센서 네트워크에서 데이터 집계를 위한 힐버트 커브 기반 데이터 보호 기법†

윤민○ 김용기 장재우*
전북대학교 컴퓨터공학과, 영상정보신기술연구소*
{myoon, ykkim, jwchang}@dblab.chonbuk.ac.kr

A Privacy Data Preserving Scheme based on Hilbert Curve for Data Aggregation in Wireless Sensor Network

Min Yoon○ YongKi Kim JaeWoo Chang*
Department of Computer Engineering, Chonbuk National University
Center for Advanced Image and Information Technology*

1. 데이터 집계를 위한 힐버트 커브 기반 데이터 보호 기법

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. 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 지원하는데이터 집계 기법(data aggregation technique)이 제안되었다[1, 2]. 이 기법은 하위 노드로부터 받은 데이터와 자신의 데이터의 대표값 (예를 들면, 최대값, 최소값, 평균값, 데이터 수, 데이터 합)만을 상위 노드로 전송한다. 한편, 센서 네트워크는 무선 통신을 수행하기 때문에 데이터에 대한 보호가 이루어지지 않는다. 이는 공격자가 데이터를 도청하여 악의적인 용도로 사용하는 것을 가능하게 한다. 따라서, 센서 네트워크에서의 데이터 집계를 위한 데이터 보호 기법에 관한 연구가 필수적이다. 그러나 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)[3], SMART(Slice-Mix-AggRegaTe)[3]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) 기반 데이터 보호 기법을 제안한다. 제안하는 기법은 센서 노드의 데이터를 통해 생성된 분할 데이터인 seed를 이웃노드에게 전송함으로써, 자신의 데이터를 은폐할 수 있다. 아울러, 변환된 데이터를 힐버트 커브에 적용하여 암호화함으로써, 센서 노드간의 통신을 수행할 때 공격자로부터 데이터를 보호 할 수 있다. 또한 센서 노드에서 암호화를 수행하여 이웃노드와의 통신을 최소화함으로써 네트워크 구성 및 집계 시 전체 네트워크 통신량을 최소화한다.제안하는 데이터 보호 기법의 알고리즘은 네트워크 구성 단계, 암호화 데이터 생성 단계, 데이터 집계 단계로 구성된다.

수행단계 1. 네트워크 구성 단계

네트워크 구성 시 각 센서 노드에 대해 메시지 전송(flooding)기법을 사용하여 싱크노드로부터의 레벨을 설정하고 이웃노드를 구성한다. 만약, 수신한 메시지의 레벨이 현재 센서 노드에 설정된 레벨과 비교하여 더 작은 값을 경우 메시지를 전송한 이웃노드를 부모노드로 저장한다. 이를 통해 트리 기반의 센서 네트워크를 구성한다.

수행단계 2. 암호화 데이터 생성 단계

네트워크가 구성되면, 각 센서 노드는 센싱 데이터를 이용하여 seed를 생성한다. seed는 자신의 센싱 데이터를 은폐를 위한 값이며, seed 값을 임의의 이웃 노드에게 전송한다. 이 때, 자신이 가지고 있는 데이터는 이웃 노드에게 전송한 seed의 값을 뺀 값을 가지고 있다. seed 교환을 통해 데이터를 변형 시킨 후, 이를 힐버트 커브(Hilbert curve)에 적용하여 데이터를 암호화한다. 이 때 힐버트 공간 채움 곡선의 시작 방향에 따라 Bottom, Top, Left, Right의 방향성을 지니게 된다. 센서 노드에서 전송하는 데이터를 보호하기 위해 데이터 값을 힐버트 ID로 맵핑

† 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구결과임

(mapping)하며, 다양한 데이터 값을 표현하기 위하여 데이터 값에 따라 전체 그리드 2n*2n 그리드 영역의 크기를 변환하고 n을 힐버트 레벨로 설정한다. 이를 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.

수행 단계 3. 데이터 집계 단계

힐버트 커브를 이용하여 암호화한 데이터는 데이터 집계를 위해 상위 부모 노드로 전송된다. 이 때 자식노드로부터 데이터를 수신한 부모노드는 수신한 메시지의key값 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

2. 성능 평가 및 고찰

제안하는 힐버트 커브 기반 데이터 보호 기법은 Intel Core2 Duo CPU 2.20GHz 및 2GB의 메모리 상에서 구현하였으며, TOSSIM 시뮬레이터를 이용하여 성능평가를 수행한다. 성능평가 대상은 제안하는 기법과 CPDA기법 및 SMART기법이며, 다양한 노드 수를 가진 센서 네트워크에서 전체 메시지 전송량 및 노드 당 평균 수명을 비교한다. 이를 위해, 센서 노드는 10개, 20개, 50개, 100개로 측정하였으며, 노드의 분포가 고른 random 데이터를 사용하였다. <그림 1>은 센서 네트워크에서 노드 간 전체 메시지 전송량을 나타낸다CPDA 기법은 초기 클러스터 구성 및 암호화된 데이터 생성 시, 클러스터 멤버 노드들간의 다수의 연산 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 <그림 2>는 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 때문에많은 전력 소비량을 보인다. 반면, 제안하는 기법은 암호화된 데이터 생성 시 적은 통신이 발생하며, 트리 기반의 네트워크이기 때문에 집계 시에도 적은 전송량을 보인다. 따라서, 에너지 소비량은 전체 네트워크에서 송수신되는 메시지 전송량과 비례함을 알 수 있다.

제안하는 기법과의 성능평가를 통해 기존 연구보다 메시지 전송량 측면에서 약10%, 에너지 소비량 측면에서 약 10~40%의 우수한 성능을 보임을 입증하였다

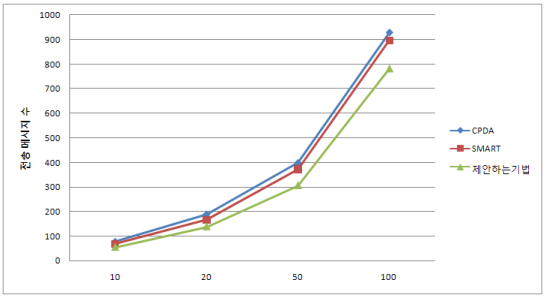

그림 1 전체 메시지 전송량

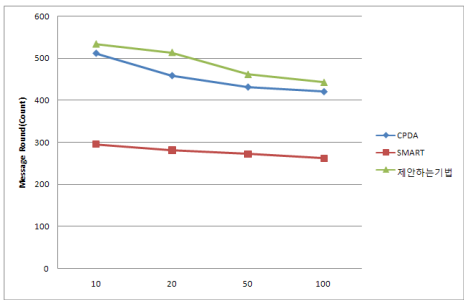

그림 2 노드 당 평균 수명

참고 문헌

[1] S. Madden, M. J. Franklin, and J. M. Hellerstein, “TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks,” OSDI, 2002.

[2] 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.

[3] 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 International Conference on Computer Communications, 2007, pp. 2045-2053.

[4] A.R. Butz, “Alternative algorithm for Hilbert’s space filling curve”, IEEE Trans, On Computers, 1971.