센서 네트워크의 보안 프로토콜과 라우팅 프로토콜의 연관성에 관한 연구

신동규*, 이용배, 장근원, 전문석
숭실대학교 컴퓨터학과
e-mail:nicesdg@empal.com

A Study on Security in Routing of Sensor Network

Dong-Gyu Shin*, Young-bae Lee, Kun-Won Chang, Moon-Seog Jun
Dept of Computer Science, Soong-sil University

요 약

센서 네트워크는 일반 네트워크에 비해 제약적인 면이 많아 일반 네트워크에서 사용하는 보안 메커니즘을 그대로 사용할 수 없는 단점이 있다. 그래서 센서 네트워크에 적합한 보안 프로토콜을 제안하기 위하여 본고 에서는 보안 프로토콜을 라우팅 프로토콜에 적합하도록 적용한다. 특정 라우팅과 그 구조에서 사용가능한 보안 프로토콜을 접목시켜 라우팅과 보안이 동시에 가능하도록 제시 한다. 또한 그에 대한 문제점 제시와 향후 발전 방향에 관해서 제안 한다.

1. 서론

센서 네트워크는 초경량과 저 전력의 무수히 많은 센서들로 이루어진 네트워크다. 센서 네트워크는 센서 노드들이 좁은 영역에 분산되어있는 형태로 구성되어있고 이 노드들의 통신으로 네트워크가 유지된다.

센서 네트워크의 개발은 우리의 삶에 편리함을 제공하는 동시에 사적인 프라이버시 침해 가능성도 커지고 있다. 일반 네트워크에서는 이런 보안적인 측면에 대해 상당히 연구가 진행 중이고 여러 가지 대응책도 연구되고 있다. 하지만 센서 네트워크에 센서 노드들에 대한 보안측면 연구는 그에 비해 대응이 부족한 현실이다. 센서 네트워크가 발전하고 있는 지금부터 함께 보안적인 측면도 연구 되어야한다.

본 논문에서는 센서 네트워크의 보안 프로토콜과 센서 네트워크에서의 라우팅 프로토콜과의 관계에서 두 가지 기법을 모두 고려할 수 있도록 통합적 센서 네트워크 보안에 관한 연구를 하였다. 보안 프로토콜과 라우팅 프로토콜에 대해 조사하고 특정 라우팅 프로토콜과 보안 프로토콜의 상호 관계를 밝혀 두 가지 프로토콜을 사용하여 센서 네트워크의 보안 라우팅을 하는 방법을 제안 하고자 한다. 2장에서는 기존의 라우팅 프로토콜과 보안 프로토콜에 관한 내용을 기술 하였고, 3장에서는 라우팅 프로토콜과 보안 프로토콜의 연관성 및 기존의 단일 프로토콜의 취약점에 대해 제시 하였다. 4장에서는 두 프로토콜의 관계성에 기반을 둔 새로운 구조를 제안 한다.

2. 관련 연구

관련연구에서는 센서 네트워크의 사용되고 있는 보안 프로토콜과 라우팅 기법에 대해서 알아보도록 하겠다.

2.1 센서 네트워크 보안 프로토콜

초기에 인증 프로토콜로 A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar의 SNEP(Secure Network Encryption Protocol)과 μTESLA(Timed Efficient Stream Loss-tolerant Authentication)를

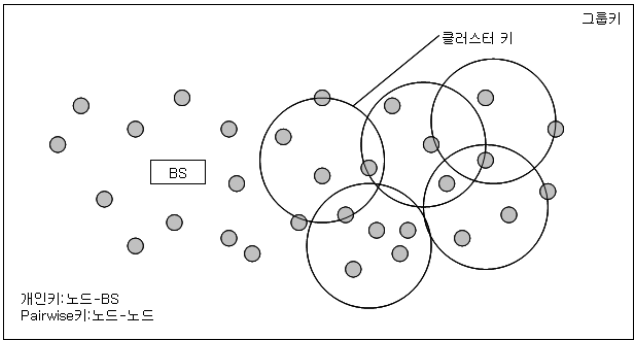
이용한 구조인 SPINS(Security Protocols for Sensor Networks)보안구조를 센서 네트워크에서 사용하였다.[1] 후에 하나의 키를 사용 하는 프로토콜로는 대량의 센서가 흩어져 있는 센서 네트워크에서 안전한 키 프로토콜 설계가 어렵다는 판단으로 그룹키 관리 방식인 베이스 스테이션과 클러스터 구조를 중심으로 한 LEAP(Localized Encryption and Authentication Protocol)프로토콜이 나타나게 되었다.[2]

LEAP는 센서네트워크의 키 관리 프로토콜이다. 센서네트워크에서 기밀성과 인증을 위해서 다중 키 메커니즘을 제공 한다.

