센서 네트워크에서 데이터 집계를 위한 힐버트 커브 기반 데이터 보호 기법

(A Data Protection Scheme based on Hilbert Curve for Data Aggregation in Wireless Sensor Network)

윤 민 † 김 용 기 ††
(Min Yoon) (Yong-Ki Kim)

장 재 우 †††
(Jae-Woo Chang)

요 약 무선 센서 네트워크에 활용되는 센서 노드는 제한된 전력, 메모리 등의 한정된 자원을 지니기 때문에, 제한된 에너지를 효율적으로 관리하기 위한 데이터 집계 기법의 연구가 활발히 진행되어 왔다. 한편, 센서 네트워크는 무선 통신을 수행하기 때문에 공격자에게 쉽게 데이터 노출될 수 있다. 따라서, 센서 네트워크에서 데이터 집계를 위한 데이터 보호 기법에 관한 연구가 필수적이다. 그러나, 기존 데이터 집계를 위한 데이터 보호 기법은 네트워크 구성 및 데이터 집계 처리 시, 다수의 연산과 데이터 전송이 발생한다. 이러한 문제점을 해결하기 위하여, 본 논문에서는 데이터 집계를 위한 힐버트 커브(hilbert curve)기반 데이터 보호 기법을 제안한다. 제안하는 기법은 트리 기반의 라우팅을 구성하여 이웃노드와의 통신을 최소화한다. 또한 seed에 기반한 힐버트 커브 기법을 통해 데이터를 암호화함으로써, 센서 노드간의 통신 시 공격자로부터 데이터를 보호할 수 있다. 마지막으로, 제안하는 기법이 메시지 전송량 및 센서노드 평균 수명 측면에서 기존 연구보다 우수함을 보인다.

키워드 : 센서네트워크, 데이터보호, 힐버트커브, 데이터집계

Abstract Because a sensor node in wireless sensor networks(WSNs) has limited resources, such as battery capacity and memory, data aggregation techniques have been studied to manage the limited resources efficiently. Because sensor network uses wireless communication, a data can be disclosed by attacker. Thus, the study on data protection schemes for data aggregation is essential in WSNs. But the existing data aggregation methods require both a large number of computation and communication, in case of network construction and data aggregation processing. To solve the problem, we propose a data protection scheme based on Hilbert-curve for data aggregation. Our scheme can minimizes communications among neighboring sensor nodes by using tree-based routing. Moreover, it can protect the data from attacker by doing encryption through a Hilbert-curve technique based on a private seed, Finally, we show that our scheme outperforms the existing methods in terms of message transmission and average sensor node lifetime.

Key words : Sensor network, data protection, Hilbert curve, data aggregation

1. 서 론

현재 유무선 통신기술의 발전 및 모바일 정보기기의 보편화에 힘입어, 시간과 장소의 제약 없이 서비스를 제공할 수 있는 센서 네트워크 기술에 대한 관심이 크게 고조되고 있다. 센서 네트워크는 시설 모니터링, 환경 모니터링 및 군 지역 감시 등의 다양한 응용에서 이용된다[1-3]. 이러한 응용분야를 지원하는 센서네트워크는 휴대용 배터리를 사용하기 때문에 적은 전력과 제한된 메모리를 지니는 제약이 존재한다. 센서 노드가 지니고 있는 이러한 제약을 극복하기 위하여, 에너지 효율성 및 네트워크의 수명 연장을 지원하는 다수의 집계 기법(data aggregation technique)이 제안되었다[4-9]. 이 기법은 하위 노드로부터 받은 데이터와 자신의 데이터의 대표값(예를 들면, 최대값(max), 최소값(min), 평균값(average), 데이터 수(count), 데이터 합(sum))만을 상위 노드로 전송한다. 한편, 센서 네트워크는 무선 통신을 수행하기 때문에, 데이터에 대한 보호가 이루어지지 않는다. 이는 공격자가 데이터를 도청하거나 고의로 왜곡시키는 것을 가능하게 한다. 따라서, 센서 네트워크에서의 데이터 집계를 위한 데이터 보호 기법에 관한 연구가 필수적이다. 그

