제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

무선 센서 네트워크에서의 안전한 클러스터 헤더 선출 기법

강동민*, 박민우*, 박선호*, 정태명**
*성균관대학교 전자전기컴퓨터 공학과
**성균관대학교 정보통신공학부
e-mail: {dmkang, mwpark, shpark}@imtl.skku.ac.kr, tmchung@skku.edu

A Secure Cluster Header Election Mechanism in Wireless Sensor Networks

Dong-Min Kang*, Min-Woo Park*, Seon-Ho Park*, Tai-Myoung Chung**
*Dept of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information Communication Engineering, Sungkyunkwan University

요 약

무선 센서 네트워크에서 클러스터링 기법은 데이터 병합을 통해 통신 대역폭 사용을 용이하게 하며, 센서 노드들간의 송수신 전력 소비를 줄일 수 있고, 노드 증가에 따른 네트워크 확장성이 용이하므로 현재 많은 연구가 되고 있다. 클러스터링 기법은 클러스터 헤더를 선출하는 것으로부터 시작된다. 기존의 클러스터 헤더 선출 기법들은 에너지 잔여량, 센서 노드의 위치, 센서 노드들의 평균 에너지 등을 클러스터 헤더 선출값으로 하여 클러스터 헤더를 선정한다. 그러나 이 기법들은 악의 적인 노드가 다른 노드의 클러스터 헤더 선출값을 변경하고, 자신의 클러스터 헤더 선출값을 증가시켜 클러스터 헤더가 될 수 있는 보안 취약점을 가지고 있다. 이와 같은 보안 취약점을 개선하기 위해 클러스터 헤더 선출값에 대한 무결성과 클러스터 헤더 선출값을 전송하는 노드의 인증이 필요하다. 본 논문에서는 one-way key chain 기법을 사용하는 안전한 클러스터 헤더 선출 기법을 제안하고, 제안한 기법에 대한 안전성을 분석한다.

1. 서론

무선 센서 네트워크(Wireless Sensor Network)는 분산된 영역에 걸쳐 특정 목적에 특화된 형태를 가지며, 일반적으로 데이터를 수집하고 전송하는 센서 노드(sensor node)와 외부 망과 연결되어 각 센서 노드들에게 받은 데이터를 기록 및 관리하는 베이스 스테이션(BS)으로 구성된다.

기존의 무선 센서 네트워크의 연구방향은 초경량, 저전력, 단거리의 통신 제약을 갖는 센서 노드들을 효율적으로 구성하고 관리하여 제한된 리소스를 효율적으로 이용할 수 있는 방안에 대한 연구가 진행되어 왔다. 그러나 유비쿼터스 컴퓨팅 환경이 홈 네트워크에 적용되면서, 무선 센서 네트워크에서 보안 문제가 대두 되었다.

그래서 최근 무선 센서 네트워크의 제한적인 자원을 고려하면서 보안 서비스를 제공하는 계층적 라우팅 프로토콜 기반의 보안 메커니즘 연구가 활발히 진행 되고 있다. 계층적 라우팅 프로토콜은 위치적으로 가까운 노드들이 클러스터를 형성하고, 클러스터 내의 노드들 중 클러스터 헤더를 선정하여, 클러스터 헤드가 클러스터 내 노드들의 데이터를 병합(aggregation)하고, 병합한 데이터를 베이스 스테이션(BS)에게 전송하는 기법이다.

클러스터링 기법에서 센서 노드간의 통신 양을 줄이고 자원을 효율적으로 소비하기 위해서는, 클러스터 헤더가 효율적으로 선출 되는 것이 중요하다. 클러스터 헤더 선출 기법으로는 LEACH (Low-Energy Adaptive Clustering Hierarchy), LEACH-C (LEACH-Centralized), HEED (Hybrid Energy Efficient Distributed clustering), EACHS (Energy Adaptive Cluster Head Selection) 등이 있다. LEACH는 모든 노드가 P의 확률로 순환하며 일정하게 클러스터 헤드가 되는 기법으로, 노드간의 에너지 소모를 균등하게 하여 네트워크 생존 시간을 최대화 시키는 기법이며, LEACH-C는 각 노드의 위치와 에너지 잔여량을 클러스터 헤더 선출값으로 하여, BS에서 직접 클러스터 헤더를 선출하는 기법이다. HEED는 노드 자신의 요소만을 클러스터 헤더 선출값으로 하여, 자신의 클러스터 헤더 선출 확률이 1이 될 때까지 확률값을 2배로 증가시켜 클러스터 헤더가 되는 기법이다. 마지막으로 EACHS는 모든 노드의 에너지 잔여량, 자신의 잔여 에너지, 이전 라운드에서 소모된 에너지를 클러스터 헤더 선출값으로 하여 선출 확률을 높이는 기법이다.

