전술 Ad-hoc 네트워크에서 하이브리드 키 관리 기법

정회원 이 윤 호*, 이 수 진*°

A Hybrid Key Management Scheme in Tactical Ad-hoc Network

Yunho Lee*, Soojin Lee*° *Regular Members*

요 약

차세대 전술통신체계인 TICN은 대용량, 고속 및 원거리 무선 통신을 위해 설계되었다. 특히 전장에서의 이동성 보장을 위해 무선 통신이 가능한 애드혹 네트워크 기술 적용을 고려하고 있다. 애드혹 네트워크에서 기밀성, 무결성 및 인증을 보장하기 위한 키 관리 기법은 매우 중요하다. 본 논문에서는 TICN과 같은 전술 애드혹 네트워크의 계층적 특성을 고려한 새로운 하이브리드 키 관리 기법을 제안한다. 즉, 충분한 에너지와 계산능력을 갖춘 상위계층 노드에서는 PKI 기반의 키 관리 기법을 적용하고, 반면 상대적으로 제한된 에너지를 가지는 하위계층에서는 에너지 효율성을 보장하기 위해 위치기반의 인증을 통한 새로운 키 관리 기법을 제안한다.

Key Words : Ad-hoc, key management, 인증, TICN

ABSTRACT

A next generation military communication system called Tactical Information Communication Network(TICN) is designed to advance into large capacity, high speed, and long distance wireless relay transmission. To support mobility in battlefield, the application of Ad-hoc networking technology to its wireless communication is being considered. In Ad-hoc network, the key management technique is very important to ensure the confidentiality, integrity, and authentication. In this paper, we propose a new hybrid key management scheme considering the hierarchical characteristics of the tactical ad-hoc such as TICN. For upper layer with sufficient energy and computation capability, we apply PKI based key management scheme. For lower layer with restricted resources, we propose a new key management scheme using the location-based authentication to ensure the energy efficiency.

Ⅰ. 서 론

우리 군은 현재 운용중인 SPIDER 체계를 대체하기 위해 고속 및 대용량 정보전송이 가능한 차세대 전술정보통신망인 TICN을 개발하여 2013년 전력화를 목표로 추진하고 있다. TICN의 부 체계(Sub-system) 중 연대급 이하의 전술통신망을 지원하는 전투무선체계는 예하 부대의 이동시에 원활한 지휘통신 및 정보유통을 보장하기 위해 Ad-hoc 네트워크 기술 적용을 고려하고 있다. 그러나 Ad-hoc 네트워크는 기존의 유선 네트워크들과는 차별화되는 특성들 때문에 보안에 취약하다. 그러므로 Ad-hoc 네트워크를 전장 환경에 적용하기 위해서는 기반기술에 대한 연구에 앞서 보안대책에 대한 연구가 반드시 선행되어야 한다. 특히, 전장상황하에서 유통될 민감 정보들에 대한 기밀성, 무결성의 보장과 함께 정당한 권한을 가지지 못한 노드들의 네트워크 참여를 차단할 수 있는 인증기술 등은 Ad-hoc 네트워크 보안을 위해 중요한 부분이다.

이와 같은 Ad-hoc 네트워크 환경에서 기밀성, 무결성, 인증과 같은 보안 목표 달성을 위한 기반이 되는

* 국방대학교 국방정보체계학과 (yunholee@gmail.com, cyberkma@gmail.com), (° : 교신저자)
논문번호 : KICS2011-08-375, 접수일자 : 2011년 8월 26일, 최종논문접수일자 : 2011년 10월 12일

키 관리는 매우 중요하다. 일반적으로 키 관리 기법은 공개키 기반 기법과 대칭키 기반기법으로 분류된다[1].

공개키 기반 키 관리 기법은 암호화 강도가 강하여 높은 안전성을 보장할 수 있는 장점이 있지만, 암복호화에 많은 시간이 소요되어 에너지 비효율적인 단점을 지닌다. 반면, 대칭키 기반 키 관리 기법은 상대적으로 암복호화에 소요되는 시간은 짧아 에너지 효율적이지만 키 탈취 취약점 및 암호화 강도는 낮은 단점을 지닌다. 따라서 군의 전술상황에서 운용될 Ad-hoc 네트워크에 키 관리 기법을 적용할 경우 에너지 효율성과 보안 강도를 함께 고려하여 적절한 방안을 모색해야 한다.

군의 임무 특성상 Ad-hoc 네트워크에 참여하는 노드들은 에너지, 계산 능력 등 자원이 상대적으로 풍부한 상위 계층 노드와 상대적으로 자원이 부족한 하위 계층 노드로 계층화[2,3]할 수 있어 차별화된 키 관리 기법의 적용이 가능하다. 즉 상위계층 노드의 경우 안전성 측면을 강화한 PKI 기반의 키관리 기법을, 자원 제약을 많이 받는 하위계층 노드들의 경우에는 노드 생존성과 안전성을 함께 고려하여 대칭키 기반의 키 관리기법을 적용하는 방법이 바람직하다. 따라서 본 논문에서는 계층화가 가능한 군 전술 Ad-hoc 네트워크에 공개키 기반 키 관리 기법과 대칭키 기반 키 관리 기법을 접목한 하이브리드 형태의 키 관리 방안을 제안한다. 또한 자원 제약을 받는 하위계층 노드의 빈번한 이동 상황을 고려해 에너지 효율적인 대칭키 기반 키 관리를 위해 하위계층 노드의 위치 정보를 이용하여 상위계층 노드가 일대일 키를 생성하여 배포하는 중앙 통제방식의 키 관리 방식을 제안한다.

