무선 센서네트워크를 위한 TEEN 기반의 안전한 그룹통신 기법

서 일 수*

요 약

무선 센서 네트워크(WSN : Wireless Sensor Network)는 계산 능력, 전력, 통신 대역폭 등 다양한 제약 조건을 가지기 때문에 기존의 보안 기법을 WSN에 적용하기는 매우 어렵다. 이러한 문제점을 해결하기 위해 본 논문에서는 무선 센서 네트워크에 적용 가능한 안전한 그룹통신 기법을 제안한다. 제안한 기법은 클러스터링 기반의 계층적 라우팅 프로토콜인 TEEN(Threshold sensitive Energy Efficient sensor Network protocol) 알고리즘에 보안 메커니즘이 결합된 형태로서, 네트워크는 센서노드, 클러스터 헤더, 베이스 스테이션(BS : Base Station)으로 이루어진다. 보다 강력한 보안성 제공과 효율적인 키 관리를 위해 제안된 기법은 비밀 키 및 공개 키 알고리즘 모두를 사용하며, 전력소모를 줄이기 위해 참여 노드들 간의 통신은 계층적 트리구조에 의해 이루어진다. 따라서 본 논문에서 제안한 기법은 강력한 보안성을 제공할 뿐만 아니라, 통신에 있어 보다 낮은 전력을 소모하므로 무선 센서 네트워크 환경에 적합하다고 할 수 있다.

Teen Based Secure Group Communication Scheme for Wireless Sensor Networks

Il Soo Seo*

ABSTRACT

It is very difficult to apply previous security protocols to WSNs(Wireless Sensor Networks) directly because WNSs have resource constrained characteristics such as a low computing ability, power, and a low communication band width. In order to overcome the problem, we proposes a secure group communication scheme applicable to WSNs. The proposed scheme is a combined form of the TEEN(Threshold sensitive Energy Efficient sensor Network protocol) clustering based hierarchical routing protocol and security mechanism, and we assume that WSNs are composed of sensor nodes, cluster headers, and base stations. We use both private key and public key cryptographic algorithms to achieve an enhanced security and an efficient key management. In addition, communications among sensor nodes, cluster headers, and base stations are accomplished by a hierarchical tree architecture to reduce power consumption. Therefore, the proposed scheme in this paper is well suited for WSNs since our design can provide not only a more enhanced security but also a lower power consumption in communications.

Key words : (WSN, TEEN, Private key, Publick key, Network Security

접수일 : 2009년 5월 18일; 채택일 : 2009년 6월 3일

* 대구대학교 컴퓨터 · IT공학부(겸임)

1. 서 론

센서 기술, MEMS 기술, 저전력 전자공학 기술, 저전력 RF 설계 기술 등의 발달로 무선 네트워크를 통하여 연결될 수 있는 소형, 저가, 저전력의 센서 노드들이 계속 개발되고 있다. 이러한 센서 노드들은 센싱, 데이터 처리, 통신 컴포넌트들로 구성되는 것이 일반적이며, 매우 많은 수의 센서 노드들이 현상의 내부나 밀접한 지역에 조밀하게 배치된 센서 네트워크를 형성하여 헬스, 군사, 홈 네트워크, 환경 감시, 공장 관리, 재난 관리 등의 다양한 응용에 적용될 수가 있다[2].

센서 네트워크에서 센서 노드의 위치는 미리 결정될 필요가 없으므로, 접근이 어려운 영역이나 재난에 대한 피해 구조를 위한 응용을 위해 임의로 배치될 수 있다. 그러므로 센서 네트워크 프로코콜은 자가 구성(self-organizing) 능력을 가지며, 센서 노드들이 서로 협력하여 동작한다. 이러한 기술의 진보는 유비쿼터스 컴퓨팅이라는 새로운 정보통신 혁명을 야기하게 되었고, 이런 사회 발전의 흐름과 끊임없이 환경을 인간 친화적으로 바꾸고 싶어 하는 인간의 욕구와 맞물려 무선 센서 네트워크(WSN : Wireless Sensor Network)의 필요성이 제기되고 있다[3, 4].

