클러스터기반 센서네트워크에서 개선된 키 분배 연구

이경효, 박익수, 정석원, 김현곤, 오병균
목포대학교 정보보호전공

A study on modified Cluster-based Key Distribution in Wireless Sensor Networks

Kyoung hyo Lee, Ic-su Park, Seok Won Jung,
Hyun-gon Kim, Byoung-kyun Oh
Department of information Security, Mokpo National University

요 약

센서네트워크는 유비쿼터스 컴퓨팅 기술의 핵심으로 자리 잡아가고 있다. 이러한 센서네트워크는 네트워크가 갖는 특성으로 인하여 일반 네트워크보다 보안에 취약하므로 안전한 통신을 위하여 센서 노드 간 키를 설정하는 것은 보안을 위한 기본적인 요구사항이 되고 있다. 센서네트워크를 클러스터링하여 각 클러스터별로 유일한 다항식을 할당하는 클러스터기반 키 분배에서 클러스터 헤더가 할당하는 다항식 부분정보(polynomial share)인 일변수 다항식 정보는 키 분배시 도청에 의하여 클러스터 헤더의 키인 이변수 다항식을 계산할 수 있었다. 따라서 본 논문에서는 클러스터헤더가 동일한 클러스터내의 센서노드들에게 다항식 부분정보를 배분할 때 다항식을 계산한 상수값을 분배함으로써 클러스터에 도청으로부터 다항식을 알아낼 수 없게 하여 센서노드 간 안전한 통신을 할 수 있게 하였다.

I. 서론

센서네트워크는 미래 유비쿼터스 사회의 광대역 통합망에 연동되는 컴퓨팅 구현을 위한 기반 네트워크로 초경량, 초전력의 많은 센서들로 구성된 무선 네트워크이다. 센서네트워크는 우리 주변의 물리적 현상을 감지하는 센서장치에 네트워크의 개념을 추가하여 사물의 존재여부 및 위치 등의 정보를 네트워크와 연동, 실시간으로 관리 제어하는 개념이다.

센서네트워크는 네트워크가 갖는 제한적인 특성으로 인해 일반 네트워크보다 훨씬 보안에 취약하다. 각 센서노드들은 제한된 연산 처리 능력만을 가지고 있고, 기존의 셀룰라 통신망과는 달리 특정 인프라 구조가 없이 각 센서 노드들이 애드혹의 형태로 구성되어 통신하게 된다. 이러한 환경으로 인해 센서노드 간에 전송되는 데이터가 외부에 쉽게 노출 되거나 변조될 위험이 존재한다. 이러한 센서네트워크의 고유한 특성으로 인해 전력소모를 최소화하는 MAC프로토콜, 기존의 주소기반의 라우팅이 아닌 데이터 질의에 기반한 라우팅 프로토콜, 보안성을 강화하기 위한 키 분배 기법 등과 관련한 연구가 폭넓게 진행되고 있다.[4]

센서네트워크에서의 안전한 통신을 위한 키 관리 기법에는 랜덤키 설정기법인 랜덤키 사전분배와 q-composite 키분배, 다항식기반 키 분배에는 이변수 다항식을 사용하는 Grid기반 키분배(격자기반)구조[4]와 Location기반 키분배(위치기반)구조[3]와 클러스터 기반이 제안되고 있다.[5]

클러스터기반[7]은 헤더에서 각 노드로 이변수 다항식에서 유도된 일변수 다항식을 전달하여 키 설정을 하는데 일변수 다항식으로부터 해더의 이변수 다항식을 얻을 수 있는 약점이 있다. 본 논문에서는 클러스터 기반의 약점을 보완하고자 헤더에서 노드로 일변수 다항식을 전달하는 대신에 이변수 다항식에 유한체의 생성원을 대입하여 얻은 값을 전달하여 클러스터 내 위

장노드가 다항식을 알아낼 수 없게 하여 센서 노드 간 안전한 통신을 할 수 있게 하였다. 본 논문은 다음과 같은 순서로 구성된다. 2장은 키 관리 구조와 관련한 연구를 살펴보고 3장은 클러스터기반의 키 분배 구조와 제안하고자 하는 키 분배 구조를 설명하고 결론과 함께 향후 연구방향을 제시한다.

