한국군사과학기술학회지 제12권 제3호, pp. 317~324, 2009년 6월

학술논문 정보기술 부문

전술 Ad-hoc 네트워크에서의 효율적인 키 관리 기법

An Efficient Key Management Scheme in Tactical Ad-Hoc Network

김 은 호* 이 수 진**
Eun-ho Kim Soojin Lee

Abstract

Tactical Information Communication Network(TICN) uses both a wireless and wired network. To support mobility in battlefield environments, the application of Ad-hoc networking technology to its wireless communication has been examined. However, Ad-hoc network is faced to many security threats due to its intrinsic characteristics. Therefore, to apply the Ad-hoc networking technology to battlefield environments and TICN, an intensive study on security countermeasure must go side by side with the development of enabling technology. In this paper, we suggest an efficient key management scheme for TICN of which the Ad-hoc networking technology is applied.

Keywords : Tactical Information Communication Network(TICN), Ad-Hoc Network, Key Management, Pairwise Key(일대일키), Node Key(노드키), Region Key(지역키)

1. 서 론

전술종합정보통신망(TICN : Tactical Information Communication Networks)은 첨단 네트워크를 통하여 전투 능력을 극대화할 수 있도록 지휘통제·무기체계 등 각 체계들이 유선과 무선으로 거미줄같이 연결된 전술통신 기반체계로서, 미래의 전장 환경에서 전장정보를 신속·정확하게 수집하여 최하위 전투원으로부터 최상급 제대의 지휘관에게 이르기까지 실시간으로 제공하는 핵심이 될 것이다[1]. 이러한 TICN의 개발을 위해 우리 군은 각종 기반기술과 운용 시나리오의 개발을 위한 연구를 적극적으로 추진하고 있으며, 무선 네트워크 구간에서는 기존에 제안되었던 Ad-hoc 네트워크 기술의 적용을 검토하고 있다.

Ad-hoc 네트워크는 기존의 기반시설이 없는 환경에서도 자체적인 네트워크 구성 및 유지가 가능하다는 장점 때문에 많은 관심과 연구의 대상이 되어 왔다. 그러나 Ad-hoc 네트워크는 유선 네트워크가 가지지 않는 고유한 특성들로 인해 각종 보안위협에 쉽게 노출될 가능성이 상존한다.

무선 매체 사용에 의한 보안 위협, 각 노드에 대한 물리적 보호의 한계, 노드 이동성에 의한 토폴로지의 동적인 변화 등 보안에 위협을 줄 수 있는 요소들이 네트워크 운용 간 계속적으로 존재하며, 특히 TICN 운용환경이 보안성이 극도로 요구되는 전장 환경임을 고려해 볼 때 그 위험성은 더욱 증가할 것이다. 그리고 이러한 보안 위협 요소들은 각종 전장정보의 유출,

† 2009년 2월 25일 접수~2009년 4월 17일 게재승인
* 육군전투지휘훈련단(BCTP)
** 국방대학교(KNDU)
책임저자 : 김은호(remove00@gmail.com)

부대 배치나 전장상황에 대한 노출로까지 이어져 전쟁의 승패를 좌우할 수도 있게 된다.

그러므로 Ad-hoc 네트워크를 전장 환경에 적용하기 위해서는 기반기술에 대한 연구와 함께 보안대책에 대한 연구도 반드시 병행되어야 한다. 특히, 전장상황 하에서 유통될 각종 민감 정보들에 대한 기밀성, 무결성 등을 보장할 수 있는 신뢰성 있는 라우팅 기술이 연구되어야 할 것이며, 정당한 권한을 가지지 못한 노드들의 네트워크 참여와 악의적 공격 행위를 사전에 차단할 수 있는 인증기술이나 침입탐지 기술도 연구되어야 할 것이다.

따라서 본 논문에서는 신뢰성 있는 라우팅 및 인증을 제공하기 위한 기반으로서 Ad-hoc 네트워크 기술을 기반으로 하는 TICN에 적합한 키 관리 기법을 제안하고자 한다. 제안된 키 관리 기법은 TICN에서 운용되는 무선 단말 노드의 제한적 성능을 고려 대칭키 기반의 키 관리 정책을 취하고 있다. 그리고 단일 비밀키의 계속적인 사용에 의한 키 노출과 통신 간 사용될 세션키 설정과정에서의 키 관련정보 노출을 방지하기 위해 확률적 키 공유기법을 적용하였으며, TICN의 계층적 네트워크 특성을 고려하여 일대일키, 노드키, 지역키로 계층화된 키 관리 구조를 취함으로써 보안성과 효율성을 향상시킨다.

