위치정보를 이용한 군 보안체계 강화 방안

김윤영* · 남궁승필**

요 약

현재 사용되고 있는 국방 PKI 시스템은 앞으로 전력화 될 무선 네트워크 환경에서 보다 많은 위협요소들이 발생할 것이다. 본 연구에서는 위치정보를 이용한 장소에 대한 접근제어 및 암호화를 통해 군 정보시스템에 접근 가능한 인증체계를 강화할 수 있는 방안을 제시하고자 한다. GPS, 센서와 같은 위치정보 수집 장치를 통하여 정보를 수집하고 인증을 위한 새로운 키를 생성한다. 이렇게 생성된 키로부터 접근제어를 위한 인증코드 생성과 데이터를 암호화한다. 본 논문은 제안된 기법을 통하여 허가되지 않은 장소에서 군 기밀정보의 접근을 통제하고 권한이 없는 사용자의 인증을 방지할 수 있을 것이다. 아울러 기존의 국방 PKI 시스템을 적극적으로 활용함으로써 다단계 접근제어가 가능하다.

Study on the scheme to reinforce military security system based on location information

Kim Yun Young* · Namkung Seung Pil**

ABSTRACT

Current PKI system will confront more dangerous elements in the wireless network. Accordingly, this study suggests a plan to strengthen authentication system plan with using access control and encryption to the location. Locational information collecting devices such as GPS and sensor are utilized to create a new key for authentication and collect locational information. Such a key encodes data and creates an authentication code for are access control. By using the method suggested by this study, it is possible to control access of a military secret from unauthorized place and to protect unauthorized user with unproposed technique. In addition, this technique enables access control by stage with utilizing the existing PKI system more wisely.

Key words : Defense PKI, Location Information, Authentication, Security Technique, Access control

접수일(2015년 5월 4일), 수정일(1차: 2015년 5월 19일)
게재확정일(2015년 5월 28일)

* 대전대학교 / 군사학과, 교신저자
** 우석대학교 / 군사학과

1. 서 론

현재 군은 첨단 정보통신기술의 발전으로 네트워크 중심의 작전환경이 조성되고 실시간 정보공유, 상황인식 및 지휘통제가 구현되어 전쟁의 양상이 변화되고 있다. 또한 이러한 군사과학기술의 발달은 무기체계의 발전은 물론 정밀타격을 가능하게 하여 전쟁수행개념에도 영향을 미칠 것이다. 군은 이러한 미래전에 대비하기 위하여 군 전용 정보시스템을 구축하여 활용하고 있다. 이를 위해 각 군의 정보시스템의 사용자 인증 및 암호화된 데이터 통신을 위해 인가된 사용자에 한하여 PC와 인증정보가 담긴 USB 암호모듈을 보급하고 있다.[1] 그러나 현재의 방법에는 몇가지 취약점이 있다. 주요 문제점은 계급 및 직책에 대한 사용자 정보를 입력하고 ID/PW에 의해 어느 정도의 접근제어를 하고 있지만 불필요한 장소와 내부자의 유출에 대한 접근제어가 이루어지지 않고 있다. 특히 전력화 예정인 무선 네트워크 통신 시스템 환경으로 인하여 이러한 취약점이 더욱 문제가 될 것이다. 또한 전 구간이 무선망으로 구성됨에 따라 적의 감청 및 전파방해, 암호키 노출 등 전자전 위협에 매우 취약하게 될 것이다. 따라서 전술환경에 적용 가능하고 비용적 측면과 암호학적 측면에서 효과적으로 적의 보안 위협에 대응할 수 있는 새로운 암호 기법이 필요하다.

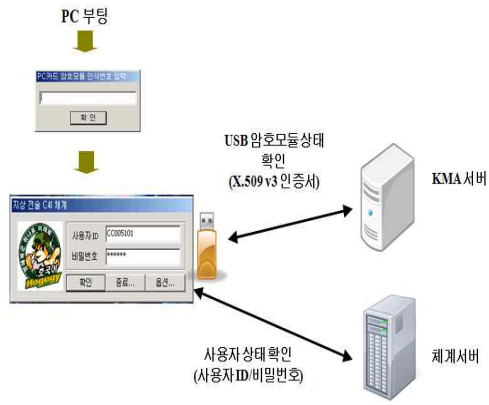
본 연구는 군 정보시스템의 대한 취약점을 분석하여 보안을 향상하기 위한 위치정보 기반의 서비스 접근제어와 데이터 암호화 기법을 제안하고, 제안 기법의 군 적용을 위한 구체적 방안과 적용 시 장점에 대하여 연구하였다.