II. 관련연구

센서네트워크에서 센서 노드 간에 안전한 통신을 위해 키를 생성하고 분배하고 갱신하는 키 관리 기법에 대해 알아본다.

2.1 랜덤키 설정기법

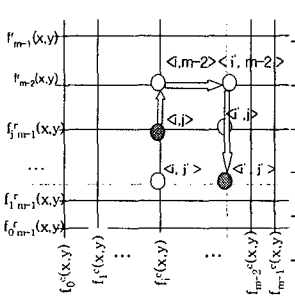
L. Eschenauer, V. Gligor가 제안한 랜덤키 설정기법은 센서 네트워크에서 센서 노드간 키 쌍(pairwise key) 설정 프로토콜로 베이스 스테이션이 다량의 랜덤키를 생성하여 키 풀(pool)에 저장된 키 집합을 무작위로 선택하여 키 링을 생성하여 센서노드에게 부여한다. 센서노드는 부여받은 키 링의 정보를 브로드캐스팅하여 이웃하는 노드들과 공유되는 키를 두 노드간의 키 쌍으로 사용하고 공유키가 없는 두 센서노드들은 경로키를 생성하여 키 쌍으로 사용한다. 이 기법은 센서노드의 개수가 많더라도 수백개 정도의 키로 기존의 키 쌍과 동일한 안전성을 제공하는 장점을 갖는다.[1][6]

H. Chan, A. Perrig, D. Song은 센서네트워크에서 키 설정을 위한 노드사이에 q개의 키를 공유하는 q-composite 스킴을 제안했는데 해쉬함수나 XOR 방식을 통한 새로운 키 생성 방식은 기존의 노드간의 통신을 위한 키 분배방식보다 노드가 공격을 당했을 때의 통신 채널의 보안성을 높일 수 있다는 장점을 가진다.[1]

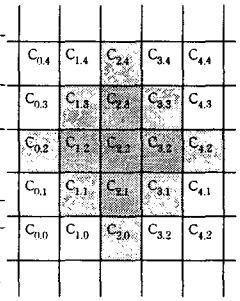
2.2 다항식 기반 키 분배 구조

D. Liu, P. Ning은 이변수 다항식을 이용하여 센서 노드 간 키 쌍을 설정하는 프로토콜인 그리드기반 키 분배구조를 제안하였다. 이 스킴은 실제 키 값을 센서노드들에게 할당하는 것이 아니라 키를 유도할 수 있는 다항식을 생성하여 분배하는 것이다. 임의의 두 센서 노드는 동일한 다항식을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다.

센서노드들이 m*m 격자(grid) 상의 행과 열이 교차하는 지점에 위치된다고 가정하면 셋업 서버는 2m개의 다항식을 생성하여 i열 j 행에 있는 센서노드에게 [그림1]와 같이 두 개의 다항식 $fci(x,y)$와 $fcj(x,y)$을 배분하여 동일한 행 또는 열에 위치한 노드들끼리는 바로 키 쌍을 생성할 수 있도록 한다. 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 있다는 장점을 가지고 있다.[4]