본 논문의 구성은 2장에서는 Ad-hoc 네트워크를 위한 키 관리 방안들에 관련한 기존 연구들을 살펴보고, 3장에서는 제안하는 기법이 적용될 TICN체계 구성과 가정사항에 대해 살펴본다. 4장에서는 본 논문에서 제안하는 키 관리 기법에 대해 기술한다. 5장에서는 제안하는 기법에 대해 안전성과 효율성을 분석하고, 6장에서 결론을 맺는다.

Ⅱ. 관련연구

Ad-hoc 네트워크에서의 보안 목표는 기존 네트워크와 유사하게 기밀성, 무결성, 인증, 가용성 등을 보장하는 것이다. 이와 같은 보안문제를 해결하기 위해 해쉬 체인 및 암호화 기법 등을 적용한 보안 라우팅 프로토콜에 대한 연구가 주를 이루고 있다. 즉 노드의 신뢰성을 증명할 수 있는 비밀키를 알고 있는 노드들만 네트워크 서비스에 참여할 수 있도록 하는 접근방법이다. Ad-hoc 네트워크에서의 키관리 기법과 관련된 연구는 크게 공개키 기반과 대칭키 기반 기법으로 분류할 수 있다.

우선, 공개키 기반의 키 관리 기법에 관한 연구들을 살펴보면 다음과 같다. 공개키 기반구조에서 사용자는 공개키와 개인키의 쌍을 간직하며, 메시지 전송시 수신자의 공개키로 암호화하여 전송하면 수신자는 자신의 개인키로 복호화하여 확인한다. 이때 상대방의 공개키가 신뢰성 있는지 여부의 확인을 위해 인증기관(Certificate Authority)의 개인키로 전자서명한 인증서가 활용되어 진다. 대부분의 연구들은 이러한 인증서 관리에 대한 효율성과 안전성에 초점을 맞추고 있다. Shamir는 [4]에서 n개의 비밀조각 중 k개 이상의 조각을 모으면 비밀키를 재구성할 수 있는 다항식을 이용한 (k,n) 임계치 기법을 제안하였고, 이를 Ad-hoc 네트워크에 적용하여 CA의 비밀키를 확인하기 위해서는 최소한 k개 이상의 노드가 협업을 해야만 가능하도록 하는 방법을 Zhou 등이 [5]에서 제안하였다. Yi는 [6]에서 Zhou의 연구를 확장하여 CA의 역할을 담당할 서버 노드를 선택할 때, 노드의 물리적인 안전성 및 자원의 정도를 고려하여 선택할 수 있는 개선된 방식을 제안하였다. Wu 등은 [7]에서 CA의 인증서를 효과적으로 업데이트하기 위한 멀티캐스트 그룹 방식을 제안하여 Yi의 연구를 추가적으로 개선시켰다. 이상의 공개키 기반의 키 관리 기법들은 암호화 강도는 강하여 보안목표 달성에 유리한 장점이 있지만, 암복화에 많은 연산량이 요구되기 때문에 자원 제약을 받는 노드들에게 적용하기에는 아직까지 무리가 따른다.

대칭키 기반의 키 관리 기법은 이동성이 없는 고정된 노드를 위한 키 관리 기법과 이동하는 노드를 위한 키 관리 기법으로 나눠볼 수 있다. 먼저 고정된 노드를 위한 키 관리 방안에 관한 연구들을 살펴보면 다음과 같다. Zhu 등이 [8]에서 제안한 LEAP 방식은 고정된 노드를 위한 대칭키 관리기법으로 기존의 단일키 방식들과는 달리 개인키, 일대일키, 클러스터키, 그룹키의 네 종류의 키를 목적에 맞게 생성 및 관리하는 기법이다. Eschenauer 등은 [9]에서 임의의 두 노드가 사전 정의된 확률을 기반으로 일대일키를 공유할 수 있도록 하는 랜덤 키 사전분배기법을 제안하였다. Chan 등은 [10]에서 랜덤 키 사전분배기법을 기반으로 q개 이상의 키를 공유하고 공유된 키들을 기반으로 일대일 대칭키를 생성함으로써 노드 탈취로 인한 영향을 줄일 수 있는 q-Composite 기법을 제안하였다. 랜덤 키 사전분배방식에서 노드들의 배치 정보를 이

용하여 두 노드간 키 공유 확률을 높일 수 있는 방법을 Du 등과, Lee 등이 각각 [11,12]에서 제안하였다.

이동하는 노드를 위한 대칭키 기반 키관리 기법에 관한 연구들은 다음과 같다. 먼저 Puzar 등은 SKiMPy[13]라는 기법을 통해 비상 구난 상황에서 이동하는 개인 단말 사이에 안전한 통신을 보장할 수 있는 대칭키 기반 키 관리 기법을 제안하였다. SKiMPy 기법은 모든 노드들이 임의의 대칭키를 생성하여 상호 교환을 통해 사전에 정의된 조건을 충족하는 최적키를 결정하고 이를 그룹키로 선정하는 방식을 채택하고 있다. Bouassida 등은 [14]에서 MANET 노드들 사이에 멀티캐스팅을 할 수 있는 그룹 정보를 사전에 구축하여 안전하고 효율적인 그룹키를 생성할 수 있는 기법을 제안하였다. Chuang 등은 [15]에서 전체 네트워크에서 노드들을 그룹 리더와 그룹 멤버로 구성된 클러스터를 형성하여 대칭키와 그룹키를 3단계로 구분하여 설립하는 TDKM(Two-layered Dynamic Key Management) 방식을 제안하였다.