각각의 알고리즘은 클러스터 헤드를 선출하는 선출값(factor)이 있다. 클러스터 헤드 선출 값을 비교하여 클러스터 헤더를 선출하게 되는데, 악의적인 사용자에 의해 보고하는 선출값이 변경 될 수 있으며, 악의적인 사용자에게 노출된 센서 노드가 클러스터 헤더가 된다. 따라서 클러스터 헤더 선출 값은 데이터 무결성과 인증이 필요하다.

본 논문에서는 클러스터 헤드를 선출하는 계층적 라우팅 프로토콜에서의 클러스터 헤드 선출 값에 데이터 무결성과 인증을 제공하는 안전한 클러스터 헤더 선출 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 클러스터링 기법과 클러스터 헤드 선출 기법에 대해 살펴보고, 3장에서는 본 논문에서 제안하는 안전한 클러스터 헤더 선출 기법을 소개하며, 4장에서는 안전성 분석을 통해 본 논문의 안전성을 평가하며, 5장에서는 본 논문의 결론과 향후 연구에 대해 제시 한다.

2. 관련연구

이 장에서는 클러스터링과 클러스터 헤더 선출 기법에 대해 소개하고, 브로드케스트 인증 알고리즘인 uTESLA 기법을 소개한다.

2.1. 클러스터링

클러스터링은 위치적으로 가까운 노드들이 클러스터를 형성하고, 클러스터 내의 노드들 중 클러스터 헤더를 선정하여, 클러스터 헤드가 클러스터 내 노드들의 데이터를 병합(aggregation)하고, 병합한 데이터를 베이스 스테이션(BS)에게 전송하는 기법이다. 클러스터링 기법의 장점은 전송 경로 설정 시 클러스터 헤더만을 통해 BS에게 전송하므로 경로 설정 오버헤드를 줄일 수 있으며, 그로 인해 라우팅 테이블의 크기도 줄일 수 있다. 또한 클러스터 헤드는 클러스터 내 노드의 데이터를 병합(agregation)하는데, 데이터 병합은 단순히 데이터를 수집하여 전송하는 것이 아니라, 데이터들의 정보를 통합하여 하나의 메시지 길이로 BS에게 전송하는 것이다. 그러므로 여러 개의 데이터를 하나의 메시지로 한번 전송 하게 되며, 이는 대역폭 사용을 용이하게 하고, 송수신 전력 소비량을 줄일 수 있다. 또한 클러스터링은 노드 증가에 따른 네트워크 확장성(scalability)을 용이하게 하므로, 수십 개에서 수십만 개의 센서들을 갖는 센서 네트워크에 적합한 기법이다.

2.2. 클러스터 헤더 선출 기법

- LEACH

LEACH 프로토콜에서는 네트워크 노드간의 에너지 소모를 균등하게 하여 네트워크 생존시간을 최대화하기 위해 분산된 환경의 클러스터 기반의 네트워크 구조로 데이터 전송을 수행 한다. 클러스터 헤드는 식 (1)의 확률 함수에 의해 결정된다.

$$P_i(t)=\begin{cases}\dfrac{k}{N-k\times(r \bmod \frac{N}{k})}, & C_i(t)=1\\ 0, & C_i(t)=0\end{cases} \quad (1)$$

위 식에서 i는 노드의 식별자, t 는 시각, N은 전체 노드의 수, k는 클러스터의 수, r은 라운드를 나타낸다. Ci(t)는 최근 r mod (N/k) 라운드 동안 클러스터 헤드였다면 0이고, 아니라면 1이다.

