전장관리체계(C4I)에서의 암호 및 인증방법 개선 방안에 관한연구★

이원만* · 구우권* · 박태형* · 이동훈*

요 약

군에서 현재 운영하는 전장관리체계는 각각의 네트워크와 별도의 암호장비를 이용하여 운용되고 있다. 운용업무별 별도의 네트워크 사용으로 체계별 보안성은 확보했으나 사용자 및 체계연동을 위한 개인인증 방법은 아직 연구과제다. 즉, 동일한 사용자가 서로 다른 체계를 운용하기 위해서는 각각의 암호모듈과 ID/PW를 부여받고 사용하고 있다. 현재 전장관리체계는 공개키 기반구조로 운용되고 있으며 암호장비는 대부분 인편을 통해 배부되어 이동간 피탈되기 쉬운 구조를 갖고 있다. 또한 전장관리체계(C4I)별 암호키를 운용하고 있어 한사람이 여러개의 암호인증모듈을 관리하는 등 암호키 운영관리에 제약 사항이 있다. 이런 공개키 기반구조(PKI)의 문제점 및 이를 보완하기 위한 ID기반의 암호시스템과 속성기반 암호시스템의 비교를 통해 차기 암호인증시스템의 구축방안을 연구하였으며 체계간 접속을 위한 인증방법 및 안전한 자료 소통을 지원하는 자료 암호화 저장 및 소통방안을 제안한다.

A Study on Improvement Methods for Encrytion and Authentication in Batt le Field Management System(C4I)

Lee Won Man* · Koo Woo Kwon* · Park Tae Hyeong* · Lee Dong Hoon*

ABSTRACT

Battlefield management systems are operated by the Public Key Infrastructure (PKI) and cryptographic equipment is distributed through the personal delivery to the enemy has deodorizing prone to structure. In addition, Per person each battlefield management system (C4I) encryption key operate and authentication module to manage multiple encr yption so, encryption key operating is restrictions. Analysis of the problems of this public key infrastructure(PKI), Id entity-Based Cryptosystem(IBC) and Attribute-Based Cryptosystem(ABC) to compare construct the future of encrypt ion and authentication system were studied. Authentication method for the connection between the system that supp orts data encryption and secure data communication, storage, and communication scheme is proposed.

Key words : C4I, PKI, Authentication, IBC, ABC

접수일(2012년 11월 30일), 수정일(1차: 2012년 12월 10일), 게재확정일(2012년 12월 11일)

★ '본 연구는 지식경제부 및 정보통신산업진흥원의 "지식정보 보안인력양성 최고정보보안전문가과정" 사업의 연구 결과로 수행되었음' (NIPA-2012-H2102-12-1001)

* 고려대학교 정보보호대학원

1. 서 론

과거의 전투상황에서는 전장이 지상, 해상, 공중 등 가시적인 어느 한 곳에서 또는 동시 다발적으로 형성되었지만 지금의 상황에서는 사이버상에서 스카다시스템 및 전장관리체계(C4I)등 을 교란하거나 마비 또는 무력화함으로써 적의 정보화 체계가 가지고 있는 취약점을 공격하여 물리적인 파괴보다 훨씬 많은 손실과 결정적 손실을 발생하게 하는 전쟁이 되고 있다. C4I체계(C4I System)란「C4체계와 정보 체계를 유기적으로 연동·통합시켜 자동화된 정보 또는 정보 체계를 운용하여 지휘관이 임무달성을 위하여 부대 운용을 계획하고, 지휘 및 통제할 수 있도록 지원하는 체계이다[1]. 아울러 미래 전장환경은 제 전장요소를 유·무선은 물론 위성통신을 포함한 강력한 네트워크로 결합하여 전장정보 공유와 신속한 지휘결심이 가능하게 하는 NCW(Network Centric Warfare:네트워크중심전)환경이 될 것이다[2][3]. 이러한 환경에서는 전장정보를 안전하게 네트워크를 통해 전달하는 것은 매우 중요한 일이다. 안전한 데이터 통신을 위해서는 데이터 암호화를 위한 암호장비 및 사용자 인증방법이 중요시되며 이를 효과적으로 운용하기 위해서는 암호키의 생성, 분배, 폐기 등 제반업무별 관리체계가 긴요하다. 현재 육군의 암호장비는 대부분 인편을 통해 배부되어 이동간 피탈되기 쉬운 구조를 갖고 있다. 그리고 이동간 소요되는 시간 및 차량 경비 등 비효율적인 면도 있다. 또한 전장관리체계(C4I)별 암호키를 운용하고 있어 한사람이 여러개의 암호인증모듈을 관리하는 등 암호키 운영관리에 제약 사항이 있다. 군에서 현재 운영하는 체계는 각각의 네트워크와 별도의 암호장비를 이용하여 운용되고 있다. 운용업무별 별도의 네트워크 사용으로 체계별 보안성은 확보했으나 사용자 및 체계연동을 위한 암호 및 인증방법은 아직 연구과제다. 즉, 동일한 사용자가 서로 다른 체계를 운용하기 위해서는 각각의 암호모듈과 ID/PW를 부여받고 사용하고 있으며 서버관리부서는 이·삼중으로 사용자 관리를 하고 있다. 비단 전장관리체계뿐 아니라 자원관리체계도 동일하다. 각각의 독립된 네트워크 망으로 운용되어 사용되고 있어서 통합 운용이 어려운 상황이겠지만 암호 및 인증방법을 개선한다면 해결 할 수 있을 것이다. 육군은 NCW환경에 적합한 전술정보통신체계(TICN : Tactical Information Communication Network)를 구축 준비중이며 현재 위성차량은 연대급 부대까지 전력화 하였다. 이러한 미래 전술정보통신 환경에서 현재와 같은 암호키 관리 방식은 운용방식, 소요인력, 비용낭비는 물론 데이터의 무결성, 가용성, 기밀성 등에 많은 제약이 따른다. 따라서 미래 전술환경에 부합한 암호장비 및 암호키의 효율적인 운영관리 및 안정적인 암호인증시스템 인프라 구축이 필요하다. 본 연구는 육군 전장관리체계(C4I)의 암호키 관리 및 인증체계 현황 분석을 통해 개선사항을 식별하고 공개키 기반구조(PKI)의 문제점 및 이를 보완하기 위한 ID기반의 암호시스템과 속성기반 암호시스템의 비교를 통한 차기 암호인증시스템의 구축을 위한 시사점을 도출한다. 또한 체계간 접속을 위한 인증방법 및 안전한 자료 소통을 지원하는 자료 암호화 저장 및 소통방안을 제안한다. 아울러 현 암호인증체계와 본 논문에서 연구한 미래 암호인증체계를 비교하고 안전성 및 보안성 측면, 경제적 측면으로 기대효과를 도출하여 미래 암호인증기반 시스템 업무의 신뢰성 있는 추진방향을 제시한다.