· 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구결과임
· 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호 2010-0023800)
· 이 논문은 2010 한국컴퓨터종합학술대회에서 '센서 네트워크에서 데이터 집계를 위한 힐버트커브 기반 데이터 보호 기법'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 전북대학교 컴퓨터공학과
myoon@chonbuk.ac.kr
†† 비 회 원 : 전북대학교 컴퓨터공학과
ykkim@dblab.chonbuk.ac.kr
††† 종신회원 : 전북대학교 IT정보공학부 교수
jwchang@chonbuk.ac.kr

논문접수 : 2010년 8월 5일
심사완료 : 2010년 10월 5일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제16권 제11호(2010.11)

러나 센서 네트워크에서 데이터 집계 기법에 관한 연구가 활성화 되었음에도 불구하고, 데이터 집계를 위한 데이터 보호 기법에 관한 연구는 아직 초보적인 단계에 있다. 대표적인 기법에는 CPDA(Cluster based Privacy Data Aggregation)[10], SMART (Slice-Mix-AggRegaTe)[10]가 존재한다. CPDA 기법은 클러스터 멤버들과의 통신을 통해 데이터를 암호화하여 집계하는 기법이며, SMART 기법은 데이터를 분할하여 이웃하는 센서 노드에게 전송하여 집계 데이터를 보호하는 기법이다. 하지만 기존 연구는 다음과 같은 문제점을 지니고 있다. 첫째, 네트워크 구성 및 데이터 집계 처리를 위하여, 다수의 연산과 데이터 전송이 발생한다. 둘째, 데이터를 암호화하지 않고 통신하기 때문에 데이터 집계를 위해 전송되는 데이터를 공격자가 취득하였을 때, 집계되는 값의 예측이 가능하다. 이러한 문제점을 해결하기 위하여, 본 논문에서는 데이터 집계를 위한 힐버트 커브(Hilbert curve)[11]기반 데이터 보호 기법을 제안한다. 이는 기존 클러스터링 기반 네트워크와는 달리 트리 기반 네트워크를 사용하고, 이웃노드와의 통신을 최소화하여 데이터를 변환함으로써 네트워크 구성 및 집계 시 연산을 최소화한다. 아울러, 힐버트 커브 기법을 적용하여 데이터를 암호화함으로써, 센서 노드간의 통신을 수행할 때 공격자로부터 데이터를 보호할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 데이터 집계를 위한 데이터 보호 기법에 대한 관련 연구를 기술하고, 3장에서는 데이터 집계를 위한 새로운 데이터 보호 기법을 제안하며, 4장에서는 제안하는 기법의 효율성을 증명하기 위해, 기존 연구와의 성능 평가를 수행한다. 마지막으로, 5장에서는 결론과 향후 연구방향을 제시한다.

2. 관련 연구

데이터 집계를 위한 데이터 보호 기법의 대표적인 연구로는 CPDA 및 SMART기법이 존재한다. CPDA 기법은 상위노드 한 개와 다수의 하위 노드들이 클러스터를 구성하고, 상위 센서 노드가 하위 센서 노드의 데이터를 집계하여 전송하는 클러스터링 기반 데이터 보호 기법이다. CPDA 기법의 수행단계는 클러스터 구성, 메시지 구성, 집계 연산의 3단계로 구성된다. 첫째, 클러스터 구성 단계는 지역적으로 데이터 집계처리를 수행하기 위한 클러스터를 구성하는 단계이다. 우선 기지국(base station)에서 클러스터 구성(HELLO) 메시지를 보내면, 이웃 노드의 클러스터 헤더 여부를 판별하여, 클러스터 헤더를 선정한다. 선정된 클러스터 헤더는 다른 클러스터에 포함되지 않은 자신의 이웃노드에게 클러스터 구성 메시지를 보냄으로써 클러스터를 구성한다. 둘째, 메시지 구성 단계에서는 클러스터 내에서 상수의 공유 키와 비밀 키를 이용하여 암호화된 데이터를 생성한다. 생성한 공유키를 각 센서 노드가 이웃 노드들과 교환하고, 각 노드에서 생성된 비밀 키를 이용하여 데이터를 암호화하여 다른 멤버에게 전송한다. 클러스터 멤버노드로부터 암호화된 데이터를 이용하여 각각의 노드는 이를 집계한다. 마지막으로, 집계 연산 단계에서는 취합한 암호화 데이터를 클러스터 헤더 노드로 전송하고, 클러스터 헤더 노드는 이를 분석하여 데이터의 합을 구한다. 즉, 클러스터 헤더는 하위 노드들의 비밀 키를 알지 못하더라도 공유 키를 이용하여 데이터 합을 계산할 수 있다. 각각의 클러스터에서 데이터 집계를 수행한 센서 노드는 TAG(Tiny Aggregation) 프로토콜[4]을 이용하여 라우팅 트리를 이용하여 상위 센서 노드로 전송한다. 한편 CPDA는 클러스터 내에서 데이터 집계처리를 수행하기 위하여 공유 키와 비밀 키를 송수신하기 때문에, 다수의 연산 및 데이터 전송이 발생하는 단점을 지닌다. 아울러, 클러스터에서 데이터 집계처리를 수행한 후 데이터를 전송할 때 데이터 보호를 보장하지 못하는 단점이 존재한다.