2. 관련연구

2.1 군 인증체계

2.1.1 국방 PKI 시스템

군 정보시스템의 보안은 로그인 단계에서 USB 암호모듈 사용자를 위한 장치 접근제어와 체계접속을 위한 사용자 인증으로 구분된다. 장치 접근제어는 메모리스틱의 USB 암호모듈을 사용하여 실제 사용자를 인증한다. 서비스 접속을 위한 사용자 인증은 USB 암호모듈의 인증서 및 암복호 기능을 활용하여 클라이언트와 서버 간에 인증 프로토콜을 통해 실시된다. 군 작전을 위한 정보시스템에서는 인증을 위해 PKI(Public Key Identification) 방식을 사용하는데, 사용자 인증 정보를 수신한 KMA(Key Management Authentication)서버에서는 수신한 인증 정보를 기반으로 사용자 인증을 수행한다.[2]



(그림 1) PKI 인증서에 의한 사용자 인증

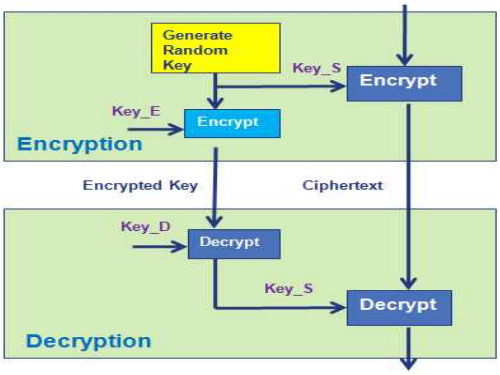
2.1.2 데이터 암·복호화

군 정보시스템에서는 비밀 전문의 보안을 위해 데이터를 암호화하여 송신한다. 상급부대에서 데이터를 암호화하여 송신하면 수신측인 예하부대에서는 Off-line으로 분배받은 보안 USB 모듈의 개인키로 데이터를 복호화한다.[2]

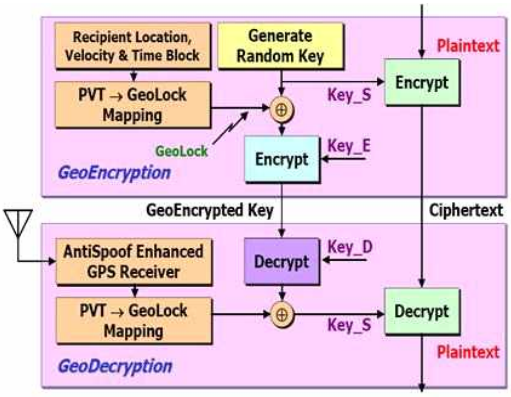
(그림 2) 데이터 암/복호화

2.2 위치정보를 이용한 인증 방법

Geo-Encrypt 기술에 대한 연구는 사용자 위치정보를 이용해 인증을 받게 하고 네트워크를 사용하도록 하려는 의도로 시작되었다. 현재는 GPS(Global Positioning System) 또는 AP(Access Point)를 이용해 위치 정보를 획득하고 획득된 정보를 이용해 암호키를 생성하도록 하는 알고리즘이 제안되어 지정된 위치 공간에서만 수신된 암호문을 해독할 수 있도록 되어 있다.[3]

