情報保護學會論文誌
第16卷 第3號, 2006. 6

센서네트워크 통신에서 대칭키 방식과 LEAP을 적용한 안전한 동적 클러스터링 알고리즘 설계

장 근 원†, 신 동 규, 전 문 석‡
숭실대학교

Desing of Secure Adaptive Clustering Algorithm Using Symmetric Key and LEAP in Sensor Network

Kun-Won Jang†, Dong-Gyu Shin, Moon-Seog Jun‡
Soongsil University

요 약

최근 무선통신기술의 발달은 센서 네트워크 관련연구를 촉진하였으며 다양한 형태의 센서 네트워크 통신방식에 적합한 방법들이 제안되고 있다. 센서 네트워크 연구방향은 제한된 자원에서 에너지효율을 극대화시키기 위한 방법과 그동안 주목받지 못했던 보안관련 연구들로 구분된다. 에너지효율을 높이기 위한 방법으로 노드간 데이터 통합과 통합을 수행하는 클러스터 헤드의 적절한 선택 알고리즘이 제안되었으며, 보안성 강화를 위해 센서에 적용 가능한 암호화 기법과 비밀 키를 관리하기 위한 방법들이 제안되고 있다. 그러나 다양한 형태의 통신방식이 존재하는 센서 네트워크에서 안전하면서도 동시에 에너지 효율성을 고려한 통합적 연구는 아직 초기단계에 있다. 본 논문에서는 자원효율적인 클러스터링 프로토콜과 다양한 통신방식에 적당한 키 관리 알고리즘을 결합하여 향후 민감한 데이터를 처리하는 센서네트워크 시스템에 적용할 수 있는 통합적 프로토콜을 제안한다.

ABSTRACT

Recent advances in wireless communication technology promotes many researches related to sensor network and brings several proposals to fit into various types of sensor network communication. The research direction for sensor network is divided into the method to maximize an energy efficiency and security researches that has not been remarkable so far. To maximize an energy efficiency, the methods to support data aggregation and cluster-head selection algorithm are proposed. To strengthen the security, the methods to support encryption techniques and manage a secret key that is applicable to sensor network are proposed, too. However, the combined method to satisfy both energy efficiency and security is in the shell. This paper is devoted to design the protocol that combines an efficient clustering protocol with key management algorithm that is fit into various types of sensor network communication. This protocol may be applied to sensor network systems that deal with sensitive data.

Keywords : *Secure sensor network, Routing protocol, Clustering, Key management*

접수일: 2006년 1월 11일; 채택일: 2006년 5월 30일
† 주저자, jaques72@naver.com
‡ 교신저자, mjun@computing.ssu.ac.kr

Ⅰ. 서 론

최근 무선통신 관련 기술의 발달로 인해 보다 작

은 크기의 센서 노드가 사용되고 있으며 통신 대역폭에 있어서도 기존의 근거리 통신에서 벗어나 보다 먼 거리의 원거리 통신도 가능해 지고 있다. 또한 상용화 측면에서 센서노드의 중요한 요구사항으로 알려져 왔던 저비용, 저전력, 다기능 센서노드의 대량생산도 현실화 되고 있다.

이러한 기술적인 진보를 근간으로 센서 네트워크 관련기술에 대한 최근의 연구가 다양하게 나타나고 있으며, 그동안 비용적인 문제로 활발하지 못했던 보안부문과 에너지 효율성에 관한 연구들도 많이 제안되고 있다. 센서 네트워크 보안과 관련된 연구는 제한된 자원을 사용하는 센서의 특성과 저비용 구조를 유지하기 위한 상용화 요구로 인해 센서에 대한 보안 측면을 등한시 하게 되었으며, 암호화 기법을 이용한 보안 솔루션 보다는 센서 네트워크 응용기술 중의 하나인 RFID tag를 이용한 개인 프라이버시 강화 기법 등이 제안되어 왔다 [1]. 그러나 단순한 사생활보호 차원으로는 무선 통신망이 가지고 있는 보안상 취약성을 해결할 수 없으며, 이를 해결하기 위한 보안 프로토콜이 제안되고 있다. 대표적인 것이 SPINS (Security Protocols for Sensor Network)[3] 과 LEAP(Localized Encryption and Authentication Protocol)[2] 이다. 에너지 효율성과 관련하여 많은 센서 시스템들은 관리자의 부재 또는 전장과 같은 적대적인 환경에서 작동해야 하므로 추가적인 전원공급이 불가능하다. 따라서 기 적용된 센서노드의 생애주기가 센서 네트워크 환경에 많은 영향을 주기 때문에 에너지 절약에 대한 방법들이 제안되고 있다. 분산처리 방식으로 정보를 수집하는 Directed Diffusion 방식[4] 과 계층적인 클러스터링 방식을 이용한 LEACH(Low-Energy Adaptive Clustering Hierarchy)[5] 프로토콜이 대표적이다.

본 논문에서는 보안성과 에너지 효율성을 동시에 고려하여 민감한 데이터를 처리하는 특정 라우팅 환경과 그 구조에서 사용가능한 보안 프로토콜을 접목시켜 적대적인 환경에서도 에너지를 최소로 사용하면서도 안전한 통신 구조를 제공하는 새로운 라우팅 프로토콜을 제안한다. 군사 시스템과 같이 민감한 데이터를 수집하는 센서 네트워크 시스템에서는 일반적인 센서네트워크 시스템과는 달리 모든 통신과정의 보안을 요구하기 때문에 발생 가능한 모든 통신구조에 대한 암호화와 키 관리 기법을 제시하였다.

