무선 센서 및 액터 네트워크를 위한 효율적인 키관리 프로토콜

(An Efficient Key Management Protocol for Wireless Sensor and Actor Networks)

김 완 주 † 남 길 현 ††
(Wanju Kim) (Kilhyun Nam)
이 수 진 ††
(Soojin Lee)

요 약 최근 센서 네트워크는 다양한 분야에서 응용되고 있으며 활발한 연구가 진행되고 있다. 그러나 센서 네트워크는 특정 현상에 대한 정보를 수집하고 이를 외부의 네트워크 관리자에게 전송하고 관리자는 전송된 정보를 이용하여 대응하는 형태로 구성되어 있어 사건에 대한 즉각적이고 적시적인 대응이 어렵다. 이러한 문제점을 극복하기 위해 센서 네트워크에 이동성과 활동성을 가져 즉시적인 대응능력이 있는 액터 노드를 포함하는 무선 센서 및 액터 네트워크(WSANs)가 제안되었다. WSANs는 센서 네트워크와 여러 측면에서 많은 공통점을 가지고 있으나, 노드들이 동등한 권한과 능력을 가지는 센서 네트워크와는 달리 자원제약이 적고 이동성을 가지는 액터 노드를 포함하고 있어 기존의 보안기술을 적용하기에는 어려움이 많다. 따라서 본 논문은 WSANs를 안전하고 효율적으로 운용하기 위해 요구되는 기밀성, 무결성, 인증 등의 보안 서비스를 제공하기 위해, 네트워크를 노드의 능력에 따라 계층적으로 구분하고 액터 하위 계층에는 일대일키(Pair-wise Key), 노드키(Node Key), 지역키(Region Key)를 활용한 키관리 프로토콜을 액터 상위 계층에는 공개키 기반의 키관리 프로토콜을 제안한다.

키워드 : 무선 센서 및 액터 네트워크, 보안, 키관리 프로토콜, 센서 노드, 액터 노드

Abstract Researches on Sensor Network has become much more active and is currently being applied to many different fields. However since sensor network is limited to only collecting and reporting information regarding a certain event, and requires human intervention with that given informtaion, it is often difficult to react to an event or situation immediately and proactively. To overcome this kind of limitation, Wireless Sensor and Actor Networks (WSANs) with immediate-reponse Actor Nodes has been proposed which adds greater mobility and activity to exisiting sensor networks. Although WSANs shares many common grounds with sensor networks, it is difficult to apply exisiting security technologies due to the fact that WSAN contains Actor Nodes that are resource-independent and mobile. This research therefore seeks to demonstrate ways to provide security, integrity and authentication services for WSAN's secure operation, by separating networks into hierarchcial structure by each node's abilities and providing different encryption key-based secure protocols for each level of hierarchy: Pair-wise Key, Node Key, and Region Key for sensor levels, and Public Key for actor levels.

Key words : Wireless Sensor and Actor Network, Security, Key Management Protocol, Sensor Node, Actor Node

1. 서 론

무선통신 기술과 내장형 컴퓨터 기술의 발전으로 관심을 받기 시작한 센서 네트워크는 최근 들어 다양한 분야에서 응용되고 있으며, 활발한 연구가 진행되고 있다. 그러나 센서 네트워크는 현상(Event)이 발생한 지역 내부 혹은 인접해서 배치되는 대량의 센서 노드들을 이용하여 현상에 대한 정보를 수집하고 네트워크 내부에서 통합 및 분석하여 싱크 노드를 통해 외부로 전송하는 것이 주목적이기 때문에 분석된 정보를 바탕으로 즉각적이고 적시적인 대응을 하기 위해서는 별도의 추가적인 노력이 필요하다.

