센서네트워크에서 효율적인 클러스터링 기법

채미연*, 송주석*
*연세대학교 컴퓨터과학과
coaldus@emerald.yonsei.ac.kr

Efficient Clustering Technique in Sensor Network

Mee-Youn Chae*, JooSeok Song*
*Dept of Computer Science, Yonsei University

요 약

암호화를 통하여 데이터의 기밀성을 유지하고, 데이터 인증과 무결성을 보장하기 위하여 MAC을 사용하는 LEAP 프로토콜의 장점과 에너지 효율성을 고려하는 LEACH 프로토콜의 방식을 접목하여 효율적인 클러스터링 기법을 제시한다.

1. 서론

센서 네트워크는 환경 및 생태감시, 군사작전, 건강관리 (Heath Care), 물류관리 (Logistics) 등 많은 분야에서 활용되고 있다. 특히, 통신대역폭이 기존의 근거리 통신에서 벗어나 원거리 통신이 가능해지고, 또한 저 비용, 저 전력, 대 용량 센서노드의 대량 생산도 현실화됨에 따라 더 많은 분야에서 센서노드를 활용할 수 있게 되고 있다.

이러한 기술적인 진보를 기초로 센서 네트워크에 대한 연구가 다양하게 나타나고 있으면, 특히 센서의 구조적 결점인 제한된 계산능력, 저장 공간, 전력으로 인해 등한시 되었던 보안 분야의 연구도 지속적으로 이루어지고 있고 다양한 보안 기법들이 발표되었다.

본 논문은 다음과 같이 구성된다. 2장에서 보안기법 중 키 관리 기법에 대한 기존 연구를 알아보고, 3장에서는 개선된 클러스터링 기법을 제안하며, 4장에서는 보안 측면에 대한 분석을 실시하고, 5장에서 마무리 한다.

2. 기존연구

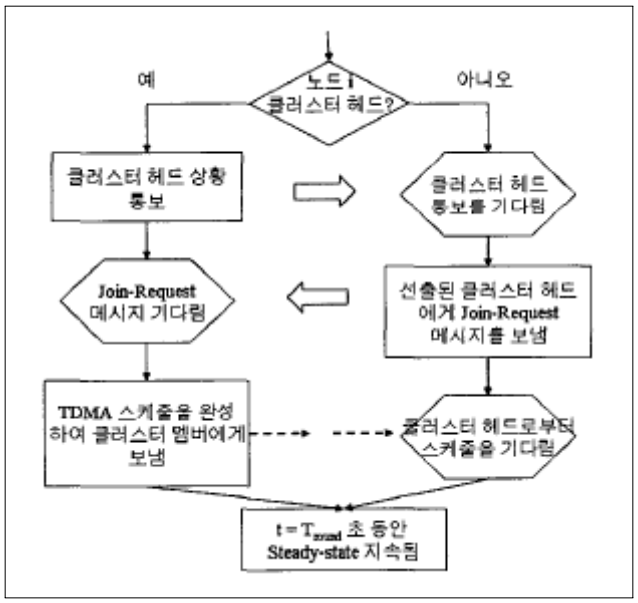
오버헤드를 최소로 하여 센서네트워크의 목적에 맞는 프로토콜로 대표적인 것이 SPINS[1] 프로토콜이다. SPINS 프로토콜은 기밀성, 사용자 인증, 무결성, 적시성의 보안 서비스를 제공하는 SNEP(Sensor Network Encryption Protocol)과 브로드캐스팅 인증 서비스를 제공하는 μTESLA로 구성된다. 인증서비스에 μTESLA를 이용하는 방법은 대칭키의 지연된 공개를 통하여 비대칭 키의 효과를 가져 올 수 있기 때문에 효과적인 인증구조를 제공한다.