본 논문의 구조는 다음과 같다. 2장에서 관련연구로 센서 네트워크 시스템에서 요구되는 보안성과 자원효율성을 고려한 제안된 연구들을 살펴보고, 3장에서는 보안과 라우팅 프로토콜을 결합한 안전한 클러스터링 프로토콜을 설계하고, 4장에서는 요구사항에 대한 평가를 하였다. 마지막으로 5장에서는 앞으로의 연구과제에 대해서 살펴보도록 하겠다.

II. 관련연구

에너지 효율성과 보안강화라는 측면은 서로 밀접한 관계가 있다. 보안은 추가적인 CPU의 사용을 통해 프로세싱 오버헤드를 유발하며, 반대로 제한된 에너지는 암호화 혹은 인증 키(key)의 생애주기를 단축시킨다. 센서 네트워크 노드의 생애주기가 만료 된다면 안전한 통신을 위하여 센서 네트워크의 재구성과 비밀 키의 재설치가 필수적이며 이는 추가적인 에너지의 사용을 유발하게 되기 때문이다. 본 논문에서는 센서네트워크 시스템이 데이터를 처리할 때 효율성뿐만 아니라 안전성을 요구하는 환경에서 적용 가능한 알고리즘을 제안한다. 따라서 보안성, 효율성과 관련하여 기존에 제안된 연구를 살펴본다.

1. 보안 요구사항

기존의 보안관련 솔루션들을 센서 네트워크에 적용하는 것은 현실적으로 불가능하다. 제한된 자원의 사용과 재충전이 불가능한 구조적 특성을 고려하지 않은 방식이기 때문이다. 무선 통신관련 기술의 발달로 가용한 자원과 저장 공간이 늘어나고 있지만 여전히 불충분하며 오버헤드를 최소로 하고 센서 네트워크에 목적에 맞는 프로토콜이 제안 되고 있다. SPINS[3] 프로토콜의 경우 오버헤드를 유발하는 비대칭 키 구조를 지양하고 대칭키 방식을 사용함에도 불구하고 데이터 암호화뿐만 아니라 메시지 인증, 사용자 인증과 같은 서비스를 제공한다. SPINS 프로토콜은 기밀성, 사용자 인증, 무결성, 적시성 등의 보안 서비스를 제공하는 SNEP(Sensor Network Encryption Protocol)과 브로드캐스트 인증서비스를 제공하는 μTESLA(Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol의 마이크로 버전)으로 구성된다. 그림 1은 브로드캐스트 인증서비스를 제공하는 μTESLA의 타임라인을 이용한 키 체인의 예를 보여주고 있다. 그림에서 키 체인의 각 키는 일치되는 타임 인터벌을 가지며 같은 인터벌에 존재하는 모든 패킷은 같은 키로 인증된다.

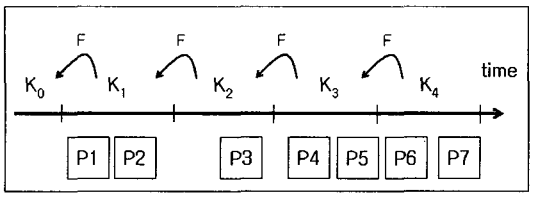


그림 1. SPINS 의 소스 인증을 위한 time-released 키 체인의 예

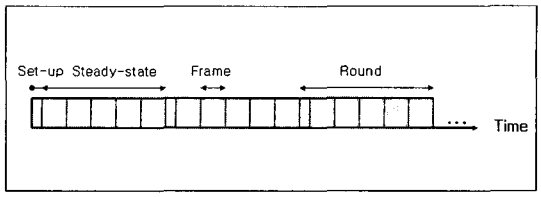


그림 2. 2단계 (Set-up / Steady-state phase)로 구성된 라운드 타임라인

수신자는 패킷을 받더라도 키가 공개될 때까지 기다려야 한다. 만약 인터벌 4에서 BS(Base Station)이 K_2를 브로드캐스트 하게 되면 $K_0 = F(F(K_2)), K_1 = F(K_2)$의 연산을 통해 수신자는 인증키를 검증할 수 있으며 패킷을 인증할 수 있게 된다. 이 방법은 대칭키의 지연된 공개를 통하여 비대칭키의 효과를 가져올 수 있기 때문에 효과적인 인증 구조를 제공한다. 또한 기존의 대칭 키 방식의 보안관련 서비스 중에서 불필요한 요소를 최대한 생략하여 오버헤드를 최소화하고 센서 네트워크 적용을 용이하게 하였다.

