클러스터 기반 구조에서의 노드 사이의 안전한 통신을 위한 pair-wise키 설정 기법

김성용,박명순
고려대학교
e-mail:bimangrok@korea.ac.kr,myongsp@ilab.korea.ac.kr

A pair-wise key establishment scheme for safety communication between nodes in Cluster-based networks

Sung-Yong Kim, Myong-Soon Park
*Dept of Computer Science, Korea University

요 약

센서 네트워크는 유비쿼터스 컴퓨팅 환경을 실현하기 위한 네트워크로 센싱 및 통신 능력으로 인간이 접근하기 어려운 다양한 곳에 설치되어 감시나 탐지 등을 통하여 데이터를 수집한다. 이러한 환경의 구현을 위하여 센서 네트워크에서 센서 노드가 수집한 데이터는 사용자에게 전달될 때 안전한 통신을 보장하기 위해 센서 노드간 키를 설정하는 것은 보안을 위한 기본적인 요구사항이 되고 있다. 따라서 초소형, 빈번한 데이터 이동, 제한적인 계산 능력 및 저장 능력 그리고 베터리 전력 사용이라는 특성을 갖는 센서 노드에 알맞은 암호화를 위한 키 관리 구조가 요구된다. 따라서 본 논문에서는 센서 네트워크에서의 효율적인 키 설정을 위해 클러스터에 기반한 구조와 다항식을 사용한 pair-wise key설정 방법을 제안 하였다.

1. 서론

센서 네트워크는 많은 수의 센서 노드들로 구성되고 센서를 통한 정보감지 및 감지된 정보를 처리하는 기능을 수행한다. 각 센서 노드들은 제한된 연산 처리 능력만을 가지고 있고 노드들이 애드혹의 형태로 구성되어 통신하게 된다. 이러한 환경으로 인하여 센서 노드 간에 전송되는 데이터가 외부에 쉽게 노출되거나 변조될 위험이 존재한다.[1] 그러므로 안전한 통신을 위하여 센서 노드간 키를 설정 하는 것은 보안을 위한 기본적인 요구사항이 되고 있다. 보다 현실적이고 원활한 유비쿼터스 컴퓨팅 환경을 구현하기 위해서는 센서 네트워크의 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리 할 수 있는 센서 네트워크상에서의 보안 메커니즘 개발이 반드시 함께 연구되어 적용되어야 한다.[2,3]

본 논문에서는 센서 네트워크에서 효율적 키 설정을 위한 클러스터 구조와 다항식을 사용한 pair-wise key설정 방법을 제안하였다. 안전한 통신을 위한 직접 키 설정을 위해 다항식을 사용하되 이를 공유하는 센서의 수를 줄이고자 클러스터 단위로 다항식을 분배하고, 클러스터 헤드에게는 근접 노드와 키를 사전에 분배하는 방식을 조합한 키 분배 구조를 제안한다. 제안한 기법은 pair-wise key의 설정에서 통신 데이터의 도청에 대해서도 클러스터 헤드의 이변수 다항식을 안전하게 하였다.

2장에서는 센서 네트워크에 기존의 키 관리 기법을 설명하고, 3장은 클러스터 기반의 키 분배 기법을 설명하고 안전한 통신을 위해 본 논문에서 제안한 메커니즘을 살펴본다. 4장에서는 본 논문의 결론과 향후 연구 방안에 대하여 기술한다.

2. 센서 네트워크에서 키 관리

2.1 센서 네트워크에서의 키 관리 기법

이 장에서는 센서 네트워크에서의 키 관리 구조로서 센서 노드 간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 연구 분야에 대해 살펴보겠다. 센서 네트워크 환경에서 센서 노드가 위협 지역에 설치된 경우 보안성은 특히 중요한데, 이를 위해 주로 센서 네트워크에 적합한 방식의 키 생성, 분배, 갱신에 관한 프로토콜이 제안되고 있다. 지금까지 제안된 센서 네트워크를 위한 키 관리 기법은 크게 그룹 키, pair-wise 키, 계층적 키 관리 기법으로 구분되며 본 장에서는 이와 같은 키 관리 기법에 대하여 간단히 기술한다.

키 셋업 서버가 그룹에 따라 키를 만들어서 분배하고 그룹 내 센서 노드들은 하나의 키를 이용하여 센서 노드 간 안전한 통신을 지원하는 그룹 키 방식[4,5]은 모든 센서가 하나의 그룹 키만 유지, 관리하면 되므로 키 관리에 있어서 효율적이다. 하지만 그룹 키가 노출 되었을 경우 그룹 전체의 통신이 위험에 처하는 단점도 있다.