대칭 키 방식의 문제점은 같은 키를 많은 사용자가 공유하였을 경우 하나의 키가 손상 되었을 때에 전체 네트워크의 안전성에도 위험이 수반된다는 것에 있다. 일반적으로, 한 그룹의 센서노드들은 수십에서 수백 개에 이른다. 기존의 센서 네트워크에 대한 연구들 중 그룹 키 생성 과정을 살펴보면, 각 노드들의 partial key를 이용하여 그룹 키를 생성하는 방식이다. 그러나, 위의 예와 같은 노드 수가 많은 그룹의 그룹 키를 생성할 경우 수십에서 수백 개의 partial key를 모두 조합한다는 것은 시간적인 측면이나 에너지 소모 측면에서 상당히 비효율적이다. 따라서 센서 네트워크에서 사용되는 다양한 통신방식에 적합하도록 키 구조를 제안하는 연구들이 있는데 대표적인 프로토콜이 LEAP[2] 프로토콜이다. LEAP은 노드간의 교환 메시지 종류가 서로 다르며, 각 종류별로 보안 요구사항이 다르다는 면에서 다중 키의 사용을 제안하였다. 기지국(BS)과 센서 노드 간 통신에는 독립적 노드 키를, 센서노드 간에는 pair-wise 키를, 센서노드와 모든 주변 이웃 노드 간에는 클러스터 키를, 네트워크 전체를 통신하기 위해서는 그룹 키를 사용하였다.

더 나아가 센서 네트워크가 제한된 자원만을 가지고 있는 단점과, 데이터 전송비용이 처리비용보다 큰 부분을 보완하기 위하여 각각의 센서노드의 데이터를 BS(베이스스테이션)이 모두 수집/처리하는 방식보다는 중간 노드(클러스터)[3][4]가 이를 통합/정제하는 방법과 모든 모드가 에너지 소비를 균등하게 할 수 있는 방법(LEACH)[5]이 제안되고 있다. 그림1은 LEACH 프로토콜에서 분산된 클러스터의 형성 순서를 보여준다.

3. 제안하는 기법

센서 네트워크에서 중요한 고려사항은 '제한된 자원으로 에너지 효율성을 어떻게 극대화 시킬 수 있는가?' 와 '저장 공간과 프로세싱 오버헤드를 최소화 하는 보안서비스를 어떻게 제공하느냐?' 이다. 이 두 가지 문제는 서로 상반되는 문제로서 에너지 효율성을 극대화시키면 보안성이 결여되고 보안성만을 강조하면 빠른 자원고갈을 유발한다. 이 논문에서는 효율적인 클러스터링 기법을 통해 센



(그림 1) LEACH 프로토콜의 분산된 클러스터 형성 순서도

서 노드 간 균형적인 생애주기를 연장하고, 에너지 소비와 프로세싱 오버헤드를 최소화하기 하면서 보안성을 유지하는 기법을 제안한다.

LEAP 프로토콜은 T_{min}(공격자가 노드를 캡쳐하는데 필요한 최소의 시간) 시간이 지나기 전에 키 생성과정을 마치고 Initial key 인 K_I를 지움으로 보안성을 높인다. 그러나 대역폭이 좁은 센서의 특성상 키를 생성하는데 사용되는 시간이 T_{est}가 길어져서 T_{min}을 초과하는 사태가 발생 시에 공격자는 노드의 메모리로부터 K_I를 획득할 수 있게 되고, 이를 이용하여 전체 네트워크의 보안이 무너질 수 있는 상황이 발생할 수 있다. 따라서 T_{est}를 최대한으로 줄이는 것이 관건이 된다. 이를 위한 방법을 LEAP프로토콜이 제시한 다중 키와 네트워크의 통신형태에 따라 키 생성 과정을 통하여 효율적인 클러스터링 기법을 제안하겠다.

모든 노드는 생성단계에서 K_I를 포함하고 있다.

- 유니 캐스트

BS와 센세 노드, 노드와 노드사이의 통신형태로이다. BS와 노드간의 통신에서는 둘 사이에 공유하고 있는 개인키로 암호화 된다. 각 노드는 K_I와 키 생성함수를 이용하여 자신의 개인키를 생성한다.

$$K_u = f_{K_I}(u)$$

노드와 노드사이의 통신에서는 pair-wise 공유키(쌍대키)로 암호화 된다. 노드 u는 자신의 IDu와 $Nonce_u$값을 브로드캐스트하면 이웃노드 v는 자신의 IDv와 인증값 MAC_{K_v} =($Nonce_u$ | IDv)를 보내온다. 노드 u는 K_I를 이용하여 K_v를 계산해 낼 수 있으므로 두 노드 사이에 쌍대키를 생성할수 있다.