LEAP은 4가지의 암호키와 키 설정 프로토콜을 가지고 있다.

표 1. LEAP 4가지 암호키

개인키	베이스 스테이션과 공유
그룹키	모든 노드와 공유(브로드캐스팅 키)
Pairwise키	다른 센서 노드와 공유
클러스터 키	이웃 노드와 공유



(그림1) LEAP의 구조

LEAP은 BS(Base Station)과의 인증을 제공한다. 그뿐만 아니라 단방향 키 체인(one-way Key Chain)을 기반으로 한 노드 간 인증 프로토콜도 제공한다. 우선 단방향 키 체인을 생성한 후 체인의 Commitment값 즉 처음 키를 각 이웃과의 Pairwise 키로 암호화 한 후 전송한다. 이러한 과정 후에 메시지를 보낼 경우 인증 키 값을 같이 보내게 되면 이웃이 처음에 받은 Commitment값과 비교하여 노드의 인증을 실행한다.

2.2 센서 네트워크 라우팅 프로토콜

라우팅 프로토콜에는 데이터 중심의 C. Intanagonwiwat et al.의 “Directed Diffusion for Wireless Sensor Networking"에서 말하는 노드가 query를 flooding하여 각 노드들로부터 라우팅 정보를 받는 방법인 Directed Diffusion 방법과 네트워크를 클러스터링 기반으로 여러 개의 구역으로 나누어서 특정 노드들을 Leader노드로 정하여서 라우팅을 하는 LEACH(Low-Energy Adaptive Clustering Hierarchy) 방법이 있다.[3][4]

LEACH는 네트워크를 클러스터링 개념을 기반으로 하여 여러 개의 클러스터들로 분할하여 각각의 클러스터 내의 특정 센서 노드에 헤드의 역할을 할당함으로써 라우팅을 수행하는 방법이다. 클러스터 헤드가 클러스터의 멤버 노드들로부터 데이터를 수집하여 데이터를 모아서 직접 BS(Base Station)로 전달한다. 이 기법의 특징은 네트워크에 있는 모든 센서 노드들에 에너지 소비를 공정하게 분산시키기 위해, 에너지 집약적인 기능을 하는 클러스터 헤드를 임의로 할당함으로써, 전체적인 에너지 효율을 높이는 프로토콜이다.

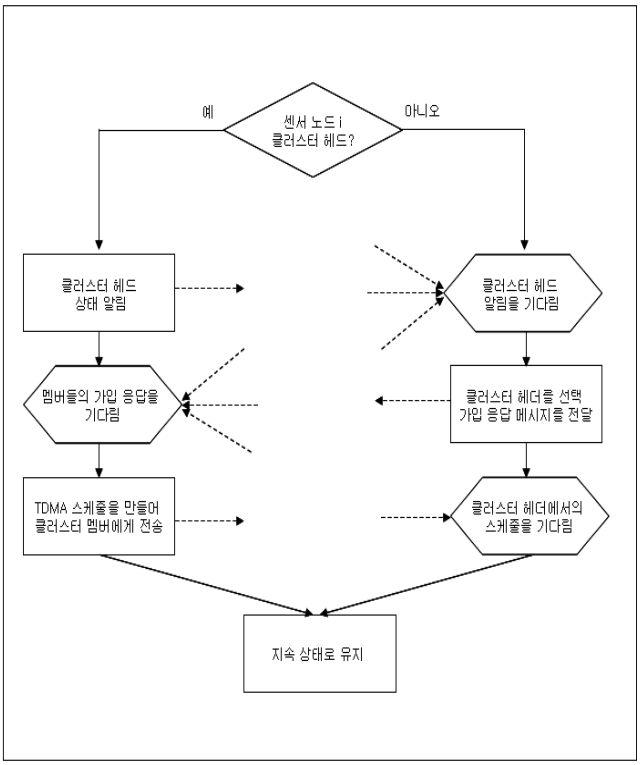
(그림2) LEACH의 Time line

각 라운드(Round)는 클러스터가 구성되는 설정(Setup) 단계와 지속 상태(Steady-state) 단계로 구성되어 진다.

