센서 네트워크에서의 위치 정보를 이용한 계층 구조 방식의 키 관리 기법

최성용*, 송주석*
*연세대학교 컴퓨터과학과
e-mail:daniel@emerald.yonsei.ac.kr

A Clustering Structure based Key Management Scheme using Locational Information in Wireless Sensor Networks

Sung-Yong Choi*, Joo-Seok Song*
*Dept of Computer Science, Yonsei University

요 약

센서 네트워크는 수많은 센서 노드들로 구성되는 네트워크이다. 각 센서 노드는 배치된 환경에서 정보를 수집하여 전송하는 동작을 한다. 하지만 정보 전송 시에 공격자에게 노출되어 정보가 공격당할 우려가 있기 때문에 안전한 통신을 위해서 키 관리 기법이 필요하다. 그러나 센서 노드의 특징인 제한적인 자원을 가지고 있다는 점 때문에 공개키 알고리즘을 적용하기 어렵고 또한 다른 키 관리 기법에도 제약 조건이 따른다. 이러한 센서 네트워크의 특징을 고려하여 기존에 연구된 키 관리 기법들을 보완할 효율적이고 안전한 키 관리 기법을 제안하고자 한다.

1. 서론

유비쿼터스 시대가 도래함에 따라 센서 네트워크가 중요한 기술로 부각되고 있다. 센서 네트워크는 특정한 지역에 배치된 수많은 센서 노드들로 이루어져 해당 지역에 대한 여러 가지 정보를 수집하는 무선 네트워크를 의미한다. 센서 네트워크는 사람이 직접 조사하기 어려운 지역을 조사할 수 있다는 장점이 있기 때문에 다음과 같은 여러 분야에서 사용되고 있다. 생태 환경 감시, 생산 기기 효율 감시, 건물 안전 감시, 지진 감시, 다양한 군 시설 등의 분야에서 사용되고 있다.[1]

센서 네트워크는 수많은 센서 노드들로 이루어져 있기 때문에 센서 노드의 특징이 네트워크에 많은 영향을 미친다. 우선 네트워크 형성을 위해 수많은 노드가 필요하기 때문에 노드의 가격이 전체 네트워크의 비용에 영향을 미친다. 따라서 센서 노드는 저장 메모리 공간과 연산 능력, 통신 능력 등 자원에 한계를 가지고 있다. 또한 센서 네트워크는 보통 무작위로 노드들이 배치된다. 무작위로 배치되고 나면 노드들 사이에 ad-hoc 네트워크를 형성한다.

센서 네트워크의 주요 역할은 배치된 환경에서 각종 정보를 수집하여 네트워크를 통해 모으는 것이다. 각 노드가 이웃 노드들과 통신하여 정보를 주고받고 이 정보를 base station으로 전달한다. 그런데 센서 네트워크가 외부 환경에 노출되어 있기 때문에 공격자가 접근하는 것이 가능하고, 원하는 공격을 쉽게 행할 수 있다. 따라서 센서 네트워크의 통신에 대한 보안 기법의 적용이 필요하다. 하지만 센서 네트워크는 다음과 같은 이유 때문에 전통적인 보안 기법의 적용이 힘들다는 문제가 있다.[1]

-센서 노드(디바이스)의 제한적인 자원
-노드에 대한 공격자의 물리적 접근 가능
-물리적인 환경과 사람과의 상호작용

따라서 안전한 통신의 핵심기술인 키 관리 프로토콜이 필요하다.[2]

정보를 전송하여 통신할 때 키를 이용하여 암호화하여 공격자로부터의 공격을 방지한다. 이를 위해서는 각 노드에 대한 효율적인 키 관리 기법이 필요하다. 하지만 여기서의 문제점은 공개키 알고리즘을 사용하기 어렵다는 것이다. 센서 노드가 자원에 한계를 가지기 때문에 계산 능력이 부족하여 공개키 알고리즘을 적용하기 어렵다. 따라서 제안된 대부분의 키 관리 기법들이 대칭키 알고리즘을 사용한다.