이러한 기존의 연구들은 계층형 전술 Ad-hoc에 그대로 적용하기에는 다음과 같은 제한점이 있다. 먼저 기존 키 관리 기법들은 대부분 비계층적인(Non-Hierarchical) 구조의 Ad-hoc 네트워크를 대상으로 한 연구들이었다. 특히, 전술 Ad-hoc과 같이 네트워크 내에 차별화된 자원과 능력을 가진 노드들이 혼합되어 계층형 네트워크를 구성하는 상황에서 전체 네트워크에 동일한 키 관리 기법을 일률적으로 적용하는 것은 에너지 효율성에서 부정적이다.

둘째로 군의 전술 환경에 적용될 계층형 Ad-hoc 네트워크에서는 임무 특성상 하위계층 노드의 빈번한 이동 상황을 고려해야할 뿐만 아니라 임무 수행을 지속할 수 있도록 키 관리에 있어 에너지 효율적으로 운영되어야만 한다. 하지만 기존의 MANET 환경을 고려한 키 관리 연구들은 비상 구난 상황에서 일시적으로 사용하기 위한 키 관리 기법들이었다. 따라서 노드 이동시에 상대적으로 자원이 부족한 하위계층 노드가 개별적으로 일대일키 생성을 위한 인증 및 키 설립 절차를 매번 반복하는 것은 에너지 비효율적이며 보안에 취약할 수 있다. 또한 하위계층 노드는 매번 생성되는 키를 관리하기 위해 메모리 저장 공간을 많이 필요로 하게 된다.

Ⅲ. 배경지식 및 가정사항

3.1 TICN 체계

TICN 체계는 무선 IP 링크의 격자형 백본을 구성하는 전달망 체계와 이동가입자의 통신소요를 지원하는 전투무선체계로 구분할 수 있다. 전달망 체계를 구성하는 핵심장비는 광대역무선전송장비 (HCTR:High Capacity Trunk Radio)로서 일반적으로 연대급 이상의 상급부대에서 운용한다. 전투무선체계는 하나의 이동가입자접속장비(MSAP: Mobile Subscriber Access Point)에 전술통제수단을 제공하는 무선통신장비인 다대역다기능무전기 (TMMR: Tactical Multi-band Multi- function Radio) 또는 음성 및 데이터 서비스를 제공하는 전술용다기능단말기(TMFT: Tactical Multi-Function Terminal)와 같은 하위 노드들이 연결되는 형태를 지닌다. TICN 체계 구성도(예)는 그림 1과 같다. HCTR과 MSAP는 일반적으로 연대급 이상의 상급 부대에서 운영하게되며 상위계층 노드의 역할을 담당하고, TMMR과 TMFT는 대대 및 중대급 이하의 소부대에서 운영하고 하위계층 노드의 기능을 수행하며 이 구간에서 Ad-hoc 네트워크 기술이 적용될 수 있다.

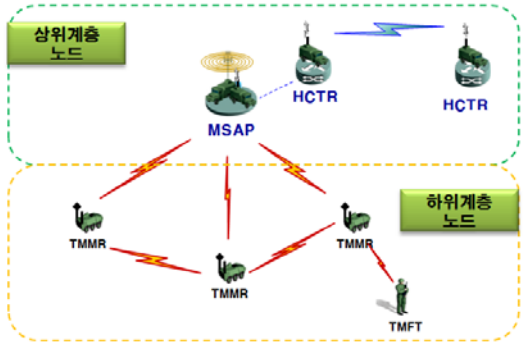

그림 1. TICN 체계 구성도(예)

3.2 가정사항

본 논문에서 제안하는 키 관리 기법은 TICN 체계와 같은 계층형 전술 Ad-hoc 네트워크에 적용되며, 제안하고자 하는 키 관리 기법에서의 기본 가정 사항을 정리하면 다음과 같다.

첫째, 상위계층 노드들은 비교적 충분한 자원과 계산능력이 보장되며 침입탐지 기법을 이용하여 자체 방호 능력을 보유하고 있는 것을 가정한다.

둘째, 하위계층 노드들은 제한된 계산 및 저장 능력을 지니며, 보안 프로토콜 적용에 있어서 노드 생존성 유지를 위해 에너지 효율성이 매우 중요한 요소이다.

셋째, 군의 임무 상황을 고려하여 하위계층 노드의 최초 전개 위치는 일정범위의 지역으로 한정 지을 수 있고 상위계층 노드와 키 설립 이후에는 임무 수행을

위해 이동할 수 있다.

넷째, 모든 노드들은 GPS 장비를 장착하여 자신의 정확한 위치를 식별할 수 있다.

Ⅳ. 제안하는 키 관리 기법

4.1 전체적인 구성

그림 2는 제안하는 계층형 전술 Ad-hoc 네트워크에서의 키 관리 운영 개념도를 도식한 것이다. 자원과 계산 능력이 뛰어난 상위계층 노드의 경우 안전성 측면을 강화한 PKI 기반의 키 관리 기법을, 자원 제약을 많이 받는 하위계층 노드들의 경우에는 에너지 효용성을 고려하여 대칭키 기반의 키 관리 기법을 제안한다.