설정에서는 모든 노드가 자신이 현재의 라운드 동안 클러스터 헤드가 될 수 있는지에 대해 이전의 라운드 동안 클러스터 헤드였는지의 여부와 효율적인 클러스터 헤드 수에 따라 결정된다. 클러스터 헤드를 결정한 후, 이 정보를 이웃 센서 노드들에게 알린다. 이를 수신한 비 클러스터 헤드 노드들은 여러 곳에서 헤드의 정보를 받을 수 있을 것이다. 이때 이 노드들은 신호의 강도에 따라 헤드를 결정하고 이 정보를 자신이 선택한 헤드에게 보내면 하나의 클러스터가 형성되어 진다. 형성되어진 클러스터는 멤버들에게 데이터 전송 순서를 지시하며, 지속 상태 단계로 이동한다.

지속 단계에서는 각 클러스터 멤버 노드들은 자신의 전송 슬롯에서 데이터를 전송하고 나머지 슬롯들에서는 Sleep모드로 대기 하여 Energy의 효율을 높인다. LEACH에서는 TDMA(time division multiple access)방식을 사용하여서 노드간 간섭을 방지 하며, 클러스터간의 간섭을 방지하기 위하여 각 클러스터들이 서로 다른 확산 코드를 사용하는 방법을 사용

하고 있다.



(그림3) LEACH의 클러스터형성 알고리즘 Flowchart

3. 라우팅 프로토콜과 보안 프로토콜의 연관성 및 단일 프로토콜의 취약점

센서 네트워크는 일반 네트워크보다 보안 적인 측면에서 상당히 취약한 점을 보이고 있다. 첫째로 센서 노드들의 제약이 심하여 다양한 보안 프로토콜을 적용하기 힘든 것이 현재의 센서 네트워크 상태이고 센서 자체가 특정지역에 밀집되어 분포되기 때문에 물리적 공격에도 대처할 방안이 없는 실정이다. 물론 센서가 파괴나 그 기능을 하지 못할 경우를 대비해 다른 센서들이 작업을 수행하지만 효율적인 측면에서 손실을 가져오게 된다. 이렇게 취약한 이유로 아주 간단한 공격에도 쉽게 네트워크가 균형이 깨지는 경우가 발생하여서 센서 네트워크 보안의 중요성이 대두 되고 있는 현실이다. 에너지 측면은 보안 프로토콜과 같이 라우팅 프로토콜에서도 중요한 문제로 대두 되고 있다. 그래서 라우팅 프로토콜 측면에서는 최소한의 에너지로 데이터를 전송하는 목적을 가지지만 에너지 측면만을 고려하다보면 보안 적 측면에서는 당연히 취약하게 될 수밖에 없다. 그렇기 때문에 두 가지 프로토콜을 서로 상호 보완적인 관계로 유지하여서 후에 센서 네트워크가 자리를 잡을 때 어느 한 부분도 취약하지 않는 신기술로 거듭날 수 있으려면 두 부분의 대해서 새로운 기술을 보유하여야 한다.

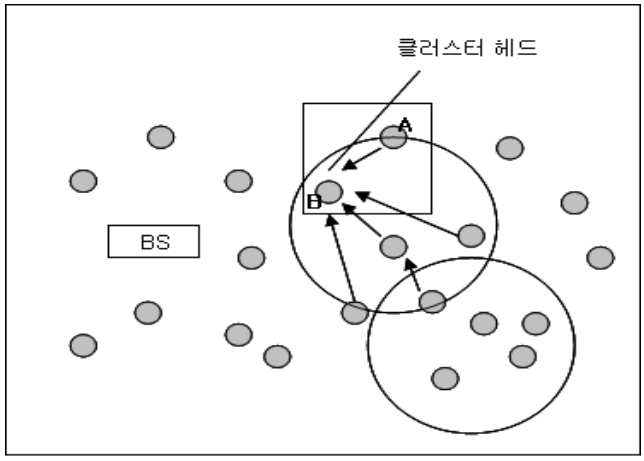
4. 라우팅 프로토콜과 보안 프로토콜의 조합

LEACH프로토콜과 LEAP프로토콜의 조합에 대해서 제안 하였다.

LEACH 라우팅 프로토콜에서는 클러스터 기반의 라우팅을 하고 있기 때문에 LEAP에서 쓰이는 4가지의 키들을 사용하여서 라우팅의 효과와 보안의 효과를 얻을 수 있다.

