연구", 데이터보호 기반 기술 Workshop 논문집, 한국전자통신연구소, pp.49~64, 1993

[23] A. Albert and R. Sandler, An Introduction to Finite Projective Planes, New York: Holt, Rinehart and Winston, 1968

[24] M. Rhee, error Correcting Coding Theory, McGraw-Hill, New York, 1989

[25] C. Liu, Introduction to Combinatorial Mathematics, McGraw-Hill, New York, 1968

[26] D. Welsh, Codes and Cryptography, Oxford Science Pub., Oxford, 1988

정 일 용(Il Yong Chung) 정회원
한국통신학회논문지 제22권 제12호 참조

이 태 훈(Tae Hoon Lee) 정회원
한국통신학회논문지 제23권 제4호 참조