본 논문에서는 하위계층에서의 임무 수행에 필요한 키를 다음과 같은 세 개로 제안한다.

- 노드키 : 상위계층 노드와 하위계층 노드 상호간 각각 설정되는 키로서 노드들이 배치되면 최초로 생성되는 키이다. 상위계층에서 개별 하위노드에게 임무 부여시나 상위계층에서 생성한 일대일키와 지역키를 분배시에 사용된다.
- 일대일키 : 하위계층 노드들이 1홉 이내의 이웃 노드와 공유하는 키로서 상위계층 노드로부터 질의나 명령을 받은 후 결과를 보고할 때 경로 상의 노드들 사이에서 기밀성, 무결성을 보장한다.
- 지역키 : 하나의 상위계층 노드와 지역내의 하위계층 노드가 함께 공유하는 키로서 매세지 브로드캐스트시 암호화 및 인증에 사용된다.

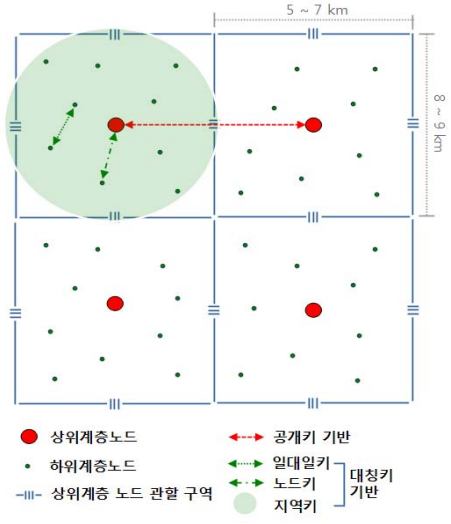

그림 2. 제안하는 키 관리 운영 개념도

4.2 용어 정리

본 논문에서 사용하는 표기법은 표 1과 같다.

표 1. 표기법

표기법	의 미
A, B ...	상위계층 노드
n1, n2 ...	하위계층 노드
$CERT_A$	TTP가 상위계층 노드에게 배부한 인증서
PK_A, SK_A	상위계층 노드의 공개키, 비밀키
N_A	노드 A가 생성한 Nonce
H(M)	메시지 M에 대한 해쉬함수 결과
F()	일방향 해쉬 함수
K_{An1}	상~하위계층 노드 사이의 노드키
K_{n1n2}	하위계층 노드 사이의 일대일키
K_{RA}	상위계층 노드 A의 지역키
L_{n1}	노드 n1의 x, y 좌표 정보
K_{ini}^{n1}	하위계층 노드의 초기 보안키

4.3 키 및 인증서 선분배 단계

노드들은 필드에 배치되기 전 오프라인에서 신뢰할 수 있는 제3자(TTP : Trusted Third Party)로부터 필요한 키와 인증서를 배부 받는다. 제안하는 기법에서는 군의 임무 특성을 고려하여 전술 Ad-hoc을 운영하는 최상급 부대인 사/군단급 제대가 인증기관(CA : Certification Authority)의 역할을 수행한다. CA는 모든 상위계층 노드의 ID와 공개키 바인딩 테이블을 유지한다. 상위계층 노드들은 CA로부터 PK_A, SK_A, $CERT_A$, PK_{CA}와 지역내 하위계층 노드의 ID, 초기 보안키 바인딩 테이블을 분배받는다. $CERT_A = E_{sk_{CA}}[ID_A \| PK_A \| T_{sign} \| T_{\exp ire}]$ 과 같으며, T_{sign}은 인증서 발급시간을 $T_{\exp ire}$는 만료시간을 의미한다. 하위계층 노드는 초기 보안키 K_{ini}^{n1}를 배부 받는다.

4.4 상위계층 노드의 키 관리

상위계층 노드에서는 대칭키 기반의 키 관리 기법이 아닌 일반적인 공개키 기반의 키 관리 기법을 적용한다.

4.4.1 인증서 확인 및 공개키 획득

상위계층 노드 사이의 인증절차는 그림 3과 같다.

4.4.2 세션키 생성

획득된 공개키를 활용하여 상위계층 노드들은 그림 4와 같은 절차를 통해 세션키를 생성하며 한 통신주

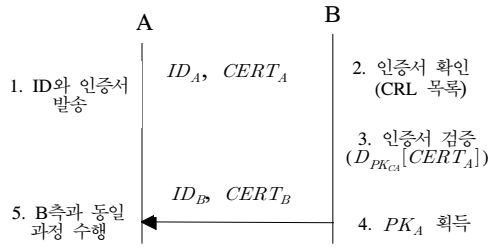

그림 3. 인증서 확인 및 공개키 획득 절차

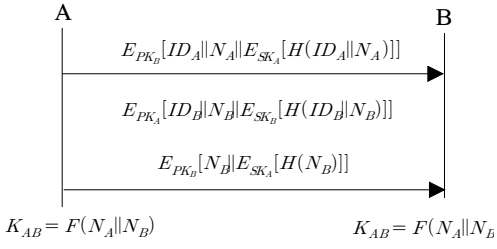

그림 4. 세션키 생성 절차

기 동안에 사용한다. 제안하는 세션키 생성 기법은 송신 노드가 메시지를 전송할 때 전체 메시지에 대해 공개키로 암호화하여 기밀성을 유지하며, 추가적으로 $H(ID_A||N_A)$ 값에 송신자의 비밀키(SK_A)로 암호화하는 전자서명 방식을 접목하여 인증 및 부인방지, 무결성 검증이 가능하다.