- HEED

HEED 프로토콜은 클러스터 헤드의 선정을 개별 노드에서 분산 처리를 통해 결정하는 알고리즘을 제안했다. 노드의 잔여 에너지를 이용하는 헤드 선정 확률 함수는 식 (2) 와 같다.

$$CH_{prob}=C_{prob}\times\frac{E_{residual}}{E_{\max}} \quad (2)$$

E_{max}는 노드의 초기 에너지, $E_{residual}$은 노드의 잔여 에너지, C_{prob}는 전체 네트워크 노드 중 클러스터 헤드 노드의 비율을 나타낸다. 이 밖에 클러스터 내의 통신비용을 두 번째 헤드 선정 기준값으로 이용하여 잔여 에너지 값이 같은 후보 노드가 있는 경우 헤드 선정을 위해 이용하였다. 통신비용은 이웃노드의 근접성이나 클러스터의 밀집도이다. 이 알고리즘은 초기에 CH_{prob}와 절대값 P_{min}(=10-4) 중 큰 값으로 시작하여 노드 자신의 CH_{prob}이 1이 될 때까지 CH_{prob} 를 2배씩 증가시키거나 1이 된 이웃 노드로부터 메시지를 수신할 때까지 반복하고 이들이 클러스터 헤드가 되도록 한다. 이러한 방법은 클러스터의 크기에 관계없이 일정 시간 내에 알고리즘이 종료되도록 하며 이웃 노드의 위치를 고려하지 않아도 되는 장점을 지닌다.

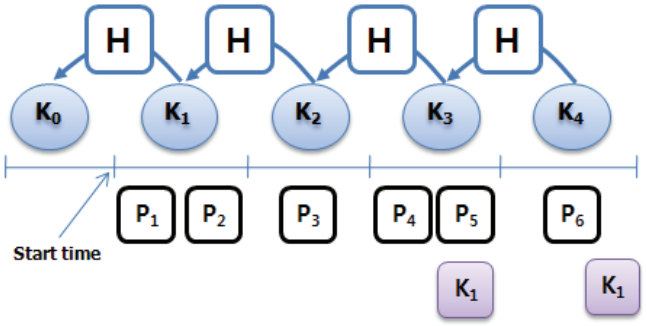
- EACHS

EACCHS는 모든 노드의 에너지 잔여량, 자신의 잔여 에너지, 이전 라운드에서 소모된 에너지를 클러스터 헤더 선출 식에 대입하여 다른 노드보다 에너지가 많으면 클러스터 헤더 선출 확률이 높아지고, 에너지가 적으면 클러스터 헤더 선출 확률이 낮아지도록 설계된 기법이다. 선출 확률은 식 (3)과 같다.

$$CH_{prob}=\frac{P}{1-\left((r+1)\bmod\frac{1}{P}\right)}\times\left[\frac{E_{residual}-E_{dissipate}}{E_{average}-E_{dissipate}}\right] \quad (3)$$

2.3. uTESLA의 인증 기법

uTESLA는 브로드케스트 통신에서 인증을 제공하기 위한 인증 알고리즘으로 센서 네트워크에 적용할 수 있도록 경량화 된 알고리즘이다. uTESLA는 일방향 해쉬 함수를 이용하여 인증 메커니즘을 제공한다. uTESLA는 아래의 (그림 1)과 같다. BS는 랜덤하게 선택된 K_n과 일방향 해쉬 함수를 이용하여 키 체인을 생성하고 각 노드에게 K_0(commitment)를 전송한다. 센서 노드들은 키 체인의 K_i를 이용하여 패킷의 MAC(message athentication code)를 생성한다. 수신 노드는 수신된 메시지의 MAC 키를 알지 못하므로 메시지를 인증 할 수 없다. 일정 시간 후에 BS는 키 체인의 키를 공개하고, 공개된 키를 받은 수신 노드는 해쉬 함수를 이용하여 MAC의 키로 사용된 랜덤키를 Kn을 알 수 있으며, K_n으로 수신한 메시지를 인증 할 수 있다.



(그림 1) 클러스터 헤드의 key chain 생성

3. 안전한 클러스터 헤더 선출 기법

이 장에서는 확률적 키 분배 방식을 사용하는 센서 네트워크에서의 안전한 클러스터 헤더 선출 기법을 제안한다.

3.1 The Design Goal

이 논문의 목적은 무선 센서 네트워크에서 안전한 클러스터 헤드 선출을 위해 보안을 제공하는 것이다. 목적을 세분화 하면 다음과 같이 3가지로 분류 될 수 있다.