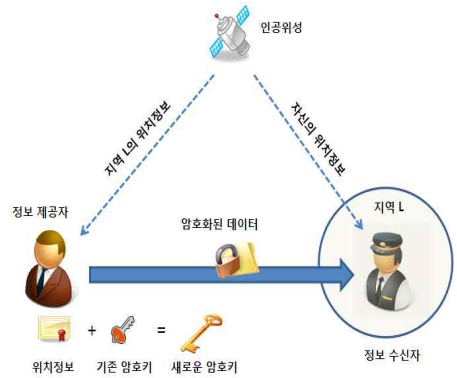


(그림 3) 기존의 데이터 암호화 알고리즘



(그림 4) Geo-encryption 알고리즘

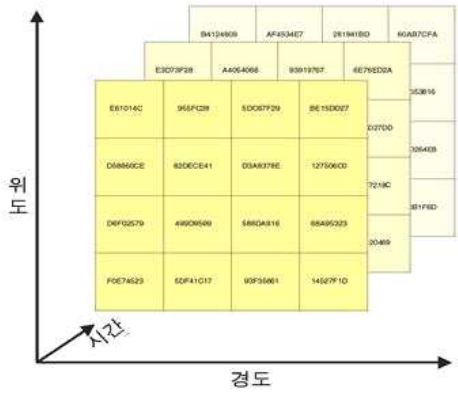
GPS 또는 AP를 이용한 Geo-Encrypt 기술의 동작 원리는 (그림 5)와 같다. GPS를 이용해 데이터를 이용하고자 하는 사용자가 존재하는 지역의 위치 정보를 얻고, 그 정보를 이용해 암호키를 생성하며, 이 키를 이용해 데이터를 암호화 한다. 암호화된 데이터를 받은 사용자는 자신의 위치정보를 GPS를 이용해 획득하고, 이 위치정보를 이용해 키를 생성하며, 생성된 키를 이용해 복호화 한다.[4][5] 정보를 암호화할 때 세션키와 함께 위치정보에서 얻은 키를 사용함으로써, 송신측과 수신측 간 약속된 지역에서만 데이터가 복호화된다. 즉, 위치정보로부터 생성된 키값을 세션키와 XOR하여 Encryption algorithm의 키로 사용하여 데이터를 암호화한다.[3][4] 여기서 XOR(exclusive or) 알고리즘은 임시 변수를 두지 않고 두 개의 변수를 배타적 논리합 비트 연산을 이용하여 교체하는 알고리즘으로서 메모리 사용을 최소화할 수 있는 장점이 있기 때문에 적용하였다.



(그림 5) GPS를 이용한 Geo-Encrypt

다만 부대 형태 및 구성, 작전에 따라 어느 정도 유추가 가능하기 때문에 일률적으로 절대적인 GPS 좌표를 직접 키로 활용하기에는 위험하다. 따라서 GPS 좌표를 이용하여 보안된 값으로 변환을 하는 특화된 맵핑 테이블을 이용하여 수많은 grid로 구분할 필요가 있다.

위도, 경도와 시간값을 이용하여 (그림 6)과 같이 3차원의 맵핑 테이블을 구성하여 시간에 따라 random하게 맵핑 테이블이 선택되도록 구성한다. 이렇게 되면 일률적으로 특정한 수에 맵핑이 되는 것의 유추를 막을 수 있고 무한히 많은 수의 맵핑 테이블을 가질 수 있다.[3] 이러한 맵핑 테이블은 일종의 보안카드나 OTP(One Time Password)처럼 활용하여 새로운 키 값을 형성하도록 할 수 있다.



(그림 6) 맵핑 테이블 구성

2.3 군 인증체계 취약점 분석

2.3.1. 장비 분실 및 악의적인 내부자

군 정보시스템 전용 PC는 노트북의 형태로 휴대가 편리하기 때문에 운용시 분실의 위험이 높다. 특히 내부자에 의한 ID, PW 분실이나 기존의 ID부여의 규칙성과 유추하기 쉬운 PW 설정은 시스템의 불법적 접근을 더욱 용이하게 할 것이다. USB 암호모듈을 이용한 체계접속 또한 USB 암호모듈 자체를 분실한다면 접속은 더욱 쉽게 이루어질 것이다.

2.3.2 국방 PKI 시스템의 인증 방식 취약점

국방 PKI 시스템 전용 인증서와 개인키는 Off-line으로 USB 암호모듈에 주입하여 각 개인이 소유한다. 결국 한번의 ID/PW 입력에 의한 사용자 인증으로 체계의 정보접근 가능하다. 또한 각 정보시스템 운영자는 정·부로 나뉘어져 2~3명의 실무자가 운영하기 때문에 사용자 인증을 위한 ID/PW의 유출이 더욱 쉽다.