2. 관련연구

2.1 IBC(Identity Based Cryptosystem)

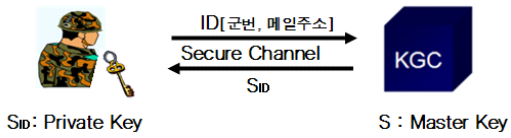
2.1.1 IBC 개요

일반적으로 공개키 암호화를 이용한 메시지 전달이나 전자서명에서의 서명검증절차 등에서 공개키에 대한 인증이 요구된다[3]. 인증서 기반의 공개키 암호시스템에서는 이와 같은 문제를 신뢰된 인증기관으로부터 공개키 인증서를 발급함으로써 해결했다. 그러나 이와 같은 공개키 인증에 대한 절차와 설계는 복잡할 뿐 아니라 사용자가 자신의 공개키에 대한 인증서를 유지 및 관리해야 하는 부담도 생기게 된다. 이는 군 전장환경에서 암호장비장애 및 인증모듈 에러시 신속대응이 제한된다. 이와 같은 문제를 해결하기 위해 제안된 것들이 ID기반 암호시스템 IBC(Identity Based Cryptosystem)과 속성 기반 암호 시스템 ABC(Attribute Based Cryptosystem)이다[4].

2.1.2 IBC 주요기능 및 특징

IBC에서는 누구나 쉽게 알 수 있는 각 사용자의 고유한 ID, 군번, 이메일 주소 등 을 이용하여 공개키가 생성되고 이 공개키가 개인키와 연결되면서, 인증서기반의 암호시스템과 같은 인증서를 필요로 하지 않는다. 이는 사용자의 공개키를 임의의 비트 스트링이 아닌 쉽게 구별할 수 있는 개인의 공개정보를 사용하기 때문이다. 따라서 사용자의 고유한 ID, 군번을 통해 사용자의 신원확인도 쉽게 할 수 있다.

예를 들어 A간부와 B간부가 암호통신을 하고자 한다고 가정하자. A간부가 B간부에게 암호문을 전송하고자 할 때 A간부는 B간부의 알려진 이메일 주소(B@army.mil) 혹은 군번만 가지고 암호화를 수행할 수 있으며, 또한 B간부가 A간부의 전자서명을 검증하고자 할 때 B간부는 A간부의 알려진 이메일 주소(A@army.mil) 혹은 군번만을 이용하여 서명을 검증할 수 있다. 결국 IBC는 ① 기존 공개키(PKI) 암호에서 요구되는 인증서의 유지 및 갱신을 위한 메커니즘이 요구되지 않고, ② 송신자는 수신자의 이메일 주소, 군번 등으로 공개키를 얻을 수 있으므로 인증서 확보를 위한 별도의 절차가 필요 없으며, ③ 사용자 ID에 시간(time stamp)정보를 첨부할 경우, 미래의 특정시점에 수신자가 복호화 할 수 있는 메시지의 전송도 가능하다는 장점을 가진다. 현재 ID기반 암호화 기법을 최초로 설계한 미국 스탠포드 대학이 설립한 Voltage 사에서는 ID기반 암호시스템을 이용한 안전한 이메일 시스템 IBE secure E-mail을 개발하여 이를 블랙베리(BlackBerry)서비스에 적용하고 있다. 블랙베리 서비스란 개인의 이메일 계정에 배달된 메일을 실시간으로 전송받아 언제 어디서나 쉽고 빠르게 이메일을 주고받을 수 있도록 해주는 서비스로 이러한 블랙베리 서비스가 제공하는 이메일 서비스를 메시지에 대한 기밀성 보장 및 사용의 편리성과 효율성을 높이기 위해 인증서가 필요 없는 ID기반의 암호화 기법이 사용되고 있다. 점점 더 많은 곳에서 사용을 원하고 있어 ID기반 암호화 기법뿐만 아니라 ID기반 서명 및 키교환 기법 등 ID기반 암호시스템의 활용이 점점 더 확대될 것으로 예상된다.

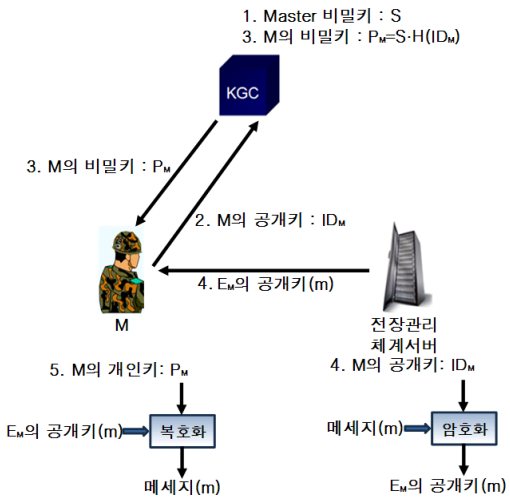


(그림 1) IBC에서 사용자 키생성

IBC는 마스터키를 통해 내부 사용자가 외부로 기밀 정보를 유출하는 등의 사고를 막기 위해 감독이나 관리를 필요로 하는 환경에서 적합하다. IBC는 사용자에 대한 모든 개인키를 알 수 있기 때문에 사건 발생 시 누구인지를 추적하거나 사고를 미연에 방지하는 효과를 볼 수 있다. 따라서 군 특수환경 및 폐쇄망에 대한 안전한 통신에 적합하다.