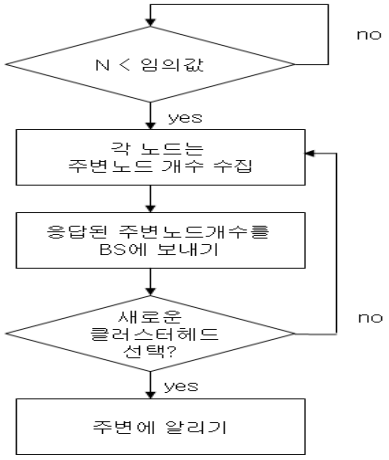
$$K_{u.v} = f_{K_v}(u)$$

키생성 과정이 Rx나고 나면 노드들은 K_I와 쌍대키 생성 과정에서 생성되었던 다른 노드들의 개인키를 삭제한다.

- 멀티 캐스트

한 노드와 노드들 간의 통신형태로서, 클러스터 키를 이용하여 암호화 된다. 이 논문에서 가장 중요하게 생각하는 부분이 클러스터 헤드를 어떻게 선정하느냐 하는 문제이다.

노드가 임의의 지역에 살포 되었을 때 각 노드들은 자신의 주변에 있는 노드들의 개수(N)를 감지하여 저장한다. BS는 노드에게 패킷을 broadcast하고, 이 패킷을 받은 모든 노드들은 응답패킷에 주변노드의 개수의 값을 넣어 응답한다. 그러면 BS는 각 노드들의 값을 분석하여 가장 큰 값을 가지고 있는 노드를 클러스터 헤드로 선정한다. 각 노드들은 주기적으로 자신의 주변노드들의 개수를 업데이트하고, 이를 BS에 통보하게 되는데, 주변노드의 수가 임계값보다 작아지면 클러스터 헤드의 임무를 중단한다.



(그림 2) 클러스터 헤드의 동적 업데이트 과정

클러스터 헤드로 선정된 노드는 자신이 클러스터 헤드가 되었음을 노드들에게 브로드 캐스트 한다. 브로드 캐스트를 위한 키 체인과 키 생성은 BS에 의뢰하여 수행되며 과정은 LEAP와 동일하다.

- 브로드 캐스트

BS와 모든 노드간 통신이다. 브로드캐스트 메시지를 누가 보냈는지에 대한 인증이 필요한데 이 경우 μTESLA를 사용한다.

4. 보안성 분석

제안된 방식은 암호화를 통하여 데이터의 기밀성을 유지하고, 데이터 인증과 무결성을 보장하기 위하여 MAC을 사용하는 LEAP 프로토콜의 장점을 그대로 살리면서 에너지 효율성을 고려하는 LEACH 프로토콜의 방식을 접목하려고 시도하였다.

클러스터 헤드가 분산된 BS의 역할을 수행함으로서 동적인 업데이트가 가능하게 되고, 노드는 BS보다 접근성

을 향상시켜 인증에 소요되는 평균시간을 단축시키는 역할을 할 수 있게 되었다.

5. 결론

센서 네트워크의 장점은 가격이 저렴함과 동시에 적용과 관리가 쉽다는 것이다. 각 노드들은 환경과 무관하게 생애 주기 동안 데이터 수집활동을 지속하여야 하며, 이를 위하여 효율적인 에너지 사용방법이 필수적인 것이다. 이를 위하여 에너지 효율성을 고려한 기존의 알고리즘을 적용하고 클러스터링 기법에 대한 연구를 하기위해 이를 제안하였다.

참고문헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," In Proceeding of Seventh Annual ACM International conference on Mobile Computing and Networks(Mobicom), July 2003

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP : Efficient Security Mechanism for Large-Scale Distributed Sensor Networks," In Proceedings. of the 10th ACM CCS '03, October 2003.

[3] T. Shepard, "A channel access scheme for large dense packet radio network," In proceeding of ACM SIGCOMM, pp. 219-230, August 1996

[4] 장근원, 신동규, 전문석, "센서네트워크 통신에서 대칭키 방식과 LEAP을 적용한 안전한 동적 클러스터링 알고리즘 설계," 정보보호학회 논문지 V16, N03, pp. 29-37 2006. 6.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications, Vol. 1, NO 4, pp. 660-670, October 2002