한편, SMART 기법은 자신의 데이터를 분할하여 이웃하는 센서 노드에게 전송함으로써 데이터 보호를 수행하는 기법이다. 이 기법은 클러스터링 기법이 지니고 있는 단점인 다수의 연산 및 통신량을 줄이기 위하여 데이터를 분할하여 수행한다. 아울러, 자신의 데이터를 임의로 분할하여 이웃 센서 노드에게 전달하기 때문에, 효율적인 데이터 보호를 지원한다. SMART 기법의 수행단계는 분할된 수집 데이터의 전송, 데이터 집계, 집계 데이터 전송 단계로 구성된다. 첫째, 각 센서 노드는 자신의 데이터를 J개로 분할하고, h홉 이내의 J-1개의 센서 노드를 선택하여 자신의 데이터를 전송한다. 둘째, 각 센서 노드는 이웃 노드들로부터 수신한 데이터를 취합한다. 마지막으로, 트리 구조의 라우팅을 통해 취합한 데이터를 싱크 노드로 전송한다. 싱크 노드는 자식 노드로부터 받은 메시지의 합을 계산함으로써, 질의 결과를 획득한다. 그러나 SMART 기법은 데이터를 분할하여 전송하기 때문에 데이터 집계 과정 시 다수의 통신을 요구하는 단점이 존재한다. 아울러, 센서노드 간의 통신 중에 전송되는 데이터를 공격자가 취득하였을 때, 집계되는 값의 예측이 가능한 단점이 존재한다.

3. 데이터 집계를 위한 힐버트 커브 기반 데이터 보호 기법

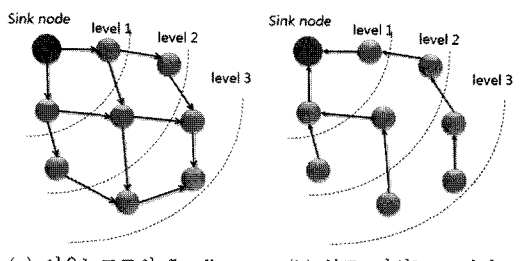
센서 네트워크에서 데이터 집계를 위한 효율적인 데이터 보호 기법 설계 시, 다음을 고려해야 한다. 첫째, 각 센서 노드는 자신의 데이터만을 알고 있기 때문에, 견고한 데이터 보호를 위하여 다른 노드와의 통신에서 데이

터를 도청하거나 왜곡시키는 공격자로부터 공격을 막을 수 있어야 한다. 둘째, 노드 간 통신을 최소화하여 네트워크의 효율(efficiency)를 최대화하여야 한다. 데이터 집계기법의 목적은 데이터 송신 양을 줄임으로써 네트워크 수명을 연장하는 것이다. 일반적으로 데이터 보호는 암호화를 위해 많은 양의 데이터를 전송하기 때문에, 가능한 적은 데이터 메시지 수와 적은 데이터 패킷을 송수신하도록 지원하여야 한다. 이를 위해, 본 논문에서는 데이터 집계를 위한 힐버트 커브 기반 데이터 보호 기법을 제안한다. 제안하는 기법은 센서 노드의 데이터를 통해 생성된 분할 데이터인 seed를 이용하여 자신의 데이터를 이웃노드에게 암호화하여 전송하기 때문에, 이웃노드와의 통신을 최소화한다. 아울러, 가공된 데이터를 힐버트 커브에 적용하여 암호화함으로써, 센서 노드간의 통신을 수행 시 공격자로부터 데이터를 보호 할 수 있다.