2.1.3 IBC의 공개키 생성 및 배포

IBC에서는 쉽게 알 수 있는 사용자군번 등 고유한 ID를 이용하여 공개키를 생성한다. 전장관리체계 사용자의 공개키는 임의의 비트 스트링이 아닌 쉽게 구별할 수 있는 사용자의 군번 및 메일주소 등 공개된 정보를 사용하기 때문에 사용자 식별도 가능해 진다. 키 생성과 배포과정을 알아보면 다음과 같다.



(그림 2) IBC 키생성과정

① KGC(Key Generation Center)는 자신의 마스터 비밀키 S를 생성한다.

② KGC는 M의 ID_M로부터 M의 개인키 P_M을 생성한다.
③ KGC는 M에게 개인키 P_M을 안전하게 전송한다.
④ 서버는 M의 공개키 ID_M을 이용하여 메시지를 암호화 후 M에게 전송한다.
⑤ M은 자신의 개인키로 암호문를 복호화하여 메시지를 획득한다.

IBC에 있어서 가장 큰 문제는 KGC에 대한 신뢰문제이다. 앞에서 언급한 PKI기반의 인증시스템은 사용자가 자신의 공개키/개인키를 생성하기 때문에 신뢰기관(CA)이 사용자의 개인키를 알 수 없다. 반면에 IBC에서는 사용자의 개인키를 KGC의 마스터키를 이용하여 생성하기 때문에 KGC가 사용자의 개인키를 알 수 있게 된다. 이렇게 사용자의 개인키를 전적으로 KGC에 의하여 생성된다는 것은 KGC가 모든 사용자의 비밀키를 알고 있다는 점에서 사용자의 개인 프라이버시 침해가 발생할 수 있다. 그러므로 KGC에게는 엄격한 관리감독 의무가 주어져야 한다. 군의 특수한 환경에서는 단일기관(기무사)이 신뢰기관으로서 KGC의 키 관리하는 방법이 현실적이고 관리측면에서 유리하다고 볼 수 있다.

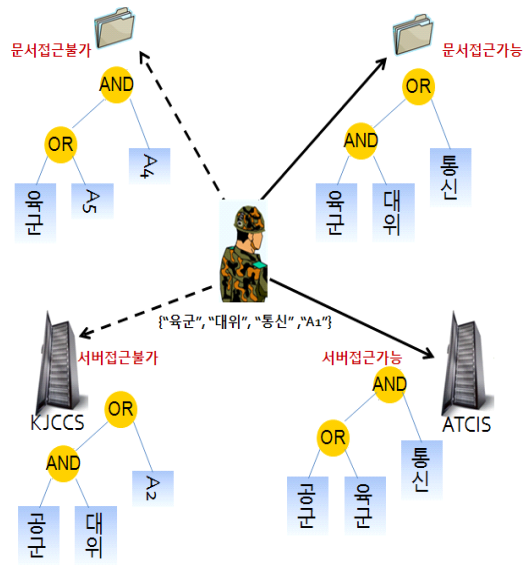
2.1.4 ID기반 공개키 갱신 및 관리

IBC에서는 군번, 메일주소 등 사용자 정보를 이용하므로 단말기와 전장관리체계 서버간에 인증서가 필요 없다. 공개키의 유효기간은 군 복무년수 및 장비수명 주기와 같든지 아니면, 좀 더 길게 해야한다. 기존 공개키 암호에서 요구되는 인증서의 유지 및 갱신을 위한 메커니즘이 요구되지 않는다.

2.2 ABC(Attribute Based Cryptosystem)

2.2.1 ABC 주요기능 및 특징

속성기반 암호시스템은 ID기반 암호 시스템의 확장된 개념으로써 기존의 ID기반 암호 시스템에서 사용자를 표현하기 위해 사용자를 유일하게 식별할 수 있는 식별자 ID를 공개키로 사용하였지만 속성 기반 암호 시스템에서는 사용자를 식별하기 위해 사용자가 가지고 있는 속성을 이용한다[5]. 예를 들어 IBC에서는 A간부의 이메일 주소 혹은 군번(A@army.mil)을 식별자로 사용하였다면 ABC에서는 A간부를 표현할 수 있는 속성들의 집합{육군, 대위, 통신, A1}을 식별자로 사용한다. 이렇게 개체를 속성들의 집합으로 표현함으로써 얻는 장점은 암호문에 대한 접근 정책을 다양화 할 수 있다는 점이다.



(그림 3) 속성기반인증

IBC에서는 A간부가 B간부의 ID (e.g. B@army.mil)를 이용하여 암호문을 생성한다면 B간부의 ID(B@army.mil)에 대응하는 비밀키를 가진 사용자, 즉 B간부만이 해당 암호문을 유일하게 복호화 할 수 있다. 그러나 ABC에서는 어떠한 속성들의 집합으로 암호화하므로 복호화 할 수 있는 개체를 유일하게 지정하기보다는 속성들의 집합을 만족하는 개체들이 복호화 할 수 있도록 할 수 있다[6]. 이러한 접근 정책은 속성간의 AND(∧), OR(∨) 등의 연산을 통해 비밀키 속성에 구현된다. 예를 들어, 암호문이 속성 집합 {육군, 대위, 작전, 통신, 보병}을 이용하여 암호화 되고 다음과 같은 접근 정책을 가진 비밀키를 소유한 사용자들 1. {{육군 ∧ 작전} ∨ {대위 ∧ 보병}, 2. {육군 ∧ 작전∧ 통신∧ 보병}, 3. {육군 ∨ 대위}, 4. {{육군∧보병}∨{대위∧포병}}, 5. {공군∧대위∧보병}∨{대위∧포병}이 존재한다면 1, 2, 3의 경우는 암호문을 복호화 할 수 있지만 4, 5 경우는 복호화 할 수 없다.