[그림1] Grid 기반 키 사전 분배



[그림2] 위치기반 키분배구조

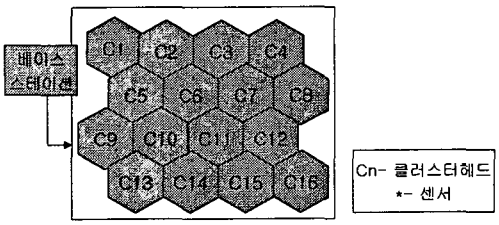
위치기반 키 분배 방식은 그리드 기반 키분배 구조에서 사용하였던 방식처럼 다항식을 분배하되 센서 필드를 셀 단위로 나누고 그 셀과 고유한 다항식을 연관시킨다. 그림[2]과같이 특정 셀에 위치하는 센서는 그 위치에 해당하는 다항식과 인접 4개 셀에 해당하는 4개의 다항식을 할당 받아 이웃 셀에 배치된 센서와 키 쌍을 생성하는 방식이다. 이 방식은 기존의 랜덤키 기반보다 이점이 있으나 다항식을 공유하는 센서의 수가 많아지면 이를 공유하는 센서의 수가 많아지므로 다항식이 노출될 수 있는 위험이 있다.[3]

2.3 클러스터 기반 키 분배 구조

클러스터 기반 키 분배 구조는 키 노출시 네트워크에 끼치는 영향을 최대한 줄이기 위해 클러스터 단위로 하나의 다항식을 공유하게 하여 센서노드들은 그 다항식을 바탕으로 노드

간 키를 공유한다. 센서노드들은 클러스터링 되어있고 각 클러스터에는 클러스터 헤더를 가지며 클러스터 헤더간에는 비밀키를 공유하고 있다.

클러스터 헤더의 전송범위는 클러스터 영역을 포함한다고 가정하고 클러스터 내 센서들의 전송범위는 임의로 변화를 주었다. 센서들은 자신의 전송범위 내에 있는 이웃 노드가 클러tm터 내에 위치할 경우 직접키를 생성하여 키 쌍을 생성할 수 있고 서로 다른 클러스터에 포함될 경우는 경로키를 생성하여 키 쌍으로 사용한다.



[그림3] 클러스터기반 센서네트워크 구조

[그림3]에서와 같이 센서네트워크의 영역을 P=n*n 육각 클러스터로 구획을 나누어 베이스 스테이션은 임의의 P개의 다항식을 생성한다. 그리고 베이스 스테이션은 각 헤더와 그 주의의 헤더들 사이에 비밀키를 분배한다. 예를들어 베이스 스테이션은 C_6의 이웃에 위치하고 있는 6개의 클러스터 헤더 C_2, C_3, C_5, C_7, C_{10}, C_{11}과의 키 Kc_6c_2, Kc_6c_3, Kc_6c_5, Kc_6c_7, Kc_6c_{10}, Kc_6c_{11}을 생성하여 클러스터 노드에게 미리 분배한다. 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.

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

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

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

· 클러스터 C에서 노드로 부분정보 전달

클러스터 C는 노드 N_1에게 다항식 $f_c(x,y)$로부터 생성된 다항식 부분 정보인

$$f_c(N_1,y) = \sum_{i,j} a_{i,j}\, N_1^i y^j$$

를 생성하여 분배한다.

클러스터 C는 노드 N_2에게 다항식 $f_c(x,y)$로부터 생성된 다항식 부분 정보인

$$f_c(N_2,y) = \sum_{i,j} a_{i,j}\, N_2^i y^j$$

를 생성하여 분배한다.

· 노드N_1과 노드N_2 사이의 키 쌍 설정

N1은 $fc(N_1,y)$를 갖고 있고, N_2는 $fci(N_2,y)$를 갖고 있으므로 N_1은 N_2의 ID를 이용하여

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

를 생성하고, N_2는 N_1의 ID를 이용하여

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

를 생성할 수 있다.

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.

Ⅲ. 클러스터기반의 다항식 값 δ를 사용한 키분배

3.1 클러스터 기반 구조에서 부분정보로부터 이변수 다항식을 획득하는 방법

클러스터 기반의 키 분배 구조에서 클러스터 C가 두 개의 노드 N_1과 N_2에 다항식의 부분정보를 전달할 때 이를 도청하면

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

두 값을 알 수 있다. 이 때 y^j에 관련 있는 계수 $a_{i,j}$와 x의 차수를 구할 수 있으면 클러스터 해더가 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 $(\frac{N_1}{N_2})^k$ 값 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^iy^j인 것이다. x^iy^j의 계수는 $f_c(N1, y)$의 y^j의 계수를 N_1^i으로 나누면

$$a_{i,j} = \frac{a_{ij}N^i}{N^i}$$

이다.