4.4.3 인증서 폐기

특정 노드가 공격자에 의해 포획되거나 기능을 상실했음을 탐지하면 해당 인증서의 효력을 상실시키고 인증서 폐기 및 취소 목록(CRL : Certificate Revocation List)에 기록 유지한다.

4.4.4 인증서 갱신

인증서 갱신은 사전에 정의된 지수 $T_{refresh}$ 값을 활용한다. 이 지수와 인증서 생성시간과 만료시간은 $T_{\exp ire} \le (T_{sign} + T_{refresh})$ 의 관계가 있고, 모든 인증서 소유자는 인증서 만료시간 내에 인증서를 갱신한다.

4.5 하위계층 노드의 키 관리

하위계층 노드의 키 관리는 노드의 에너지 효율성과 보안성을 함께 고려하여 대칭키 기반의 키 관리 기법을 적용한다. 특히, 군 전술환경을 고려하여 빈번하게 이동하는 노드에 대한 대칭키 생성의 효율성과 보안 취약성 해소를 위해 본 논문에서는 하위계층 노드의 위치 정보를 이용하여 상위계층 노드에서 일대일 키를 생성하고 노드키로 암호화하여 분배하는 새로운 키 관리 방식을 제안한다.

4.5.1 노드키 설립

노드키 설립 절차는 그림 5와 같다. 먼저 하위계층 노드들이 지역내에 배치되면 상위계층 노드들은 자신을 알리는 beacon 신호를 전송하게 된다. 하위계층 노드는 신호세기가 가장 센 상위계층 노드에게 자신의 ID와 Nonce 그리고 무결성 확인을 위한 H(ID||Nonce) 해쉬값을 초기 보안키로 암호화 하여 전송한다. 상위계층 노드는 초기 보안키 바인딩 테이블을 이용하여 노드 인증 및 데이터 무결성 검증을 실시하게 되고 이상이 없으면 노드키(K_{An1})를 생성하여 초기 보안키로 암호화하여 재전송한다. 하위계층 노드는 전송받은 노드키를 이용하여 정상적으로 수신하였음을 알리고 초기 보안키는 삭제한다.

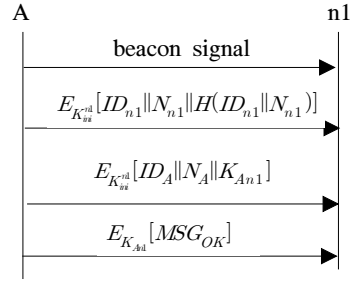

그림 5. 노드키 설립 절차

4.5.2 지역키 설립

상위계층 노드와 하위계층 노드 사이에 노드키가 설립되면, 그림 6처럼 상위계층 노드는 지역키(K_{RA})를 생성하여 노드키로 암호화하여 전송하게 된다.

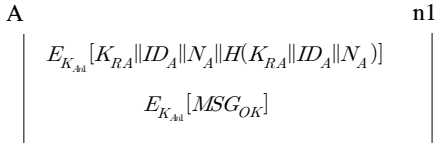

그림 6. 지역키 설립 절차

4.5.3 일대일키 설립

본 논문에서 제안하는 키 관리 기법은 필드에 배치되는 모든 노드들은 GPS를 장착하여 운영됨을 가정하고 있다. 상위계층 노드와 하위계층 노드 사이에 노드키와 지역키가 설립된 이후에 지역내 1홉 거리의 이웃 노드들간 일대일키 설립 과정은 다음의 절차를 따른다.

- 단계 1 : 먼저 하위계층 노드들은 자신의 좌표 L_{n1} (x_{n1},y_{n1}) 정보를 노드키로 암호화하여 상위계층 노드에게 전송한다.
- 단계 2 : 상위계층 노드들은 지역내 모든 노드들의 위치정보를 수집하고, 인접 상위계층 노드들과 상호 교환한다.
- 단계 3 : 사전에 정의된 일대일키 설립을 위한 임계 거리 이내의 노드간 일대일키를 생성하여 노드키로 암호화해서 전송한다. 이때 하위계층 노드의 저장공간을 고려하여 이웃 노드간 최단 거리 순으로 최대 5개의 일대일키를 생성하여 배포한다.

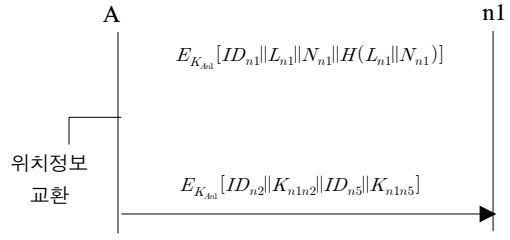

그림 7. 일대일키 설립 절차

4.6 노드 이동에 따른 인증 및 키 갱신

하위계층 노드들은 초기 키 설립이 완료되면 임무 수행에 필요한 이동이 가능하다. 이때 사전에 설정된 임계 거리 이상을 이동하면 상위계층 노드에게 자신의 변동된 위치정보를 노드키로 암호화하여 전송한다.