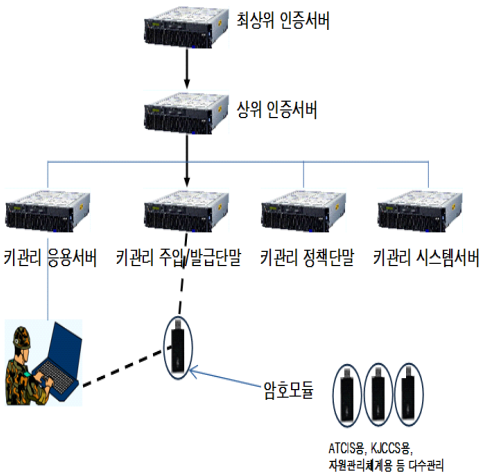
이와 같이 속성 기반 암호는 다양한 접근 정책을 구현함으로써 ID기반 암호가 가지는 접근 정책의 제한성을 극복할 수 있다.

3. 전장관리체계 암호 및 인증 모델연구

국방관련 암호 및 인증체계는 전장관리정보체계를 위한 키관리체계(KMI), 자원관리정보체계를 위한 국방인증체계(MPKI), 행정기관 연계 정보시스템을 위한 행정전자서명 인증체계(GPKI)로 구분한다[7].

3.1 전장관리체계 암호 및 인증방법

군에서 현재 운용하는 체계는 폐쇄망으로 각각의 암호장비를 이용하여 운용되고 있다. 운영업무별 별도의 네트워크 사용으로 체계별 보안성은 확보 했으나 사용자 및 체계연동을 위한 개인정보인증 방법은 아직 완벽하지 못하다. 즉, 동일한 사용자가 서로 다른 체계를 운용하기 위해서는 체계별 사용자 인증을 위한 다수의 암호모듈과 ID/PW를 부여받고 사용하고 있다. (그림4)처럼 체계별 다수의 암호모듈이 필요하다.



(그림 4)전장관리체계 PKI구조

사용자 신원과 전자문서의 변경여부를 확인할 수 있도록 공개키 암호화 방식을 이용한다[8]. 아래표는 암호모듈인증을 통한 접속체계와 국방인증서를 통한 접속체계로 분류하였다.

<표 1> 암호모듈 인증 정보체계

구 분	체계명	인증방식	접속망
전장관리 체계	KJCCS	암호모듈	KJCCS
	ATCIS	암호모듈	SPIDER
	ATCIS-R	암호모듈	KT
	D체계	암호모듈	연합통신 /위성
자원관리 체계	E체계	암호모듈	국방망

<표 2> 국방인증 정보체계

구 분	체계명	인증방식	접속망
자원관리 체계	F체계	웹/ 인증서	국망망
	G체계		
	부대별 운용체계		

위 표처럼 암호모듈인증 및 국방인증서를 통한 접속체계로 이원화되어있어 관리상 제약이 있고 전장관리체계(C4I)는 각각의 폐쇄망별 키관리서버(KMA), 암호모듈, 통신보안장비, 체계서버(APP/DB)등 그에 필요한 장비 및 네트워크 환경을 구축하기 위해 소요되는 예산 및 관리가 중복되게 운영되고 있다.

사용자 역시 업무의 직책으로 상황을 제대별, 부대별로 실시간 공유하기 위해서는 동일인이 각각의 체계에 접속 운영해야 할 소요가 필요하기 때문에 암호모듈도 한사람이 2개 이상을 갖게된다. <표3>는 육군의대표적인 주요 전장관리체계의 인증방식을 비교한다.

<표 3> ATCIS, KJCCS 인증방식 비교

구 분	인증방식	접속망	인증인원
ATCIS	ATCIS 전용 암호모듈	ATCIS망 (폐쇄망)	모듈1개당 1명
KJCCS	KJCCS 전용 암호모듈	KJCCS망 (폐쇄망)	모듈1개당 최대5명
※ KJCCS는 자원절약 차원에서 5명 이하 등록사용			

똑같은 장비임에도 불구하고 각 전장관리체계의 사용자 및 시스템 연동이 제한되어 동일장비를 구축한 것이다. AS업체도 이중계약으로 예산을 낭비하고 있다.

3.2 전장관리체계 암호 및 인증방법 개선모델

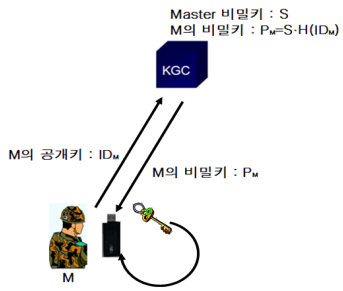
현재 국방관련 암호 및 인증체계를 반영하여 전장관리정보체계 접속체계가 여러개(ATCIS, KJCCS등)일 때 혹은 기관이 여러개(육,해,공)일때 ID기반 암호화 기법과 ID 기반 서명기법을 개선 모델로 제시한다. 제시하는 ID 기반 암호시스템은 개체를 속성 집합으로 표한하는 속성 기반 암호 시스템으로 확장할 수 있다. 본 절에서는 ID 기반 암호시스템을 중점으로 하여 개선 모델을 제시한다.

