U-센서네트워크에서의 Pairwise key 설정 기법

이경효○, 정석원, 오병균
목포대학교
{mediakh○, jsw, obk}@mokpo.ac.kr

A pairwise key establishment scheme for USN

Kyoung Hyo Lee○, Seok Won Jung, Byeong-Kyun Oh
Department of information Security, Mokpo National University

요 약

센서네트워크는 유비쿼터스 컴퓨팅 사회에서 핵심 기술로 부각되고 있다. 이러한 센서네트워크는 노드들이 노출되거나 데이터 전송 시 일반 네트워크보다 보안에 취약하므로 안전한 통신을 위하여 센서 노드 간 키를 설정하는 것은 보안을 위한 기본적인 요구사항이 되고 있다. 본 논문에서는 배치된 센서네트워크에서 셋업서버의 오버헤드를 줄이기 위하여 네트워크를 클러스터링하고 각 셀 안에 클러스터 헤더와 노드들을 배치한 후 클러스터내의 노드사이의 안전한 통신을 하기위한 pairwise key를 설정하는 기법을 제안하였다.

1. 서 론

센서네트워크는 많은 수의 센서노드들로 구성되고 센서를 통한 정보감지 및 감지된 정보를 처리하는 기능을 수행한다. 각 센서노드들은 제한된 연산 처리 능력만을 가지고 있고 노드들이 애드혹의 형태로 구성되어 통신하게 된다. 이러한 환경으로 인하여 센서노드 간에 전송되는 데이터가 외부에 쉽게 노출되거나 변조될 위험이 존재한다[9]. 그러므로 안전한 통신을 위하여 센서 노드 간 키를 설정하는 것은 보안을 위한 기본적인 요구사항이 되고 있다.

센서네트워크에서 센서노드들에게 키를 분배 할 때 베이스 스테이션에서 노드에 사용될 키 정보를 만들어서 각 노드에 사전에 전달하였다. 그러나 센서네트워크의 구성 후 노드를 추가 할 때 네트워크의 구성에 변화를 필요로 하였다.

본 논문에서는 배치된 센서네트워크에서 셋업 서버의 오버헤드를 줄이기 위해 location based와 같이 센서네트워크를 나누고 각각의 셀 안에 여러 개의 노드들을 배치하여 하나의 셀 안에는 클러스터헤더와 다른 노드들로 구성하게 하였다. 사전 분배에서 셋업 서버는 클러스터헤더게만 이변수 다항식을 분배하고 모든 노드들이 target field에서 배치된 후 클러스터헤더는 home cell내의 노드들에게 polynomial share를 분배한다. 이와 같은 과정에서 이변수 다항식에서 유도된 일변수 다항식을 전달하여 키 설정을 하는데 일변수 다항식으로부터 해더의 이변수 다항식을 얻을 수 있는 약점이 있다. 이 문제점을 해결하기위해 클러스터 헤더의 이변수 다항식으로부터 유도한 유한체상의 일변수 다항식을 사용하여 키분배를 하는 방법을 제안한다. 제안한 기법은 pairwise key의 설정에서 통신 데이터의 도청에 대해서도 클러스터헤더의 이변수 다항식을 안전하게 하였다.

2장은 센서네트워크를 위한 다항식 기반 키분배 기법을 설명하고 3장은 클러스터 기반의 키분배 기법을 설명하고 유한체 상의 랜덤 변수와 이변수 다항식으로부터 생성한 일변수 다항식을 이용하여 두 노드 사이에 pairwise key설정하게 한다. 4장은 결론과 함께 향후 연구 방향을 제시한다.

"본 논문은 정보통신부 선도기반 기술 개발 사업 중 한국전자통신연구원의 ETRI "RFID/USN용 센서태그 및 센서노드 기술개 발" 과제의 연구결과로 수행된 것입니다"

2. 관련연구

센서네트워크에서 센서 노드 간에 안전한 통신을 위한 키 관리에는 랜덤키 사전분배 구조와 다항식기반 키 분배 구조 등이 있다.