센서 네트워크의 이러한 문제점을 해결하기 위해 제안된 센서 및 액터 네트워크(WSANs : Wireless Sensor Actor Networks, 이하 WSANs)는 자원의 제약이 적으면서도 이동성을 가지는 액터(Actor)를 네트워크에 포함시키고, 센서 노들들이 수집한 정보를 이용하여 액터가 적절한 대응이 가능하도록 하고 있다. 때문에 산불 감시 및 대응, 홈 네트워크에서의 침입자 감시 및 대응,

· 이 논문은 2007 한국컴퓨터종합학술대회에서 '무선 센서 및 액터 네트워크를 위한 효율적인 키관리 프로토콜'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 국방대학교 전산정보학과
sizipus1@gmail.com
†† 종신회원 : 국방대학교 전산정보학과 교수
khnam@kndu.ac.kr
cyberkma@kndu.ac.kr

논문접수 : 2007년 9월 27일
심사완료 : 2007년 11월 30일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제13권 제7호(2007.12)

군사작전시 적 탐지 및 대응 등의 응용 분야에 실질적으로 활용이 가능한 네트워크 형태이다[1].

WSANs는 기반구조 없이 구성되는 네트워크이며 무선통신을 사용하는 등 여러 가지 측면에서 센서 네트워크와 공통점을 가진다. 따라서 WSANs에서는 센서 네트워크에서 적용되고 있는 많은 기술들을 필요로 하고 있다. 그러나 모든 노드들이 동등한 권한과 동일한 능력을 가지는 센서 네트워크와는 달리 액터를 포함하고 있기 때문에 센서 네트워크에서의 기술을 WSANs에 그대로 적용하는 것은 불가능하며, 이러한 문제점은 보안 기술의 적용에 있어서도 마찬가지이다. 따라서 WSANs에서의 보안을 위해서는 기본적인 보안 요구사항들을 만족시키면서 기존 센서 네트워크와는 차별되는 WSANs만의 특성을 만족시킬 수 있는 새로운 보안기술의 개발이 요구된다.

그러므로 본 논문에서는 WSANs의 통신망 구조와 보안 요구사항들에 대해서 살펴보고 WSANs에 적합한 안전한 라우팅과 데이타 전송 및 인증 등을 보장하기 위한 효율적인 키관리 프로토콜을 제안한다. 이후 제안한 프로토콜의 성능분석을 통해 프로토콜의 안전성과 효율성을 입증한다.

2. 관련연구

센서 네트워크에서의 보안 목표는 기존 네트워크와 유사하게 기밀성, 인증, 무결성, 가용성 등을 보장하는 것이다. 이러한 보안 목표를 달성하기 위해 센서 네트워크 보안에 대한 연구는 크게 두 가지 방향으로 진행되어 왔다. 첫째는 센서 네트워크 보안 서비스 구조로서 센서 네트워크에 적합한 신뢰관계 설정 모델을 제시하여 인증 구조를 제안한다[2]. 둘째, 센서 네트워크를 위한 키관리 구조로서 센서 노드 간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키관리 분야가 있다[3-5].

SPINS[2]은 데이타의 기밀성과 노드간 데이타 인증을 보장하는 SNEP구조와 브로드캐스팅되는 데이타의 인증을 위한 u-TESLA로 구성되어 있으며, LEAP[3]은 이전의 단일키 방식들과 달리 개인키, 일대일키, 클러스터키, 그룹키의 네 종류의 키를 이용하여 보안요구사항을 해결하였다. WSANs을 위한 키 관리 프로토콜로서 HSS[4]는 WSANs의 네트워크를 Mix-key 암호기법을 활용한 싱크-액터 레이어와 경량 키관리 기법을 활용한 액터-센서 레이어로 나누어서 서로 다른 보안 매커니즘을 제안한다.

그러나, 기존에 제안된 키 관리 프로토콜은 센서 및 액터 네트워크의 통신망 구조와 보안요구사항을 제대로 반영하지 못하고 있다. 따라서, 본 논문에서는 WSANs에 적합한 키관리 프로토콜을 제안한다.

3. 통신망 구조 및 보안 요구사항

3.1 통신망 구조

WSANs의 통신망 구조는 전체적으로 그림 1의 형태를 가진다. 기존 센서 네트워크와의 가장 큰 차이점은 센서 노드와 싱크 노드 사이에 센서 노드에 비해 저장용량, 계산능력, 통신능력이 우수하고 이동성을 가지는 액터 노드들이 포함된다는 것이다.