2. 전술종합정보통신망(TICN)

가. TICN의 체계 구성

TICN 체계는 무선 IP 링크의 격자형 백본을 구성하는 전달망, 이동가입자의 통신소요를 지원하는 전술이동통신망, 전투무선망을 기본으로 구분할 수 있다.

각 부체계를 구성하는 핵심장비는 광대역무선전송장비(HCTR : High Capacity Trunk Radio), 전술용 라우터, 전술용교환기, 전술이동통신장비 등으로 나뉘며, 그 중 전술이동통신장비는 서비스의 교환·제어 기능과 무선접속기능(기지국)을 지원하는 이동가입자접속장비(MSAP : Mobile Subscriber Access Point)와 음성 및 데이터 서비스를 수행할 수 있는 전술용다기능단말기(TMFT : Tactical Multi-Function Terminal), 전술지휘 및 통제수단을 제공하는 무선통신장비인 다대역다기능무전기(TMMR : Tactical Multi-band Multi-role Radio)로 구성된다[2].

나. TICN에서의 Ad-hoc 네트워크 운용

TICN 체계의 하위구조는 하나의 MSAP에 수많은 노드인 TMFT, TMMR이 연결되는 형태로, 말단 병사가 휴대하고 있는 노드(TMFT 및 TMMR)를 가지고 자료를 수집하여 상위 제대로 전송하면 MSAP에서 집결하여 전술라우터 및 전술용교환기를 거쳐 HCTR을 통해 전파하는 형태이다.

Ad-hoc 네트워크는 TICN 운용개념의 핵심으로서, 전술환경에서의 신속한 이동성을 보장하고, 수분 내 네트워크 환경 하에서의 작전이 가능할 수 있도록 지원할 것이다[3]. 그리고 네트워크 밀집도가 유동적이고 링크 연결 상태가 비대칭적이며, 적으로부터 재밍이 발생되는 상황에서도 아군의 망을 자생적으로 재구성하고, 안전하게 전술정보를 전송할 수 있도록 해주는 기반이 될 것이다[4,5].

다. TICN에서의 정보보호 요구사항

TICN에서의 정보보호 요구사항은 일반적인 보안목표와도 부합하는 기밀성, 무결성, 가용성, 인증성 및 부인방지 등을 보장하는 것으로 내부 또는 외부의 침입자에 의한 정보의 파괴, 변조, 불법유출 등의 위협으로부터 정보를 보호하는 것이다[6].

3. TICN에 적합한 키 관리 기법

TICN에 적합한 키 관리 기법을 제안하기 위한 설계 중점으로 체계를 구성하는 이동 단말들의 성능을 고려하여 빠른 연산 속도와 키 관리를 위한 별도의 구성요소가 불필요한 대칭키 기반의 키 관리 기법[7,8]을 적용하였으며, 기존의 단일 비밀키 위협에 대한 단점을 극복하기 위해 확률적 키 공유 기법을 적용하였다. 또한 TICN 네트워크의 계층적 구조와 소통되는 다양한 메시지의 형태 및 보안수준을 고려하여 계층적 구조의 키 관리 기법을 채택하였다.

가. 전체적인 구성 및 가정

현재 TMMR은 MSAP 및 TMMR 상호간에는 peer-to-peer 방식으로 통신이 가능하나 TMFT는 MSAP를 접속점으로 연결·운용된다. 따라서 본 논문에서는 MSAP와 TMMR만을 대상으로 Ad-hoc 네트워크 구성이 가능하다는 전제하에 키 관리 기법을 제안하며 TICN에 적합한 키 관리 기법을 제안하기 위한 설계

중점을 고려하여 일대일키, 노드키, 지역키의 세 개의 키로 구분한다. 각 키의 운용개념은 다음과 같다.

1) 일대일키(Pair-wise Key)

노드가 지역 내 한 홉 이내의 노드와 공유하는 키로서 상위계층으로부터 질의나 명령을 받은 후 결과를 상위계층에 보고할 때 경로 상의 노드들 사이에서 데이터의 무결성을 보장한다.

이때 지역 내의 상위계층 노드 역시 하나의 노드로 간주하여 일대일키를 생성한다.

2) 노드키(Node Key)

지역 내 각각의 노드가 상위계층 노드와 공유하는 키로서 이동노드가 수집된 정보를 상위계층의 노드로 보고시 데이터의 암호화나 지역키의 갱신과 같은 민감한 데이터의 암호화에 이용한다. 예를 들어 TICN에서는 이동노드가 수집한 적의 이동상황, TOT를 위한 적 부대위치, 화생방 오염지대 확인 등의 정보를 보고할 때 사용될 수 있다.