이와 같이 현재 센서 네트워크에서의 주요 이슈는 기기의 소형화, 센싱 능력, 그룹 관리, 안전하고 효율적인 라우팅이며, 표준화를 위한 아이템으로는 그룹관리를 위한 키 관리와 안전한 라우팅을 위한 전송 프로토콜 분야가 주요 이슈가 된다. 라우팅은 상황인지(context aware)라는 새로운 인자가 부가되어서, 소규모 컴퓨팅 환경에서의 상황인지 방법을 통하여 이웃한 센서 기기의 오동작을 인식하고 우회루트 발견을 실시간적으로 처리할 수 있는 경량의 프로토콜 개발을 목표로 한다. 주변 환경을 감시하고 데이터를 수집하는 용도로 이용될 수 있는 센서 네트워크는 스마트 홈이나 사무, 공장 자동화는 물론 미래에 구현될 유비쿼터스 컴퓨팅에서 인간과 환경의 상호작용을 가능하게 하는 핵심 기술로 인식되고 있다. 이러한 센서 네트워크는 사용목적에 의존적인 성향이 있으며, 실제 구현에 있어서도 상당한 제약이 따른다. 대표적인 제약사항은 다음과 같다[5].

우선 센서 노드의 수는 수십 개에서 수만 개 정도까지 응용에 따라 가변적이며, 네트워크 일부분의 장애가 전체 네트워크에 영향을 주어서는 안된다는 점과 네트워크의 토폴로지가 자주 바뀔 수 있다는 것이다. 또한 센서 노드는 배터리 용량, 정보의 처리 및 저장 능력, 통신 기능이 충분하지 못한 것이 일반적이다. 특히 배터리에 의존하는 센서 노드의 가동시간에 대한 제약사항은 매우 중요한 요소이며, 이를 해결하기 위한 저 전력 설계는 센서 네트워크 구현에 필요한 결정적 기술로 인식된다. 따라서 하드웨어뿐만 아니라 프로토콜, 운영체제, 미들웨어, 보안(security) 등의 모든 기능에 대한 구현은 가급적 저전력 환경이 최대한 보장된 설계기법이 적용되어야 한다. 또한 센서 네트워크 기반의 서비스에 대한 기술적 발전과 구현이 구체화되면서 센서 네트워크 상에서의 보안 기술에 대한 연구도 활발해지고 있다. 일반적으로 센서 네트워크는 PC의 컴퓨팅 환경과 비교할 때, CPU의 능력은 물론 저장 공간, 대역폭, 전원 등 많은 요소에서 한계적 제약 사항을 갖는다. 그러나 보안에 대한 요구는 일반 인터넷 환경에서의 요구되는 수준과 최소한 동등해야 하므로 이에 적합한 연구가 이루어져야 한다[3, 6].

본 논문에서는 센서 노드들의 배터리 소모를 줄임과 동시에 그룹 간 안전한 통신을 보장하는 방법을 설계하였다. 센서 네트워크의 저전력 설계를 위하여 TEEN 알고리즘을 적용하였고, BS와 각각의 센서 노드들은 BS의 통신보다 보안성 측면에서 우수하면서도 배터리 소모를 줄일 수 있는 안전한 그룹 통신에 대해서 제안하였다.

본 논문의 구성은 다음과 같다.

제 2장에서는 관련 연구에 대한 배경을 설명하

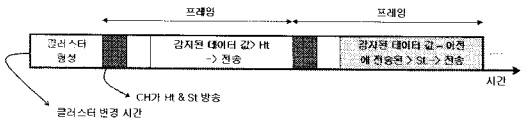
였고, 제 3장에서는 저전력 기반의 안전한 그룹 통신 기법을 제안하였으며, 제 4장의 분석에 이어 마지막 제 5장에서는 결론을 맺는다.