대칭 키 방식의 문제점은 같은 키를 많은 사용자가 공유하게 되었을 때, 하나의 키가 손상되면 전체 사용자의 안전성이 위험하다는 것이다. 따라서 키에 대한 관리가 중요하다. 센서 네트워크에서 사용하는 통신은 다양한 형태[10]로 이루어진다. BS가 센서노드에게 질의를 보내거나 노드간 데이터를 전송하거나 노드에서 BS로 최종데이터를 전송하는 등의 서로 다른 형태의 통신구조가 존재한다. LEAP[2] 프로토콜은 이와 같은 다양한 통신방식에 적합하도록 개인키, 쌍대 키(Pairwise key), 클러스터 키, 그룹 키와 같은 4가지 형태의 키 구조를 제안한다. 이를 위하여 생산과정 중에 마스터키를 삽입[9]하고 센서 시스템 적용 후에 마스터키를 통해 파생키를 생성하여 인증과 암호화에 사용한다. 또한 파생키를 생성한 후 마스터키를 영구 삭제하여 공격자에 의해 손상되더라도 그 피해를 최소화 하도록 하고 있다.

2. 자원 요구사항

센서 네트워크는 제한된 자원만을 소유한다. 센서 네트워크에서 발생하는 에너지 소비의 유형은 데이터 처리와 전송이다. 일반적으로 데이터 전송비용이 처리 비용보다 크기 때문에 각각의 센서노드의 데이터를 BS에서 모두 수집하여 처리하는 방식보다는 중간 노드가 이를 통합, 정제하여 필요한 정보를 BS로 보내는 방법이 제안되고 있다[4].

센서 노드는 데이터를 보내는 경우를 제외하고 에너지 절약을 위해 대기상태로 된다[5]. 그러나 데이터 수집 노드의 경우는 수집활동, 데이터 통합, 전송 등의 활동을 위해 지속적으로 에너지를 사용하기 때문에 조기에 자원고갈에 빠지게 된다. 따라서 효율적인 데이터 통합을 위하여 클러스터를 구성하는 방법[12][13]과 모든 노드가 에너지소비를 균등하게 할 수 있도록 하는 방법(LEACH)[5]이 제안되고 있다. 그림 2에서처럼 LEACH의 연산은 라운드로 구분되며 각 라운드는 클러스터를 형성하는 set-up 단계와 데이터가 노드에서 클러스터 헤드로 전송되는 steady-state로 이루어지며 반복적으로 클러스터 헤드가 선출된다. LEACH 프로토콜은 모든 노드의 균형적인 에너지사용을 위하여 분산된 클러스터헤드 선택 알고리즘을 사용한다(그림 3). 즉 각 라운드 별로 적당한 수의 클러스터 헤드를 선택하여 운영하고 한번 선택되었던 노드들은 일정 라운드가 지날 때까지 다시 클러스터 헤드가 될 수 없다. 결과적으로 모든 노드가 차례로 클러스터 헤드가 되록 하여 에너지가 균등하게 소비된다.

Ⅲ. Secure Dynamic Clustering Protocol

센서 네트워크와 관련된 중요한 고려사항은 제한된 자원으로 에너지 효율성을 어떻게 극대화 시킬 수 있는지와 저장 공간과 프로세싱 오버헤드를 최소화하여 보안 서비스를 적용할 수 있느냐 이다. 그동안의 연구는 주로 에너지 효율성에 관하여 이루어져 왔으며 센서노드의 제한된 자원으로 인하여 보안성에 대한 연구는 활발하게 이루어 지지 않았다. 더불어 이 두 가지 문제는 교환조건(trade off)에 해당한다. 에너지 효율성을 극대화시키다 보면 보안성이 결여되고 보안성만을 강조하면 빠른 자원고갈을 유발한다. 본 연구에서는 제한된 자원을 효율적으로 사용하

는 방법을 이용하여 민감한 데이터를 처리하는 환경에서 적은 자원을 요구하는 대칭키 방법을 적용하였으며, 더불어 대칭키 방식에서 키 관리 방식의 어려움을 해결하기 위하여 센서네트워크 시스템의 다양한 통신형태에 적합한 키 관리 메커니즘을 제안한다.

본 연구는 효율적인 클러스터링 기법을 통해 센서 노드간 균형적인 에너지 소비를 유도하여 센서 네트워크의 생애주기를 연장하고, 에너지 소비와 프로세싱 오버헤드를 최소로 할 수 있는 보안기법 그리고 키 관리 기법을 제안하여 적대적 환경에서 데이터를 취급하는 센서 네트워크 시스템에 적용 가능하도록 하였다. 먼저 센서 네트워크에서 사용되는 통신 형태와 키 교환 알고리즘을 살펴보고 이를 이용하여 안전하게 클러스터를 형성하기 위한 방법을 제안한다. 클러스터를 형성한 후 안전하게 데이터를 교환할 수 있는 방법에 대해서도 제안한다.