3) 지역키(Region Key)

하나의 상위계층 노드가 관리하는 지역 내의 상위계층 노드와 이동 노드가 공유하는 키이며, 상위계층 노드가 지역 내의 노드들에게 질의나 명령을 브로드캐스트 메시지로 전달할 때 메시지의 암호화 및 인증에 활용한다. 전술적 상황에서는 상위노드에서 하위노드로 일제히 신속하게 전달해야 하는 작전명령이나 혹은 각 노드가 배치된 지역의 상황을 파악하기 위한 질의 등이 빈번하게 발생할 수 있는데, 이러한 경우에 지역키를 이용하여 해당 메시지를 지역 내로 브로드캐스트하면 된다.

각 키의 운용 개념도는 Fig. 1에서 보는 바와 같으며, 본 논문에서 제안하고자 하는 키 관리 기법에서의 기본 가정 사항들을 정리하면 다음과 같다.

첫째, 노드는 다소 제한된 저장용량, 계산능력, 통신능력을 가지며 랜덤하게 배치되고, 배치된 후 상위계층 노드가 지원하는 지역범위 내에서 고정 및 이동하며 운용된다. 또한, 상위계층 노드는 할당된 지역을 자유롭게 이동할 수 있으며 할당된 지역 내의 모든 노드들과 일방향 한 홉 통신이 가능하고 충분한 저장공간과 계산능력을 갖고 있다.

둘째, 무선통신의 취약성으로 인해 모든 무선 통신 패킷은 악의적인 공격자에게 노출될 수 있고 상위계층 노드는 악의적인 공격자의 공격을 탐지할 수 있는 능력을 가진다. 또한, 상위계층 노드는 자체적으로 충분히 안전성을 확보할 수 있다.

셋째, 모든 노드들은 배치되기 전 키 생성을 위해 확률적 키 공유 기법에 의해 믿을 수 있는 제 3자인 상위제대 키 관리 서버로부터 대량의 오프라인 키 집합에서 부분키 집합을 할당받아 저장하고, 의사난수 함수와 강력한 암호화 알고리즘을 내장한다.

마지막으로 노드의 초기배치나 추가 시 악의적인 공격자에게 노드가 포획되어 사전 저장된 키 정보가 노출되는 시간 T_{exposure}는 노드가 이웃노드를 발견하고 키를 설립하는 시간 $T_{discovery}$보다 항상 크다.

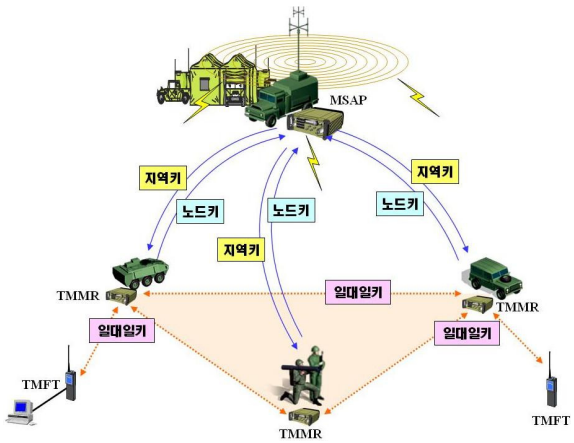

Fig. 1. 계층적 키 관리 운영 개념도

나. 계층별 키 관리 구조 제안

1) 오프라인 키 선 분배

각 노드는 필드에 배치되기 전에 L개의 키로 구성된 키 집합(Key Pool)에서 m개의 서로 다른 비밀키로 구성된 부분키 집합을 오프라인 상의 키 관리 서버로부터 분배받는다[9,10].

확률적 키 공유기법을 적용함에 있어서는 L과 m의 값이 중요한 의미를 가짐으로 우선 L과 m의 관계를 확률적 모델링에 의해 분석해 보고자 한다.

만약 임의의 두 노드 간에 공유되는 키가 1개뿐이라고 가정했을 경우 인접된 두 노드 간에는 공유키가 존재할 수도 있고 존재하지 않을 수도 있어 노드 연결성에 문제가 발생한다. 반면, 공유키가 많으면 임의의 두 노드 간 연결성은 높아지지만, 각 노드가 저장해야 할 부분키 집합의 양은 증가하기 때문에 하나의

노드가 공격자에 의해 잠식되었을 때에는 L에서 많은 부분이 공격자에게 노출된다. 따라서 노드 잠식 시 키 집합 L에서 노출되는 정보를 최소화하면서도 임의의 두 노드간의 연결성을 최대화할 수 있도록 공유키의 개수와 L, m의 값은 결정되어야 한다.