각 센서 노드 간 서로 다른 키를 이용하는 pair-wise 키

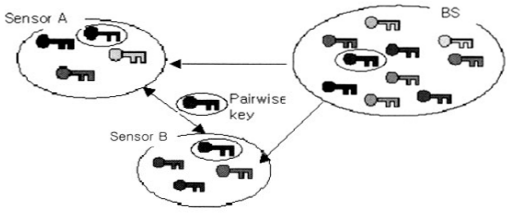
방식은 센서 노드별로 서로 다른 키를 사용하여 각 노드와 통신하므로 키가 노출 되어도 다른 센서 노드는 안전한 통신을 보장한다는 장점이 있다. 하지만 각 센서 노드는 다른 모든 센서 노드와의 키를 저장해야하기 때문에 제한적인 저장 공간을 가지는 센서 노드에게는 제약이 따르는 단점이 있다. 그러므로 효율적인 pair-wise 키 관리 방법에 대한 다양한 연구가 진행되고 있으며 대표적으로 랜덤 키 풀 기반방식[6,7]과 다항식 및 그리드 기반 키 사전 분배 방식[8]등이 있다.

다양한 보안 레벨에 따라 서로 다른 메커니즘을 이용하여 데이터의 암호화를 수행하는 계층적 키 관리 방식[9,10]은 네트워크의 일부가 노출되어도 다른 부분은 안전할 수 있게끔 레벨 별로 보안을 달리 제공하여 효율적인 에너지 소비가 가능한 장점이 있다. 하지만 다양한 보안 레벨을 기준에 따라 정해야하는 단점을 가지고 있다.

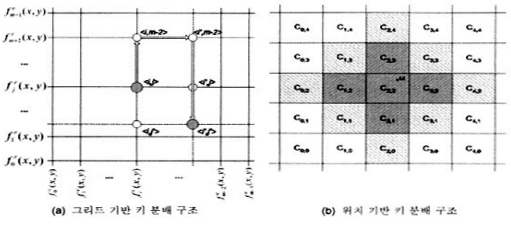
2.2 랜덤 키

L. Eschenauer, V. Gilgor가 센서 네트워크에서의 안전한 통신을 지원하기 위해 센서 노드간 pair-wise key 설정 프로토콜을 제안하였다.[11](그림1)과 같이 베이스 스테이션은 다량의 랜덤 키를 생성하여 이를 키 풀(pool)에 저장하고 키 풀에서 무작위로 임의의 키 셋을 선택하여 각 센서 노드에게 분배한다. 센서 노드 A,B는 부여 받은 키 셋에서 서로 공유하는 키가 없는 두 센서 노드들은 경로키를 생성하여 pair-wise key로 사용한다.

H. Chan, A. Perrig, D.Song은 센서 네트워크에서의 키 설정을 위한 노드 사이에 q개의 키를 공유하는 q-composite 스킴을 제안하였는데 해쉬 함수나 XOR 방식을 통한 새로운 키 생성방식은 기존의 노드 간의 통신을 위한 키 분배 방식 보다 노드가 공격을 당했을 때의 통신 채널의 보안성을 높일 수 있는 장점을 가진다.[7]



(그림1)랜덤 키 분배 구조



(그림2)다항식 기반 키 분배 구조

K = hash(k1 || k2 || ....||kq)

2.3 D. Liu, P. Ning은 센서 노드간 pair-wise key 설정 프로토콜로서 다항식을 이용한 그리드 기반 키 분배 구조를 제안하였다.[8] 기존 스킴과의 두드러지는 차이점은 실제 키 값을 센서 노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배한다는 것이다. 임의의 두 센서 노드가 동일한 t차 다항식을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다.

(그림 2)의 (a)와 같이 동일한 행 또는 열에 위치한 노드들은 서로 간에 pair-wise key를 바로 생성할 수 있다. 동일한 i에 있는 임의의 두 노드는 i행에 부여된 다항식을 동일한 열 j에 위치한 임의의 두 노드는 j열에 부여된 다항식을 공통적으로 갖고 있기 때문이다. 즉, 임의의 두 노드에 대해서 한 노드는 $<c_i, r_i>$에 위치하고, 다른 노드는 $<c_j, r_j>$에 위치할 때, $c_i = c_j$이면, 두 노드는 $f^{c}_{c}(x,y)$를 공통적으로 공유하고, $r_i = r_j$이면, 두 노드는 $f^{r}_{r}(x,y)$를 공유함으로써 각 센서의 ID를 이용하여 공유키를 설정할 수 있다.