이와 같은 논점에 근거해서 다음과 같이 논문을 구성하였다.

2장은 기존에 연구되어진 키 관리 기법들을 소개한다. 3장은 제안하는 키 관리 기법에 대해 설명한다. 4장은 제안하는 기법을 분석하고 5장에서는 연구의 결론을 맺는다.

2. 관련 연구

센서 네트워크의 키 관리 기법에 관하여 수많은 연구가 이루어지고 있다. 대표적인 연구를 분류해보면 KDC-based schemes, Pair-wise schemes, Random key

predistribution schemes 등으로 나눌 수 있다.

A. KDC-based schemes[3]

다른 노드들에 비해 성능이 뛰어나고 믿을 수 있다고 가정하는 KDC(Key Distribution Center)가 모든 노드에 대해 키를 분배하는 방식이다. KDC(주로 base station)가 노드들이 배치되기 전에 모든 노드에게 하나의 마스터키를 분배하고, 노드들이 배치되고 나면 이 마스터키를 이용하여 각 노드는 안전한 통신을 하게 된다.

이 기법의 장점은 각 노드가 하나의 키만 저장하면 되기 때문에 저장 공간을 적게 차지하고, 또 간단하고 효율적이라는 것이다. 하지만 보안상의 문제가 많다. 우선 모든 노드가 동일한 키를 사용하기 때문에 하나의 노드가 공격자에게 공격을 당해 키가 노출된다면 전체 네트워크가 모두 위험해진다는 것이다 Kerberos[5]가 이 방법에 속한다.

B. Pair-wise key schemes[6]

Pair-wise 키는 두 노드만이 유일하게 공유하는 키이다. 통신을 위해서 각 노드는 이웃 노드들 과 pair-wise 키만 가지고 있으면 된다. 하지만 센서 네트워크는 무작위로 배치되는 특징이 있기 때문에 배치되기 전에 어느 노드가 자신의 이웃 노드인지 알 수 없다는 문제가 있다. 따라서 이웃 노드와의 pair-wise 키만 가질 수가 없다.

이를 해결하는 방법이 full pair-wise key 기법[6]이다. 이 기법은 각 노드가 다른 모든 노드에 대한 pair-wise 키를 가지는 방식인데, 가장 확실한 보안성을 제공한다. 왜냐하면 하나의 노드가 공격자에게 공격당하여 노출당한다고 하더라도 해당 노드를 제외한 모든 노드는 안전하기 때문이다. 공격당한 노드만 네트워크에서 제외하면 되는 것이다. 또한 모든 노드에 대한 pair-wise 키를 가지기 때문에 통신 거리 안에 있다면 모든 노드와의 통신이 가능해 진다. 하지만 이 기법을 실질적으로 센서 네트워크에 적용하기 어렵다. 전체 네트워크에 속하는 노드의 개수를 N이라 하면 각 노드가 저장해야하는 키의 개수는 N-1개이다. 하지만 센서 네트워크는 수많은 센서 노드로 구성되어 있기 때문에 N이 매우 크다. 노드의 저장 공간에 한계가 있기 때문에 모든 키를 저장할 수 없다. 네트워크의 크기가 증가할수록 노드의 필요한 저장 공간이 선형적으로 증가한다.

또 다른 pair-wise key 기법에 SPINS[4]가 있다. SPINS에서는 각 노드가 base station과 하나의 키를 공유하면서 네트워크에 배치된다. 네트워크의 동작에 필요한 다른 키들은 그 키에서 추가적으로 생성된다. 따라서 각 노드는 하나의 키를 가지고 base station은 각 노드와의 대칭키를 모두 가지고 있다. 하나의 노드가 공격을 당해 노출된다고 하더라도 그 노드와 base station과의 통신만 위협을 받는다. 하지만 bast station이 모든 노드와의 키를 공유하고 있기 때문에 base station이 유일한 취약점이어서 공격자의 집중적인 공격의 대상이 된다.