3.2.1 IBE를 이용한 전장관리체계 암호 기법

- 설정(Setup) : 설정 알고리즘은 보안 상수을 입력으로 하여 기관(Authority)의 마스터 비밀키(master secret key, MSK) 와 공개 파라미터 (Public Parameter, PP)을 생성한다. 즉 기관 k의 마스터 비밀키와 공개 파라미터는 MSK_k, PP_k.
- 사용자 비밀키 생성(Key Generation) : 기관의 집합 $S \subseteq \{1,2,....,n\}$에 대한 접근권한을 가지고 ID를 확인자로 사용하는 사용자는 다음과 같은 과정을 통해 비밀키를 발급 받는다.
  1. 기관 $k \in S$는 사용자의 확인자인 ID의 접근권한을 확인한다.
  2. 기관은 ID에 대응하는 비밀키를 자신의 MSK를 이용하여 생성한다.
  3. 기관은 사용자에게 비밀키를 안전하게 전송하고 사용자는 자신의 기관에서 받은 비밀키들을 안전하게 저장한다.
- 암호화(Encryption) : ID에 대응하는 메시지 M에 대한 암호문을 생성하기 위해 기관의 집합 $S' \subseteq \{1,2,....,n\}$을 선택하고 각 S'에 포함된 기관들의 공개 파라미터를 이용하여 암호문을 생성한다.
- 복호화(Decryption): 암호문을 복호화하기 위해 사용자는 각 기관으로 받은 자신의 비밀키를 입력으로 하여 다음과 같이 계산한다.
  1. $S' \subseteq S$ 을 만족하는지 확인한다.
  2. 암호문의 ID와 자신의 비밀키의 ID가 일치하면 암호문을 자신의 비밀키들로 복호화하여 메시지 M을 얻는다.

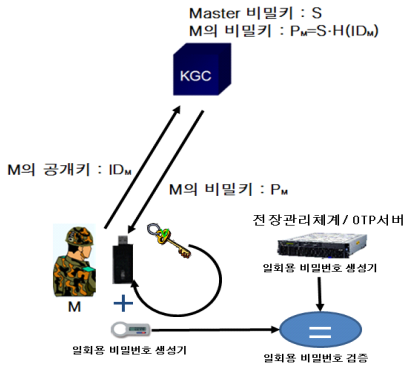
3.2.2 IBS를 이용한 전장관리체계 인증기법

- 설정(Setup), 사용자 비밀키 생성(Key Generation) : IBE와 동일하다.
- 서명(Sign) : ID에 대응하는 메시지 M에 대한 서명을 생성하기 위해 기관으로부터 받은 자신의 서명키을 입력으로 한다. 기관의 집합 $S' \in S$을 선택하고 서명을 생성한다.
- 검증(Verify) : ID, M에 대응하고 기관의 집합 $S' \in S$ 포함된 서명을 S'에 포함된 기관에 대한 공개키와 사용자 공개키 ID와 M을 입력으로 하여 서명을 검증한다.



(그림 5) IBE 이용한 전장관리체계 키교환

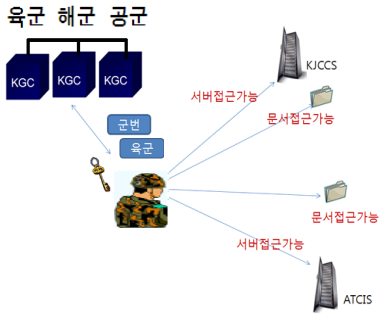
또한 (그림6)처럼 OTP한 전장관리체계 접속으로 암호모듈 및 사용자 인증을 강화 시킬 수 있다.



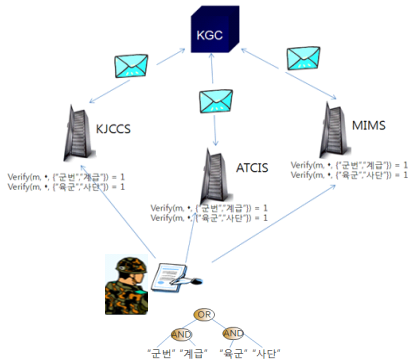
(그림 6) IBE 및 OTP 이용한 사용자 인증

3.2.3 ABC를 이용한 전장관리체계 암호 및 인증기법

다중 속성기반 암호 시스템은 사용자(개체)의 속성들의 집합을 다중기관에서 식별하기 위해 사용자가 가지고 있는 속성을 이용한다. 각 기관별 인증되는 속성값중에 인증되는 값들이 다르게 구현할 수 있고 해 기관의 인증을 받기위한 식별 속성값에 따라 비밀키 값도 정책적으로 변경 할 수 있다. 각 기관별 인증값들에 따라 서로 다른 사용자간의 공통된 속성값으로 원하지 않는 인증이 될 수 있는 충돌위험의 소지도 있지만 사용자(개체) 속성들의 집합으로 표현함으로써 다중기관에 접근할 수 있는 정책을 정할 수 있고 문서에 대한 대한 접근성도 다양화 할 수 있다.



(그림 7) Multi-Authority 접근절차



(그림 8) Multi-Authority 서명접근절차

4. 전장관리체계 암호 및 인증 기법

제안한 기법의 구성에 필요한 겹선형 함수(bilinear map)에 대해 살펴본다.

겹선형 함수(Bilinear Maps).

G_1과 G_2가 위수를 소수 q로 갖는 순환 군(group)이라고 하자. 군 G_1과 G_2에서 모두 이산대수문제(Discrete Logarithm Problem)가 어렵다고 가정하자. 겹선형 함수(bilinear map)는 다음과 같은 성질을 갖는 $G_1 \times G_1$에서 군 G_2위로 맵핑되는 함수

$e : G_1 \times G_1 \rightarrow G_2$이다:

(1) 겹선형성 (Bilinearlity):

임의의 군 원소 $g \in G_1$와 $a, b \in Z_q^*$에 대하여 $e(g^a, g^b) = e(g,g)^{ab}$을 만족한다.

(2) 비소실성 (Non-degeneracy):

$e(g,g) \neq 1$을 만족시키는 $g \in G_1$가 존재한다.

(3) 계산 가능성 (Computability):

임의의 $g_1, g_2 \in G_1$에 대해서 $e(g_1, g_2)$를 계산하는 효율적인 알고리즘이 존재한다.

4.1 전장관리체계 암호 기법

여러개의 기관이 포함된 ID기반 암호 기법은 다음과 같이 설정, 비밀키 생성, 암호화, 복호화의 4개의

알고리즘들로 구성된다. 아래의 기법은 Boneh와 Franklin의 IBE 기법[9]을 변형하여 구성한다.