2.3.3 무선 네트워크의 근본적인 취약점

전력화중인 차기 전술정보통신체계는 유/무선 체계를 통합한 미래 전장환경의 핵심 전술통신 기반체계이다. 이는 각 군의 정보시스템이 지휘소에서부터 말단 제대까지 무선으로 데이터를 송/수신하게 된다.[6] 일반적으로 무선이라는 특성으로 인하여 유선보다 다양한 보안 위협요소가 존재하고 외부의 공격자에 의해 쉽게 접근 가능할 수 있다. 무선 환경에서 각 군의 정보시스템은 무선 AP의 역할을 하는 MSAP(Mobile Subscriber Access Point)을 통하여 데이터를 송·수신한다. 이러한 무선이라는 환경은 은폐된 환경을 제공하고 시스템의 불법적 접근 및 자료 유출을 더욱 용이하게 할 것이다.[2]

라우터 암호장비를 통과한 패킷은 MSAP의 무선랜 구간에서 각 전술용 단말기로 보내진다. 이는 MSAP의 넓은 전파반경으로 인해 은폐된 지역에서 외부의 단말기 등으로 불법적 접속이 가능하고 특히 도청(Eavesdropping) 및 패킷 스니핑(Sniffing)을 통하여 공격자가 다양한 암호 분석기술로 패킷에 포함된 암호키 및 데이터가 유출될 것이다.

3. 군 적용 방안

3.1 위치정보 적용 방법

3.1.1 위치정보를 이용한 접근제어 절차

① 사용자는 서버에게 군 정보체계 전용 서비스 접근을 요청한다.

② 서버는 사용자에게 군 정보체계 전용 서비스 접근을 위한 인증 코드를 요청한다.

③ 사용자는 해당 위치정보를 이용하여 위치키 LK를 생성한다. 위치키 LK는 실내 AP 또는 GPS로부터 수신한 위도, 경도로 표현된 위치정보를 인증과정에서 사용자에게 배포한 세션키 SK를 암호화키로 이 용하여 암호화하여 생성한다.

$LK = E_{SK}\{위치정보\}$

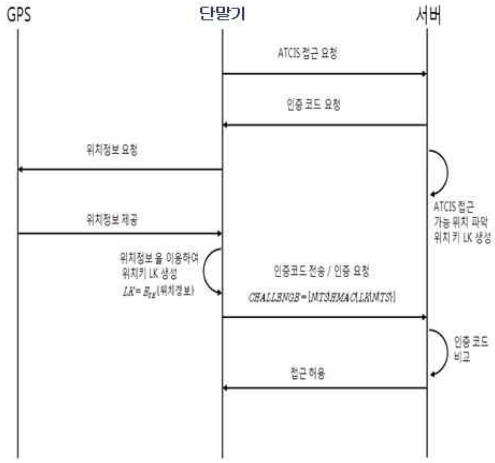
④ 생성된 LK를 이용하여 사용자는 다음과 같은 권한 인증 요청을 서버에게 보낸다. 여기서 HMAC은 키를 사용하여 해쉬값을 생성하는 알고리즘을 의미하며, N은 임의의 난수를 의미하며, TS는 당시의 시간값으로 인증 요청을 재사용하는 공격을 방지한다.

$CHALLENGE = [N \mid TS \mid HMAC\{LK \mid N \mid TS\}]$

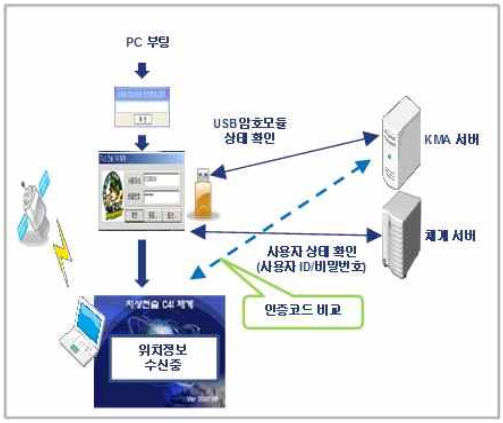
⑤ 서버는 사전에 저장된 군 정보체계 전용 서비스 단말기의 허가지역 정보로부터 위치정보와 인증단계에서 얻은 세션키 SK를 입력하여 위치키 LK

를 생성한다. 생성된 위치키를 이용하여 ④에서 사용자측이 보낸 인증 요청값을 직접 생성한다. 자신이 생성한 인증 요청값과 수신된 인증 요청값을 비교한다.