우선 MSAP의 최하 운용부대가 대대급이며, 1대의 MSAP에 다수의 TMMR이 운용된다고 가정하였고, 공유키 K의 개수를 3개로 설정하여 L과 m의 관계에 대한 분석을 실시하였다. 분석 결과 임의의 두 노드 사이에 3개의 비밀키들을 공유할 확률은 식 (1)과 같고, 이를 그래프로 표시하면 Fig. 2와 같다.

$$P_s(3) = \frac{C_3^L C_{2(m-3)}^{L-3} C_{m-3}^{2(m-3)}}{(C_m^L)^2} \quad (1)$$

이 그래프를 통해 L이 고정된 상태에서 m의 값이 변할 때 임의의 두 노드 사이에 3개의 키를 공유할 확률을 알 수 있다.

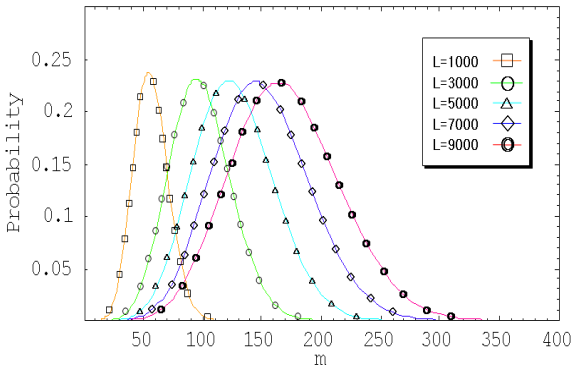

Fig. 2. L값에 대한 m의 확률(k=3일 경우)

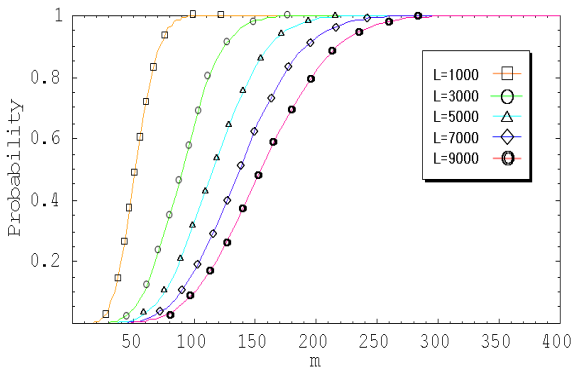

Fig. 3. L값에 대한 m의 누적확률(k=3일 경우)

2) 일대일키(Pair-wise Key)의 설립

일대일키는 노드가 자신과 한 홉 거리의 노드들과 공유하는 키를 의미하며 전체 네트워크를 대상으로 하여 노드, 상위계층 노드 구분없이 모두 동일한 노드로서 키 설립에 참여한다. 본 논문에서 사용되는 표기법을 정리하면 Table 1과 같으며, 일대일키의 설립 절차를 도식화하면 Fig. 4와 같다.

Table 1. 제안하는 프로토콜에서 사용되는 표기법

구 분	설 명
ID_{S_i}	노드 S_i의 ID
A	상위계층 노드
MSG[1||2]	메시지 M1과 M2의 결합
Ek[msg]	키 k를 이용하여 msg를 암호화
Dk[msg]	키 k를 이용하여 msg를 복호화
MAC(key,msg)	key에 의해 생성된 msg 인증코드
F_K	의사 난수 함수
K_i	부분키 집합 내의 상호 공유키
N_{S_1}	노드 S_1이 생성한 난수
K_{S_i}	노드 S_i의 공유키
$K_{S_1S_2}$	노드 S_1과 S_2 사이의 일대일키
K_{N_i}	상위노드A와 노드S_i 사이의 노드키
K_{Ri}	상위노드A와 노드S 사이의 지역키

3) 노드키(Node Key)의 설립

노드키는 상위계층 노드가 지역 내의 각각의 노드와 공유하는 키로서, 노드 S_i와 상위계층 노드 A 사이의 노드키 설립절차를 도식화하면 Fig. 5와 같다.

노드키를 설립 후 상위계층 노드는 지역 내 노드들의 ID와 노드키를 바인딩 테이블에 기록 유지한다. Table 2는 바인딩 테이블의 예이다. 상위계층 노드는 충분한 저장공간과 계산능력 및 안전성을 확보하고 있으므로 바인딩 테이블의 유지는 상위계층 노드에게 운용상의 부담을 주지는 않는다.