C. Random key predistribution schemes[7]

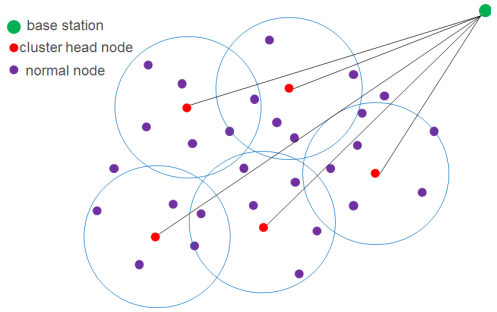
Random key predistribution 기법은 노드들의 평균 degree가 어느 threshold 이상이 되면 랜덤 그래프가 높은 확률로 연결된다는 점을 이용하는 기법이다. 모든 두 이웃 노드가 어떤 확률 p로 pair-wise 키를 가지면 전체 네트워크의 노드들이 키 수립 과정이 끝나고 확률적으로 전체 네트워크가 연결되며 통신이 가능해지는 것이다. 각 노드는 배치 전에 키 집합을 가진다. 이 키 집합은 전체 키 풀에서 무작위로 선택된다. 모든 노드가 배치되고 나서 각 이웃 노드는 서로 공통적으로 가지고 있는 키를 이용하여 안전한 통신을 하게 된다. 키와 노드가 무작위로 배치되기 때문에 이웃 노드 간에 공통키가 존재하지 않을 수도 있다. 이는 각 노드에 배치되는 키의 숫자와 전체 키 풀의 크기를 적절히 조정함으로써 공통키가 있을 확률을 증가시킬 수 있다.

[7]에서는 이웃 노드 간의 공통키가 1개가 아닌 q(>1)개 이상을 가져야 하는 기법을 제안하였다. 1개 이상의 키를 이용하여 통신을 하기 때문에 공격자의 노트 캡처 공격에 대해 조금 더 안전하다. 하지만 q개의 공통키를 p 확률 이상으로 가지기 위해서는 전체 키 풀의 크기가 감소하여야 한다. 이는 공격자의 키 풀에 대한 공격을 더 쉽게 만든다.

이상에서 언급한 것처럼 확률에 근거한 랜덤 키 기법들은 효율적인 키 관리를 제공한다. 하지만 네트워크가 밀집하게 분포하지 않거나 노드의 밀도가 일정하지 않을 경우 네트워크의 연결성을 보장하지 않을 가능성이 있다. 또한 확률적인 연결성을 제공하기 때문에 전체 네트워크가 연결되지 않게 될 수도 있다.

3. 제안하는 기법

앞에서 살펴본 다른 키 관리 기법들의 단점을 보완하고 효율적인 키 관리를 위해 위치 정보를 이용하는 계층 구조의 키 관리 기법을 제안한다.



(그림 1) 네트워크 구조

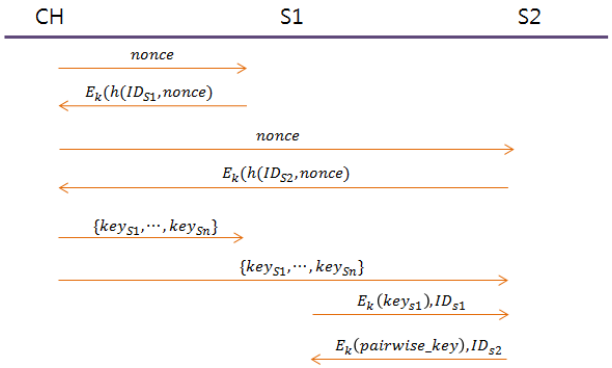
전체적인 네트워크의 구성은 그림 1과 같다. 하나의 base station이 여러 개의 cluster head(CH) 노드를 관리하고 각 CH 노드는 자신의 통신 범위 안에 있는 노드들을 관리한다. CH 노드를 중심으로 계층 구조를 형성하고 이 CH 노드들은 중간 관리자의 역할을 한다. 기존의 연구들에서는 사각이나 육각 모형 등의 계층 구조를 가지는데 반해, 본 논문에서 제안하는 기법은 원 모양의 구조를 가

진다. CH 노드의 통신 거리만큼의 지역을 관리하는 것이 더 현실적이다. CH 노드는 일반 노드에 비해 통신 거리가 더 길다.