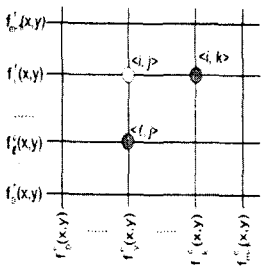
2.1 Random key predistribution scheme

L. Eschenauer, V. Gligor가 제안한 랜덤키 설정기법은 센서 네트워크에서 센서 노드 간 키 쌍(pairwise key) 설정 프로토콜로 베이스 스테이션이 다량의 랜덤키를 생성하여 키풀에 저장하고 키풀(pool)에서 무작위로 임의의

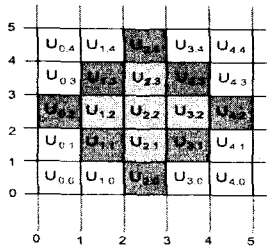
키집합을 선택하여 키 링을 생성하여 센서노드에게 부여한다. 센서노드는 부여받은 키 링의 정보를 브로드캐스팅하여 이웃하는 노드들과 공유되는 키를 두 노드간의 키 쌍으로 사용한다. 두 링크 또는 그 이상 떨어져 있으면서 서로 공유하는 키가 없는 임의의 두 노드가 공유키를 갖기 위해서는 path key를 생성하여 공유한다. Path key를 설정하고자 하는 두 노드간의 direct link path를 통해 키를 교환하여 공유키를 설정한다. 하나의 센서노드가 자신의 키 링에서 사용하지 않은 키 중 하나를 path key로 설정한 후 해당 노드까지 이르는 path상에 있는 중간 노드들을 거쳐 상대노드에게 전송한다. 이때 path키 정보는 중간 노드들 간의 공유키로 암호화 되어 전송한다. 이 기법은 센서노드의 개수가 많더라도 수백개 정도의 키로 기존의 키 쌍과 동일한 안전성을 제공하는 장점을 갖는다[6].

2.2 Grid 기반 키분배 구조

D. Liu, P. Ning은 이변수 다항식을 이용하여 센서 노드 간 키 쌍을 설정하는 프로토콜인 그리드기반 키 분배 구조를 제안하였다. 임의의 두 센서 노드는 f(x,y) = f(y,x)을 만족하는 동일한 다항식을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다. 센서노드들이 [그림1]에서와 같이 m*m 격자(grid) 상에 위치된다고 가정한다. 셋업 서버는 2m개의 다항식을 생성하여 i열 j 행에 있는 센서노드에게 [그림1]와 같이 두 개의 다항식 $f_i^r(x,y)$와 $f_j^c(x,y)$를 분배한다. 만일 동일한 행 또는 열<i,k>위치에 있는 노드와는 $f_i^r(j,k) = f_i^r(k,j)$인 성질을 이용하여 공유키를 만든다. 동일한 행



[그림2] Grid based key predistribution scheme



[그림3] Location based predistribution scheme

또는 열에 위치한 노드들끼리는 바로 키 쌍을 생성할 수 있도록 하고 노드가 같은 행 또는 열에 위치하지 않은 경우에는 같은 행 또는 열에 위치한 다른 노드들로 경로를 만든 후 경로키를 사용해서 공유키를 만든다.

이와 같이 Grid 기반 키분배 구조는 동일한 행이나 열에 위치하지 않는 두 노드가 키 쌍을 설정하는 경우에도 각 센서 노드의 ID를 통해 센서노드의 위치를 바로 파악할 수 있고 센서위치정보를 이용하여 상대 센서 노드에 이르는 경로를 보다 쉽게 찾을 수 있다. 하지만 다항식이 노출 될 경우 이 좌표에 할당된 다항식을 사용하는 모든 센서들이 노출되는 문제점이 있다[3].