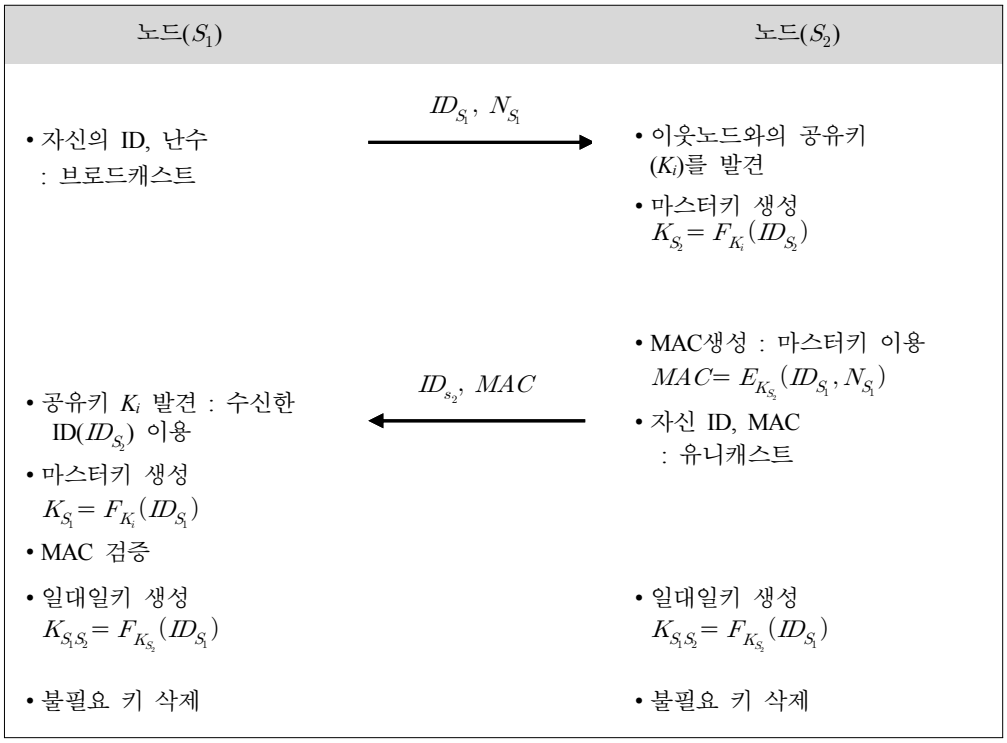

Fig. 4. 일대일키 설립 절차

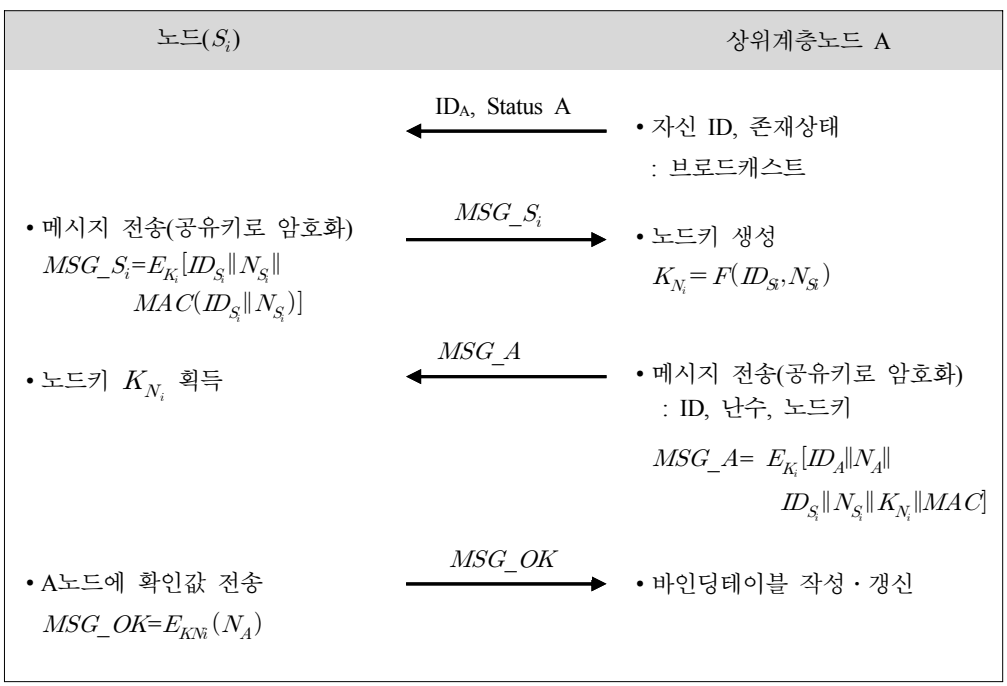

Fig. 5. 노드키 설립 절차

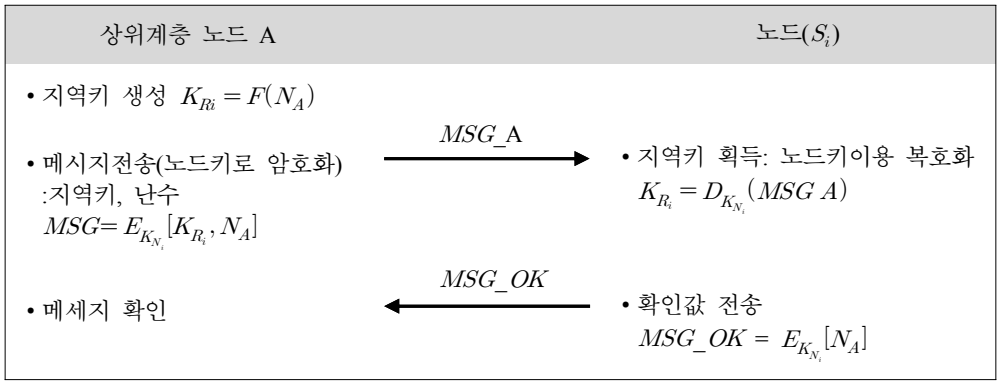

Fig. 6. 지역키 설립 절차

Table 2. 상위계층 노드의 바인딩테이블(예)

No	Node_ID	Key_Info
1	0x37b1	16da322a
2	0x23da	b2a8d234
3	0xdc49	72a78b02
⋮	⋮	⋮

4) 지역키(Region Key)의 설립

지역키는 상위계층 노드가 자신의 지역 내에 존재하는 모든 노드와 공유하는 키로서, 설립 절차를 도식화하 Fig. 6과 같다.

이러한 과정을 거쳐 설립된 지역키는 보안상 취약해질 수 있기 때문에, 상위계층 노드는 지역키 생성 시 키의 유효시간을 설정 후 유효시간이 만료되면 지역 내 전체 노드에게 키 갱신을 알리고 동일한 방법으로 새로운 지역키를 생성하여 분배한다.

5) 노드 추가 및 삭제시의 키 갱신

추가되는 노드는 필드에 배치되기 전 오프라인에서 부분키 집합을 할당받아 저장한다. 이 후 각 노드는 일대일키와 노드키 설립 절차를 거친 후 네트워크에 정상적으로 참여하게 된다. 지역키의 설립은 상위계층 노드의 지역키 유효시간이 경과 후 키 재설립시 새롭게 설립된 지역키를 상위계층 노드로부터 전송받아 사용한다.