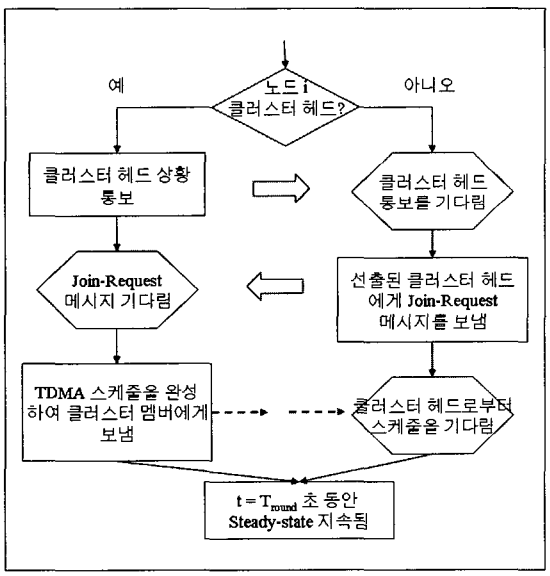


그림 3. LEACH 프로토콜의 분산된 클러스터 형성 순서도

1. 기호 및 정의

본 연구에서 사용할 키의 종류는 개인 키, 쌍대 키, 클러스터 키, 마스터 키 [2]등이 있다. 모든 노드는 생산단계에서 마스터키(K^m)를 포함하고 있으며, 생성된 키는 통신 중에 전송되지 않으며 키 생성 함수 f(u)에 의해 만들어진다. 다음은 노드 u의 아이디를 통한 개인 키(K_u) 형성과정을 보여준다. BS는 키를 저장하지 않으며 필요할 때 연산을 통해 생성하여 사용한다.

$$K_u = f_{K^m}(u) \tag{1}$$

센서노드에서 가장 많이 사용하는 노드간의 통신을 위해 쌍대 키(K_{uv})를 생성하여 공유하여야 한다. 다음은 노드 u와 v가 쌍대 키를 형성하는 과정이다. 노드 u, v는 키 생성함수를 각각 적용하여 쌍대 키를 생성한다.

$$K_{uv} = f_{K_v}(u) \tag{2}$$

클러스터 헤드와 클러스터의 각 노드간의 통신을 위해 클러스터 내에서 키를 생성하여 공유하여야 한다. 다음은 클러스터 헤드 u와 모든 클러스터의 노드 v_1, v_2, v_3, ..., v_m,와 클러스터 키(K_c)를 생성하고 이를 공유하는 과정이다. 노드 u는 임의의 값 r을 생성하고 키 생성함수를 통해 클러스터 키를 생성한다. 생성된 클러스터 키는 쌍대 키로 암호화 하여 클러스터의 노드에게 전송된다. MAC는 메시지 인증 코드이며 C는 카운터 값이다.

$$K_c = f_{K_u}(r)$$
$$u \rightarrow v_i : E_{\langle K_{ui}, C\rangle}(K_c), MAC(K_{uv_i}, C | E_{\langle K_{ui}, C\rangle}(K_c)) \tag{3}$$

노드를 각각 u, v라고 했을 때, 암호화 메시지 D를 전달하는 과정은 다음과 같다. 이때 의미론적 보안(Semantic security)을 위하여 카운터 C를 추가하여 보낸다. 암호화 키는 통신형태에 따라서 틀려진다.

$$u : D = E_{\langle K_{uv}, C\rangle}(M)$$
$$u \rightarrow v : D, MAC(K_u, C | D) \tag{4}$$

브로드캐스트는 μTESLA [3]을 이용한다. μTESLA는 느슨한 동기구조(Loosely synchronized scheme)를 사용하며 타임라인을 구성하고 키 체인과 결합한다. BS는 패킷의 메시지 인증 코드(MAC)를 계산하기 위해 현재 시간간격 t를 사용한다. 시간간격 t가 종료되고 지연시간 i후에 키 값 K_t를 공개하면 수신 노드 v는 수신된 패킷을 인증할 수 있다. 따라서 노드가 추가될 때 새로운 노드는 키 체인의 인증 값 $K_i = F(K_{i+1})$와 마스터 키를 알아야 하고, 단방향 키 체인의 키 공개 일정과 느슨한 시간 동기가 되어야 한다. 따라서 BS가 새롭게 추가될 노드 u에게 보내는 메시지는 현재 시간 T_s, 과거 시간간격 i에서

사용된 단방향 키 체인의 키 K_i, 시간 간격 i에 시작 시간 T_i, 시간간격의 지속시간 T_{dura}, 지연시간 δ 를 포함한다. 새로운 노드 v는 브로드캐스트 인증을 위해 요청 메시지를 보내며 수신자를 증명하기 위해 넌스(Nonce)를 포함한다. 요청을 받은 BS는 인증에 필요한 메시지를 보낸다.

$$v \rightarrow BS: N_v$$
$$BS \rightarrow u: T_s|K_i|T_i|T_{dura}|\delta, MAC(K_v, N_v|T_s|K_i|T_i|T_{dura}|\delta) \quad (5)$$

데이터 통합을 통해 에너지 효율성 높이기 위해서 동적 클러스터링 방법을 사용한다 [5]. 균등한 에너지 소비를 위해 센서 네트워크의 노드는 확률 $P_u(t)$에 의해 임의로 클러스터 헤드가 되며 한번 역할을 한 후 $P_u(t) = 0$이 되어 일정 라운드까지는 클러스터의 노드 역할만을 하게 된다. 클러스터를 형성하기 위해 전체 센서노드 N 중에서 넌 클러스터 헤드 노드가 확률 $P_u(t)$을 계산하여 다음 라운드 r+1에서 클러스터 헤드가 될지를 결정한다. 각 라운드에서 선출되는 클러스터 헤드의 수는 k이다.