2.3 Location 기반 키분배 구조

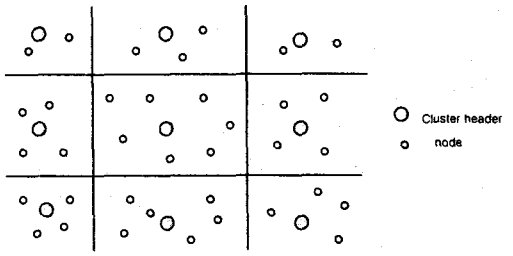
위치기반 키 분배 방식은 그리드 기반 키분배 구조에서 사용하였던 방식처럼 f(x,y) = f(y,x)을 만족하는 다항식을 분배하되 센서필드 S를 [그림3]과 같이 직사각형 구조로 나누고 각 셀의 좌표를 (i,j)로 표시하여 그 셀과 고유한 다항식을 연관시킨다. 특정 노드 u_{ij}에 다항식 $f_{ij}(x,y)$를 할당한다. 특정 셀에 위치하는 센서는 그 위치에 해당하는 다항식과 인접 4개 셀에 해당하는 4개의 다항식을 할당 받아 이웃 셀에 배치된 센서와 pairwise key를 생성하는 방식이다. 예를 들어 [그림3]의 좌표(2,2)에 있는 센서 $u_{2,2}$에게 셋업서버는 노드 u가 위치한 셀과 인접한 네 개의 셀에 해당하는 polynomial share $f_{2,2}(u_{2,2},y)$, $f_{2,1}(u_{2,2},y)$, $f_{1,2}(u_{2,2},y)$, $f_{2,3}(u_{2,2},y)$, $f_{3,2}(u_{2,2},y)$를 배분한다. 센서 배치후 특정 두 센서가 pairwise key를 셋업하고자 하면, 우선 같은 공통의 다항식이 있는지 확인하여 공통의 다항식이 있으면 이전 연구에 설명 되어있는 polynomial based key distribution방법으로 키를 설정한다. 셀을 추가하면서 각각의 셀에 위치한 노드들이 compromised 센서의 ID들을 기억하고 있으므로 다항식이 노출 될 수 있는 위험이 있다.[4]

3. 제안된 클러스터기반 키 분배구조

기존의 다항식 기반 키분배 구조에서 다항식의 노출로 인한 키 노출시 네트워크에 끼치는 영향을 최대한 줄이기 위해 네트워크를 클러스터링 하여 클러스터 단위로 하나의 다항식을 공유하게 하여 센서노드들은 그 다항식을 바탕으로 노드 간 키를 생성하여 공유한다. 즉 하나의 다항식을 공유하는 센서네트워크의 영역을 하나의 클러스터로 제한하여 다항식을 공유하는 센서의 수를 제한하여 향상된 보안 효과를 기대할 수 있다. 같은 클러스터 영역에 있는 센서들 중 자신의 전송범위에 있는 센서들은 공통의 다항식을 사용하고 서로의 ID를 이용하여 pairwise key를 만들 수 있어 키풀 크기에 상관없이 직접키를 설정할 수 있다. 또한 클러스터 내의 센서들은 클러스터에 배치되면 그 후에 클러스터 헤더로부터 다항식 부분정보를 분배받기 때문에 기존의 방법보다 사전에 분배하는 정보의 양을 줄일 수 있다.

센서가 다른 클러스터 영역에 있어서 경로키를 만들어야하는 경우도 클러스터 헤드간의 키는 센서가 배치되기 전에 미리 분배되어있으므로 클러스터 헤드를 통해 안전하게 경로키를 다른 클러스터에 있는 센서노드에게 전달할 수 있다.

클러스터 헤더의 전송범위는 클러스터 영역을 포함한다고 가정한다. 센서들은 자신의 전송범위 내에 있는 이웃 노드들과 클러스터 헤드로부터 분배받은 다항식 부분정보를 이용하여 pairwise key를 생성할 수 있다. 임의의 두 센서가 동일 클러스터 내에 위치할 경우 직접키를 생성하여 pairwise key를 생성할 수 있고 서로 다른 클러스터에 포함될 경우는 경로키를 생성하여 pairwise key로 사용한다[10]. 제안 메커니즘의 구조는 다음 [그림3]과 같다. 또한 베이스 스테이션은 소수 q에 대하여 유한체 F_q 상에서 임의의 t차 이변다항식(bivariate)을 아래와 같이 생성한 후 각 클러스터 헤더에게 임의의 다항식을 선택하여 분배한다.



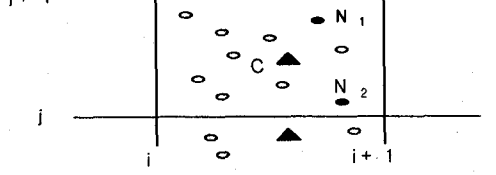
[그림 4] cluster based key distribution scheme

$$f_c(x,y) = \sum_{i,j} a_{ij}\, x^i y^j$$

단, 이 다항식은 $f_c(x,y) = f_c(y,x)$를 만족해야 하고, 클러스터헤더 C_n에게 분배된 다항식은 $fc_n(x,y)$이다.[1]

클러스터 C내에 노드 N_1, N_2가 존재한다고 하자. 노드 N_1, N_2 사이의 키 쌍은 다음의 절차에 따라 설정한다.

