SRC 프로토콜의 성능 개선을 위한 메커니즘

송태일○ 홍충선
경희대학교 컴퓨터공학과
tisong@networking.khu.ac.kr, cshong@khu.ac.kr

Mechanism for improvement of SRC Protocol

Tae-ill Song○ and Choong Seon Hong
Department of Computer Engineering, Kyung Hee University

요 약

SRC 프로토콜은 BCDCP 클러스터 라우팅 기법과 페어와이즈 키와 디지털서명을 이용한 키 분배 프로토콜을 결합한 클러스터링 기반 보안 프로토콜이며, 초기 키 생성 및 분배, 주기적인 키 재 생성, 센서 추가 및 삭제 단계로 구성되어 있다. 본 논문에서는 SRC 프로토콜의 한계점인 페어와이즈 키의 선분배를 이용한 보안방법의 개선과 에너지 사용량을 개선하기 위한 초기 키 생성 및 분배단계를 분리하여 초기 키 생성 단계와 분배단계를 제시한다.

1. 서 론

무선 센서 네트워크는 다수의 센서 노드들이 넓은 지역에 무작위로 배치되어 구성되는 무선 네트워크이다. 센서 노드는 제한된 에너지와 메모리, 계산능력을 효율적으로 이용하여 에너지 자원을 오래 사용하는 방법이 필요하다.[1]

무선 센서 네트워크에서는 통신 에너지를 줄이는 것이 큰 과제이며, 이를 해결하기 위하여 클러스터링 기반 라우팅 기법이 사용된다. 본 논문에서는 클러스트링 기반의 보안 프로토콜인 SRC(Secure rotation of cluster-head) 프로토콜[2]의 키분배 단계를 세분화하여 에너지 소모 및 메모리량을을 개선하는 프로토콜을 제안한다.

2. 관련연구

클러스터를 통하여 데이터를 전송하는 대표적인 기법은 LEACH[3]와 BCDCP[4] 라우팅 기법이 있다. SRC 프로토콜은 BCDCP를 기반으로 한 프로토콜로, 주기적인 클러스터 헤더의 재 선출을 이용하여 싱크홀 어택을 회피하고 효율적인 에너지 사용, 동적 키 재사용 및 분배를 목적으로 하고 있다. SRC 프로토콜에서는 [6]에서 제안한 디지털 서명을 이용한 키 분배 프로토콜을 적용하여 보안성을 향상시켰다.

3. 제안사항

본 논문에서는 SRC 프로토콜의 한계점인 센서노드의 배치전 페어와이즈 키의 선분배를 이용한 보안방법의 개선과 초기 센서노드들의 클러스터링시 소모되는 에너지 사용량을 개선에 중점을 두고 있다. 이를 위하여 SRC 프로토콜의 초기 키 생성 및 분배 단계를 초기 키 생성 단계와 초기 키 분배단계로 분리하였다. 키가 선분배 되어있지 않는 상황에서 의사역행렬을 이용하여 베이스 스테이션과 모든 노드간의 신뢰성 있는 키를 생성하여 분배하는 초기 키 생성단계, 베이스 스테이션을 이용하여 클러스터 헤더와 맴버들에게 효율적으로 그룹키를 분배하고 에너지를 관리하는 키 분배과정을 제안한다.

3.1 가정사항

1. 모든 센서 노드는 단방향 해쉬 함수와 암호화 알고리즘(대칭, 비대칭)이 선분배 되어있다.
2. 모든 센서와 베이스 스테이션의 X, Y 행렬의 행과 열의 크기는 각각 같은 크기를 사용한다.
3. A는 m×n 행렬이다. 행렬 A의 의사역행렬은 A^g이며, rank(A^g)=rank(A)이다.
4. 베이스 스테이션은 물리적공격, 해킹등의 보안상 안전한 상태이다.