- 설정(1^{κ}) : 설정 알고리즘은 보안 상수 $\kappa \in Z^{+}$를 입력으로 받고 다음과 같이 작동한다.
  1. 적절한 크기의 소수 q를 생성하고 (G_1, G_2, e)을 생성한다. 이 때 G_1과 G_2는 소수 q을 위수로 갖는 순환군들이고, $e : G_1 \times G_1 \rightarrow G_2$는 어드미서블 겹선형함수(admissible bilinear map)이다.

  G_1의 임의의 생성원 g와 암호학적인 해쉬 함수 $H_1 : \{0,1\}^{*} \rightarrow G_1^{*}$을 선택한다.

  2. 기관 k는 임의의 난수 $s_k \in Z_q^{*}$를 선택하고 $g_k = g^{s_k}$ $(1 \le k \le n)$을 계산한다. 시스템 전체의 공개 상수 (public parameter, PP)와 마스터 비밀키 MSK를 다음과 같이 설정한다.

$$PP = (G_1, G_2, e, q, g, g_1, g_2, \ldots, g_n, H_1),$$
$$MSK = (s_1, s_2, \ldots, s_n).$$

- 비밀키 생성(MSK, PP, ID) :

  기관의 집합(각 전장관리체계(ATCIS, KJCCS) 및 육·해·공) $S \subseteq \{1,2,\ldots,n\}$에 대한 접근권한을 가지고 ID를 확인자로 사용하는 사용자는 다음과 같은 과정을 통해 비밀키를 발급받는다.
  1. 각 기관 $k \in S$는 사용자의 확인자인 ID의 접근권한을 확인한다.
  2. 각 기관은 $Q_{ID} = H_1(ID)$를 계산하고 ID에 대응하는 비밀키 $S_{k(ID)} = Q_{ID}^{s_k}$을 생성한다.
  3. 각 기관은 사용자에게 $S_{k(ID)} = Q_{ID}^{s_k}$를 안전하게 전송하고 사용자는 자신의 비밀키 $SK_{ID} = (S, S_{k(ID)} = Q_{ID}^{s_k} (k \in S))$을 안전하게 저장한다.

- 암호화(M, PP, ID):

  ID에 대응하는 메시지 M에 대한 암호문을 생성하기 위해 기관의 집합 $S' \subseteq \{1,2,\ldots,n\}$과 임의의 난수 $r \in Z_q^{*}$을 선택하고 다음과 같이 계산한다.

$$CT_{ID} = (S', C_1, C_2) =$$
$$\left(S', g^r, M \cdot e(\prod_{k \in S} g_k, Q_{ID})^r\right)$$

- 복호화(PP, CT_{ID}, SK_{ID}):

  암호문 $CT_{ID} = (S', C_1, C_2)$을 복호화하기 위해 사용자는 자신의 비밀키 $SK_{ID} = (S, S_{k(ID)} = Q_{ID}^{s_k} (k \in S))$를 입력으로 하여 다음과 같이 계산한다.
  1. $S' \subseteq S$ 인지 확인한다. 만약 식이 성립하면 다음을 계산한다.
  2. $C_2 \cdot e(C_1, \prod_{k \in S'} S_{k(ID)}^{-1}) = M$

정확성(Correctness)

암호문 $CT_{ID} = (S', C_1, C_2) =$

$$\left(S', g^r, M \cdot e(\prod_{k \in S} g_k, Q_{ID})^r\right)$$

과 비밀키 $SK_{ID} = (S, S_{k(ID)} = Q_{ID}^{s_k} (k \in S))$가 각각 암호화와 비밀키 생성 알고리즘을 통해 올바른 형태로 생성되었을 때 다음의 계산을 통해 메시지 M을 얻을 수 있다.

$$\begin{aligned} C_2 \cdot e(C_1, \prod_{k \in S'} S_{k(ID)}^{-1}) &= M \cdot e(\prod_{k \in S'} g_k, Q_{ID})^r \cdot \\ & \quad e(g^r, \prod_{k \in S'} S_{k(ID)}^{-1}) \\ &= M \cdot e(g^{\sum_{k \in S'} s_k}, Q_{ID})^r \cdot \\ & \quad e(g^r, Q_{ID}^{-\sum_{k \in S'} s_k}) \\ &= M \end{aligned}$$

4.2 전장관리체계 인증 기법

여러개의 기관이 포함된 ID 기반 서명 기법은 다음과 같이 설정, 서명키 생성, 서명, 검증의 4개의 알고리즘들로 구성된다. 아래 기법은 Cha와 Chun의 IBS 기법[10]을 변형하여 구성한다.

- 설정(1^{κ}), 서명키 생성(MSK, PP, ID) : 위의 ID 기반 암호 기법과 동일하다.
- 서명(M, SK_{ID}, ID) : ID에 대응하는 메시지 M

에 대한 서명을 생성하기 위해 자신의 서명키 $SK_{ID} = (S,\ Q_{ID}^{s_k}\ (k \in S))$을 입력으로 한다. 기관의 집합 $S' \in S$과 임의의 난수 $r \in Z_q^*$을 선택하고 다음과 같이 서명 값 $SIG_{ID} = (S',\ U,\ V)$을 계산한다.

1. $U = H_1(ID)^r$을 계산한 후 $h = H_2(M, U)$을 생성한다.
2. $V = \left(\prod_{k \in S} S_{k(ID)}\right)^{r+h}$을 계산한다.

• 검증(PP, SIG_{ID}):

서명 값 $SIG_{ID} = (S',\ U,\ V)$을 다음과 같이 검증한다.

1. $h = H_2(M, U)$을 계산하고 $e(g,\ V) =^{?} e\left(\prod_{k \in S'} g_k,\ U Q_{ID}^h\right)$인지 확인한다.
2. 식의 등호가 성립하면 검증을 통과한다.