$$P_u(t) = \frac{k}{N - k\left(r \bmod \frac{N}{k}\right)} \quad (6)$$

2. 통신형태

센서 네트워크에서 사용하는 통신형태로는 유니캐스트, 멀티캐스트, 브로드캐스트 등이 있다. 먼저 유니캐스트 형태의 예는 노드에서 BS, 노드와 노드간의 통신이다. 노드에서 BS로의 전송은 클러스터 헤드가 데이터를 수집, 정제하여 통합데이터를 보낼 때 이루어지고 노드와 BS간에 공유하고 있는 개인 키를 통해 암호화 한다. 이때 CSMA 방식을 사용한다. 노드간의 통신은 클러스터의 노드가 클러스터 헤드에게 기초자료(Raw data)를 전송할 때 발생하며 공유하고 있는 쌍대 키를 통하여 이루어진다.

$$u \rightarrow BS: E_{\langle K_u, C\rangle}(M), MAC(K_u, C|E_{\langle K_u, C\rangle}(M)) \quad (7)$$
$$u \rightarrow v: E_{\langle K_{uv}, C\rangle}(M), MAC(K_{uv}, C|E_{\langle K_{uv}, C\rangle}(M))$$

멀티캐스트 형태의 예는 노드와 노드간의 통신이다. 즉, 클러스터 헤드가 질의 메시지를 클러스터의 모든 노드에게 전송할 때 발생하며 클러스터 키를 통해 암호화 한다. 클러스터 헤드 u가 클러스터의 모든 노드 $v_1, v_2, v_3, \ldots, v_m$, 에게 메시지를 보내는 형식은 다음과 같다.

$$u \rightarrow v_i: E_{\langle K_c\rangle}(M), MAC(K_c, E_{\langle K_c\rangle}(M)) \quad (8)$$

브로드캐스트는 BS와 센서 네트워크 모든 노드간의 통신이다. 브로드캐스트 통신형태에서는 암호화는 하지 않으며 브로드캐스트 메시지를 누가 보냈는지에 대한 소스 인증이 필요하다. 정의에서같이 동기방식을 사용하기 때문에 메시지 인증 코드는 시간간격 i 후에 공개되는 K_i^T를 이용하여 검증할 수 있다.

$$BS \rightarrow *: M, MAC(K_i^T, M) \quad (9)$$

3. 클러스터 형성

클러스터의 형성과정은 그림 3을 참조한다. 센서 네트워크의 응용분야의 따라 통신과정의 보안이 요구되지 않을 수도 있지만 본 연구는 민감한 데이터를 사용하는 응용분야를 목적으로 하였기 때문에 클러스터에 대한 운용과 클러스터 내에서 사용하는 모든 통신은 보안을 필요로 한다고 가정 하였다.

먼저 클러스터 헤드로 선출된 노드는 자신이 클러스터 헤드임을 센서 네트워크 전체에 브로드캐스트 하여야 한다. 브로드캐스트를 위해서는 키 체인을 생성하고 연산을 통해 모든 키 값을 구하여야 한다. 그러나 키 체인의 저장과 키 값을 구하기 위한 연산은 많은 자원을 필요로 하기 때문에 제한된 자원의 센서 노드가 수행하는 것은 비실용적이다. 따라서 키 체인의 생성과 필요한 연산 모두를 BS에게 의뢰하여 브로드캐스트를 수행한다. 이때 클러스터 헤드와 BS간의 통신은 유니캐스트 형태를 사용한다.

$$u \rightarrow BS: E_{\langle K_u, C\rangle}(M), MAC(K_{K_u}, C|E_{\langle K_u, C\rangle}(M))$$

클러스터 헤드 u로부터 브로드캐스트 요청을 받은 BS는 이를 수행 하고 타임라인에 따라 시간 i가 지난 후 키를 공개한다. 센서 네트워크 각 노드들은 수신된 브로드캐스트 메시지를 임시로 저장하였다가 나중에 공개된 키를 통하여 메시지를 인증하고 다음단계를 준비한다.

$$BS \rightarrow *: u, MAC(K_i^T, u)$$

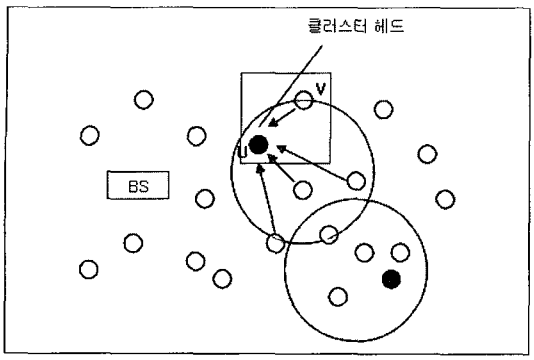


그림 4. 클러스터 헤드의 선택

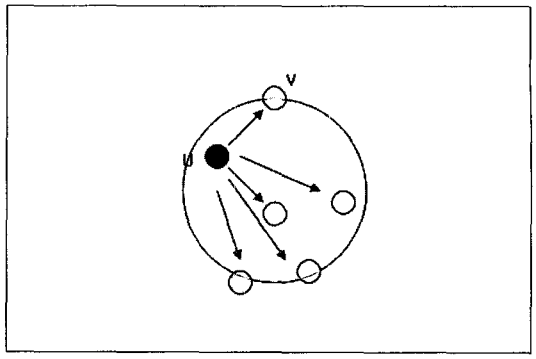


그림 5. TDMA 스케줄 전송

수신 노드 v는 브로드캐스트 메시지 인증이 성공한 후 최소의 통신에너지를 사용할 수 있는(Lowest energy path) 클러스터 헤드 u를 선택하여 u와 이웃을 형성한다.