2. 관련 연구

본 장에서는 센서 네트워크 라우팅 알고리즘의 하나인 TEEN에 대한 내용과 센서 네트워크의 보안에 대한 사항을 고찰한다.

2.1 TEEN 프로토콜

TEEN(Threshold sensitive Energy Efficient sensor Network protocol)은 센서 노드들이 주기적으로 전송할 데이터를 가지지 않는다는 점을 제외하고, LEACH(Low-Energy Adaptive Clustering Hierarchy)[7]와 유사하게 동작한다. LEACH가 사전적 센서 네트워크에 적합한 특성을 가지지만, TEEN은 시간 임계적인 데이터를 처리한다는 점에서 반응적 센서 네트워크에 적합하다. TEEN은 LEACH의 클러스터 형성 기법을 사용하나, 데이터 전송 단계에서는 다른 방법을 사용한다.



(그림 1) TEEN의 동작

(그림 1)과 같이 TEEN의 센서 노드들은 클러스터 결정시간에 클러스터 해드가 방송한 임계값인 Ht와 St에 따라 현재 감지된 데이터를 전송할지를 결정한다. 즉, 감지된 데이터의 값이 처음으로 Ht를 초과하면, 이를 저장하여 해당 시간 슬롯에 전송한다. 이후에는 감지된 데이터의 값이 저장된 값보다 St이상 큰 경우에 저장하고, 해당 시간 슬롯에 전송한다[1].

TEEN은 지진, 폭발 등과 같은 응용에서 요구되는 시간 임계적인 데이터가 실시간적으로 전달된다. 또한 임계값이 클러스터 형성 결정 시간에 방송되므로 응용에 따라 사용자가 에너지 소비와 센서 네트워크 상태 판단의 정확성을 조절할 수 있다는 특징을 가진다. 그러나 감지된 데이터의 값이 임계치에 도달하지 않는 경우 네트워크로부터 데이터를 얻어낼 수가 없으므로, 모든 노드가 수명을 다한 경우에도 네트워크의 상태를 판단할 수 없다. 또한 클러스터내에서 TDMA 스케줄링을 사용하여 시계 임계적 데이터의 보고에 지연을 가지며, 모든 노드들이 해당 슬롯에 전송할 데이터를 가지는 것이 아니므로 자원이 낭비될 수 있다.

2.2 센서 네트워크 보안

센서 네트워크는 계속하여 널리 사용될 기술로 판단되고 있다. 그러나 실제 적용되는 무선 센서 네트워크 구성에 대한 연구와 개발이 주류를 이루어 왔을 뿐, 보안에 대한 연구는 상대적으로 소외되어 왔다. 하지만 최근 센서 네트워크 기반의 서비스에 대한 기술이 구체화되면서 센서 네트워크상 보안에 대한 필요성이 중요하게 대두되고 있다.

센서 네트워크의 활용 사례는 다음과 같으며, 적용 범위의 확장성을 고려하면 필요에 따라 적정한 수준의 보안 기능을 충족해야 한다는 당위성이 형성된다[8-10].

- 비상 대응 정보 분야 : 센서 네트워크는 건물, 사람, 수송 경로에 대한 상태 정보를 취할 수 있다. 이렇게 수집된 센서 정보는 비상 대응 담당자에게 안전하고 신속하게 전송되어야 한다.
- 에너지 관리 분야 : 에너지 관리는 원격으로 이루어질 경우 보다 효과적일 수 있다. 즉, 주위 환경의 기온과 순간 전력 등에 따른 전선에 부과되는 전력 소모량을 원격으로 감지할 수 있으며 이로 인한 자동적 전력 부하 분산 관리를 통해 전력 과부하에 따른 단전 사고

등을 미연에 방지 할 수 있다.