따라서 클러스터 해드가 노들들에게 이변수 다항식의 부분정보로 일변수 다항식을 전달하는 것은 도청에 의한 공격이 가능하다.

3.2 제안 클러스터 기반 키 분배 구조

3.1절에서 살펴보았듯이 클러스터 헤더가 노드에게 다항식의 부분정보를 전달할 때 일변수 다항식을 전달하게 되면 도청에 의한 공격이 가능하게 된다.

본 논문에서는 다항식의 부분 정보로 일변수 다항식을 전달하는 대신에 노드의 식별자와 이변수 다항식을 이용하여 상수 값을 전달하여 위와 같은 공격법에 대처를 가능하게 했다.

클러스터 C 안에 노드 N_1과 N_2가 존재한다고 하자. g를 유한체 F_q 상의 생성원이라고 하자. 노드 k=1,2에 대해 N_k에게 전달하는 부분정보를

$$\delta_k = f(g,g)^{Nk} = (\sum_{i,j} a_{i,j}g^ig^j)^{Nk}$$

라고 하자. 이 경우 각 노드에게 전달되는 값이 상수 값이므로 이로부터 이변수 다항식을 찾는 것은 불가능하다.

· 클러스터 C에서 노드N_i로 부분정보 전달

클러스터 헤더 C는

$$\delta_1 = f(g,g)^{N1} = (\sum_{i,j} a_{i,j}g^ig^j)^{N1}$$

를 계산하여 노드 N_1에게 부분정보 δ_1을 전달한다.

마찬가지로 크러스터 헤더 C는

$$\delta_2 = f(g,g)^{N2} = (\sum_{i,j} a_{i,j}g^ig^j)^{N2}$$

을 노드 N_2에게 전달한다.

· 두 노드의 키 공유

두 노드는 상대 노드 식별자를 받아 N_1은

$$\delta_1^{N2} = \{(\sum_{i,j} a_{i,j}g^ig^j)^{N1}\}^{N2}$$

를 계산하고 N_2는

$$\delta_2^{N1} = \{(\sum_{i,j} a_{i,j}g^ig^j)^{N2}\}^{N1}$$

을 계산하면

$$\delta_1^{N2} = \delta_2^{N1}$$

이므로 이 값을 공유키로 할 수있다.

클러스터 헤더가 일변수 다항식을 전달하는 대신에 상수 값 δ를 분배함으로써 이웃노드들과 키 쌍을 생성할 때 도청에 의한 공격으로부터 안전하다.

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 이변수 다항식을 사용한 클러스터 기반의 키 쌍 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 해더가 일변수 다항식을 전달하는 대신에 상수 값 δ를 분배함으로써 이웃 노드들과 키 쌍을 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 방안이 추가로 연구 되어야한다. 또한 제안한 키 설정 메커니즘

을 이용하여 센서노드의 전송범위 내에 위치하나 동일하지 않은 클러스터에 있는 센서노드들과의 경로키를 설정하는 방안에 대한 향후 연구도 필요하다.

[참고문헌]

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

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

[3] 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.

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

[5] 나재훈, 채기준, 정교일, "센서네트워크 보안 연구 동향", 전자통신 동향분석 제20권 제1호 (한국전자통신연구원), p112~122, 2005.

[6] 남상엽, 송병훈, " 무선센서네트워크 활용" 상학당, 2006.나재훈, 채기준, 정교일, "센서네트워크 보안연구 동향", 전자통신 동향분석 제20권 제1호 (한국전자통신연구원), p112~122, 2005.

[7] 천은미, 도인실, 오하영, 박소영, 이주영, 채기준, 이상호, 나재훈, "센서네트워크에서의 안전한 통신을 위한 클러스터 기반 키 분배 구조," 정보처리학회논문지C, 제12권-C권 제4호, p473~480, 2005.