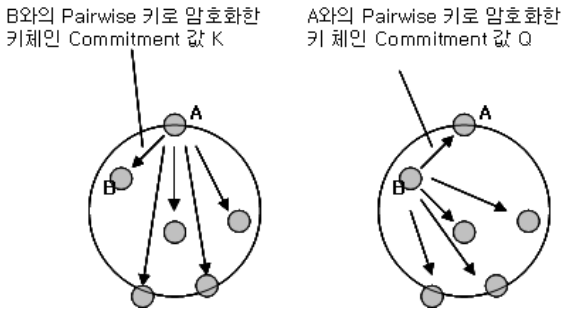
LEACH에서 클러스터 헤드를 결정 하는 과정에서는 노드들 간에 통신이 이루어진다.

여러 보안 프로토콜들은 BS과 노드들 간의 인증에 대해서 체계화 되어있다. LEACH 프로토콜을 사용함에 헤드를 정하고 클러스터를 형성하는 과정에서의 노드들 간의 보안 프로토콜을 LEAP을 사용하여서 제안 하였다.



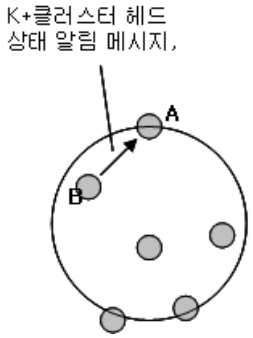
(그림 4) 센서네트워크의 LEACH프로토콜의 클러스터 헤드

Phase 1. 노드는 각 노드들에게 자신의 키체인 Commitment값을 각 이웃과의 Pairwise 키로 암호화 한 후 이웃에게 전송한다. (그림5)



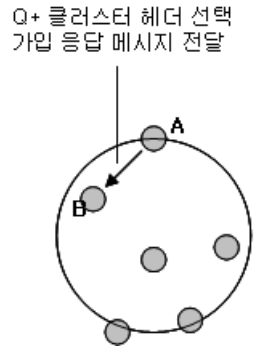
(그림5) Phase 1.

Phase 2. 노드는 특정 노드로부터 메시지가 입력될 경우 인증 키 값으로 복호화 한 후 Commitment값을 비교 하여 인증을 한다. 이때 특정 노드가 클러스터 헤드 노드일 때 메시지는 클러스터 헤드 상태 알림 메시지를 나타낸다. (그림 6)



(그림 6) Phase 2.

Phase 3. 각 노드들의 인증 과정을 통해 LEACH의 클러스터 헤더 선택 과정에서의 메시지를 암호화 할 수 있다. (그림 7)



(그림 7) Phase 3.

5. 결론 및 향후 발전 과제

라우팅 프로토콜과 보안 프로토콜의 연관성 제시와 라우팅 프로토콜 수행 과정에 보안 프로토콜을 실행시켜 인증을 수행하였다.

노드들 간의 인증을 통하여 공격자가 클러스터 헤드를 식별하지 못함으로 인해 노드들의 정보를 가지고 있는 클러스터 헤드의 보안을 보장 할 수 있으므로 신뢰성이 확보 되었다. 이와 같이 라우팅 과정에서 행해지는 공격에 대해 보안 프로토콜을 적용하여 사용하게 된다면 향후 센서 네트워크가 실용화 되는데 크게 도움이 될 것이다.

하지만 센서 네트워크의 제약 사항인 에너지 부분에서는 이와 같은 보안 프로토콜 수행은 에너지의 사용량을 증가시키기 때문에 최적화된 방안이라고는 할 수 없다. 그렇기 때문에 더욱 연구하여야할 과제는 센서 노드들이 라우팅을 하지 않을 동안에 센서의 에너지가 보존 되고 있는데, 이 에너지를 적절히 활용하여 보안 메커니즘을 적용한다면 에너지 측면에서도 효율을 기대 할 수 있다.

참고문헌

[1]A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th ACM/IEEE International Conference on MobiCom, 2001.

[2]Sencun Zhu, Sanjeev Setia, and Sushil Jajodia."LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," In Proc. of the 10th ACM CCS '03, Oct. 2003.

[3]C. Intanagonwiwat et al., "Directed Diffusion for Wireless Sensor Networking," IEEE/ACM Transactionson Networking, Vol.11, No.1, Feb. 2003,pp.2-16.

[4]Wendi B. Heinzelman et al., "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. on Wireless Communications, Vol.1, No.4, Oct. 2002, pp.660-670.

[5]S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and Mani B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Network," Proc. of WETICE'02,2002.

[6] S.H.Kim, Y.S. Kang. B.H. Chung, K.I.Chung "U-센서 네트워크 보안 기술 동향" 전자통신동향분석 제 20권 제 1호 2005년 2월

[7] J.H.Nah, K.J..Chae, K.I. Chung, "센서 네트워크 보안 연구 동향" 전자통신동향분석 제 20권 제 1호 2005년 2월