- 의료 모니터링 분야 : 가까운 미래에는 각 사람의 신체 정보 상태를 센서 네트워크를 통해 원격으로 모니터링을 할 수 있고 이를 통해 의료 시스템과 연계함으로써 의료 서비스의 획기적인 변화를 가능케 할 수 있다.
- 군수 물류, 재고 관리 분야 : 과잉 생산된 물자가 공급이 부족한 지역으로 신속하게 이동될 수 있는 메커니즘을 센서 네트워크를 통해 실현한다. 이 영역은 전 세계를 시장으로 하며 물류 현황 정보에 대한 신속, 정확한 파악과 처리에 크게 기여될 수 있다.
- 전투지역 관리 분야 : 전투 지역의 무기, 전투 차량, 군인에 대한 정확한 정보를 실시간적으로 수집, 관리함으로 전투 현황에 대한 정보의 혼란을 최소화 할 수 있다.

이러한 센서 네트워크에서 센서 노드는 공개 키 암호화 알고리즘을 위한 다양한 정보와 성능을 제공하기 어렵다. 또한 대칭 키 방식은 패킷 당 필요한 인정 정보가 1Kbyte로서 센서 네트워크에 적용하는데 적합하지 않다.

2.2.1 센서 네트워크 시스템 전제 조건

보안 요구사항을 제시하기 전에 실제적인 요구사항과 시스템 구성도를 정의하는 요구는, 일반적인 센서 네트워크 상에서 일반적인 보안 요구사항을 충족하기 위한 목적을 갖는다.

무선망을 이용한 센서 노드 통신 방법은 브로드캐스팅(broadcasting) 방식이 주로 적용된다. 이 방식은 센서 네트워크 서비스 특성상 최소한의 자원 소모에 적절한 보안적 요구사항을 만족하는 수준을 제공하는 것이다[11]. BS는 충분한 자원을 갖고 있으며 많은 센서 노드와의 통신과 관리의 중심적 역할을 수행한다. 센서 네트워크를 위해 운영되는 센서 노드는 안전하지 않은 위치에 설치된다. 각 노드에게 브로드캐스팅 하는 것은 안전하지 않은 무선망에서 공격자(adversary)의 도청이 언제든지 가능하며, 메시지의 재사용 공격에 매우 취약하다. 그러나 BS는 외부 망과의 게이트웨이 및 센서 네트워크 중심에 있으므로 언제나 안전해야 하며, 각 노드는 이러한 BS와의 통신을 위해 초기 설치 시 마스터 키 값을 할당 받는다.

2.2.2 센서 네트워크 보안 요구사항

(1) 데이터 비밀성

센서 네트워크 환경의 많은 응용에서는 민감한 데이터 교류가 노드 간에 빈번하게 이루어진다. 따라서 허가된 노드 이외에 민감한 정보를 볼 수 없도록 해야 하며, 비밀 키로 데이터를 암호화한 상태에서 데이터 교환이 이루어져야 한다. 즉 데이터 비밀성을 보장해야 한다.

(2) 데이터 인증

메시지 인증은 센서 네트워크 상의 많은 응용에서 중요한 요구사항이다. 공격자는 쉽게 메시지를 삽입 할 수 있기 때문에 수신자는 정책방향 설정 과정에서 사용되는 데이터가 원래 작성자로부터 온 것인지를 확인해야 한다. 양단간 통신인 경우 데이터 인증은 순수한 대칭 키 메커니즘을 통해 이루어질 수 있다. 송신자와 수신자는 모든 데이터 통신에 대한 메시지 인증 코드(MAC : Message Authentication Code) 값을 생성하기 위한 개인키를 공유한다. 정확한 MAC 값이 수신되어질 경우 수신자는 송신자에 의해 보내진 메시지의 진위를 검증하게 된다. 그러나 브로드캐스팅 통신 방법에서 공유되는 개인키는 모든 수신자들과 송신자간에 공유되어야 하며, 수신자들 중 악의적인 수신자는 공유키를 알고 있기 때문에 송신자를 가장해서 MAC 값을 생성할 수 있다는 단점을 갖는다. 따라서 일반적으로 공개키 방식을 통한 브로트캐스팅 통신 방식을 취해야 한다. 그러나 공개키 방식은

실제적인 컴퓨팅 파워나 자원 소요가 크므로, 이러한 문제점을 해결하기 위해 지연된 키 노출과 단방향 함수 키 체인(chain)이 활용된다.