키 설정 과정은 다음과 같이 세 단계로 나눌 수 있다.

a. 초기화 단계(Initialization phase) : 각 노드들이 배치되기 전에 base station이 각 CH 노드와 모든 노드에게 동일한 사전 키 K를 분배한다. K가 모두 분배되면 모든 CH 노드와 일반 노드들이 네트워크에 배치된다. 배치된 후, 각 CH 노드는 자신의 통신 거리 안에 위치하는 노드들을 관리하는 역할을 한다. 이 거리 안의 범위를 CH 노드의 지역(zone)이라고 하겠다. 이 지역은 원의 형태로 표현이 되고 통신 거리에 따라 넓이가 정해진다. 이웃하는 지역들은 서로 겹치는 부분이 존재해야 하고 모든 노드는 적어도 하나 이상의 지역에 속해야 한다. 이를 위해 CH 노드의 숫자가 적정량 이상 있어야 하고 효율적인 배치가 이루어져야 한다. 효율적인 배치를 위해서 노드의 위치 정보를 이용한다. 이에 대해서는 뒤의 분석 부분에서 언급하겠다.

b. 키 수립 단계(Key establishment phase) : 네트워크의 배치가 이루어지고 나면 각 CH 노드는 난수를 생성하여 자신의 지역에 broadcasting하게 되고 해당 지역에 위치하는 노드들은 이 난수를 수신한다. 각 노드는 수신한 난수를 자신의 ID를 이용하여 one-way hash시켜 자신의 키를 생성한다. 이 키를 사전에 배치된 사전키 K로 암호화시켜 해당 CH에게 보낸다. CH는 노드들로부터 받은 키들을 모아서 키 리스트로 저장하고 다시 이 값들을 모두 K로 암호화하여 다시 한 번 broadcasting한다. 각 노드들은 해당 지역에 위치하는 노드들의 키로 이루어진 키 리스트를 가진다. 이 키 리스트를 이용해 이웃 노드와의 pair-wise 키를 생성한다. 한 노드(S1)가 자신의 키를 K로 암호화하여 자신의 ID와 함께 이웃 노드(S2)에게 전달한다. S2 노드는 S1 노드의 키와 자신의 키를 해시하여 pair-wise 키를 생성한다. 이를 S1 노드의 ID와 함께 저장한다. 그리고 이 pair-wise 키를 S1 노드의 키로 암호화하여 자신의 ID와 함께 보낸다. S1 노드는 자신의 키로 복호화 하여 pair-wise 키를 알아낸 후 S2 노드의 ID와 함께 저장한다.



(그림 2) 키 수립 프로토콜

c. 통신 단계(Communication phase) : 세 가지 경우로 나누어 생각할 수 있다.

<표 1> Notations

CH	cluster head 노드
S_n	센서 노드
ID_n	노드의 ID
nonce	임의로 생성된 난수
$E_k(M)$	M을 k의 키로 암호화한 값
h(M)	M을 hash한 값
key_{sn}	센서노드 S_n의 고유 키
$\{key_1,\cdots,key_n\}$	키 리스트

-같은 지역에 위치하는 노드 간의 통신 : 노드가 같은 CH의 지역에 위치하는 노드와 통신을 할 때에는 해당 지역에 속한 이웃 노드 간에는 pair-wise 키가 생성되어 있기 때문에 이를 이용해 통신한다.

-이웃 지역에 위치하는 노드 간의 통신 : 노드가 이웃하는 지역(겹치는 노드 부분이 있는 지역)에 위치하는 노드와 통신을 할 때에는 두 지역에 겹쳐서 위치하는 노드를 통해 통신한다. 우선 겹쳐서 위치하는 노드로 메시지를 전달하고 이 노드는 다시 메시지를 목적 노드로 전달한다. 노드가 두 지역에 겹쳐서 존재할 경우에는 두 지역에 속해있는 서로 다른 두 노드와 pair-wise 키를 가지고 있기 때문에 통신이 가능하다.