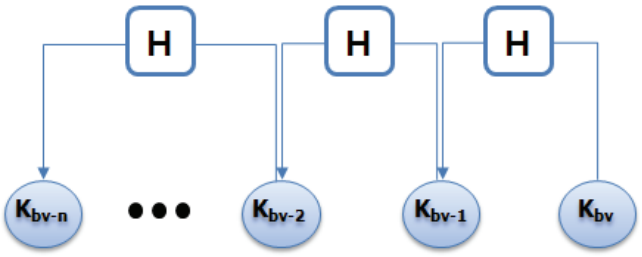
- 권한이 없는 센서 노드들은 클러스터 헤더 선출에 참여 할 수 없다.
- 공격자는 다른 노드의 클러스터 헤더 선출 값을 변경 할 수 없으며, 클러스터 헤더 선출을 컨트롤 할 수 없다.
- 클러스터 헤더가 선출 되면 한 라운드 동안 클러스터 헤더는 변경되지 않는다.

3.2 동작 과정

확률적 키 분배 방식을 사용하는 센서 네트워크에서의 안전한 클러스터 헤더 선출 기법의 동작 과정은 다음과 같다.

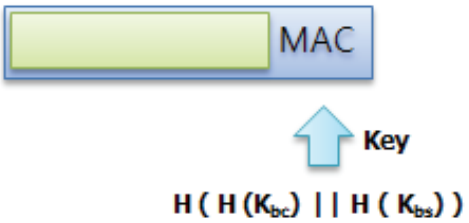
센서 네트워크가 전개되기 전에, 모든 센서 노드는 BS와의 유일한 공유키 한 쌍과 각 노드를 식별할 수 있는 ID를 가지고 있다. 또한 확률적 키 분배 방식을 사용하므로, 전체 키 풀에서 랜덤하게 키를 분배 받아, 같은 키를 공유한 노드끼리 데이터를 송수신하고, 같은 키를 공유하지 않은 노드는 다른 노드를 통해 데이터 송수신을 한다.

네트워크가 전개 된 후, 지역적으로 가까운 노드들이 클러스터링을 형성하고, 클러스터 헤더를 선출하게 되는데, 최초의 클러스터 헤더 선정은 LEACH 기반의 클러스터 헤더 선출 알고리즘에 따라 랜덤하게 선택 된다. 랜덤하게 선택된 클러스터 헤드는 아래의 (그림 2)와 같이 BS와 공유한 비밀키로 키 체인(key chain)을 만든다. (그림 2)에서 K_{bc}는 BS와 클러스터 헤드가 공유한 비밀값 이자 키 체인을 만드는 commitment이며, K_{bc-n}까지 n개의 키 체인을 일방향 해쉬 함수를 사용하여 n개 만큼 생성한다. 클러스터 헤드는 라운드가 시작되면, K_{bc-n}부터 일정한 시간 간격으로 K_{bc-1}까지 클러스터 내의 노드들에게 전송한다.



(그림 2) 클러스터 헤드의 key chain 생성

클러스터 헤드가 아닌 센서 노드들도 BS와 센서 노드만이 공유한 비밀키로 키 체인을 생성한다. 그리고 클러스터 헤드로부터 키 체인의 키를 받았을 때, 각각의 센서 노드가 생성한 키 체인을 붙이고(concatenate, ||) 그 값을 해쉬하여, MAC의 키로 사용한다.



(그림 3) MAC의 키로 사용

이와 같은 방법으로 클러스터 헤더 선출 값이 되는 에너지 잔여량을 메시지에 넣고 데이터를 전송하게 되면, 전송하는 센서 노드 이외의 어떠한 노드도 데이터를 변경할

수 없다. 또한 확률적 키 분배 방식을 사용하므로, 에너지 잔여량을 보고하는 센서노드와 클러스터 헤드간의 공유되는 키가 없을 때, 다른 노드를 통해 전송하게 되는데, 이 때 중간 노드도 MAC의 키를 알 수 없기 때문에 메시지 안의 데이터를 변경 할 수 없다.