(3) 데이터 무결성

통신 상에서 데이터 무결성은 수신자가 수신한 데이터의 위·변조 여부를 확인하는 것으로, SPINS에서는 데이터 인증을 통한 데이터 무결성을 보장한다.

(4) 데이터 신성성(Freshness)

데이터 신선성은 예전에 보낸 데이터에 대한 재사용을 방지하기 위한 기술로서, 가장 최근에 보낸 데이터임을 보장하는 보안 서비스다. 일반적으로 두 종류의 타입이 있다[6].

첫째, 단순한 신성성은 계수기(counter)를 통해 분해된 메시지의 순서화를 제공하며, 수신된 메시지를 통해 해당 송신자가 보낸 것임을 확인한다. 두 번째의 완전한 신성성 보장은 임의의 난수 값을 통해 요청-응답에 대한 전체적인 순서화를 제공하므로서, 수신된 메시지가 이전에 수신자가 보낸 요청메시지에 대한 응답인지를 확인한다.

본 논문에서는 무선 센서 네트워크에서 인접한 노드간 유사 정보의 중복 전달로 인한 에너지 낭비를 줄이기 위한 데이터 결합(data aggregation)이 필요하다는 특성을 고려할 때, 클러스터링 기반의 계층적 라우팅 특성이 있는 TEEN 알고리즘을 적용하였다. 또한 안전한 그룹 통신을 위해 BS와 각 센서 노드들은 공개키와 개인키를 사용하는 방법을 적용하였다.

3. 그룹 통신을 위한 메커니즘 제안

본 장에서 TEEN 라우팅 프로토콜 기반의 안전한 그룹 통신을 위한 방법을 제안한다.

3.1 표기법

제시된 논문에서는 각 센서 노드들로 구성된 그룹들은 TEEN 라우팅 프로토콜로 구성된다. 센서 노드들 중 클러스터 헤드는 각 그룹에 대한 공유된 대칭키를 가진다. 각각의 센서 노드들은 자신의 단일 대칭키를 가진다. 그리고 BS는 자신의 공개키와 개인키를 가진다.

K_{pub}	베이스 스테이션(base station)의 공개키
K_{pri}	베이스 스테이션(base station)의 개인키
K_g	각 그룹에 대한 공유된 대칭키
K_s	단일 센서 노드의 대칭키
$E(K, M)$	키 K로 메시지 M의 암호화
$X\|Y$	X와 Y 연결 표시
IV	초기화 백터 값(제시된 방법에서는 타임 스탬프 사용)

3.2 프로토콜의 수행

3.2.1 패킷 구성

본 논문에서 제시한 방법에서는 네트워크를 구성하기 위해 배치되기 전에 센서 노드들은 각각 K_s, K_g 정보가 포함되어 임의의 장소에 배치된다. 그리고 센서 노드들은 하나의 클러스터에 해당하는 일종의 그룹 단위로 구성된다. 이 때 사용되는 라우팅 프로토콜은 TEEN를 이용하며, 선정된 클러스터 헤더 노드는 BS로부터 BS의 공개키인 K_{pub}를 전송 받는다. 즉 클러스터 헤더에는 K_s, K_g, K_{pub} 정보가 포함되어 있다. 이는 BS와 클러스터 헤더 사이 전송되는 메시지를 암호화하기 위한 키 정보들이다. (그림 2)는 본 논문에서 제안된 BS와 클러스터 헤더 간에 주고 맞는 패킷의 포맷 형태이며, BCH(Base station-Cluster head) 패킷으로 표현한다.