-이웃하지 않는 지역에 위치하는 노드 간의 통신 : 노드가 이웃하지 않는 지역에 위치하는 노드와 통신을 하기 위해서는 여러 지역을 거쳐서 통신을 해야 한다. 이 문제는 네트워크상의 라우팅이 해결한다.

4. 분석

A. 가정 조건

본 논문이 제안하는 기법이 성립되기 위해서는 몇 가지 가정이 필요하다.

먼저, 네트워크가 구성될 때 노드들이 밀집하게 배치되어야 한다. 밀집하게 배치되지 않으면 네트워크 내 노드의 밀도가 일정하지 않아지고, 각 지역에 속하는 노드의 개수의 차이가 커진다. 이렇게 되면 네트워크의 구성이 매우 비효율적이고 노드 간의 통신에도 문제가 생긴다.

또한, 키 수립 단계가 진행되는 동안 사전 배치된 키 K에 대한 안정성이 보장되어야 한다. 이 단계에서는 키의 교환을 위한 통신이 K에 의해 보안이 되기 때문에 K가 안전하다는 가정이 있어야 한다. 공격자의 공격은 키 수립 단계 이후 가능하고 그 전까지는 네트워크 초기의 짧은 시간으로 안전하다고 가정한다. 사전 키 K는 이 과정에서만 사용된다.

B. 개선 사항

본 논문이 제안하는 기법이 기존의 기법들에 비해 향상되는 점들은 다음과 같다.

여러 개의 CH 노드를 사용함으로써 base station의 역할을 나눠서 대신하도록 한다. 이는 base station으로 집중되는 공격을 여러 CH 노드로 분산시켜 base station이 공격당할 위험을 줄인다. 하나의 base station이 집중 공격

받는 single point of failure 취약점을 방지할 수 있다. 또 네트워크를 나눠서 관리하기 때문에 하나의 CH 노드가 공격자에게 공격당해 노출되더라도 해당 지역을 제외한 다른 지역은 안전할 수 있다. 하지만 CH 노드의 개수에 따라 전체 네트워크의 비용이 증가한다.

Full pair-wise key scheme이 가지고 있는 저장 공간 한계의 문제도 해결할 수 있다. 각 노드가 모든 노드에 대한 pair-wise 키를 가지는 것이 아니라 자신이 위치하는 지역 내에 있는 노드들에 대한 pair-wise 키만 가지면 되기 때문이다. 전체 노드의 개수를 N, CH 노드의 개수를 S라고 한다면, 평균적으로 각 노드가 N/S의 키를 가진다. 따라서 S가 커질수록 저장하는 키의 개수가 줄어들 것이다.

Random-Key Predistribution 기법의 단점인 연결성을 100% 보장하지 못한다는 점을 보완할 수 있다. 각 노드는 이웃 노드와의 pair-wise 키를 모두 가지고 있기 때문에 모든 이웃 노드와 통신이 가능하다. CH 노드의 배치에 따라 각 지역이 이웃 지역과 겹치는 노드가 존재한다면, 전체 네트워크의 연결성을 보장할 수 있다.

C. 고려 사항

키 관리가 CH 노드가 관리하는 지역 단위로 이루어지기 때문에 CH 노드의 역할이 중요하다. 가장 중요한 점은 CH 노드의 적절한 배치이다. 네트워크의 연결성과 비용적인 효율성을 고려해야 한다. 우선 각 노드가 저장할 수 있는 저장 용량을 고려하여 담당하는 지역의 노드의 개수가 알맞도록 배치되어야 한다. 이를 위해 네트워크의 밀집한 배치가 필요하다. 각 센서 노드가 랜덤하게 배치 될수록 균형적으로 위치할 것이다. 네트워크의 연결성을 보장하기 위해서는 이웃 지역과 공유하는 노드(겹쳐서 위치하는 노드)가 존재해야 하고 각 노드는 하나 이상의 지역에 존재하도록 배치되어야 한다. CH 노드의 개수를 증가시키면 위의 두 가지 조건을 만족시킬 수 있다. 하지만 CH 노드는 일반 노드에 비해 성능이 뛰어난 노드이기 때문에 가격이 더 비싸다. CH 노드의 개수가 증가할수록 전체 네트워크의 비용이 증가한다. 따라서 비용을 고려해 배치될 CH 노드의 개수를 정해야 할 것이다. CH 노드 배치를 위한 알고리즘은 배치 전에 예상되는 위치(expected location[8])를 이용한다. 각 CH 노드의 배치가 예상되는 위치를 알면 그 위치에 맞게 배치 위치를 정하고 오차에 따라서 조절한다. 예상되는 위치와 실제 위치는 오차(deployment error)가 존재한다. 이 오차는 확률밀도함수(probability density function)에 의해 결정된다.[8]