클러스터 C는 N_1, N_2 식별자를 갖는 노드에게 다항식 $f_c(x,y)$로부터 생성된 다항식 부분 정보를 생성하여 분배한다. $f_c(N_1,y) = \sum_{i,j} a_{ij}\, N_1^i y^j$ $f_c(N_2,y) = \sum_{i,j} a_{ij}\, N_2^i y^j$



[그림 5] Nodes in a same cell

N1은 $fc(N_1,y)$를 갖고 있고, N_2는 $fci(N_2,y)$를 갖고 있으므로 두 노드들의 ID를 이용해 다항식을 생성한다.

$$fc(N_1,N_2) = \sum_{i,j} a_{ij}\, N_1^i N_2^j \;,\; fci(N_2,N_1) = \sum_{i,j} a_{ij}\, N_2^i N_1^j$$

앞에서 가정한 다항식 $fci(x,y)$의 성질에 따라 $fci(N_1,N_2) = fci(N_2,N_1)$ 이므로 두 센서 노드는 동일한 키를 공유할 수 있다.

이변수 다항식 f(x,y)를 사용한 다항식 기반 키 분배 구조에서 클러스터 C가 두 개의 노드 N_1과 N_2에 다항식의 부분정보를 전달할 때 이를 도청하면 $f_c(N_1, y) = \sum_{i,j} a_{ij} N_1^i y^j$, $f_c(N_2, y) = \sum_{i,j} a_{ij} N_2^i y^j$ 두 값을 알 수 있다.

이 때 y^j에 관련 있는 계수 a_{ij}와 x의 차수를 구할 수 있으면 클러스터 헤더가 가지고 있는 이변수 다항식을 알 수 있으며 이를 통해 클러스터 내의 모든 노드의 키 쌍을 알 수 있게 된다.

두 다항식 $f_c(N_1, y)$와 $f_c(N_2, y)$의 y^j 계수를 나누면 $\frac{a_{ij}N_1^i}{a_{ij}N_2^i} = (\frac{N_1}{N_2})^i$ 이 된다. 그런데 $f_c(x, y) = f_c(y, x)$ 이므로 i가 가질 수 있는 값은 다항식 부분정보인 $f_c(N_1, y)$의 y의 차수 중에 있다. 따라서 도청한 두 노드의 N_1과 N_2 값과 y의 차수 k들에 대해 $(\frac{N_1}{N_2})^k$ 값을 계산하고 도청으로 얻은 $(\frac{N_1}{N_2})^i$ 과 비교한다. 만약 같은 값이 나왔다면 k=i 임을 알 수 있는 것이고 이변수 다항식의 y^j가 있는 항이 $x^i y^j$인 것이다. $x^i y^j$의 계수는 $f_c(N1, y)$의 y^j의 계수를 N_1^i으로 나누면 $a_{ij} = \frac{a_{ij}N^i}{N^i}$ 이다. 따라서 클러스터 해드가 노드들에게 이변수 다항식의 부분정보로 일변수 다항식을 전달하는 것은 도청에 의한 공격이 가능하다.

이러한 이유로 인하여 $f_0(x, y) = F_0(y)$을 만족하는 값을 사용하여보자. 여기서 x를 만족하는 수는 유한체 Fq 상의 자연수이므로 1부터 선택해서 계산한다.

그러나 노드 N_1에게 분배하는 부분정보$F_0(N_1)F_0(y)$을 도청하면, $F_0(N_1)F_0(N_1) = F_0(N_1)^2 \in Fq$ 이므로 $F_0(N_1)$의 계산이 가능하게 된다[8].

$F_0(N_j) = \sum_i a_i N_j^i$ for j=1,2,...,k 이므로 k개의 연립방정식을 통해 f(x,y)의 계산이 가능함을 알 수 있다.

클러스터 헤더의 키인 이변수 다항식을 통한 부분정보인 일변수 다항식 $f_c(N_1, y)$을 전달하는 과정에 도청이

가능하므로 $f_c(N_1, y)$을 전달하는 대신에 클러스터 헤더로부터 선택한 난수를 포함한 방법을 제안하였다. 클러스터 헤더는 random number r을 선택하여 $(r, f_o(x, y))$을 생성하여 분배한다. $f_o(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ 은 부분정보의 노출로 공격이 가능함으로 사용하지 않는다.

$<r, f_o(x, y), F(y)>$에서 $f_o(x, y) = F_0(y)$를 만족하여야하므로 x를 만족하는 수는 유한체 Fq 상의 자연수이므로 1부터 선택해서 계산한다.