구체적인 필드 내용을 살펴보면, *type* 필드는 패킷의 유형들이며, ID_{src}, ID_{dst}, ID_g는 각각 소스

$type$	ID_{src}	ID_{dst}	ID_g	$E(K_{pub}, IV \mid type \mid ID_{src} \mid ID_{dst} \mid ID_g \mid seq \mid data)$

(그림 2) BS와 클러스터 헤더 간 전송 패킷 형식

노드의 아이디인 ID_{src}, 목적지 노드의 아이디인 ID_{dst}, 그룹의 아이디인 ID_g이다. *seq* 필드는 패킷의 순서 번호(seqeuence number)이며, *data* 필드는 데이터를 전달하기 위해 사용된다. IV 값은 패킷이 전송될 시점의 타임스탬프 값이다.

또한 클러스터 헤더와 자식 노드들 간의 통신을 위해서는 각 그룹에 대한 공유된 대칭키로 암호화하여 메시지를 전송한다. (그림 3)은 클러스터 헤더와 자식 노드들 사이에 주고받는 패킷의 포맷 형태이며, CHCN(Cluster head-Child node) 패킷으로 표현한다.

ID_{src}	ID_{dst}	ID_g	$E(K_g, IV \mid E(K_{ch}, IV \mid ID_{child} \mid E(K_{child}, IV \mid data)))$

(그림 3) 클러스터 헤더와 자식 노드 간 전송 패킷 형식

클러스터 헤더와 자식 노드들 사이에 전송되는 패킷은 전체적으로 각 그룹이 공유하고 있는 대칭키로 암호화된다. K_{ch}는 클러스터 헤더의 공개 키이다.

3.2.2 통신 프로토콜

제안된 통신 시스템에서 전체적인 시스템 구성은 (그림 4)와 같으며 메시지 전송을 위해서 수행되는 절차는 다음과 같다. (그림 5)는 본 논문에서 제안된 전체 프로토콜이다. 그리고 클러스터 헤더 선정은 클러스터링 기반 계층적 라우팅 프로토콜인 TEEN을 기반으로 한다.

(1) 센서 노드 배치 절차

1단계 : 센서 노드들을 임의의 위치에 배치하기 전에 각각의 K_s, K_g 정보를 센서 노드에 탑재하여 배치한다.

2단계 : BS는 클러스터 헤더가 선정되면, 이때 클러스터 헤더 노드에 자신의 공개키를 전송한다.

3단계 : BS의 공개키를 받은 클러스터 헤더 노드는 자신의 키 정보를 BS의 공개키로 암호화 하여 인증 확인 절차를 수행한다.

(2) BS와 클러스터 헤더 간 전송 절차

1단계 : BS와 클러스터 헤더 사이 전송은 (그림 2)의 패킷 형식을 이용한 송신과 수신이 이루어진다. 클러스터 헤더는 브로드캐스팅되는 하위 자식 노드들 간의 암호화된 메시지들을 데이터 결합 과정의 수행을 통하여 데이터 중복도 피하고 전력 낭비도 줄인다.

2단계 : 클러스터 헤더는 자식 노드들간의 메시지를 BS의 공개키로 암호화하여 BS에게 전송한다.

3단계 : BS는 클러스터 헤더로부터 전달 받은 암호화된 메시지를 자신의 개인키로 복호화 하여 싱크(sink)를 통해 외부 네트워크로 전송된다.