$$v \rightarrow u: v, MAC(K_v, u|v)$$

노드 u, v는 각각 연산을 통해 쌍대 키를 생성한다. 쌍대 키가 생성되면 두 센서 노드 간에 안전하게 통신할 수 있다.

$$K_{uv} = f_{K_u}(u)$$

쌍대 키가 생성되면 클러스터 참여 메시지(Join-request)를 클러스터 헤드 u에게 보낸다.

$$v \rightarrow u: E_{\langle K_{uv}, C\rangle}(M), MAC(K_{uv}, C|E_{\langle K_{uv}, C\rangle}(M))$$

클러스터에 참여할 노드가 정해지면 클러스터 헤드 u는 TDMA 스케줄을 구성하고 이를 클러스터의 노드에게 보내야한다. 클러스터 헤드와 클러스터 노드사이의 통신을 위하여 먼저 클러스터 키를 생성한다.

$$K_c = f_{K_u}(r)$$

생성된 클러스터 키는 클러스터에 참여한 모든 노드에게 보낸다.

$$u \rightarrow v_i: E_{\langle K_{uv_i}, C\rangle}(K_c), MAC(K_{uv_i}, C|E_{\langle K_{uv_i}, C\rangle}(K_c))$$

클러스터 키를 사용하여 TDMA 스케줄을 안전하게 클러스터의 모든 노드에게 전송할 수 있으며 이때 멀티캐스트 형태의 통신방법을 사용한다.

$$u \rightarrow v(*): E_{\langle K_c\rangle}(M), MAC(K_c, E_{\langle K_c\rangle}(M))$$

4. 데이터 전송

클러스터 형성이 완성되면 클러스터에 속한 각 노드는 할당받은 타임 슬롯 (Time slot) 기간 동안에 데이터를 클러스터 헤드에게 보내게 된다. 이러한 동작을 위해 BS가 각 노드들에게 동기 신호를 보내며 각 노드들은 안전한 클러스터링 단계를 같은 시간에 시작할 수 있다.

$$v \rightarrow BS: N_v$$
$$BS \rightarrow u: T_s|K_i|T_i|T_{dura}|\delta, MAC(K_v, N_v|T_s|K_i|T_i|T_{dura}|\delta)$$

각 넌 클러스터 헤드 노드는 할당된 전송시간 이외에는 에너지 절약을 위하여 정지모드에 들어간다. 클러스터 헤드는 클러스터의 각 노드로부터 데이터를 수집하여 데이터 통합과정과 관련 없는 데이터의 삭제를 수행한다.

$$v \rightarrow u: E_{\langle K_{uv}, C\rangle}(M), MAC(K_{uv}, C|E_{\langle K_{uv}, C\rangle}(M))$$

클러스터 노드들로부터 결과데이터를 얻게 되면 클러스터 헤드는 이를 BS에게 보낸다. 일반적으로 클러스터 헤드와 BS간의 간격은 원거리이며 데이터 메시지의 크기는 비교적 크다. 따라서 이러한 과정은 많은 에너지가 소비된다. 전송방식은 고정된 확장형 코드(fixed spreading code)와 CSMA [5]를 이용한다. 즉 다른 노드가 BS 확장형 코드를 사용하여 전송 중 이라면 기다리고 그렇지 않으면 데이터를 전송한다.

$$u \rightarrow BS: E_{\langle K_u C\rangle}(M), MAC(K_{K_u}, C|E_{\langle K_u C\rangle}(M))$$

Ⅳ. 평가분석

이 장에서는 제안한 프로토콜에 안전성 및 에너지 효율성과 관련하여 살펴보도록 하겠다. 보안성에 대해서는 센서 네트워크가 요구하는 데이터 기밀성, 무결성, 인증, 초기성에 대해서 평가하고 에너지 효율성에 대해서는 시간당 에너지 소비량을 평가 하였다.

1. 보안성

제안한 프로토콜은 암호화를 통해서 데이터의 기밀성을 유지하며 또한 기본적인 암호화 구조 이외에 의미론적 안정성을 제공한다. 즉, 동일한 평문을 통하여 여러 번 암호화를 수행할 경우 공격자가 이를 예측할 수 있으므로 각 메시지마다 카운터 값을 추가하여 매번 다른 암호문이 발생하도록 하였다. 카운터 값은 송신자와 수신자 사이에 전송되지 않으며 송신자와 수신자가 메시지를 보낼 때 각각 증가시켜 보관한다. 마지막으로 데이터 인증과 무결성 보증을 위하여 MAC를 사용하였다.