상위계층 노드는 하위계층 노드로부터 변경된 위치 정보를 수신하면 인접 노드의 위치 정보를 고려하여 일대일키를 재생성하여 분배한다.

만약 하위계층 노드가 새로운 상위계층 노드로부터 신호 강도가 강한 beacon 신호를 수신하면, 기존 상위계층 노드의 관할 지역을 이탈한 것으로 판단하게 되며 그림 8과 같은 인증 및 키 갱신 절차에 들어가게 된다. 먼저 하위계층 노드 n1은 자신의 ID와 가장 최근에 보고한 최종 위치 정보인 L_{n1-old}을 바뀐 관할지역 상위계층 노드 B에게 기존 노드키로 암호화해서 전송한다. 노드 B는 이를 인접 상위계층 노드들에게 전송한다. 노드 A가 $E_{SK_A}[E_{K_{Ain1}}[ID_{n1}||L_{n1-old}]]$ 메시지를 수신하면, 해당 메시지를 복호화하여 노드 n1에 해당되는 최종 위치 정보를 비교 확인함으로써 해당 노드를 인증하게 되며, 그 결과를 B에게 전송한다. 이때 노드키 K_{An1}를 공개키로 암호화하여 전송한다. 노드 B는 새로운 노드키(K_{Bn1})와 지역키(K_{RB})를 생성하여 기존 노드키(K_{An1})로 암호화하여 노드 n1에게 전송한다. 노드 n1은 새로 분배받은 노드키(K_{Bn1})로 자신의 ID와 위치정보를 암호화하여 상위계층 노드 B에게 전송하고, 노드 B는 일대일키를 생성하여 배포한다.

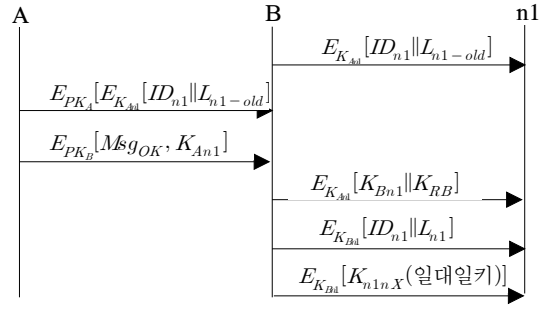

그림 8. 지역 이탈시 인증 및 키 갱신 절차

4.7 노드 추가 및 삭제에 따른 키 갱신

추가되는 하위계층 노드들은 필드에 배치되기 전 오프라인에서 지정된 영역의 상위계층 노드와 통신할 초기 보안키를 할당받는다. 필드 배치 후 상위계층 노드와 초기 보안키를 이용한 암호통신을 통해 노드키, 인증서, 지역키, 일대일키를 배부받아 네트워크에 정상적으로 참여할 수 있다.

하위계층 노드들은 외부 공격자에 의해 잠식되어 비정상행위를 할 수 있다. 이러한 비정상행위 노드가 탐지되면 네트워크의 안전성 유지를 위해 잠식된 노드와 관련된 키에 대한 갱신 절차가 필요하다. 본 논문에서 제안하는 키 갱신절차는 다음과 같다.

- 단계 1 (일대일키 삭제) : 일단 상위계층 노드가 잠식된 노드를 탐지하게 되면, 해당 노드와 일대일키를 유지하고 있는 인접 노드에게 노드키를 이용한 보안통신을 통해 일대일키 삭제를 통보하여 해당 노드를 네트워크로부터 고립시킨다.
- 단계 2 (지역키 갱신) : 상위계층 노드는 새로운 지역키를 재생성하여 잠식된 노드를 제외한 관할 지역내 모든 노드에게 전파한다.
- 단계 3 (노드키 삭제) : 상위계층 노드에서 유지하던 잠식된 노드의 노드키를 삭제한다.
- 단계 4 (인접 상위계층 노드에게 전파) : 잠식된 노드에 대한 정보를 인접한 상위계층 노드에게 전파하여 해당 노드가 이동하여 네트워크에 참여할 수 없도록 한다.

V. 성능 분석

키 관리 방식에 따라 높은 안전성 보장은 에너지

효율성을 저하시키는 경우가 대부분이다. 본 연구에서는 제안하는 키 관리 방식은 계층별 서로 상이한 자원으로 임무를 수행하는 군의 특수 상황을 고려하여 계층별 차별화된 키 관리 방식을 제안하고 있다. 본 논문에서는 상위계층 노드의 에너지는 충분함을 가정하여 일반적인 공개키 기반의 암호화 기법을 적용하고 있음으로 성능분석에 있어서는 하위계층 노드에만 국한하여 실시하며, 안전성과 효율성 측면에서 각각 분석을 실시한다.

5.1 안전성 분석

본 논문에서는 상위계층 노드가 비정상 행위를 하는 하위계층 노드를 탐지할 수 있는 침입탐지시스템을 보유하고 있는 것을 가정하고 있다. 따라서 Ad-hoc 네트워크에게 발생할 수 있는 Wormhole 공격, Sybil 공격, Sinkhole 공격, Spoofing 공격, Altering 공격 등을 하는 노드를 상위계층 노드가 탐지하면 본 논문에서 제안하고 있는 키 갱신 절차에 따라 잠식된 노드의 키를 삭제하고, 새로운 키를 생성하여 안전하게 배포하여 잠식된 노드를 네트워크로부터 고립시킬 수 있어 키 관리에 있어 전후방 안전성 확보가 가능하다.