정확성(Correctness)

$$SIG_{ID} = (S',\ U,\ V) = \left(S',\ H_1(ID)^r,\ \left(\prod_{k \in S} S_{k(ID)}\right)^{r+h}\right)$$

서명 알고리즘을 통해 올바른 형태로 생성되었을 때 다음의 계산을 통해 메세지 M에 대한 서명을 검증할 수 있다.

$$e(g,\ V) =^{?} e\left(\prod_{k \in S} g_k,\ U Q_{ID}^h\right)$$

$$\Leftrightarrow e\left(g,\ \left(\prod_{k \in S} S_{k(ID)}\right)^{r+h}\right) =^{?} e\left(\prod_{k \in S} g_k,\ Q_{ID}^r\ Q_{ID}^h\right)$$

$$\Leftrightarrow e\left(g,\ \left(Q_{ID}^{\sum_{k \in S} s_k}\right)^{r+h}\right) =^{?} e\left(g^{\sum_{k \in S} s_k},\ Q_{ID}^{r+h}\right)$$

5. 암호 및 인증모델의 비교분석

5.1 암호 및 인증 모델의 보안요건 분석

지금까지 두 가지 방식의 암호기반 인증방식을 알아보았다. 본 장에서는 미래전술통신 환경을 기준으로 보안 위협을 5가지 관점에서 분석한다[11].

1 기밀성 : 암호화 방식을 이용하여 전송 및 저장정보의 기밀성 유지
2 무결성 : 정보의 조작 및 변경여부를 확인
3 가용성 : 언제어디서나 접근 및 이용가능
4 부인방지 : 명령확인자 및 사용자 식별기능을 제공
5 단말인증 : 선택된 단말기 사용자만이 해당 체계 및 정보에 접근하는 기능

또한 강력한 인증을 보장하는 OTP 인증을 분석한다. OTP사용은 은행 및 금융기관에서 사용자 인증을 위해 예금이체시 사용되고 있으며 강력한 알고리즘으로 인증이 보장된다. 전장관리체계에서도 암호모듈 및 단말기 인증시 강력한 사용자 인증이 될 수 있지만 적에 의해 피탈시 그만큼 쉽게 위험에 빠진다. 단순한 OTP사용은 비밀번호 생성기를 분실하였거나 제3자에 의해 도난당했을 경우 부인방지를 할 수 없고 중간자 공격이 가능하여 기밀성 및 무결성을 보장할 수 없다.

<표 4> 보안요건 장단점 분석

보안요건	PKI	IBC	OTP	ABC
기 밀 성	○	○	X	○
무 결 성	○	○	X	○
가 용 성	△	○	○	○
부인방지	○	○	X	○
단말인증	○	○	○	○

5.2 키관리 장단점 비교

PKI 암호기반을 이용하는 경우, 암호화 또는 서명검증 시작 전에 공개키에 대한 인증할 수 있는 통신채널이 필요하다. 따라서 안전한 채널형성을 위한 통신 프로토콜 전송횟수가 증가하게 되고 수신자 공개키 검증을 위해 신뢰할 수 있는 제3자(CA)의 공개키

관리가 필요하다. 신뢰할 수 있는 제3자(CA)에 의한 공개키 인증을 통해 공격자의 임의 공개키 사용문제를 해결하고 중간자 공격을 예방 할 수 있다. 이 경우 각 단말기에 필요한 공개키 저장파일은 네트워크 상에 존재하는 통신단말의 개수만큼의 키를 가지고 있어야 된다. 그리고 공캐키 생성과 분배과정이 필요함은 물론이다. 그러나 암호모듈의 인증서 유효기간이 만료되어 갱신이 필요한 경우와 고장수리를 위해 외부 반출 후 인증서를 갱신하는 경우 등의 인증서 갱신과 폐기목록(CRL) 관리가 필요하다. 전군에서 운용중인 수많은 암호모듈의 인증서 관리를 위해서는 상당한 인력과 인증시스템이 필요하게 된다. 또한 장비를 AS하는 비용이 추가적으로 든다. 그러나 IBC방식에 있어서는 사용자의 고유ID(군번)를 이용하게 되므로 갱신절차가 필요 없게 되어 키 관리가 단순하게 된다. 소규모 환경에서 제3자인 인증기관 없이 당사간의 인증과 키 분배를 하는 경우 거래와 통신의 신속성과 비용이 절약될 수 있다[12]. 기본적으로 키 폐기 기능은 필요 없으나 한번 개인키가 노출될 경우 갱신이 필요하게 된다. 또한 IBC 암호기반을 사용하는 단말기의 고장수리를 위해 외부 반출하는 경우 개인키 삭제 후 재 주입이 필요하게 된다. 개인키가 노출될 경우 심각한 위험에 빠지기 때문이다. 전장관리체계 보안서버(KMA)에서 생성하는 PKI방식의 공개키/개인키 쌍과는 달리 IBC 방식은 중앙의 KGC에서 마스터키를 이용하여 개인키를 생성하기 때문에 개인키의 안전성이 문제가 되지만 군의 특수한 환경에서는 이러한 시스템 구조가 적합하다. 단일기관에서 집중관리하는 것이 적 위협에 대응하기 좋기 때문이다. 또한 개인키의 안전성 문제 때문에 대형 공중망보다는 단일 KGC가 운영하는 일정규모의 폐쇄망에 적합한 구조라고 할 수 있다. 군에서는 기무사 및 기타 중앙기관 등, 법으로 지정된 기관이 KGC를 운영한다면 큰 문제가 되지 않을 것이다.