⑥ 인증 요청값이 일치하면 사용자가 정해진 위치에 있음을 확인하고 접근을 허용한다.



(그림 7) 위치정보를 이용한 접근제어



(그림 8) 위치정보를 이용한 국방 PKI 접근제어의 예

(그림 8)는 군의 장비들에서 위치정보를 이용한 접근제어의 순서를 그림으로 표현하였다.

3.1.2 위치정보를 이용한 데이터 암호화 절차

① 군 정보체계 전용 서비스 단말기 사용자의 데이터 요청을 받은 서버는 Client의 위치정보와 미리 저장된 맵핑함수 F를 이용하여 위치키 LK를 만든다.

② 이 위치키와 암호키(SK)를 XOR하여 암호블럭를 생성한다.

③ 데이터는 암호키 SK를 이용하여 암호화하고 암호블럭을 Client의 공개키를 이용하여 암호화하여 Client로 송신한다.

$Payload = E_{pu}(SK \oplus LK) \mid E_{sk}(DATA)$

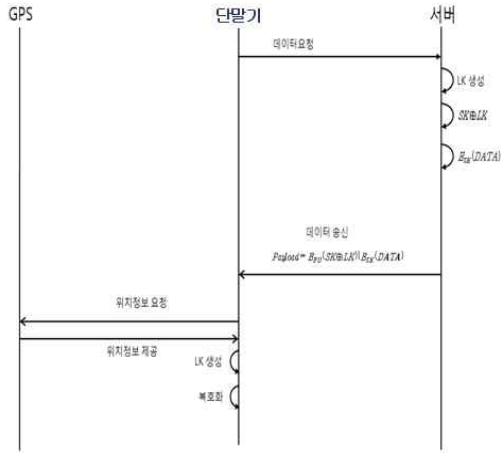
④ Client는 위치 수신장비로부터 자신의 위치정보를 획득한다.

⑤ Client는 수신 데이터에 포함된 공개키 암호화된 암호블럭을 개인키로 복호화한다.

⑥ 수신된 위치정보는 서버와 동일한 맵핑 테이블 F′를 이용하여 위치키 LK를 생성한다.

⑦ 위치키 LK를 이용하여 복호화된 암호블럭(SK⊕LK)으로부터 SK를 계산한다.

⑧ Client는 복원된 암호키(SK)를 이용하여 암호화된 데이터를 복호화한 후, 데이터를 사용한다.



(그림 9) 위치정보를 이용한 데이터 암호화

(그림 10)는 군의 장비들에서 위치정보를 이용한 데이터 암호화의 순서를 그림으로 표현하였다.