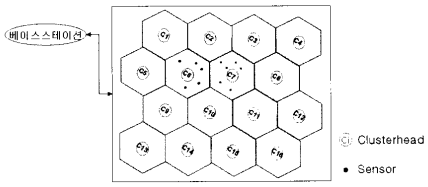
D. Liu, P. Ning이 제안한 또 다른 다항식 기반 키 분배 방식은 위치 기반(location based) pair-wise key 설정 프로토콜이다.[12] 그리드 기반 키 분배 구조에서 사용하였던 방식처럼 다항식을 분배하는데, 그리드 방식이 i행 j열에 있는 센서 노드에게 두개의 다항식을 배분하였다면 여기서 제안하는 방법은 (그림2)의 (b)와 같이 센서 필드를 셀 단위로 나누고 그 셀과 고유한 다항식을 연관시킨다. 그리하여 특정 셀에 위치하고자 하는 센서는 그 위치에 해당하는 다항식과 그 셀 인접 4개 셀에 해당하는 4개의 다항식이 할당되어 이웃 4개 셀에 배치된 센서와 pair-wise key를 생성한다.[13]

3. 클러스터 기반 키 분배 메커니즘

기존의 다항식 기반 키 분배 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 노드간 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 센서들은 공통의 다항식을 사용하고 서로의 ID를 이용하여 pair-wise key를 만들 수 있어 키풀 크기에 상관없이 직접 키를 설정할 수 있다. 또한 클러스터 내의 센서들은 클러스터에 배치되면 그 후에 클러스터 헤드로부터 다항식 부분정보를 분배받기 때문에 기존의 방법보다 사전에 분배하는 정보의 양을 줄일 수 있다. 센서가 다른 클러

스터 영역에 있어서 경로키를 만들어야하는 경우도 클러스터 헤드간의 키는 센서가 배치되기전에 미리 분배되어 있으므로 클러스터 헤드를 통해 안전하게 경로키를 다른 클러스터에 있는 센서노드에게 전달 할 수 있다.

클러스터 헤더의 전송범위는 클러스터 영역을 포함한다고 가정한다. 센서들은 자신의 전송범위 내에 있는 이웃 노드들과 클러스터 헤드로부터 분배받은 다항식 부분 정보를 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. 제안 메커니즘의 구조는 다음 [그림3]과 같다. 또한 베이스 스테이션은 소수 q에 대하여 유한체 Fq 상에서 임의의 t차 이변다항식(bivariate)을 아래와 같이 생성한 후 각 클러스터 헤더에게 임의의 다항식을 선택하여 분배한다.



[그림 3]제안한 센서 네트워크 구조

$fc(x,y) = \Sigma a_{ij}x^iy^j$

단, 이 다항식은 fc(x,y) = fc(y,x)의 성질을 만족해야 한다. 클러스터 헤드 Ci에게 분배된 다항식을 fci(x,y)라고 한다. 임의의 클러스터 영역에 센서들이 임의로 배치되면 클러스터 헤드는 자신의 클러스터에 존재하는 센서들의 존재 여부를 파악한 후 이 센서들에게 다항식에서 생성된 다항식 부분정보를 분배한다. 예를 들어 클러스터 헤드 Ci는 해당하는 클러스터에 위치하는 모든 센서들에게 다항식 fci(x,y)로부터 생성된 다항식 부분정보를 생성하여 분배하는데, 노드는 Ni에게 분배되는 다항식 부분정보는 fci(Ni,y)이다.

$f_c(N_1,y) = \sum a_{i,j} N_1^i y^j \quad f_c(N_2,y) = \sum a_{i,j} N_2^i y^j$

N1은 fc(N1,y)를 갖고 있고, N2는 fci(N2,y)를 갖고 있으므로 두 노드들의 ID를 이용해 다항식을 생성한다. $fc(N1,N2) = \Sigma a_{i,j} N1^iN2^j$, $fci(N2,N1) = \Sigma a_{i,j} N2^iN1^j$ 앞에서 가정한 다항식 fci(x,y)의 성질에 따라 fci(N1,N2) = fci(N2,N1) 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 N1과 N2에 다항식의 부분정보를 전달할 때 이를 도청하면 $fc(N1, y) = \Sigma a_{i,j}N1^iy^j$, $fc(N2, y) = \Sigma a_{i,j}N2^iy^j$ 두 값을 알 수 있다. 이 때 y^j에 관련 있는 계수 ai,j와 x의 차수를 구할 수 있으면 클러스터 헤더가 가지고 있는 이변수 다항식을 알 수 있으며 이를 통해 클러스터 내의 모든 노드의 키쌍을 알 수 있게 된다.