<표 6> PKI와 IBC 주요 특징 비교

구 분	P K I	I B C
개인키 생성주체	사 용 자	K G C
개인키 관리주체	사 용 자	사 용 자 K G C
키 생성 방향	개인키 → 공개키	공개키 → 개인키
공개키 인증방법	사용자 공캐키를 CA개인키로 서명하여 공개키 인증서 생성	사용자 공개키에 KGC 비밀키를 첨가하여 개인키 생성
암호화	수신자 공개키로 암호화 수신자 개인키로 복호화	수신자 공개키로 암호화 수신자 개인키로 복호화
전자서명	송신자 개인키로 서명 송신자 공캐키로 검증	송신자 개인키로 서명 송신자 공캐키로 검증
사용환경	대형 공중망	폐쇄망
경제성	인증서 관리 비용 필요	추가 비용 없음
장 점	개인 프라이버시	공개키 인증 불요
단 점	공개키 인증서 관리 및 검증과정 필요함	KGC 신뢰 필요 군 특수환경에 적합

6. 결 론

ID기반 암호 기술은 복잡한 인증서 관리가 필요 없으며 PKI를 구축하지 않아도 되므로 국방 예산비용 절감 효과가 크다. 특히 군의 특수한 환경에서 자체적인 보안통신을 제공하는데 활용 가능하다. 자원의 효율적 운용측면에서도 현재의 각 체계별 사용자 인증방식과 암호인증방식은 단일화 통합인증방식으로 개선되어한다. 또한 차기 정보체계시스템은 공통된 정보보호기반 위에 각각의 운용업무체계를 설계하고 각 서버별 사용자 정보를 공유해서 인증하도록 인증방법

을 개선해야한다. 정보체계는 점점 늘어가고 있으며 과학기술의 발전 및 요구되는 추가 기능에 따라 C2, C3, C3I, C4I, C4ISR 그리고 C4ISR+PGM 등으로 지속적으로 발전하고 있다[13]. 현재 국방부 주관으로 국방통합정보관리소 구축사업을 하고 있으나 구체적인 체계통합 및 서버별 인증 방법에 대한 연구가 필요하다. 국방통합정보관리소 구축사업간 체계 통합시부터 기본 바탕이 되는 정보보호기반이 제대로 구축되지 않으면 재투자 및 재구축 될 소지가 많다.

특히, 군 업무상 특화된 분야의 사용자 인증은 각 정보체계별, 각 군 부대별에서가 아니라 최상위 중앙본부에서 사용자 정보를 관리해야 하며, 부대전 · 출입시 및 전·평시 어디서나 체계 접근이 쉽도록 각 부대별로 사용자ID생성이 아니라 전군 통합적으로 사용자 ID인증 및 관리가 필요하다. 또한 C4I체계 및 위성통신장비 등 지휘통신장비가 계량되고 개선되고 있다[14]. 앞으로도 첨단장비는 계속 개발될 것임은 분명하기 때문에 각 군 및 각 제대별 운용되고 있는 정보체계의 인증방법은 통합적으로 관리해야 한다[15]. 그러나 이는 모두 유선인증방식으로 무선 환경에서는 인증이 불가하다. 차후 차기 무선환경 및 IPV6로 재구성된다면 대부분의 장비는 새로운 장비로 교체되어야 함은 당연하다. 앞으로 차기 TICN환경에서는 무선환경이 구축될 것인데 무선암호 보안인증방법도 연구해야 할 과제임[16]에 틀림없다.

참고문헌

[1] 육군야전교범 6-10 육군 전술지휘정보체계

[2] 수원대학교, NCW환경에 부합한 국방 KMI구축방안 연구 2012.8

[3] 고려대학교, 미래전술환경에 부합한 국방KMI/PKI 구축방안 조사분석 이동훈 2010.12

[4] 임종인, 이동훈, 금융분야 안전한 암호이용에 대한 연구

[5] A. Sahai and B. Waters, Fuzzy identity-based encryption, EUROCRYPT'05, 2005, vol. 3494, pp. 457-473.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, ACM-CCS'06, 2006, pp. 89-98.

[7] 국방정보화업무 훈령 5장 국방인증체계 구축 및 운영 2011.2.7.

[8] 전자서명, http://blog.daum.net/_blog/BlogTypeView.do?blogid= 0ECpo&articleno=12690844&admin=#ajax_history_home)

[9] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in CRYPTO'01, 2001, vol. 2139, pp.213-229.

[10] J. C. Cha and J. H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups", in PKC'03, 2002, vol. 2567, pp.18-30.

[11] 국방부, "국방 암호키 운용 및 보안관리지침", 2006.11

[12] 정보통신연구진흥원, 인터넷 PKI 시스템 설계를 위한 ID기반의 암호 및 인증기술에 관한 연구, 2001.7

[13] 국방과학연구소, "전술 정보통신체계(TICN) 사업현황" 2007

[14] 김은호 이수진" TICN에 적합한 키 관리기법에 관한 연구",국방과학기술 제1권 제1호, 2008.10

[15] 김영성 이수진,"전장관리체계의 PKI기반 키 관리 시스템에 관한 연구"국방과학기술 제2권 제2호, 2009.6

[16] 한국국방연구원," NCW를 대비한 국방인증체계 종합발전 연구", 2008.10

[저 자 소 개]

이 원 만 (Won-man Lee)

2004년 홍익대학교 컴퓨터공학사 졸업
2011년~ 현재 고려대학교 정보보호대학원 석사과정

email : elviron@korea.ac.kr

박 태 형 (Tae-hyeong Park)

2002년 고려대학교 서양사학과 학사 졸업
2004년 고려대학교 일반대학원 행정학과 석사 졸업
2011년 2월 고려대학교 정보보호대학원 박사 졸업
2011년 3월~현재 고려대학교 정보보호대학원 연구교수

email : mosto2004@korea.ac.kr

구 우 권 (Woo-kwon Koo)

2006년 고려대학교 수학과 이학사 졸업
2008년 고려대학교 정보경영공학과 공학석사 졸업
2008년~현재 고려대학교 정보보호대학원 박사과정

email : kwk4386@korea.ac.kr

이 동 훈 (Dong-hoon Lee)

1983년 고려대학교 경제학과 경제학사 졸업
1987년 Oklahoma University 전산학 석사 졸업
1992년 Oklahoma University 전산학 박사 졸업
1993년~1997년 고려대학교 전산학과 조교수
1997년~2001년 고려대학교 전산학과 부교수
2001년~현재 고려대학교 정보보호대학원 교수

email : donghlee@korea.ac.kr