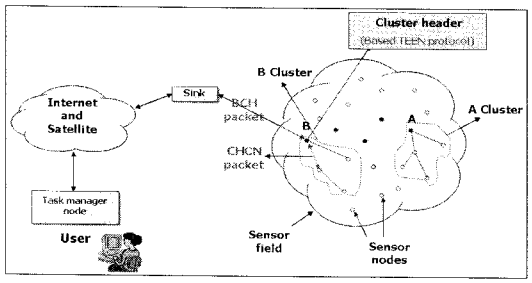
(3) 클러스터 헤더와 자식 노드들 간의 메시지 전송 절차

1단계 : 클러스터 헤더와 자식 노드들 사이 메시지 전송은 (그림 3)의 패킷 형식을 이용하여 송 · 수신되어진다.

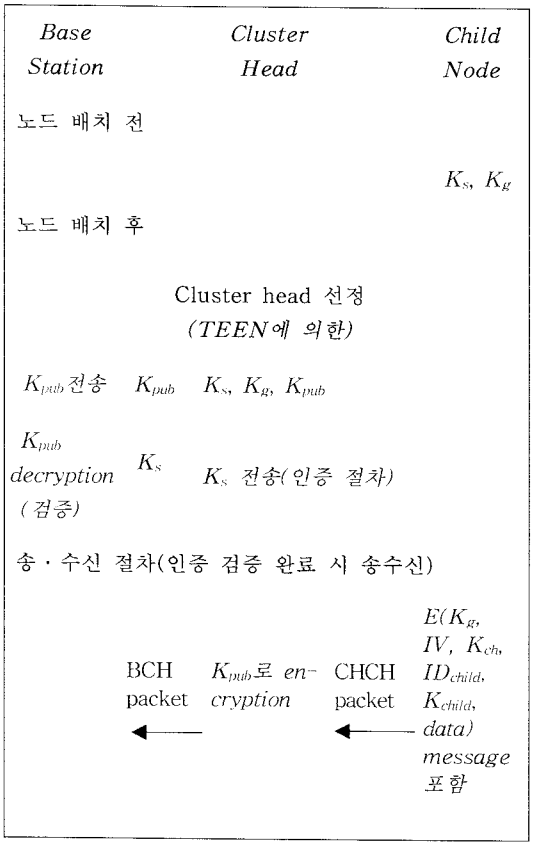
2단계 : 각각의 자식 노드들은 브로드캐스팅하며, 이때 전송 할 메시지는 자신의 단일 대칭키로 암호화 한다.

3단계 : 클러스터 헤더는 각각의 자식 노드들로부터 받은 암호화된 메시지를 자신의 단일

대칭키를 이용한 복호화로 메시지를 검증한다. 또한 중복된 메시지를 제거 한 후, BS의 공개키를 이용하여 메시지를 암호화하여 BS로 전송한다.



(그림 4) 전체적인 센서 네트워크 구성



(그림 5) 제안 방식의 프로토콜

4. 분 석

본 장은 본 논문의 제안 방식에 대하여 센서 노드의 에너지 소모 측면과 신뢰성 있는 그룹 통신의 구현에 대한 분석과 고찰을 설명한다.

첫째, 센서 노드의 에너지 소모 측면에서 제안한 프로토콜은 이웃한 노드 간의 유사한 정보의 중복 전달로 인한 에너지 낭비를 줄이는 방안이 제시되었다. 데이터 결합 기능을 가진 클러스터링 기반 계층적 라우팅 방식 중 TEEN 프로토콜 방식을 적용하여, 클러스터 헤더가 자식 노드들의 중복된 데이터를 처리 해주는 데이터 결합의 기능을 수행하도록 하였다.

두 번째는 BS와 클러스터 헤드 사이 통신과 클러스터 헤드와 자식 노드 사이에 안전한 통신이 보장된다는 점이다. 본 논문에서 제시한 두 가지 형태의 패킷은, BS와 클러스터 헤드 사이에서 전송 되는 BCH(Base station-Cluster head) 패킷과 클러스터 헤드와 자식 노드사이에 전송 되는 CHCN(Cluster head-Child node) 패킷이다. BCH 구조는 BS의 공개키로서 전체 메시지를 암호화하여 BS와 클러스터 헤더 사이의 안전하고 신뢰성 있는 통신을 보장한다. CHCN 구조에서는 자식 노드들은 자신의 단일 대칭키로 암호화하여 클러스터 헤더에게 전송하고, 클러스터 헤더는 다시 자신의 단일 대칭키로 암호화 한 후, 전체 메시지를 BS의 공개키로 암호화하여 BS로 전송한다.