또한 전장상황 하에서의 노드는 주로 적대적 환경(Hostile Environment)에서 운용되므로 악의적인 공격자에 의해 잠식되어 키가 노출될 수 있고 정상적인 기능을 소멸할 가능성을 가지고 있다. 따라서 노드가 네트워크 내에서 삭제되었을 경우 키를 갱신하는 과정을 통해 네트워크의 안전성을 확보해야 한다. 노드 삭제시의 키 재설립 절차는 Fig. 7과 같다.

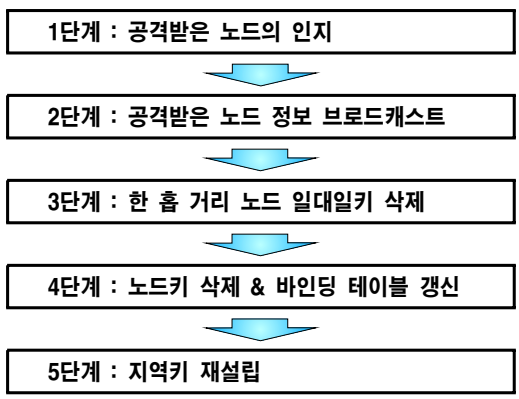

Fig. 7. 키 재설립 절차

4. 성능분석

가. 안전성 분석

1) 확률적 키공유 적용에 따른 안전성 분석

확률적 키 공유기법은 노드가 필드에 배치되기 전, 오프라인상의 키 풀에 저장된 대량의 키 집합에서 일정량의 부분키 집합을 분배받아 저장한다. 이러한 접근방법은 하나의 마스터키에 의존해 비밀통신에 필요한 세션 키들을 생성함에 따라 마스터키 노출 시 전체 시스템의 안전성에 영향을 받게 되던 기존의 접근방법에 비해 키 노출에 의한 위험성은 훨씬 감소한다.

TICN을 구성하는 각 노드들은 대량의 키 풀에서 부분키 집합만을 저장한 상태로 배치되기 때문에, 전체 키 풀에 대한 정보는 공격자가 상당히 많은 수의 노드를 잠식시키지 못하는 한 밝혀내기가 어려우며, 일부 노드만 공격하여 잠식시켰을 경우에는 해당 노드들이 가진 부분키 집합만 노출되기 때문에 시스템의 전체적인 안전성에 문제를 일으키지는 않는다.