또한 클러스터 헤더도 데이터를 받았을 때, 즉시 이 값이 유효한 값인지 알 수 없다. 클러스터 헤더가 생성한 K_{bc-i}값은 알 수 있어도 K_{bs-i}값을 알지 못하기 때문이다. 그래서 센서 노드는 클러스터 선출을 위한 메시지를 전송한 후에 K_{bs-1} 값을 전송하여 메시지의 인증과 무결성을 증명하게 된다. 만약 메시지와 MAC 값이 다르면 악의적인 노드가 공격을 시도한 것으로 간주하고 에너지 잔여량을 다시 보고 받게 된다.

4. 안전성 분석

본 논문은 확률적 키 분배 방식을 사용하는 센서 네트워크에서 클러스터 헤더 선출값에 대한 무결성과 인증을 제공한다. 기존의 uTESLA 기법은 데이터 무결성을 제공할 수 있지만 확률적 키 분배 방식을 사용하므로, 같은 키를 공유한 악의적인 센서 노드에 의해 재전송 공격에 노출된다. 하지만 본 논문에서 제안한 기법은 클러스터 헤더의 키 체인만으로 클러스터 헤더 선출값을 MAC으로 인증하여 전송하는 것이 아니라, 각각의 센서 노드들도 키 체인을 생성하여, 둘의 해쉬값으로 클러스터 헤더 선출값을 MAC으로 인증하여 전송하기 때문에, 같은 키를 공유한 센서 노드도 메시지를 만들 수 없다. 따라서 클러스터 헤더 선출값의 무결성과 클러스터 헤더 선출값을 전송하는 노드의 인증을 제공할 수 있다.

5. 결론 및 향후 연구

본 논문에서 제안하는 계층적 라우팅 프로토콜에서의 안전한 클러스터 헤더 선출 기법은 클러스터 헤더의 키 체인과 센서 노드의 키 체인을 사용하여 메시지 무결성과 인증 메커니즘을 제공한다. 따라서 클러스터 헤더 선출시, 악의적인 노드에 의해 클러스터 헤더 선출값이 변경되지 않으며, 공정한 클러스터 헤더를 선출 할 수 있고, 악의적인 노드에 의한 잘못된 정보 전송을 막을 수 있었다.

향후 연구로는 본 논문에서 제안하는 안전한 클러스터 헤더 선출 기법에 대한 시뮬레이션을 구축하여, 본 논문의 안전성을 증명 할 것이다. 또한 무선 센서 네트워크에서의 안전하고 효율적인 정보 전달을 위해서 악의적인 노드를 탐지하는 기술에 대한 연구를 수행할 것이다.

참고문헌

[1] A.D. Amis, R. Prakash, T.H.P. Vuong, and D. T. Huynh. “Max-min d-cluster formation in wireless ad hoc networks”, In Proceedings of IEEE INFOCOM 2002, March 1999.

[2] B. Parno, A. Perrig, and V. Gligor. “Distributed detection of node replication attacks in sensor networks”, In IEEE Symposium on Security and Privacy, May 2005.

[3] H. Chan and A. Perrig. “PIKE: Peer intermediaries for key establishment in sensor networks”, In Proceedings of IEEE Infocom, March 2005.

[4] H. Chan, A. Perrig, and D. Song. “Random key predistribution schemes for sensor networks“, In IEEE Symposium on Security and Privacy (S&P), pages 197 - 213, May 2003.

[5] O. Younis and S. Fahmy. “Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach”, In Proceedings of IEEE INFOCOM 2004, March 2004.

[6] Zhang zhenjiang; Liu yun, “An Energy-Efficient Redundant Nodes Tree Mechanism for Wireless Sensor Networks”, International Conference on Systems and Networks Communication, pp. 63 - 63, October 2006.

[7] G.Gupta and M.Younis, “Fault-tolerant clustering of wireless sensor networks”, In Proceeding of IEEE Wireless Communications and Networks Conference, pp. 1579 - 1584, March 2003.

[8] Chonggang Wang, Sohraby, K., Bo Li, Daneshmand, M., Yueming Hu, “A survey of transport protocols for wireless sensor networks Network”, IEEE Vol 20, Issue 3, pp. 34 - 40, May-June 2006.

[9] A. Manjeshwar and D. P. Agrawal, “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks”, 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

[10] Al-Kahtani, M.S.; Mouftah, H.T., “A stable clustering formation infrastructure protocol in mobile ad hoc networks”, IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, August 2005.