따라서 WSANs은 세가지 서로 다른 노드의 능력을 고려하여 통신망을 계획하고 운영한다. 센서 노드는 배치된 지역에서 고정 운영되며 액터 또는 싱크의 요구에 응답한다. 액터는 할당된 지역에서 센서 노드에게 쿼리를 전송하고 노드의 응답을 종합하며 필요시 적절한 행동을 취한다. 싱크는 액터와 유사한 역할을 하거나 필요시 액터나 센서 노드의 활동을 통제한다. 또한 싱크는 외부 네트워크와의 연결 통로 역할을 수행하여 외부의 임무관리노드(Task Manager Node)가 전체 네트워크를 모니터링하고 통제하는 역할을 수행할 수 있도록 한다.

액터와 액터간의 통신은 한 홉 또는 멀티홉 통신이 가능하고, 액터와 센서간 통신에 있어서는 액터는 자신이 책임지는 지역내의 센서 노드에게는 한 홉 통신이 가능하나 센서는 통신능력의 제한으로 액터까지는 멀티홉 통신경로의 설정이 필요하다. 그림 2는 WSANs의 통신 운용 개념도이다.

WSANs에서 액터는 이동성을 가지므로 액터의 이동에 따른 라우팅 경로의 변경은 수시로 발생하며 액터들은 서로 조정(Coordination)을 통해 자신의 책임지역을 분배하므로 지역(Region)은 변경될 수 있다.

3.2 보안 요구사항

무선통신의 취약성으로 인해 WSANs의 모든 통신 패킷은 적에게 노출될 수 있다. 또한 악의적인 공격자는 패킷의 기밀성, 무결성 등을 위협하는 공격이 가능하며 DoS 공격 등을 통해 네트워크의 가용성을 위협할 수 있다.

WSANs에서 키분배시의 키정보 등 민감한 데이타는 적에게 노출되었을 경우 네트워크 전체가 심각한 위협

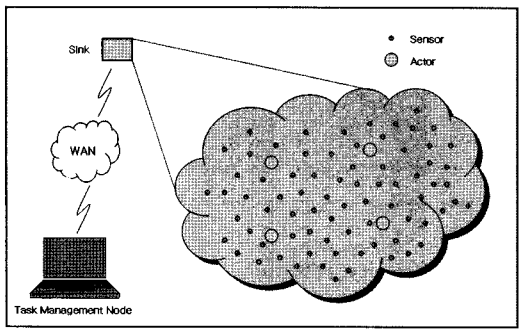


그림 1 WSANs 네트워크 구조

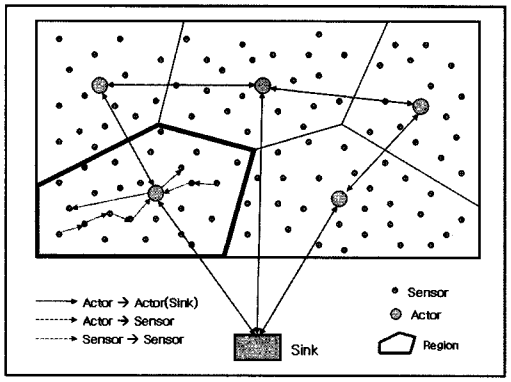


그림 2 WSANs 통신운용 개념

에 처할 수 있으므로 암호화 등을 통해 기밀성을 달성해야 하며, 악의적인 공격자는 통신망 상에 비교적 손쉽게 불법적인 메시지를 삽입할 수 있으므로 메시지에 대한 인증도 필요하다. 이외에도 메시지의 수신자는 메시지의 송신자가 정당한 사용자인지를 판단할 수 있어야 하며 수신된 메시지가 중간에 변경이 없음을 보장받아야 한다. 재연공격 등에 대비하여 데이타의 신선성도 보장되어야 한다. 따라서, 네트워크 내의 모든 데이타에 대해 기밀성(Confidentiality), 인증(Authentication), 무결성(Integrity), 가용성(Availability)이 요구된다.