3.2 초기 키 생성단계

초기 키 생성단계에서는 [5]에서 제안한 행렬을 이용하여 무선 센서 네트워크상에서의 비대칭키를 경량화하여 분배하는 방법을 사용하며, 아래와 같이 키 분배하는 단계를 설정 한다.

각 단계에 대한 설명은 다음과 같다.

1. 초기 배치된 센서 노드는 m×n 차원의 행렬 X와 의사역행렬 X^g, 그리고 센서의 정보(에너지, 메모리등)와 클러스터링이 될 준비가 되었다는 Request Message를 베이스 스테이션에 전송한다.
2. 정보를 받은 베이스 스테이션은 n×k 차원의 행렬 Y를 생성하고 전송받은 X^gX 값과 생성한 Y를 결합하여, X^gXY, X^gXYY^g, 그리고 전송받은 센서 노드의 정보를 바탕으로 선출한 각 센서 노드들의 클러스터 헤더의 ID를 전송한다.
3. 각 센서는 베이스 스테이션으로 부터 전송된 값을 이용하여 행렬 Y를 도출해 내어 행렬 XY값을 도출하고, XY^gY의 값을 베이스 스테이션에 전송하여 상호 비밀값 XY를 도출하게 된다.

3.3 초기 키 분배단계

"본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 육성지원 사업의 연구결과로 수행되었음" (NIPA-2011-C1090-1131-0005)
Dr. CS Hong is the corresponding author.

초기 키 분배단계는 키 생성단계에서 생성된 비밀키를 이용하여 베이스 스테이션이 각 클러스터 헤더와 클러스터 맴버, 해당 클러스터의 그룹키를 생성할 시드값을 분배하는 단계이다.

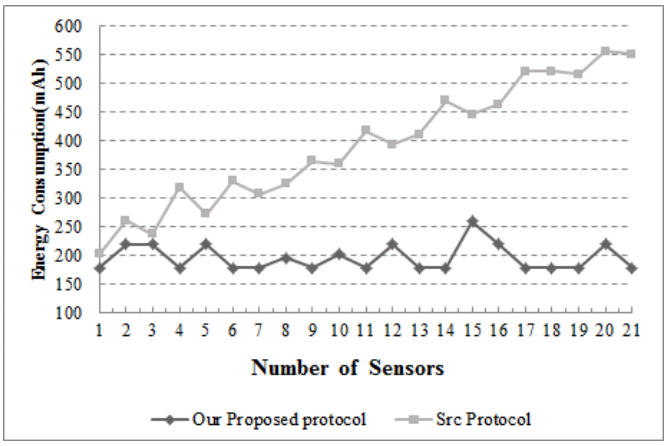
각 단계에 대한 설명은 다음과 같다.

1. 베이스 스테이션은 선출된 클러스터 헤더에게 클러스터 리스트와 그룹키를 생성할 수 있는 시드 값을 베이스 스테이션과 센서 노드간의 공개키로 생성된 비밀키로 암호화 하여 전송한다.
2. 베이스 스테이션은 각 클러스터 맴버에서 그룹키를 생성 할 수 있는 시드 값을 베이스 스테이션과 센서 노드간의 공개키로 생성된 비밀키로 암호화 하여 전송한다.
3. 베이스 스테이션은 클러스터 헤더 대 클러스터 헤더 전송이 필요할 경우, 하위 클러스터 헤더와 상위 클러스터에게 상호 동일한 비밀키값을 생성할 시드 값을 베이스 스테이션과 센서 노드간의 공개키로 생성된 비밀키로 암호화 하여 전송한다.

4. 성능평가

시뮬레이션에 사용된 모델은 표준 ZigBee 센서를 기준으로 하며, Omnet++ 시뮬레이터를 사용하여 제안된 알고리즘과 SRC 프로토콜의 에너지 소모량을 비교한다. 그리고 모든 센서 노드들의 클러스터링이 끝난 시점에서 베이스 스테이션, 클러스터 헤더의 키 메모리 사용량을 비교하였다.