(그림 10) 위치정보를 이용한 데이터 암호화의 예

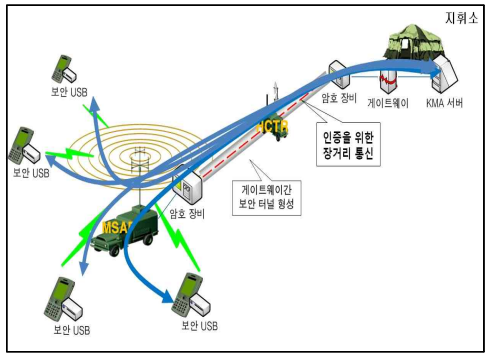
4. 제안 기법의 장점

4.1 TICN 전력화 비용 문제 해소

현재까지 합참에서 거론된 차기 전술 정보통신 체계(TICN, Tactical Information Communications Network)를 위한 암호화 방안으로 전송 구간별, 장비별 암호장비를 구축하는 방안이 제시되고 있다.[7] TICN체계는 Wibro 기반의 이동기지국 개념의 전술 이동통신체계(MSAP, Mobile Subscriber Access Point)를 바탕으로 무선환경을 제공하기 때문에 최하급 제대까지 실시간 작전지시 및 상황전파가 이루어지게 될 것이다.[6] 따라서 최하급 제대에서 활용할 수 있는 휴대폰 형태의 전술 이동통신 단말기(TMFT, Tactical Multi-Function Terminal)나 전술 다대역 다기능 무전기(TMMR, Tactical Multiband Mutirole Radio)까지 암호장비가 장착될 예정이다.[7] 그러나 이 방안의 문제점은 TICN의 개발중인 모든 장비에 암호장비를 완벽히 구축하는 것은 불가능하다는 것이다. 모든 단말에 암호장비를 적용하면 TICN의 유무선 체계는 암호학적으로 완벽하지만 일반적으로 전력화 비용문제로 인하여 많은 단말들이 암호장비를 적용받지 못할 것이다. 더욱이 2016년부터 4조원 이상의 비용이 들어갈 예정으로 보안장비까지 장착하게 된다면 전력화되기까지 상당한 기간이 더 소요될 것이다. 따라서 기존의 라우터 암호장비와 TICN의 각 체계별 암호장비의 순차적 전력화 수준을 고려한다면 전력화 순위가 낮은 대다수의 일반 단말은 보안 기능이 충분하지 않은 채로 음성 및 데이터가 네트워크상에 노출되는 문제점이 있다. 이러한 문제점을 해결하기 위해 위치정보 송수신모듈을 MSAP 서버로부터 설치, 관리 되면 적은 비용으로 암호장비가 적용되지 않는 구간에서 많은 수의 TMFT 및 TMMR에 강력한 접근제어 및 암호화가 가능하게 할 것이다. 따라서 제안하는 방법은 TICN 전력화시 발생하게 될 엄청난 암호장비 전력화 비용을 획기적으로 줄일 수 있을 것이다.

4.2. 시스템 안정성 향상

현재의 국방 PKI에 의한 인증방법을 그대로 사용하게 되면 최하급 제대의 TMMR이나 TMFT에서 기밀내용을 송수신하기 위해 (그림 11)과 같이 사용자 인증을 위해 상급부대의 KMA 서버와의 장거리 통신을 하게 될 것이다. 이렇게 되면 인증을 위해 많은 장비로부터 엄청난 양의 트래픽이 발생하게 되고 정작 중요한 시간에 통신이 제한될 수도 있을 것이다.



(그림 11) 현 보안체계가 적용된 TICN 인증 모습

또한 위와 같은 문제점을 막기위해 MSAP에 인증을 위한 KMA 서버를 추가로 설치하려면 비용적인 문제도 발생할 것이다. 하지만 제안하는 방법처럼 위치정보 송수신모듈을 갖춘 MSAP의 서버 형태가 되면 큰 비용을 들이지 않고 기존의 보안 강도를 유지하면서 트래픽은 현저히 줄일 수 있을 것이다.

4.3. 기존의 암호화 방법의 취약점 보완

현재 유선 네트워크 상에서는 군 전용 정보체계 서비스 접속을 위해 USB 암호모듈을 사용하고 있다. 이 암호모듈은 군 전용 정보체계 서비스 접속시 사용자 인증을 위해 사용되며 비밀 전문 데이터 전송간 암호화하는 기능을 한다. 또한 IP레벨의 라우터 암호장비를 사용하여 전송구간을 보호한다. 하지만 USB 암호모듈은 분실하기 쉬우며 ID/PW만 알면 쉽게 인증 및 접근 가능하다. 더욱이 장차 무선 네트워크로 구성이 된다면 이러한 문제점은 더욱 심각해질 것이다. 무선 AP에 대한 접속만 가능하면 기밀 데이터에 쉽게 접근 가능하기 때문에 은폐된 장소나 타 지역으로 이동하여 기밀 데이터를 반출하거나 접속할 것이다. 따라서 본 연구에서 제안한 위치정보 송수신 모듈을 활용하면 허가된 장소(GPS 절대 좌표 및 센서가 수신하는 값)가 아니면 군 전용 정보체계 서비스에 접근이 불가능하며 데이터가 암호화되어 불법적으로 반출이 불가능하게 된다.

