무선 센서 & 액터 네트워크를 위한 효율적인 키관리 프로토콜

김완주° 남길현 이수진

국방대학교

sizipus1@gmail.com khnam@kndu.ac.kr cyberkma@kndu.ac.kr

Efficient Key management Protocol for Wireless Sensor and Actor Networks

Wanju Kim° Kilhyun Nam Soojin Lee

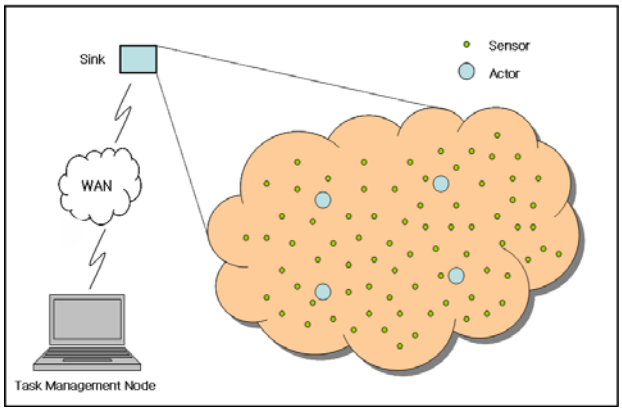
Korea National Defense University

1. 서 론

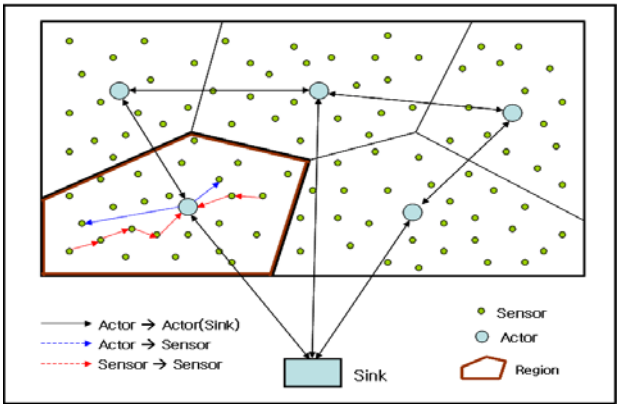
최근 센서 네트워크는 다양한 분야에서 응용되고 있으며 활발한 연구가 진행되고 있다. 그러나 센서 네트워크는 특정 현상에 대한 정보를 수집하고 이를 외부의 네트워크 관리자에게 전송하고 관리자는 전송된 정보를 이용하여 대응하는 형태로 구성되어 있어 사건에 대한 즉각적이고 적시적인 대응이 어렵다. 이러한 문제점을 극복하기 위해 센서 네트워크에 이동성과 활동성을 가져 즉시적인 대응능력이 있는 액터 노드를 포함하는 무선 센서&액터 네트워크(WSANs : Wireless Sensor Actor Networks, 이하 WSANs)가 제안되어 산불 감시 및 대응, 홈 네트워크에서의 침입자 감시 및 대응, 군사작전시 적 탐지 및 대응 등의 분야에 실질적으로 활용이 가능한 네트워크로 발전되고 있다.[1]. 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 논문에서는 먼저 WSANs의 통신망 구조와 보안 요구사항들에 대해서 살펴본 후, WSANs에 적합한 안전한 라우팅과 데이터 전송 및 인증 등을 보장하기 위한 효율적인 키관리 프로토콜을 제안하고 성능분석을 통해 제안된 프로토콜의 안전성과 효율성을 입증한다.

2. 본 론

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 보안기술의 적용에 있어서도 마찬가지이다. 따라서 WSANs에서의 보안을 위해서는 기본적인 보안 요구사항들을 만족시키면서 기존 센서 네트워크와는 차별되는 WSANs만의 특성을 만족시킬 수 있는 새로운 보안기술의 개발이 요구된다.



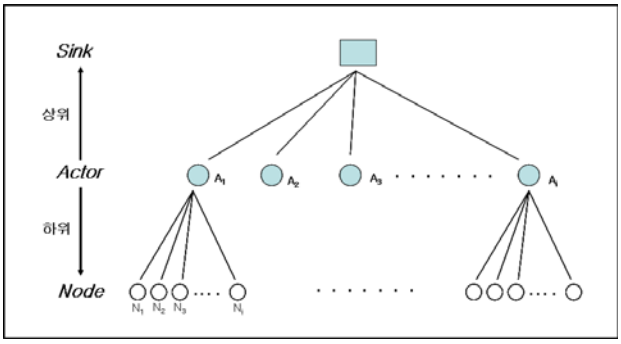
<그림 1> WSANs 네트워크 구조



<그림 2> WSANs 통신운용 개념

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][3]. 둘째, 센서 네트워크를 위한 키관리 구조로서 센서 노드 간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키관리 분야가 있다[4][5]. 그리고 WSANs을 위한 키관리 연구는 [6][7]등이 있다.

본 논문에서 제안하는 접근방법은 <그림 3>과 같이 센서 네트워크와는 차별되는 WSANs의 네트워크 구조에 기



<그림 3> WSANs의 계층적인 구조

반한다. 즉, 액터를 중심으로 상위계층은 비교적 충분한 자원과 연산능력이 보장되므로 공개키에 기반한 접근 방법을 적용하며 액터를 중심으로 하위계층은 제한된 연산, 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 데이터의 무결성을 보장한다. 이때 지역내의 액터는 하나의 센서 노드로 간주하여 일대일키를 생성한다.
- **Node Key(노드키)** : 지역내 각각의 센서 노드가 액터와 공유하는 키로서 수집된 정보의 보고시 데이터의 암호화, 지역키의 갱신 등 브로드캐스트되는 민감한 데이터의 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 유지하는 키로서 노드의 개인키와 공개키, 인증서를 모두 포함한다.

제안된 기법의 안전성 분석은 네트워크 내의 노드가 악의적인 공격자에 의해 포획되거나 손실되었을 경우 이를 인지할 수 있다는 가정을 기반으로 한다. 본 논문에서 제안하는 키관리 프로토콜은 ID기반의 스킴으로서 모든 메시지에 대한 인증이 이루어짐으로 사실상 내부 공격자에 대해서만 고려하면 된다. 센서 노드가 공격자에 의해 손실되었을 경우 노출되는 키 정보는 이웃 센서 노드들과 공유하는 일대일키와 액터 노드와 공유하는 노드키, 지역키이다. 센서 노드의 손실이 발생되었을 경우 주위 노드와 설정한 일대일키를 제거하고 액터 노드는 관리 지역내에 지역키 갱신 메시지를 브로드캐스트후 해당 센서 노드와 설정한 노드키를 삭제후 바인딩테이블을 갱신한다. 이후 액터 노드는 관리하는 지역에 지역키를 재생성하여 각각의 노드키를 이용하여 유니캐스트로 분배한다.

제안하는 기법의 통신비용과 계산비용은 네트워크의 규모와 상관없이 노드의 밀집도에 따라 결정된다.

3. 결 론

본 논문은 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 스킴을 제안하였으며 WSANs 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 수학적 기법이나 시뮬레이션을 통해 정확히 분석해 보고자 한다. 그리고, 싱크 노드가 없을 경우를 고려 Threshold Cryptography 기법 등을 통한 분산 CA 환경도 고려하고자 한다.

4. 참고문헌

[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] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Network", Proc. of the 9th ACM conference on CCS, pp. 41-47, 2002

[5] H. Chan, A. Perring, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," IEEE Symposium on Security and Privacy, pp. 197-213, 2003.

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

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