두 다항식 fc(N1, y)와 fc(N2, y)의 y^j 계수를 나누면 $a_{ij}N^i1/a_{ij}N^i2= (N1/N2)^i$ 이 된다. 그런데 fc(x, y) = fc(y, x)이므로 i가 가질 수 있는 값은 다항식 부분정보인 fc(N1,y)의 y의 차수 중에 있다. 따라서 도청한 두 노드의 N1과 N2 값과 y의 차수 k들에 대해 $(N1/N2)^k$ 값을 계산하고도청으로 얻은 $(N1/N2)^i$ 과 비교한다. 만약 같은 값이 나왔다면 k=i 임을 알 수 있는 것이고 이변수 다항식의 y^j 가있는 항이 x^iy^j인 것이다. x^iy^j의 계수는 fc(N1, y)의 y^j 의계수를 $N1^i$으로 나누면 $ai,j = aijN^i/N^i$이다. 따라서 클러스터 헤드가 노드들에게 이변수 다항식의 부분정보로 일변수 다항식을 전달하는 것은 도청에 의한 공격이 가능하다.

이러한 이유로 인하여 fo(x, y) = F0(y)을 만족하는 값을 사용하여보자. 여기서 x를 만족하는 수는 유한체 Fq상의 자연수이므로 1부터 선택해서 계산한다.

그러나 노드 N1에게 분배하는 부분정보F0(N1)F0(y)을도청하면, $F0(N1)F0(N1) = F0(N1)^2 \in Fq$ 이므로 F0(N1)의 계산이 가능하게 된다[14].

$F0(Nj) = \Sigma aiNj^i$ 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 fc(N1, y)을 전달하는 과정에 도청이 가능하므로 fc(N1, y)을 전달하는 대신에 클러스터 헤더로부터 선택한 난수를 포함한 방법을 제안하였다. 클러스터 헤더는 random number r을 선택하여 (r, fo(x, y))을 생성하여 분배한다. $fo(x, y) = \Sigma a_{i,j} x^iy^j$ 은 부분정보의 노출로 공격이 가능함으로 사용하지 않는다. <r, fo(x, y), F(y)>에서 fo(x, y) = F0(y)를 만족하여야하므로 x를 만족하는 수는 유한체 Fq 상의 자연수이므로1부터 선택해서 계산한다.

노드 N1과 N2의 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 N1과 N2의 식별자와 fo(x, y) = F0(y)의 값에 클러스터 헤더에서 선택한 난수 r을 곱한 값은

r* F0(N1)F0(y)과 r* F0(N2)F0(y)이 된다.

N1은F0(N1)F0(y)를 갖고 있고, N2는 F0(N2)F0(y)를 갖고 있으므로 두 노드의 ID를 이용하여 r* F0(N1)F0(N2), r*F0(N2)F0(N1)를 생성할 수 있다. 앞에서 가정한 다항식 fci(x,y)의 성질에 따라 r*F0(N1)F0(N2) = r*F0(N2)F0(N1) 이므로 두 센서 노드는 pairwise key를 공유할 수 있다.

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

4. 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 F0(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] 나재훈, 채기준, 정교일. “센서 네트워크 보안 연구 동향” 전자통신 동향 분석 제20권 제 1호(한국 전자통신 연구원).p112~122,2005

[2] I. F. Akyildiz, W. Su, Y. Sankaraubramaniam and E. Cayirci, "A Survey on Sensor Networks," IEEE Com-munications Magazine, 2002.

[3] D. W. Carman. P. S. Kruus, and B. J. Matt, "Con-straint and approaches for distributed sensor network security." Technical Report#00-010, NAI Labs, 2000

[4] S. Zhu, S. Setia and S. Jajodia, "LEAP:Efficient Security Mechanisms for Large-Scale Distributeed Sensor Networks,"Proc. of the 10th ACM Conference on CCS, pp210-217,2003.

[5] J. D. Richard and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Network," Proc. of ACM Workshop on SASN, pp.83-93, 2003.

[6]L. Eschenauer and V. D. Gligor, “A Key-Management Scheme for Distributed Sensor Network,"Proc.of the 9th ACM Conference on CCS,pp.41-47,2002.

[7] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks, "Proc. of IEEE Symposium on Security and Privacy,pp197-213,2003.

[8] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks,"Proc. of the 10th ACM Conference on CCS,pp52-61,2003.

[9] G. Jolly, M. C. Kuscu, P. Kokate and M. Younis, " A Low Energy Key Management Protocol for Wireless Sensor Networks, "Proc. of the 8th IEEE International Symposium on Computers and Communication, 2003.

[10] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M.B. SrivasTava, "On Communication Security in Wireless Ad-Hoc Sensor Network,"Proc. of WETICE,pp.139-144,2002

[11]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,pp41-47,2002.

[12] D. Liu and P. Ning, "Location-Based Pairwise Keys Establishments for Static Sensor Networks," SASN'03 First ACM Workshop on the Security of Ad Hoc and Sensor Networks,2003.

[13]“The Network Simulator:ns-2," http://www.isi.edu/nsnam/ns

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