4.1 에너지 소비량 비교

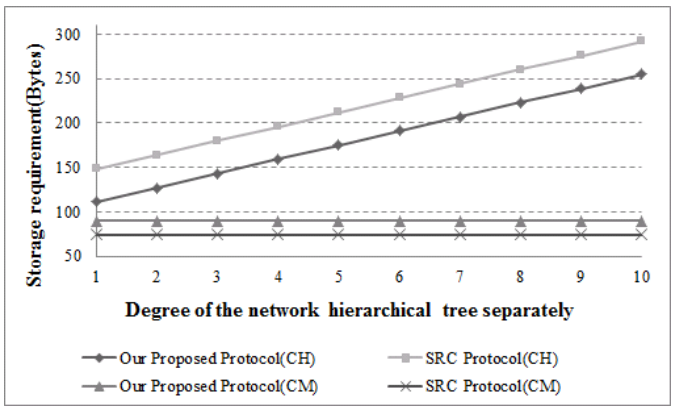


[그림 1] 평균 에너지 소비량 비교

[그림 1]는 에너지 소비량을 측정한 결과로, 비교대상인 SRC 프로토콜은 클러스터내의 노드가 많아질수록 에너지 소모가 증가하나 제안된 프로토콜은 베이스 스테이션에게 메시지를 전송받아 연산하게 되므로 모든 노드가 평균적으로 일정한 에너지를 소모하게 된다.

4.2 키 저장 메모리량 비교

본 논문에서는 [4]에서 측정한 값을 이용하여 그룹키와 페어와이즈 키를 16바이트로 설정하여 시뮬레이션 하였다. [그림 2]에서 볼 수 있듯이 클러스터 헤더와 클러스터 맴버들의 키 요구량을 측정한 결과로 클러스터 헤더는 17%, 클러스터 맴버는 18%의 메모리가 절약하는 것을 알 수 있다.



[그림 2] 센서 노드의 키 저장 요구량 측정

5. 결론 및 향후 연구

본 논문은 SRC 프로토콜의 선행조건인 페어와이즈 키의 선분배 문제와, 노드들의 에너지 소비량을 최소화 하는데 그 목적을 두고있다. 행렬을 이용하여 베이스 스테이션과 센서노드 간의 비대칭키를 효율적으로 분배하여 기존 프로토콜에 비하여 메모리 요구량 개선했으며, 베이스 스테이션을 이용하여 평균 에너지 소비량을 개선했다. 차후 키 재사용 단계의 에너지 소모와 신뢰성에 관한 연구를 진행하여 프로토콜을 개선할 예정이다.

6. 참고문헌

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y and Cayirci, E, “A survey on sensor networks“, IEEE Communications Magazine, Vol 40, No.8, pp102-114, Aug 2002

[2] Zhiqiang Ruan, Qiaoliang Li, Sujun Li ,“A Secure Routing Protocol for Clustered Sensor Networks” , 4th International Conference on Wireless Communications, Networking and Mobile Computing, 12-14 Oct 2008.

[3] Heinzelman, W.B, Chandrakasan, A.P, Balakrishnan, H, “An application-specific protocol architecture for wireless microsensor networks“, IEEE Transactions on Wireless Communications, Oct 2002

[4] Muruganathan, S.D., Ma, D.C.F., Bhasin, R.I., Fapojuwo, A.O, “A centralized energy-efficient routing protocol for wireless sensor networks” , Communications Magazine, IEEE, pp. 8-13 March 2005

[5] Md. Mokammel Haque, Al-Sakib Khan Pathan, Choong Seon Hong, Eui-Nam Huh, “An Asymmetric Key-Based Security Architecture for Wireless Sensor Networks“, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, Vol.2, No.5, pp.265-279, October 2008

[6] J. Abraham and K.S. Ramanatha, “Security Protocols for Wireless Sensor Networks based on Tiny Diffusion and Elliptic Curves“. Proceeding of Networks and Communication System, pp 35-40, March 29-31 2006