5.2 효율성 분석

하위계층 노드에서 노드키, 지역키, 일대일키를 생성함에 있어서의 효율성을 측정하기 위해 통신비용, 저장공간 요구량에 대해 본 논문에서 제안하는 기법과 유사한 대칭키 기반 키 관리 기법인 LEAP 그리고 이동형 Ad-hoc 네트워크 기반의 대칭키 관리 기법인 TDKM과 각각 성능 비교를 실시한다.

5.2.1 통신비용

통신비용은 각 노드가 키 설정을 위해 주고받는 메시지의 횟수에 비례한다. 네트워크 전체 사이즈를 N, 이웃 노드와의 밀집도를 d라고 할 때 LEAP의 경우는 각 노드들이 인접 이웃 노드와의 직접적인 통신으로 키를 생성하는 방식으로 통신비용은 전체 네트워크 사이즈에는 반비례하고 밀집도의 제곱근에 비례하는 아래 식 (1)의 관계를 가진다.

$$\text{통신비용} = (d-1)^2/(N-1) \quad (1)$$

전체 네트워크 사이즈 N에서 k개의 클러스터가 존재하고, 각 클러스터에 n개의 멤버노드가 존재한다고 가정하면, TDKM의 경우 일대일키와 지역키를 생성하기 위한 전체 통신비용은 아래 식 (2)와 같다. 즉, 일대일키 설정을 위한 통신비용은 각 클러스터 별로 멤버 노드 사이에 서로 다른 대칭키를 설정하는 비용이며, 지역키 설정을 위한 통신비용은 각 클러스터 별로 멤버 노드에게 그룹키를 전달하는 비용이다.

$$\text{통신비용} = k \times n(n-1) + k \times n \quad (2)$$

여기서 n = N/k 이므로, TDKM의 통신비용은 N^2/k로 다시 표현할 수 있다. 즉 전체 네트워크 사이즈의 제곱근에 비례하며 클러스터 수에 반비례한다. 반면, 제안하는 기법의 경우 노드키, 지역키, 일대일키 생성을 위한 전체 통신비용은 아래 식 (3)과 같다.

$$\text{통신비용} = 3N + 2N + 2N \quad (3)$$

즉, 제안하는 기법은 상위계층 노드에서 키를 생성하여 배포하는 특성으로 인해 이웃 노드와의 밀집도와 관계없이 일정한 통신비용을 유지하게 되며 특히 각 노드에서 소요되던 키 생성 비용도 없게 되는 장점을 지닌다.

일반적으로 전체 네트워크 사이즈가 N일 때 클러스터의 수 k는 N의 5% 범위 이내로 설정함으로 N에 비해 k를 상대적인 상수로 가정하면, 통신비용 복잡도를 제안하는 기법은 $O(N)$, TDKM는 $O(N^2)$으로 표현할 수 있다. 또한 네트워크 사이즈 N이 일정한 상수 값이라고 가정하면 그림 9와 같이 통신비용 복잡도를 LEAP은 $O(d^2)$, 제안하는 기법은 $O(1)$로 나타낼 수 있으며, 제안하는 기법이 효율적임을 알 수 있다.

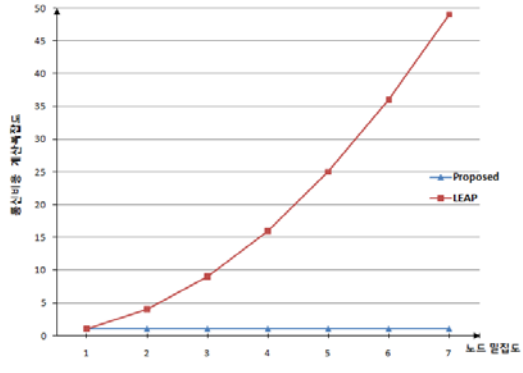

그림 9. 통신비용 계산복잡도 비교

5.2.2 저장공간 요구량

저장공간 요구량은 각 노드가 저장해야할 키의 개수에 비례한다. 네트워크 전체 사이즈 N, 클러스터 수

k, 멤버 노드 수 n, 노드 밀집도를 d라고 할 때, LEAP 기법의 경우 1개의 개인키, 1개의 그룹키, d개의 일대일키와 d개의 클러스터키를 각 노드가 유지해야 한다. TDKM 기법은 n-1개의 일대일키와 1개의 그룹키를 각 노드가 유지해야 한다. 반면 제안하는 기법은 최대 5개의 일대일키, 1개의 노드키, 1개의 지역키와 자신의 최종 위치정보를 하위계층 노드가 유지하게 된다. 제안하는 기법과 LEAP, TDKM의 저장공간 요구량을 비교하면 표 2와 같다. 일반적으로 클러스터 헤더를 전체 노드의 5% 범위 이내에서 선정함을 고려할 때, 전체 네트워크 사이즈 200, 클러스터 수 10, 멤버 노드 수 20, 노드 밀집도 10, 키 사이즈 4Byte, 위치좌표 사이즈 2Byte인 경우를 고려하면 LEAP의 경우 88Byte, TDKM의 경우 80Byte의 저장 공간을 필요로 하는 반면, 제안하는 기법은 최대 30Byte의 저장공간 만을 요구하게 됨으로 상대적으로 매우 효율적임을 알 수 있다.