제안하는 데이터 보호 기법의 알고리즘은 네트워크 구성 단계, 암호화 데이터 생성 단계, 데이터 집계 단계로 구성된다. 첫째, 네트워크 구성 단계에서는 이웃노드 및 부모, 자식 노드를 설정하여 트리를 구성한다. 둘째, 암호화 데이터 생성 단계에서는 seed 교환 및 힐버트커브를 위한 방향성 key를 통해 센싱 데이터를 암호화한다. 마지막으로, 데이터 집계 단계에서는 데이터 집계를 위하여 암호화된 데이터를 부모 노드로 전송하고 및 이를 바탕으로 집계를 수행한다.

3.1 네트워크 구성 단계

제안하는 기법은 트리를 기반으로 네트워크를 구성한다. 먼저, 각 센서 노드에 대해 메시지 전파(flooding)기법[12]을 사용하여 싱크 노드로부터의 레벨(level)을 설정하고, 이웃노드를 구성한다. 만약, 수신한 메시지의 레벨이 현재 센서 노드에 설정된 레벨과 비교하여 더 작은 값일 경우 메시지를 전송한 이웃노드를 부모 노드로 선정한다. 이를 부모 노드에게 자식 노드가 되었음을 알림으로써, 트리 기반의 네트워크를 구성한다. 예를 들면, 그림 1(a)와 같이 싱크 노드에서부터 네트워크 구성 메시지를 전송함으로써, 라우팅을 시작하고, 메시지를 수신한 센서 노드는 각 이웃에게 메시지 전파를 수행한다.



(a) 이웃노드로의 flooding (b) 부모·자식노드 결정

그림 1 네트워크 구성 단계

이 후, 각 센서 노드는 이웃 노드들의 정보를 수집하고, 그림 2(b)와 같이 자신의 부모 노드를 선정하여 조인 메시지를 보냄으로써, 네트워크를 구성한다.

한편, 특정 노드가 부하가 많이 걸리는 것을 방지하기 위하여, 자식 노드 수의 임계값(δ)을 설정한다. 이를 통해, 임계값 이후에 전송되는 조인된 메시지를 반송함으로써, 자식 노드에게 다른 부모 노드 선정을 요구한다.

3.2 암호화 데이터 생성 단계

네트워크가 구성되면, 각 센서 노드는 센싱 데이터를 이용하여 seed를 생성한다. seed는 자신의 센싱 데이터를 가공하기 위한 값이며, seed 값을 부모 노드를 제외한 임의의 이웃 노드에게 전송한다. 이 때, 자신이 전송하고자 하는 데이터는 이웃 노드에게 전송한 seed의 값을 뺀 값을 가지고 있다. 예를 들어, 그림 2와 같이 A노드가 B노드에게 seed값 Sa를 전송하였을 때, B노드는 자신의 데이터 b와 A노드에게 받은 seed값을 더한 b+Sa를 가지며, A노드는 자신의 데이터 a에서 B노드로 전송한 seed 값을 뺀 a-Sa 값을 가진다. 이는 공격자로부터 원(raw) 데이터의 획득을 막을 수 있으며, 데이터 집계 시 사용자에게 정확한 질의 결과를 제공한다.

seed 교환을 통해 데이터를 힐버트 커브(Hilbert curve)에 적용하여 데이터를 암호화한다. G.Peano에 의해 제안된 힐버트 커브[11]는 공간 영역 변환 기법으로 2^n*2^n 그리드로 분할된 영역에 힐버트 공간 채움 곡선(Hilbert space filling curve)을 사용하여 ID를 부여함으로써, 2차원의 영역을 1차원으로 변환한다. 이 때, 힐버트 공간 채움 곡선의 시작 방향에 따라 Bottom, Top, Left, Right의 방향성을 지니게 된다. 예를 들어 그림 3과 같이 레벨 2의 4*4 그리드 영역은 4개의 힐버트 커브 진행 방향에 따라 16개의 서로 다른 힐버트 ID를 가진 1차원의 정보로 변환된다.