SNEP는 비 대칭키 방식의 오버헤드를 줄이기 위하여 대칭키 방식을 사용한다. 대칭키 방식에서 만약 한 개의 노드가 공격자에 의해 해킹을 당한다면 공격자가 정보를 조작하여 원하지 않은 데이터가 BS에게 전달 될 수 있다. 또한 그 노드를 통하여 클러스터 헤드와 이웃노드와의 관계를 형성하여 센서네트워크 시스템 전체에 영향을 끼치게 된다. 따라서 SNEP과 같은 대칭키 기법은 에너지 효율을 목적으로 한 클러스터링 프로토콜에는 적합하지 못하다. 본 연구에서 제안한 키 관리 프로토콜을 사용하면 노드와 노드, 노드와 BS간 존재하는 다양한 통신형태에 적합한 키 관리 메커니즘을 제안한다. 따라서 기 제안된 에너지 효율을 목적으로 한 data-aggregation 혹은 data-fusion 기법에 적합한 보안기법을 제공할 수 있다. 또한 하나의 노드가 손상되어 쌍대키, 클러스터 키를 공격자가 얻는다 할지라도 다른 노드들의 키는 얻을 수 없기 때문에 손상의 범위는 해당 클러스터나 이웃노드에 국한되어 더 이상의 피해를 막을 수 있다. 만약 손상된 노드가 발견된다면 모든 키에 대한 재발급을 통하여 손상된 노드가 더 이상 시스템에 접근하는 것을 막아야 한다. 다음으로 공격자가 BS를 가장하여 악의적인 패킷을 전체 센서 네트워크 시스템에 삽입할 수 있으므로 브로드캐스트에 대한 인증을 필요로 하는데 SNEP에서 사용하는 μTESLA 방식을 적용하여 이를 방지 하였다. SPINS와 비교하여 제안기법이 갖는 오버헤드는 각 라운드별로 형성하는 클러스터와 클러스터 헤드의 선출 시 발생한다. 클러스터 형성을 위하여 각 노드는 클러스터 헤드 여부를 결정한 후 이를 브로드 캐스트 한다. 또한 클러스터를 형성하면서 클러스터 키와 쌍대 키를 추가적으로 생성하여야 한다. 표 1은 본 논문에서 적용한 응용프로토콜과 SPINS 기법과의 보안성능을 비교하였다.

2. 에너지 효율성

그림 6과 7은 클러스터링 방식을 적용하지 않은 MTE (Minimum Transmission Energy) Routing 방식과 보안성을 고려하지 않은 클러스터링 방식인 LEACH 프로토콜 그리고 제안기법을 비교한 결과를 보여주고 있다. 본 평가결과를 통해 제안기법이 클러스터링 방식보다 에너지 사용량은 증가하지만 보안성을 제공하면서도 MTE 방식과 비교하여 에너지 효율성이 우수함을 알 수 있다.

표 1. 보안성능 비교

구 분	SPINS	제안기법
사용 key의 개수 (노드당)	1	4
노드 손상 시 영향	센서네트워크 전체 영향 가능	이웃노드 혹은 해당 클러스터에 국한
data-aggregation 혹은 data-fusion에 적용여부	적용 불가능	다양한 키 제공으로 적용가능
Broadcast 메시지 인증	μTESLA적용	μTESLA적용
추가적인 Overhead	-	클러스터 형성, 클러스터 키와 쌍대 키 생성

본 논문에서 제안한 기법과 다른 프로토콜과의 성능평가를 위해 NS-2(Network Simulator 2)에 구현된 에너지 모델을 사용하였다. 시뮬레이션을 위해 (0, 0)와 (100, 100) 좌표 사이에 100개의 노드를 랜덤하게 분포 시켰으며 싱크 노드는 (50, 200) 좌표에 배치하였다. 각 노드의 데이터 처리 시간은 25μs 각 노드의 초기 에너지는 2J로 설정하였으며 에너지가 고갈될 때까지 주기적으로 데이터를

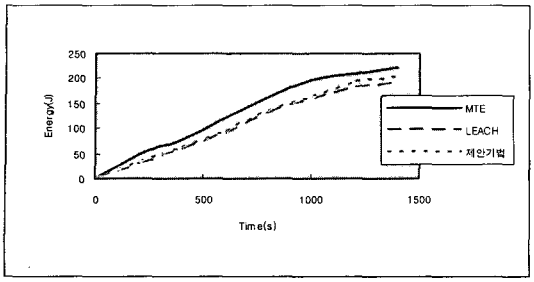


그림 6. 시간에 따른 총 소비 에너지

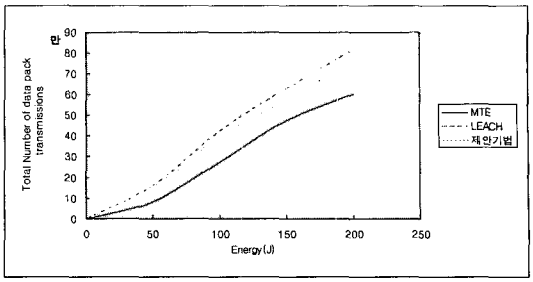


그림 7. 전체 에너지에 따른 총 전송 패킷 수

전송하는 것으로 가정하였다. 표 2는 실험에 사용된 각종 파라미터 값을 나타낸다.

표 2. 시뮬레이션 파라미터(20라운드 클러스터 헤드 결정)

파라미터	값
노드수	100
네트워크 크기	100m * 100m
싱크 노드 위치	(50, 200)
제어 패킷 크기	5 bytes
클러스터 헤드 선출 확률	0.05
각 노드의 초기 에너지	2J

3. 최근 연구동향

센서네트워크 시스템과 관련된 최근 연구동향을 살펴보면 키 관리기법으로 공통키 사용을 통하여 센서의 키 전송, 수용과정을 제거한 방법[14]이 제안되고 있으며 라우팅 기법으로는 라우팅 트리인 QSRT (Query Specific Routing Tree) 알고리즘을 적용하여 부분 집계 및 패킷 합병의 수행시점을 조절함으로써 메시지 전송 비용을 줄인 기법[15] 이 제안되고 있다. 또한 데이터 관리 기법으로 Hilbert 곡선을 이용하여 센서 노드들을 선형화하고 각 센서에게 데이터 공간을 균일하게 배분시키는 동적인 데이터 분산 방식을 적용한 기법[16] 등이 제안되고 있다.