노드 N_1과 N_2의 ID를 주고 받은 값에 클러스터 헤더로부터 선택한 난수 r을 곱한 값을 두 노드간의 pairwise key로 공유한다. 두 노드간의 pairwise key를 공유하는 과정을 살펴보면 다음과 같다.

노드 N_1과 N_2의 식별자와 $f_o(x, y) = F_0(y)$의 값에 클러스터 헤더에서 선택한 난수 r을 곱한 값은

$r* F_0(N_1)F_0(y)$과 $r* F_0(N_2)F_0(y)$이 된다.

N_1은$F_0(N_1)F_0(y)$를 갖고 있고, N_2는 $F_0(N_2)F_0(y)$를 갖고 있으므로 두 노드의 ID를 이용하여

$r* F_0(N_1)F_0(N_2)$, $r*F_0(N_2)F_0(N_1)$를 생성할 수 있다.

앞에서 가정한 다항식 $fci(x,y)$의 성질에 따라 $r*F_0(N_1)F_0(N_2) = r*F_0(N_2)F_0(N_1)$ 이므로 두 센서 노드는 pairwise key를 공유할 수 있다.

즉 두 노드의 ID를 교환한 값에 난수 r을 사용하여 이변수 다항식을 찾는 것은 불가능하게 하였다..

Ⅳ. 결론

센서네트워크에서의 키 관리 구조로서 센서 노드 간 안전한 통신을 위해 키를 생성하고 분배하고 갱신 하는 키 관리 연구의 보안성은 매우 중요하다. 본 논문에서는 센서네트워크를 클러스터링하고 이변수 다항식을 사용한 pairwise key 설정 방법에서 클러스터 헤더가 노드에게 이변수 다항식의 부분정보를 할당할 때 일변수 다항식을 보내는 경우 이를 도청하면 클러스터 해더의 이변수 다항식을 찾을 수 있음을 보였다.

이를 해결하기 위해 클러스터 헤더가 노드들에게 일변수 다항식을 전달할 때 f(x,y)를 사용하는 대신에 x값을 유한체 Fq상의 자연수를 대입한 $F_0(y)$값에 두 노드의 ID를 대입한 값과 클러스터 헤더가 선택한 난수를 포함한 값을 전달함으로써 이웃노드들과 pairwise key를 생성할 때 도청에 의한 이변수 다항식의 노출을 막을 수 있도록 키 분배 구조를 설계하였다.

그러나 본 논문에서 제안한 방식은 기존에 제안된 방법과의 시뮬레이션을 통한 그 효율성을 증명하는 방안과 제안한 키 설정 메커니즘을 이용하여 센서노드의 전송범위 내에 위치하나 동일하지 않은 클러스터에 있는 센서노드들과의 경로키를 설정하는 방안에 대한 향후 연구도 필요하다.

[참고문헌]

[1] C.Blundo, A.De Santis, A. Herzbergs, S.Kutten, U.Vaccaro, and M.Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology- CRYPTO '92, LNCS 740, pages 471-486, 1993.

[2] T. Dimitriou, I. Krontiris, and F. Nikakis, Key Establishment in sensor networks with resiliency against node capture and replication, December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (Mobihoc) 2004.

[3] D. Liu,P. Ning, Establishing Pairwise Keys in Distributed Sensor Networks, Proc. of the 10th ACM conference on Computer and communications Security (CCS), pp. 52-61. 2003.

[4] D. Liu, P. Ning, location-Based Pairwise Key Establishments for Static Sensor Networks, SASN' 03 First Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[5]L. Eschenauer and V. D. Gilgor, A Key-Management Scheme for Distributed Sensor Networks, Proc. of the 9th ACM conference on Computer and communications security, pp.41-47, 2002.

[6] H. Chan, A. Perrig, and D. Song, Random Key Predistribution Schemes for Sensor Networks, IEEE Symposium on Security and Privacy, pp.197-213, 2003.

[7] D.Lin and P,Ning, Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, In Proc. of the 10th Annual Network and Distributed System Security Symposium, pp.263-276,2003.

[8] IEEE P1363/D13, Standard Specification for Public Key Cryptography,1999.

[9] 나재훈, 채기준, 정교일, "센서네트워크 보안 연구동향" 전자통신 동향 분석 제20권 제1호(한국 전자통신연구원), p112~122,2005