4. WSANs에 적합한 키관리 프로토콜 제안

4.1 전체적인 구성 및 Notation

4.1.1 전체적인 구성

본 논문에서 제안하는 접근방법은 센서 네트워크와는 차별되는 WSANs의 네트워크 구조에 기반한다. 즉, 액터를 중심으로 상위계층은 비교적 충분한 자원과 계산능력이 보장되므로 공개키에 기반한 접근 방법을 적용하며 액터를 중심으로 하위계층은 제한된 계산, 저장, 통신 능력을 감안하여 대칭키에 기반한 접근방법을 적용한다.

액터 하위 계층에는 액터 노드에서 전송되는 메시지와 센서 노드에서 보고되는 메시지의 보안성을 유지하기 위한 세 개의 키로 이루어진 키관리 구조를 제안한다. 제안하는 키관리 구조는 다음과 같다.

- Pair-wise Key(일대일키) : 센서 노드가 지역내 한 홉 이내의 센서 노드와 공유하는 키로서 액터로부터 질의나 명령을 받은 후 결과를 액터에게 보고할 때 경로 상의 센서 노드들 사이에서 데이타의 무결성을 보장한다. 이때 지역내의 액터는 하나의 센서 노드로 간주하여 일대일키를 생성한다.
- Node Key(노드키) : 지역내 각각의 센서 노드가 액터와 공유하는 키로서 수집된 정보의 보고시 데이타의 암호화, 지역키의 갱신 등 브로드캐스트되는 민감한 데이타의 암호화에 이용한다.
- Region Key(지역키) : 하나의 액터가 관리하는 지역내의 액터와 센서 노드가 공유하는 키이며 액터가 지역내의 센서들에게 질의나 명령을 브로드캐스트 메시지로 전달할 때 메시지의 암호화 및 인증에 활용한다.

액터 상위 계층에는 MANET에 적합하도록 제안된 일반적인 공개키 구조를 적용하여 보안 요구사항을 달성한다. 사용되는 공개키 구조는 WSANs의 액터 상위 계층에서 하나의 액터가 다른 액터 또는 싱크와 보안성을 유지하는데 사용되는 키로서 노드의 개인키와 공개키, 인증서를 모두 포함한다.

4.1.2 Notation

본 논문에서 사용되는 Notation은 다음과 같다.

Notaton	Description
S(Sink)	싱크 노드 또는 베이스스테이션
A	액터 노드
PK_A, SK_A, $CERT_A$	액터 A의 공개키, 비밀키, 인증서
PK_{CA}, SK_{CA}	CA의 공개키와 비밀키
$S_1,S_2,..S_i$	센서 노드
M1 ‖ M2	메시지 M1과 M2의 결합
K_{IP},K_{IN}	일대일키와 노드키 생성을 위한 초기키
E_k[msg]	키 k를 이용하여 msg를 암호화
D_k[msg]	키 k를 이용하여 msg를 복호화
f ( )	일방향 해쉬 함수
MAC(key,msg)	key에의해 생성된 msg의 인증코드
F_K	의사 난수 함수

4.2 액터 하위 계층의 키관리

4.2.1 일대일키(Pair-wise Key) 설립

일대일키는 센서 노드가 자신과 한 홉 이내의 노드들과 공유하는 키를 의미하며 본 논문에서 제안하는 스킴에서는 전체 네트워크를 대상으로 하여 센서 노드, 액터 노드, 싱크 노드의 구분없이 모두 동일한 노드로서 키 설립에 참여한다. 일대일키의 설립절차는 그림 3과 같다.

4.2.2 노드키(Node Key) 설립

노드키는 액터 노드가 지역내의 각각의 센서 노드와 공유하는 키이다. 액터는 자신의 ID와 존재상태를 지역내에 브로드캐스트한 후, 센서 노드는 사전에 분배된 K_{IN}을 이용하여 자신의 ID를 암호화 후 액터에 전송한다. 액터는 전송받은 센서의 ID와 랜덤한 난수를 이용하여 노드키 K_{N_i}를 생성한 후 센서 노드에 전송한다. 노드키 설립완료 후 센서 노드는 사전에 분배된 키를 삭제한다.