본 논문에서는 센서 노드에서 전송하는 데이터를 보호하기 위해 데이터 값을 힐버트 ID로 맵핑(mapping, 변환)한다. 따라서 다양한 데이터 값을 표현하기 위하여 데이터 값에 따라 전체 2^n*2^n 그리드 영역의 크기를 변환하고 n을 힐버트 레벨이라 표현한다. 예를 들어 데이터 값이 14일 경우, 최소 그리드 영역 사이즈는 4*4가 되므로 힐버트 레벨은 2가 된다. 데이터 값이 50일 경우, 이 값은 8*8 그리드 영역에서 힐버트 ID를 가지므

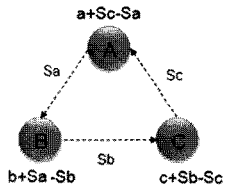


그림 2 이웃노드와의 seed 교환

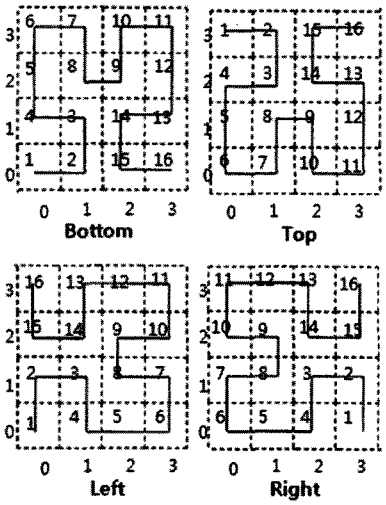


그림 3 4가지 힐버트 커브의 방향성의 예

로 힐버트 커브의 레벨은 3이 된다. 이러한 정보를 바탕으로 각 센서노드는 자신이 수집한 데이터 값을 힐버트 ID로 변환하고 그에 따른 힐버트 커브의 방향성, 힐버트 레벨 정보를 함께 전송함으로써 암호화를 수행한다. 암호화된 데이터의 타입은 <key(direction,level), data_x, data_y> 형태로 이루어져 있다. key는 힐버트 커브의 시작 방향(direction)과 힐버트 커브 레벨(Hilbert-Curve Level)로 이루어져 있으며, data_x, data_y는 힐버트 커브에 의해 변환된 데이터의 ID 좌표이다. 예를 들어, 그림 3에서 센서 노드에서 생성된 데이터 값이 14일 때 이를 힐버트 커브의 Bottom 방향으로 변환한 ID는 4*4 그리드 영역에서 (2,1)의 좌표를 가진다. 따라서 암호화된 데이터는 <key(B, 2), 2, 1>의 형태를 가진다.

3.3 데이터 집계 단계

힐버트 커브를 이용하여 암호화한 데이터는 데이터 집계를 위해 상위 부모 노드로 전송된다. 이 때 자식노드로부터 데이터를 수신한 부모노드는 수신한 메시지의 key값 즉, 힐버트 커브의 방향성과 힐버트 레벨을 분석한다. 만약, 자식노드의 힐버트 커브의 방향성과 자신의 방향성이 다른 경우, 자식 노드의 데이터를 자신의 힐버트 커브의 방향성에 맞추어 재조정한다. 아울러 힐버트 커브를 분석하여, 그리드 크기를 조정한다. 마지막으로 이를 하나의 데이터로 집계하고, 힐버트 커브에 다시 적용하여 상위 노드로 전송한다.