2) 공격자의 유형별 형태에 따른 분석

안전성 분석을 위해 TICN내의 상위계층 노드에서는 악의적인 공격행위를 능동적으로 탐지해 내고 대응할 수 있는 침입탐지 시스템이 운용되고 있다 가정하며, 공격자의 유형에 따른 안전성 분석은 다음과 같이 3가지로 구분해 볼 수 있다.

첫째, TICN에 구성되었던 적이 한 번도 없는 외부 공격자인 경우, 부분키 집합에 대한 정보가 전무(全無)하다고 판단할 수 있으므로 일대일키, 노드키, 지역키의 설립과정에 참여할 수 없기 때문에 외부 공격자에 의한 공격은 제안된 키 관리 기법의 안전성에 위협이 될 수 없다.

둘째, TICN을 구성하는 내부의 이동 노드가 공격자인 경우에는 부분키 집합을 이용하여 제안된 키 관리 기법의 모든 과정에 합법적으로 참여할 수 있게 된다. 따라서 암호학적 기법을 적용한 예방책만으로는 차단 또는 배제가 불가능한 공격에 해당되기 때문에 침입탐지 시스템 등의 능동적인 대응책이 필요하지만, 본 논문의 범위를 벗어나는 분야이므로 직접적으로 다루지는 않는다.

셋째, 배치된 노드가 적에게 잠식된 경우에는 공격자는 해당 노드가 가진 비밀키들을 이용하여 TICN내에서 비밀을 요하는 통신에 참여할 수도 있고, 악의적 공격들을 시도할 수도 있게 되기 때문에 제안된 키 관리 기법에 의해 공격을 차단하거나 배제시킬 수는 없으며, 상위계층의 노드에서 중앙집중 방식의 침입탐지 시스템을 이용하여 탐지 및 차단시키는 것이 최선의 방어책이다.

3) 키의 재설립에 대한 안전성 분석

노드의 삭제 시 키의 재설립을 위한 절차(Fig. 7) 중, 공격받은 노드의 인지 단계에서 상위계층 노드는 지역 내 노드에 대한 이상을 탐지하고 이에 대한 대책을 수립하게 되며, 공격받은 노드의 ID를 지역내 모든 노드에게 브로드캐스트하여 인지토록 한다. 또한 공격받은 노드와 한 홉 거리에 있는 노드들의 일대일키를 삭제하는 과정을 통해 공격자가 일대일키를 이용한 추가적인 공격을 할 수 없도록 한다.

상위계층 노드가 지역 내 모든 노드에게 지역키 갱신 메시지를 브로드캐스트하게 되면 지역내에서 사용하던 지역키는 더 이상 유효하지 않으므로 공격자에 의해 공격받은 노드가 이후 지역 내 다른 노드에게 자신이 상위계층 노드인 것처럼 속이는 공격을 할 수 없게 된다. 그리고 바인딩테이블에 저장된 해당 노드의 노드키를 삭제함으로써 더 이상 공격받은 노드의 노드키가 유효하지 않게 되어 후방안전성을 보장한다.

마지막으로 네트워트내 지역키를 재설립하는 단계를 통해 지역 내 정상적인 노드들에게 노드키를 이용하여 지역키를 암호화하고 유니캐스트 방식으로 전송함으로써 키 재설립 과정에서의 안전성을 보장한다.

나. 효율성 분석

1) 계산비용

제안하는 키 관리 기법의 계산비용은 각 이동노드에서 메시지를 암호화 및 복호화 하는 횟수로 구할 수 있다. 일대일키, 노드키, 지역키의 계산비용 산출을 위한 메시지 암·복호화 연산횟수는 각각 3회, 4회, 2회이다. 노드의 밀집도를 d, 네트워크 사이즈를 N이라 하면 제안하는 키 관리 기법에서의 계산 비용은 식 (2)와 같다.

$$\text{계산비용} = (3d)N + 4N + 2N \quad (2)$$

식 (3)에서 $(3d)N$은 전체 노드가 일대일키를 설정하는데 드는 계산비용이며 $4N$은 노드키를 계산하는 비용, $2N$은 지역키를 생성하는데 드는 계산비용이다. 이때 네트워크 사이즈가 일정하다면 계산비용은 노드의 밀집도에 따라 결정되며 값은 $O(d)$가 된다.