노드키를 설립후 액터 노드는 지역내 센서 노드들의 ID와 노드키를 저장하는 바인딩 테이블에 기록 유지하고, 액터 노드들은 싱크 노드의 바인딩 테이블에 자신의 바인딩 테이블을 업데이트하여 차후 조정(Coordina-

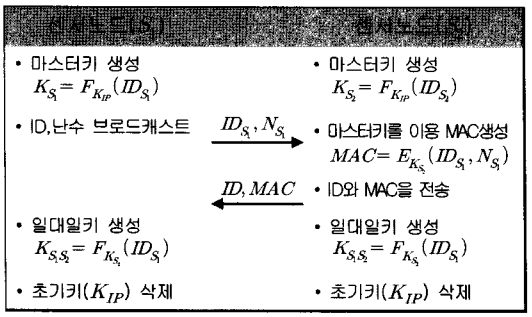
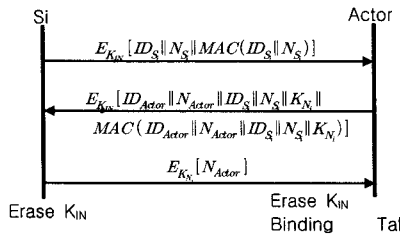


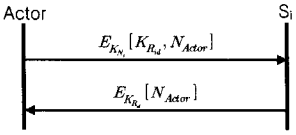
그림 3 일대일키 설립절차

tion)을 통해 다른 액터가 지역내 센서를 관리할 때 싱크 노드의 바인딩 테이블을 활용하여 자신의 바인딩 테이블을 최신화 함으로써 노드키 설립절차를 다시 시행할 필요가 없도록 한다. 센서 노드 S_i와 액터 A 사이의 노드키 설립절차를 도식하면 다음과 같다.



4.2.3 지역키(Region Key) 설립

지역키의 설립은 다음의 절차를 따른다. 액터 노드가 임의의 난수를 활용하여 랜덤한 키 $K_{R_{id}}$를 생성한다. 여기서 *id*는 액터 노드가 책임지고 있는 지역의 지역 식별자 이다. 이후 노드키 K_{N_i}를 이용하여 지역키를 암호화한 후 각각의 센서 노드에 분배한다.



액터는 지역키 생성시 키의 유효시간을 설정 후 유효시간이 만료되면 지역내 전체 센서 노드에 키갱신을 알리고 동일한 방법으로 새로운 지역키를 생성하여 분배한다.

4.3 액터 상위 계층의 키관리

액터 상위 계층에서는 대칭키 개념의 키관리 스킴을 적용하지 않고 MANET에 적용되어진 일반적인 공개키 기반의 암호화 기법을 활용한다. 제안하는 매커니즘에서는 싱크 노드가 인증기관(CA : Certification Authority)의 역할을 수행한다. 키관리 및 인증은 다음과 같이 수행한다.

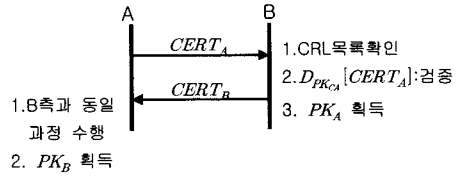
• 키 및 인증서 선분배 단계 : 각각의 액터 A는 오프라인에서 신뢰할 수 있는 제3자로부터 PK_A, SK_A, $CERT_A$, PKC_A를 할당받아 저장한다. 여기에서,

$$CERT_A = E_{SK_{CA}}[A \| PK_A \| T_{sign} \| T_{expire}]$$

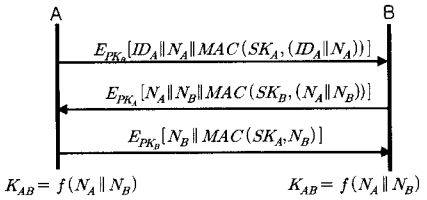
과 같으며, T_{sign}은 인증서의 발급시간을 T_{expire}는 인증서의 만기시간을 의미한다. 각각의 인증서는 동일한 유효기간을 갖는다. 또한 싱크는 PK_{CA}, SK_{CA}, $CERT_{CA}$와 네트워크 내 액터들의 ID와 공개키를 공개키 바인딩 테이블에 저장한다.