그림 4는 제안하는 데이터 보호 기법의 전체적인 알고리즘을 나타낸다. 이 때, 네트워크 구성 단계(line 2-10)에서는 기지국에서 메시지 전파기법을 통해, 라우팅 구성 메시지를 각 센서 노드에게 전송하고, 이를 수신한 센서 노드는 이웃노드와 부모, 자식 노드를 선정한다(line 1-3). 암호화 데이터 생성 단계에서는 seed와 key(방향성, 레벨)을 생성하여 이웃노드와 교환하고, 데이터를 힐버트 커브에 적용하여 암호화한다(line 4-6). 마지막으로, 데이터 집계 단계에서는 집계를 위해 자식노드에서 부모 노드로 전송하고, 이를 수신한 부모 노드는 데이터를 집계한다(line 7-12).

```
HilbertCurve_DataPrivacy Algorithm
01. Start_Flooding(initLevel, base_stationID)
02. Make_NeighborInfor();
03. Choose Parent();
04. seed = Make_seed();
05. HKey = Make_key();
06. key = Enc(seed, HKey);
06. send_key(key);
07. for (query epoch) {
08.     Aggre_Data = 0;
09.     for (every child node) {
10.         Aggre_Data += receive_massage(); }
11.     Aggre_Data = Aggre_Data - seed;
12.     Sending_Message(Aggre_Data, Parent); }
End of Algorithm
```

그림 4 제안하는 데이터 보호 기법 알고리즘

4. 성능 평가

본장에서는 제안하는 힐버트 커브 기반 데이터 보호 기법의 효율성을 검증하기 위하여, 성능평가를 수행한다. 성능평가 대상은 제안하는 기법과 CPDA기법 및 SMART기법이다. 각각의 알고리즘은 cygwin 기반의 TinyOS 1.15 상에서 구현하였으며, 구현환경은 표 1과 같다. 또한, TinyOS에서 제공하는 시뮬레이터 TOSSIM을 이용하여 성능평가를 수행한다. 본 실험에서는 다양한 노드 수를 가진 센서 네트워크에서 전체 메시지 전송량 및 노드 당 평균 수명을 비교한다. 이를 위해, 센서 노드는 10개, 20개, 50개, 100개로 측정하였고, 노드의 분포가 고른 random 데이터를 사용하였다.

그림 5는 센서 네트워크에서 노드 간 전체 메시지 전송량을 나타낸다. 이 때, 메시지 전송량은 클러스터 구성 및 집계 시의 데이터 전송 수를 합한 것이다. 전체 노드 수가 100개일 때, 제안하는 기법, CPDA, SMART에서 전체 메시지 전송량은 평균 782개, 929개, 897개이다. CPDA 기법은 초기 클러스터 구성 및 암호화된 데이터 생성 시, 클러스터 멤버 노드들간의 다수의 연산

표 1 구현 환경

CPU	Intel Core2 Duo E4500 2.20GHz
Memory	2G
Simulator	TOSSIM
Compiler	gcc compiler

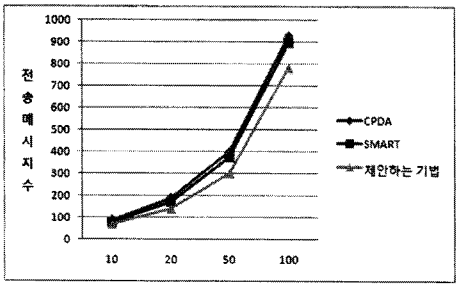


그림 5 전체 메시지 전송량

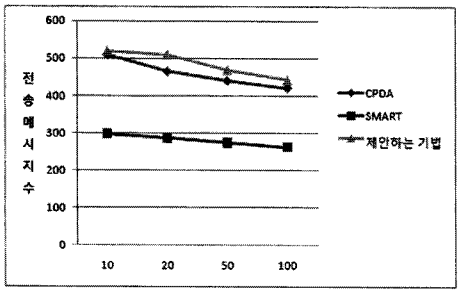


그림 6 노드당 평균 수명

및 통신이 이루어지기 때문에 가장 많은 메시지 전송이 발생한다. SMART 기법은 센서 데이터를 분할하여 전송하기 때문에, 집계 과정에서 다수의 연산 및 통신이 발생한다. 반면, 제안하는 기법은 센서마다 독자적인 힐버트 커브를 사용하기 때문에, 데이터의 암호화를 수행할 때 다른 노드와의 통신이 적게 발생한다. 따라서, 제안하는 기법의 메시지 전송량이 타 기법에 비해 약 10%의 개선된 성능을 보임을 알 수 있다.