2) 통신비용

통신비용은 각 노드가 키 설정을 위해 메시지를 주고 받을 때 소요되는 모든 비용의 합으로 나타낼 수 있다. 즉, 일대일키, 노드키, 지역키의 설립시 발생되는 통신비용의 합이 제안하는 키 관리 기법의 통신비용이 되며, 식 (3)과 같다.

$$\text{통신비용} = (2d)N + 4N + 2N \quad (3)$$

식 (3)에서 $(2d)N$은 전체노드가 일대일키를 설정하기 위한 통신비용이며, $4N$은 노드키를 설정하는 통신비용, $2N$은 지역키를 설정하는 통신비용이다.

3) 키 저장공간 요구량

이동노드는 키 집합로부터 할당받은 부분키 집합 'm', 이웃 노드들과 공유하는 일대일키 저장공간 'D'와 노드키 저장공간, 지역키 저장공간을 각각 요구하며, 상위계층노드는 부분키집합 'm', 일대일키 저장공간 'D', 지역내 각각의 노드와 공유하는 노드키 저장공간 $2(N-1)$과 지역키 저장공간이 필요하다. 따라서 각각의 키 저장공간 요구량은 식 (4), 식 (5)와 같으며, 이는 운용되는 이동노드의 성능을 고려하여 볼 때 충분히 수용할 수 있는 저장공간 요구량이다.

$$\text{이동노드} = m + D + 2 \text{ (노드키+지역키)} \quad (4)$$

$$\text{상위계층노드} = m + D + 2(N-1) + 1 \quad (5)$$

5. 결 론

미래전은 기동수단의 발달, 무기체계의 사거리 및 위력증대, C4I체계의 발전 등으로 인하여 전장이 점차 확대되고 있고 공간을 넘어선 입체전의 양상으로 발전하고 있다. 이를 지원하기 위해 군에서 개발을 추진중인 TICN은 미래의 다양한 전장 환경을 선도하기 위해 기존의 인프라 기반의 네트워크와는 달리 이동성을 가진 노드들 간의 멀티홉을 통해 데이터를 전달하는 Ad-hoc방식으로 운용되어질 것이다.

그러나 Ad-hoc 네트워크는 악의적인 노드, 비인가된 노드, 비협조적인 상황에서 외부의 공격에 의해 잠식된 노드, 내부의 손상된 노드 등에 의해 다양한 보안위협에 직면할 가능성이 높다. 따라서 이러한 Ad-hoc 네트워크를 전장환경에 적용하기 위해서는 다양한 보안위협을 해결하여 보다 보안성이 강화된 네트워크 운용이 전제되어야만 한다.

이에 본 논문에서는 Ad-hoc 네트워크를 기반으로 한 TICN에 적합한 키 관리 기법을 제안하였다. 단일키 사용에 의한 키노출 위험을 감소시키기 위해 확률적 키 공유기법을 적용하였으며, 네트워크에 참여하는 이동 노드의 자원제약적 특성을 고려하여 대칭키 기반의 키 관리 기법을 적용하였다. 그리고 TICN의 계층적 네트워크 운용 특성에 부합되면서 전장상황 하에서 발생가능한 다양한 메시지들에 대한 기밀성 및 무결성을 보장하기 위해 계층화된 키 관리 기법을 제안하였으며, 각 키의 설립절차를 정의하고 노드의 추가와 삭제 시 안정성을 보장하기 위한 키 재설립 절차를 정의하였다.

본 논문을 통해 제안된 Ad-hoc 네트워크 기반의 TICN에 적합한 키 관리 기법은 향후 전장 네트워크 환경에서 무선노드에 대한 기본적인 보안대책 강화에 크게 기여할 것으로 판단되며, 이와 비슷한 구조를 가진 다른 전술 네트워크 환경에도 널리 활용될 수 있을 것으로 기대된다.

References

[1] http://kor.samsungthales.com

[2] 합참, 군 전술종합정보통신체계 운영개념서, 2006.

[3] 전자통신동향분석 제18권 제2호, 2003. 4.

[4] Charles E. Perkins, Ad-hoc Networking, Addison Wesley, 2001.

[5] C. K. Toh, Ad-hoc Mobile Wireless Networks : Protocols and Systems, Prentice Hall PTR, 2002.

[6] 국방대학교, 정보시스템 보안론, 2003.

[7] N. Asokan, P. Ginzborg, "Key Agreement in Ad-hoc Network", Computer Communications Volume 23, 2000.

[8] Laurent Eschenauer, Virgil D. Gligor, "A Key Management Scheme for Distributed Sensor Networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, 2002.

[9] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", IEEE Network, 13(6) : 24-30, Nov/Dec, 1999.

[10] S. Zhu, S. XU, S. Seita, S. Jajodia, "Establishing Pairwise Keys for Secure Communication in Ad-hoc Networks : A Probabilistic Approach", In Proceedings of the 11th IEEE Conference on Network Protocols (ICNP'03), 2003.