• 인증서 폐기 : 하나의 액터 노드가 공격자에 의해 포획되거나 기능을 상실했을 때 해당 인증서의 효력을 상실시키고 각각의 액터는 인증서 폐기 및 취소 목록(CRL : Certificate Revocation List)에 기록 후 유지한다.

• 인증서 인증 및 세션키의 생성 : 액터 상위 계층의 두 노드(액터-액터 또는 액터-싱크)사이의 인증절차는 다음의 과정을 따른다.



인증절차를 수행한 후 각각의 노드는 상대의 공개키를 획득한다. 이후 상대의 공개키를 활용하여 노드 사이의 세션키를 다음의 절차로 생성하여 한 통신주기에 활용한다.



노드 A와 B는 위의 세 단계를 통해 세션키 K_{AB}를 얻고 이를 통해 데이타를 암호화한다. 두 노드사이의 통신이 완료되면 세션키는 즉시 삭제한다.

• 인증서 갱신 : 인증서 갱신은 사전에 정의된 지수 $T_{refresh}$ 값을 활용하며 이 지수와 인증서 생성시간과 만료시간은 $T_{expire} \leq (T_{sign} + T_{refresh})$의 관계가 있다. 모든 인증서 소유자는 $T_{refresh}$ 내에 인증서를 갱신해야만 한다.

5. 성능분석

5.1 안전성

안전성 분석은 네트워크 내의 노드가 악의적인 공격자에 의해 포획되거나 손실되었을 경우 이를 인지할 수 있다는 가정을 한다.

본 논문에서 제안하는 키관리 프로토콜은 ID기반의 스킴으로서 모든 메시지에 대한 인증이 이루어짐으로 사실상 내부 공격자에 대해서만 고려하면 된다.

센서 노드가 공격자에 의해 포획되었을 경우 노출되는 키 정보는 이웃 센서 노드들과 공유하는 일대일키와 액터 노드와 공유하는 노드키, 지역키이다. 센서 노드의 노드 포획이 발생되었을 경우 이를 인지하여 주위 노드와 설정한 일대일키를 제거한다. 이를 통해 포획된 노드에 의한 악의적인 공격이 이루어지는 것을 방지할 수 있으며, 액터 노드는 관리 지역내에 지역키 갱신 메시지를 브로드캐스트 후 해당 센서 노드와 설정한 노드키를 삭제 하고 바인딩테이블을 갱신한다. 따라서, 포획된 노드가 액터 노드인 것처럼 속이는 공격이 수행될 수 없게 되며, 또한 포획된 노드와 맺었던 노드키를 삭제함으로써 포획된 노드는 더 이상 유효한 노드로서의 역할을 수행할 수 없게 된다.

이후 액터 노드는 관리하는 지역에 지역키를 재생성하여 각각의 노드키로 암호화하여 유니캐스트로 분배한다.

액터 노드와 싱크 노드는 일반적인 센서 노드에 비해 스스로 상당한 안전성을 확보할 수 있으므로 전체 네트워크의 안전성분석에 중요한 요소로 판단하지 않는다. 하지만 액터 노드가 악의적인 공격자에 의해 손실되었을 경우 해당 액터 노드가 관리하고 있는 지역에 있는 센서 노드들의 노드키와 지역키가 노출되므로 다른 정당한 액터 노드에 의해 키의 재설정이 요구된다. 또한 조정에 의한 지역의 재편성 시에도 노드키와 지역키의 재설정이 요구된다.

5.2 효율성

본 논문에서는 노드의 연산량, 메모리 저장공간 요구량, 통신비용 등은 자원제약이 적은 액터 노드와 싱크 노드에 대해서는 고려하지 않는다. 따라서 자원제약이 큰 센서 노드만을 고려시 다중키에 의한 키관리 프로토콜인 LEAP과 성능비교를 통해 효율성을 입증한다.