5. 결 론

본 논문에서는 센서 노드들의 배터리 소모를 최소화하면서 그룹 간 안전한 통신을 제공하기 위한 방법을 제안하였다.

센서 네트워크의 저전력 설계를 위하여 클러스터링 기반 계층적 라우팅 프로토콜 방식 중 하나인 TEEN 알고리즘의 적용 방안을 제시하였다. 또한

두 가지 형태의 패킷 전송 방식을 제안하여 BS와 클러스터 헤드, 클러스터 헤드와 자식 노드들 사이에 이루어지는 송 · 수신의 안전성을 보장하였다. 특히 안전한 그룹 통신을 위해서 대칭키와 공개키 암호 알고리즘이 결합된 형태로 BS와 클러스터 헤더, 클러스터 헤더와 자식노드들 간의 안전성과 송수신자들의 신뢰를 확보하였다.

본 논문에 대한 추가적 과제로는 제안에 대해 더 높은 신뢰를 보장하는 분석 방법을 적용하여 구체적 검증 결과를 반영할 필요성과, 센서 네트워크의 효율성과 안전성을 보장하는 저전력 소모기법에 대한 지속적인 관심과 연구를 통하여 별도의 개선된 방안이 제시되어야 할 필요성이 있다.

참 고 문 헌

[1] Arati Manjeshwar and Dharma P.Agrawl, "TEEN:A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks", Proceedings of the 15th International Parallel and Distributed Processing Symposium, 2001.

[2] Ian F.Akuildiz et al., "A survery on Sensor Networks", IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, 2002.

[3] 정보통신부, "u-센서 네트워크 구축 기본 계획", 2004.

[4] K. Sorabi et al., "Protocols for Self-Orgnization of a Wirelss Sensor Network", IEEE Personal Communication, Vol. 7, No. 5, pp. 16-27, 2000.

[5] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS : Security Protocols for Sensor Networks", Wireless Network Journal (WINET), Vol. 8, No. 5, pp. 521-534, 2002.

[6] Y. J. Zhao, R. Govindan, and D. Estrin, "Computing Aggregates for monitoring Wireless Sensor Networks", The First IEEE International Workshop on Sensor Networks Protocols and Applications(SNPA 2003), Anchorage, AK. USA, 2003.

[7] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of the IEEE Hawaii International Conference on System Sciences (HICSS), Vol. 8, pp. 1-10, 2000.

[8] H. Abrach, S. Bhatt, J. Carlson, H. Dui. Rose, A. sheth, B. Shucker, J. Deng, and R. Han, "MANTIS : System Support for Multimodal Network of In-Situ Sensors", In Proc. of 2nd ACM Workshop on Wireless Sensor Networks and Applications(WSNA 2003), San Diego, CA, 2003.

[9] B. J. Bonfils and P. Bonnet, "Adaptive and Decentralized Operator Placement for In-Network Query Processing", IPSN 2003, LNCS 2634, 2003.

[10] H. Han, A. Perrig, and D. Song, "Random Key Prdistribution Schemes for Sensor Networks", Appears in IEEE Symposium on Security and Privacy, 2003.

[11] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Cullar, and K. Pister, "System architecture disrections for networks sensors", ASPLOS 2000, Cambridge, 2000.

서 일 수

1992년 경일대학교 컴퓨터공학과 (공학사)

1994년 경일대학교 컴퓨터공학과 (공학석사)

2005년 대구대학교 컴퓨터정보공학과(공학박사)

2008년~현재 대구대학교 컴퓨터 · IT공학부 겸임교수