V. 결 론

센서 네트워크의 가장 큰 장점은 적용과 관리가 용이하다는 것이다. 일단 적용이 된다면 환경과 무관하게 데이터 수집활동을 센서 노드 생애주기 동안에 지속적으로 할 수 있다. 그러나 제한된 자원과 재충전 방식의 비실용성으로 인하여 그 사용기간이 단축될 수 있기 때문에 효율적인 에너지 사용방법이 많이 제안되어 왔으며 이로 인해 보안 서비스를 탑재하기가 어려웠던 것이 사실이다. 그러나 민감한 데이터를 다루는 적대적인 환경에서는 센서네트워크 시스템의 안전성이 무엇보다 중요하다. 이를 위하여 본 논문에서는 기 제안된 대칭키 암호화 알고리즘을 사용하되 하나의 노드가 손상되더라도 그 영향을 최소로 할 수 있으며 에너지 효율성을 고려한 기존의 알고리즘을 적용하기에 적합한 다양한 키를 생성하고 이를 관리하기 위한 기법을 제안하였다. 향 후 연구과제로는 보안 요구정도에 따라서 보안성과 효율성의 등급을 적절하게 조절하기 위한 방법이 필요하며 이를 통해 서로에 대한 영향력과 실제 적용되었을 때의 결과에 대한 연구가 필수적이다. 일반적인 데이터를 수집하는 경우는 낮은 보안등급을 적용하고 민감한 데이터를 취급하는 경우에는 높은 보안등급을 적용하여야만 하기 때문이다. 본 연구는 센서 네트워크에서 사용가능한 다양한 형태의 통신방식에 대해서 높은 보안등급을 요구하는 응용서비스에 적합하도록 하였다. 향후 연구로는 응용서비스에 따른 차별적인 보안등급 적용과 이와 관련한 에너지 효율성에 대한 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," *Auto ID Center White Paper*, November 2002.

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms

for Large-Scale Distributed Sensor Networks," *In Proceedings. of the 10th ACM CCS '03*, October 2003.

[3] 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.

[4] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," *In Proceedings. of Fourth Annual ACM International conference on Mobile Computing and Networks(Mobicom)*, August 2000.

[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.

[6] R. Gennaro and P. Rohatgi, "How to sign digital streams," *Advances in Cryptology - Crypto '97, In Burt Kaliski, editor*, pp. 180-197, 1997.

[7] P. Rohatgi, "A compact and fast hybrid signature scheme for multicast packet authentication," *In 6th ACM Conference on Computer and Communications Security*, November 1999.

[8] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," *IEEE Symposium on Security and Privacy*, May 2000.

[9] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *In Advances in Cryptology, Proceedings of CRYPTO' 92, LNCS 740*, pp. 471-486, 1993.

[10] C. Karlof, N. Sastry, U. Shankar, and D. Wagner, "TinySec: TinyOS Link Layer Security Proposal," Unpublished manuscript, version 1.0, July 2002.

[11] C. Karlof and D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *To appear in Proceeding of First IEEE Workshop on Sensor Network Protocols and Applications*, May 2003.

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

[13] T. Kwon and M. Gerla, " Clustering with power control," *In proceeding of MILCOM*, vol. 2, November 1999.

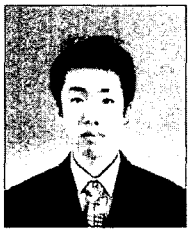
[14] 정윤수, 황윤철, 이건명, 이상호, "무선 센서 네트워크를 위한 클러스터 기반의 효율적 키 관리 프로토콜," 한국정보과학회논문지 (I), 33(2), pp. 131-138. 2006.

[15] 송인철, 노요한, 현동준, 김명호, "센서 네트워크에서의 데이터 수집을 위한 라우팅 기법," 한국정보과학회논문지 (D), 33(2), pp.188-200, 2006.

[16] 임용훈, 정연돈, 김명호, "데이터 기반 센서 네트워크에서 다차원 영역 질의를 위한 동적 데이터 분산," 한국정보과학회논문지 (D), 33(1), pp. 32-41, 2006.

〈著者紹介〉

장 근 원 (Kun-Won Jang) 학생회원
1998년 2월: 고려대학교 영어영문학과 졸업
2003년 2월: 숭실대학교 정보과학대학원 정보통신학과 석사
2003년 3월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, Sensor Network, DRM, 스테가노그래피



신 동 규 (Dong-Gyu Shin) 학생회원
2004년 2월: 천안대학교 컴퓨터학과, 정보처리학과 졸업
2006년 2월: 숭실대학교 컴퓨터학과 석사
2006년 3월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, 멀티미디어 보안, Sensor Network, RFID

전 문 석 (Moon-Seog Jun) 정회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1989년 3월~7월 Morgan State University 조교수
현재 숭실대학교 정교수
〈관심분야〉 전자상거래 보안, 인터넷 보안, 멀티미디어 보안, 인증시스템