CH 노드의 성능 또한 고려되어야 한다. CH 노드의 디바이스로 어느 정도의 통신 거리를 가지는 디바이스를 선택할 것인지를 정해야 한다. 통신 거리에 따라서 trade-off가 존재한다. 통신 거리가 증가하게 되면 CH 노드가 관리하는 지역의 넓이가 증가한다. 노드들이 밀집하게 배치되어 있기 때문에 평균적으로 지역의 넓이에 비례하여 포함되는 노드의 개수가 증가한다. 노드의 개수가 증가하면 각 노드가 저장해야 하는 키의 개수도 증가한다. 따라서 통신 거리가 어느 정도 이상으로 증가하게 되면 각 노드의 저장 공간의 한계 때문에 필요한 키를 모두 저장할 수 없게 된다. 반대로 통신 거리가 감소하게 되면 CH 노드가 관리하는 지역의 넓이가 감소한다. 모든 노드가 적어도 하나의 지역에 속하기 위해서는 모든 노드를 포함할 수 있도록 CH 노드가 배치되어야 하는데 하나의 지역의 넓이가 감소하면 전체 네트워크를 위해 필요한 CH 노드의 개수는 증가한다. 위에서 살펴본 바와 같이 CH 노드의 개수의 증가는 전체 네트워크의 비용의 증가로 이어진다.

5 결론

본 논문에서 제시하고 있는 기법은 기존의 기법들에 비해 보안적인 측면에서 향상되는 것을 알 수 있다. 하지만 CH 노드에 의한 비용 발생으로 전체 네트워크의 비용이 증가하는 문제점이 있다. 앞으로 효율적인 CH 노드의 배치 방법에 대한 연구를 계속 진행하여 이런 문제점을 보완해 나갈 계획이다.

참고문헌

[1] A.Perrig, J,Stankovic, D.Wanger “Security in Wireless Sensor Networks” Communications of the ACM - Wireless sensor networks, Volume 47 Issue 6, 2004.

[2] Junqi Zhang , VijayVaradharajan “Wirelesssensor network key management survey and taxonomy” Journal of Network and Computer Applications, 2010.

[3] Y.Cheng, D.P.Agrawal “Efficient Pairwise Key Establishment and Management in Static Wireless Sensor Networks” Mobile Adhoc and Sensor Systems Conference, 2005.

[4] A.Perrig, R.Szewezyk, V.Wen, D.Culler, J.D.Tygar “SPINS:Security protocols for sensor networks” Seventh Annual international Conference on Mobile Computing and Networks(MobiCom 2001), p189-199, July 2001.

[5] J. Steiner. C. Neuman, and J. Schiller “Kerberos: An authentication service for open network systems” In Usenir Winrer Conference. pages 191-202. January 1988.

[6] W.Du, J.Deng, S,Han, P.K.Varshney, J.Katz, A.Khalli “A pairwise key predistribution scheme for wireless sensor networks” ACM Transactions on Information and System Security (TISSEC), Volume 8 Issue 2, May 2005.

[7] H. Chan, A. Perrig, and D. Song “Random Key Predistribution Schemes for Sensor Networks” Proc. IEEE Symp. Security and Privacy, May 2003.

[8] F.Anjum “Location dependent key management in sensor networks without using deployment knowledge” Wireless Networks, Volume 16, Number 6, 1587-1600 October 2010.