표 2. 저장공간 요구량 비교

비 고	저장공간 요구량
제안하는 기법	최대 8
LEAP	2d + 2
TDKM	n

Ⅵ. 결 론

향후 우리 군에 도입될 TICN체계에 적용될 Ad-hoc 네트워크 기술은 고정된 인프라가 존재하지 않는다는 점과 연산 능력 및 배터리 용량이 적은 이동성 있는 노드들로 구성된다는 점 때문에 기존의 보안 메커니즘을 그대로 적용할 수 없다. 특히 군에 적용될 전술 Ad-hoc의 경우 상위계층 노드의 경우 비교적 충분한 자원과 계산능력이 보장되는 반면 하위계층 노드들은 자원 제약으로 인해 노드의 수명 주기 연장과 안전성을 동시에 고려한 키 관리 기법이 요구된다. 이에 본 논문에서는 상위계층 노드에서는 공개키 기반의 키 관리 기법을 하위계층 노드에서는 대칭키 기반의 키 관리 기법을 제안하였다. 특히 하위계층 노드의 경우 군의 특성상 빈번한 이동을 고려하여 에너지 효율성과 보안성을 함께 강화하기 위해 하위계층 노드의 위치를 기반으로 상위계층 노드가 일대일키를 생성하여 분배하는 새로운 키 관리 방식을 제안하였으며, 성능 분석을 통해 그 안전성과 효율성을 입증하였다.

향후에는 상위계층 노드의 기능 결함에 따른 안전한 대체 방안 및 GPS가 없는 하위계층 노드에 대한 키 설립 방안에 대한 연구를 추가로 실시할 예정이다.

참 고 문 헌

〔1〕 A. M. Hegland, E. Winjum, S.F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks" *IEEE Communications Surverys & Tutorials*, 3rd Quarter 2006

〔2〕 M. Bohge, and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks", *In ACM workshop on Wireless Security*, 2003

〔3〕 Y. Cheng, D.P. Agrwal, "An improved key distribution mechanism for large-scale hierachical wireless sensor networks," *Journal of Ad Hoc Networks*, vol. 5, pp. 35-48, 2007

〔4〕 A. Shamir, "How to Share a Secret," *Communication of ACM*, vol. 22, pp.612-613 Nov. 1979

〔5〕 L. Zhou and Z.J. Haas, "*Securing Ad Hoc Network*," IEEE Networking Mag., vol.13, pp.24-30, Nov. 1999

〔6〕 S. Yi and R. Kravets, "MOCA: MObile Certificate Authority for Wireless Ad Hoc Networks," *in Proceedings of 2nd Annual PKI Research Workshop*, pp. 65-79, April, 2003

〔7〕 B. Wu, J. Wu, E.B. Fernandez, M. Ilyas, S. Magliveras, "Secure and efficient key management in mobile ad hoc network," *Journal of Network and Computer Applications*, vol 30, pp. 937-954, August 2007

〔8〕 S. Zhu, S. Setia, and S.Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *in Proceeding of CSS'03*, 2003

〔9〕 L. Eschenauer, and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *in Proceeding of 9th ACM conference on CCS*, Nov. 2002

〔10〕 H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," *IEEE Symp. Security and Privacy*, pp. 197-213, 2003

〔11〕 W. Du, J. Deng, Y.S. han, S. Chen, and P. Varshney, “A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowlege,” *in Proceeding of IEEE INFOCOM*, pp. 586-597, 2004

〔12〕 J. Lee, T. Kwon, and J. Song, “Location-Aware Key Management using multi-layer grids for WSN,” *Applied Cryptography and Network Security ’06, LNCS 3989*, pp. 390-404, 2006

〔13〕 M. Puzar, J. Andersson, T. Plagemann, Y. Roudier, “SKiMPy; A Simple Key Management Protocol for MANETs in Emergency and Rescure Operations,” *in Proceeding of ESAS ’05*, 2005

〔14〕 M. Bouassida, I. Chrisment, and O. Festor, “Group Key Management in MANETs,” *International Journal of Network Security*, Vol.6, No.1, pp. 67-79, Jan. 2008

〔15〕 I. Chuang, W. Su, C. Wu, J. Hsu and Y. Kuo, “Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks,” *in Proceedings of IEEE Wireless Communications and Networking Conference*, pp.4145-4150, March 2007

〔16〕 박귀순, 황정섭, “미래 전장 환경변화에 따른 TICN 체계 요구 기능 및 능력,” *Telecommunications review*, 제 20권, 2호, pp.196-206, 4월, 2010년.

이 윤 호 (Yunho Lee) 정회원

1999년 2월 육군사관학교 전자공학과 학사

2005년 2월 서울대학교 컴퓨터공학과 석사

2009년 1월~현재 국방대학교 국방정보체계 박사과정

<관심분야> 무선통신보안, 키 관리, 침입탐지

이 수 진 (Soojin Lee) 정회원

1992년 2월 육군사관학교 전산학과 학사

1996년 2월 연세대학교 컴퓨터과학과 석사

2006년 2월 한국과학기술원 전산학과 박사

2006년 3월~현재 국방대학교 국방정보체계학과 교수

<관심분야> 침입탐지, 무선통신보안, 키 관리, 보안정책