센서 노드들은 주로 자신과 한 홉 이내의 이웃노드들과 통신하며 키를 생성하고 데이타를 전달한다. 그러므로 통신비용과 계산 비용은 네트워크의 규모와 상관없이 노드의 밀집도에 따라 결정된다.

노드의 밀집도를 d, 네트워크 사이즈를 N이라 하면 제안하는 프로토콜의 계산 비용은 일대일키를 설립하는 비용 $(2d+1)N$, 노드키 설립비용 $4N$, 지역키 설립비용 $2N$의 합으로 구해진다. 이러한 계산비용을 LEAP과 비교해 보면 LEAP과 제안하는 프로토콜의 네트워크 사이즈가 동일한 값이라면 계산복잡도는 LEAP이 $O(d^2)$이 되고 제안하는 프로토콜은 $O(d)$가 되므로 효율적임을 알 수 있다. 통신비용은 네트워크에서 일대일키, 노드키, 지역키의 설립시 발생되는 통신비용의 합으로 나타낼 수 있다. 따라서 통신비용은 $2dN+3N+2N$이 된다.

저장공간 요구량은 액터하위 계층만을 고려시 센서 노드는 이웃노드들과 공유하는 일대일키 저장공간 D와 노드키 저장공간, 지역키 저장공간을 각각 요구한다. 따라서 액터하위 계층의 센서노드의 저장공간 요구량은 $D+2$가 된다. 저장공간 요구량을 LEAP과 비교해 보면 LEAP의 저장공간 요구량은 $3D+2+L$(L:키체인 저장공간) 이므로 만약, 이웃노드의 수가 20일 때 LEAP은 키체인을 제외하고 62개의 키 저장공간을 요구하며 제안하는 프로토콜은 22개의 키 저장공간만을 요구하므로 LEAP에 비해 1/3수준의 저장공간만이 요구된다.

6. 결론 및 향후연구

본 논문은 WSANs을 위한 효율적인 키관리 프로토콜을 제안하였으며, WSANs의 구조적 특성을 감안하여 보안 기법의 적용은 계층적인 방법에 의해 수행된다. 액터를 기준으로 자원의 제약이 적은 액터 상위 계층은 공개키 알고리즘에 기반한 보안 스킴을 제안하였고, 자원의 제약이 큰 액터 하위 계층은 대칭키 알고리즘에 기반한 보안 스킴으로 일대일키, 노드키, 지역키를 이용한 키관리 프로토콜을 제안하였다.

또한 WSANs에 적합한 키구조를 정의하고 각각의 키를 설립하는 절차를 세부적으로 제안하였으며 이를 통해 기존 센서 네트워크에서 적용되었던 기법을 WSANs에 적용할 수 있는 방안을 제시하였다.

향후 연구에서는 제안된 기법의 안전성과 효율성을 시뮬레이션을 통해 정확히 분석해 보고자 한다. 그리고, 싱크 노드가 없을 경우를 고려 Threshold Cryptography 기법 등을 통한 분산 CA 환경도 고려하고자 한다.

참 고 문 헌

[1] I.F. Akyildiz and I.H. Kasimoglu, Wireless Sensor and Actor Networks : Reseach challenges, Ad Hoc Networks Journal (Elsevier), Vol.2, No.4, pp. 351-367, October 2004.

[2] A. Perring, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, SPINS : Security protocol for sensor networks, *MobiCom* 2001, pp. 189-199, July 2001.

[3] S. Zhu, S. Setia and S. Jajodia, LEAP:Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, CCS'03, pp. 62-72, October 2003.

[4] X. Cao, M. Huang, Y. Chen and G. Chen, "Hybrid Authentication and Key Management Scheme for WSANs," ISPA Workshops 2005, pp. 454-465, 2005.

[5] F. Hu and X. Cao, "Security in Wireless Actor & Sensor Networks(WASN):Towards A Hierarchical Re-Keying Design," Proc. of the ITCC'05, 2005.