데이터 집계를 위한 노드 당 에너지 소모를 측정하기 위하여, 그림 6은 노드 당 평균 수명을 나타낸다. 각 센서 노드의 전력량을 5000mJ로 설정하고, 전력량이 0mJ가 될 때까지의 주기를 측정한다. 전체 노드 수가 100개일 때, 제안하는 기법, CPDA, SMART에서 노드 당 평균 수명은 각각 443, 421, 262 주기이다. CPDA기법은 클러스터 구성 및 데이터 암호화 과정에서 다수의 연산이 발생하기 때문에, 가장 많은 에너지 소모를 보인다. 또한, SMART 기법은 데이터 집계 시 분할 데이터를 전송하여 대부분의 노드가 다수의 통신을 하기 때문에, 많은 전력 소비량을 보인다. 반면, 제안하는 기법은 암호화된 데이터 생성 시 적은 통신이 발생하며, 트리 기반의 네트워크이기 때문에 집계 시에도 적은 전송량을 보인다. 결과적으로, 제안하는 기법이 메시지 전송량 측면에서 타 기법에 비해 10-40%의 개선된 성능을 보임을 알 수 있다.

5. 결론 및 향후 연구

본 논문에서는 데이터 집계 처리를 위한 데이터 보호 기법을 제안하였다. 이는 기존 클러스터링 기반 네트워크와는 달리 트리 기반 네트워크를 사용하여, 네트워크 구성 및 집계 시 연산을 최소화하였다. 아울러, 힐버트 커브 기법을 적용하여 데이터를 암호화함으로써, 센서 노드간의 통신을 수행할 때 공격자로부터 데이터를 보호한다. 마지막으로 성능평가를 통해 제안하는 기법이 기존 연구인 CPDA 및 SMART 기법에 비해 메시지 전송량 측면에서 약 10%, 에너지 소비량 측면에서 약 10-40%의 우수한 성능을 보임을 입증하였다. 향후 연구로는 제안한 기법을 실제 센서 네트워크에 적용하여, 제안하는 기법의 효율성을 입증하는 것이다.

참 고 문 헌

[1] http://firebug.sourceforge.net, The firebug project, 2008.
[2] http://www.cens.ucla.edu, James reserve microclim-ate and video remote sensing, 2008.
[3] http://www.greatduckisland.net/, Habitat monitoring on great duck island, 2008.
[4] S. Madden, M. J. Franklin, and J. M. Hellerstein, "TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks," OSDI, 2002.
[5] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net. (MobiCOM '00)*, 2000.
[6] W. R. Heinzelman, "Application-Specific Protocol Architectures for Wireless Networks," *Ph.D. thesis, Massachusetts Institute of Technology*, 2000.
[7] O. Younis and S. Fahmy, "HEED: a Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor networks," *IEEE Trans. Mobile Computing*, vol.3, no.4, pp.366-79, 2004.
[8] S. Lindsey, C. Raghavendra, and K. M. Sivalingam, "Data Gathering Algorithms in Sensor Networks Using Energy metrics," *IEEE Trans. Parallel and Distributed Systems*, vol.13, no.9, pp.924-35, Sept. 2002.
[9] K. Du, J. Wu, and D. Zhou, "Chain-based Protocols for Data Broadcasting and Gathering in Sensor Networks," *Int'l. Parallel and Distributed Processing Symp.*, 2003.
[10] W.B. He, X. Liu, H. Nguyen, K. Nahrstedt, T. Abdelzaher, "PDA: privacy-preserving data aggregation in wireless sensor networks," *in Proceedings of the 26th IEEE Int'l Conf. on Computer Communications*, pp.2045-2053, 2007.
[11] A.R. Butz, "Alternative algorithm for Hilbert's space filling curve," *IEEE Trans, On Computers*, 1971.
[12] Panthachai, Y., Keeratiwintakorn, P., "An energy model for transmission in Telos-based wireless sensor networks," *Int'l joint conf. on computer science and software engineering*, 2007.