4.4. 기존 기법과의 암호 강도 비교 분석

본 논문에서 제안하는 기법은 사용자의 분실과 내부자에 의한 불법 접속, 데이터 유출을 막기 위하여 기존의 국방 PKI 시스템의 취약점을 보완하였다. 따라서 접근제어를 위한 다음과 같은 LK 생성과 메시지 인증코드 생성/검증 과정이 추가 되었다.

$$LK = E_{SK}\{\text{위치정보}\},$$

$$CHALLENGE = [N \mid TS \mid HMAC\{LK \mid N \mid TS\}]$$

또한 다음과 같이 데이터 암호화를 위한 LK 생성의 연산과정이 추가되었다.

$$LK = F\{\text{위치정보}\},$$

$$Payload = E_{pu}(SK \oplus LK) \mid E_{sk}(DATA)$$

<표 1> 기존 기법과의 비교

구분	로그인 단계			로그인 후 장소 이탈시		
	인증	서비스 접근제어	데이터 암호화	인증	체계 접근 제어	데이터 암호화
현 보안체계	1회 (PKI 인증서)	1회 (사용자 정보)	1개의 키 (SK)	-	-	1개의 키 (SK)
제안 기법	1회 (PKI 인증서)	2회 (사용자 정보, 허가된 장소)	2개의 키 (SK, LK)	-	1회 (허가된 장소)	2개의 키 (SK, LK)

제안 기법은 로그인 단계에서 기존 방법에 비해 접근제어를 2회 실시한다. 계급/직책과 같은 사용자 정보에 따라 서비스를 제한하는 방법과 환경정보를 바탕으로 사용 가능 지역을 제한하는 방법이 병행된다. 또한 데이터 암호화를 위해 LK를 추가함으로써 유추가 불가능한 강력한 암호 키를 획득하게 된다.

5. 결 론

본 논문은 위치정보를 이용하여 군 전용 정보체계 서비스의 보안을 향상하는 방안을 제안하였다. 위치정보는 GPS 및 센서 등을 활용하여 수신하고 Server와 Client의 암호모듈에 의해 새로운 키값인 LK를 생성하게 된다. 이러한 키값을 활용하여 군 전용 정보체계 서비스에 대한 접근제어용 인증코드를 만들고 기존의 암호키와 결합한 새로운 키를 생성함으로써 장소에 대한 접근제어 및 데이터 암호화를 강화하였다. 제안 기법은 소프트웨어적인 형태로 구축이 가능하여 비용적으로 효과적일 것이다. 물론 별도의 암호모듈 및 서버에서 암호화 키를 생성하는 과정에서 오버헤드가 발생하지만 현재 컴퓨터 및 통신기술의 발달에 따른 진화적인 전력화 전략을 통해 컴퓨팅 능력이 증대되고 기존의 PKI 시스템과 적절하게 연동하게 된다면 이러한 단점은 극복 가능할 것이라 판단된다. 또한 위치정보를 포함한 새로운 형태의 암호화 방식을 통하여 군을 포함한 국가 중요 정보망의 보안이 더욱 향상되길 기대한다.

참고문헌

[1] Ground Tactical C4I system User Guideline, DAPA, pp. 1-2~2-3, 2007

[2] Ajou Univ TNRC, “Wireless Network Security Structure & Invation Search/Reaction Technology Research”, JCS, pp. 63~78, 2008.

[3] D. E. Denning and L. Scott, "Geo-Encryption: Using GPS to Enhance Data Security," GPS World, Apr, 2003.

[4] A. Al-fugaha and O. Al-Ibrahim, "Geo-encryption Protocol for Mobil Networks, "Computer Communications, vol. 30, Issue 11-12, pp. 2510-2517, Sep, 2007.

[5] Hsien-Chou Liao Yun-hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users", Information Technology Yournal, 7(1), pp. 63-69, 2008.

[6] Tactical Information Communications Network Operational guide book, Army HQ, pp. 2-3~3-7, 2006.

[7] Tactical Information Communications Network Operation FM reference 1-2, Army HQ, pp. 2-26~27, 2015.

[저 자 소 개]

김 윤 영 (Yun-young Kim)

2003년 2월 육군사관학교 공학사
2011년 2월 아주대학교 컴퓨터공학과 공학석사
현재, 대전대학교 군사학과 박사과정

email : kyy646464@naver.com

남궁승필 (Seung-Pil Namkung)

2004년 2월 경기대학교 박사
현재, 우석대 군사학과 교수/학과장

email : nksp1234@naver.com