실시간 유비쿼터스 센서 네트워크에서 비밀분산기법에 기반한 효율적인 키관리에 관한 연구

손 상 철° 윤 미 연 이 광 겸 신 용 태
숭 실 대 학 교 일 반 대 학 원 컴 퓨 터 학 과
{yelhorse°, myyoon, goodwin77, shin}@cherry.ssu.ac.kr

Study on Efficient Key Management of Secret Sharing Technique in Real Time Wireless Sensor Network

Sangchul Son° Miyoun Yoon Kwangkyum Lee Yongtae Shin

Dept. of Computing, Soongsil University

요 약

센서 네트워크 기술은 정보를 수집하고 전송함에 있어서 사람의 개입 없이 모든 동작이 이루어진다. 이러한 센서 네트워크 환경에서는 센서 노드들의 에너지와 컴퓨팅 능력, 통신능력이 극히 제한적이기 때문에 전통적인 보안 기술을 적용하는 것은 문제점이 있다. 따라서 본 논문에서는 센서 네트워크의 물리적인 제한적 환경과 컴퓨팅 능력을 고려하여 기존의 비밀분산 기법에 기반을 둔 보안 메커니즘으로 실시간 환경에서 각 센서 노드들의 에너지 효율적인 계층적 키관리 기법에 대해 제안한다.

1. 서론

센서 네트워크는 유비쿼터스(ubiquitous) 컴퓨팅을 위한 기반이 되는 네트워크로 초경량, 저전력의 많은 센서 노드들이 어떠한 자료 수집을 위해 넓은 지역이나 제한된 지역에 설치되어 무선으로 통신을 주고받는 네트워크이다. 센서 네트워크는 애드 혹 네트워크와 유사하지만 여러 가지 차이점이 존재한다. 예를 들어 애드 혹 네트워크는 네트워크가 형성된 후 자유로이 네트워크 내에 가입·탈퇴를 할 수 있고 그러한 이유로 항상 이동성을 고려해야 하는 특성을 가지고 있다. 하지만 센서 네트워크는 각 센서 노드가 임의대로 네트워크 내에 가입·탈퇴가 불가능하고 센서 자체의 이동성은 지원하지만 어플리케이션에는 의존하지 않는다. 또한 센서 노드는 애드 혹 노드보다 배터리의 제약과 프로세싱 능력에 많은 제약을 받으며 애드 혹 네트워크에는 없는 싱크 노드를 가지고 있다. 따라서 각 노드의 인증을 받기 위한 절차가 애드 혹 네트워크와는 다른 방식을 갖는다. 이와 함께 애드 혹 네트워크는 각각의 노드가 정보 수집의 주체가 될 수도 있고 매개체가 될 수도 있으나 센서 네트워크는 서로 분산된 센서 노드의 부분 정보들이 합쳐져 하나의 완성된 정보를 얻게 된다. 특히 실시간 센서 네트워크에서는 인증되지 않은 센서가 침입하여 위조된 데이터를 전달하거나 라우팅 과정에서 정보가 유출되는 것은 방지되어야 한다.

따라서 각 센서 노드들 간에 신뢰적인 통신을 하기 위한 인증 과정이 필요하고 이런 인증 과정에서 쓰이는 키관리 기법이 필요하다. 본 논문의 2장에서는 기존에 소개되고 있는 센서 네트워크의 보안 메커니즘과 비밀분산기법 등을 분석하고 3장에서는 본 논문에서 제안하는 키관리 기법을 소개하며 마지막으로 4장에서 결론과 향후 연구과제에 대해 제시하고 설명한다.

2. 관련연구

[1]은 센서 네트워크에서 센서 노드의 대표 노드를 선출하는 메커니즘을 제안하였다. 이 메커니즘은 물리적 거리와는 상관없이 하나의 센서가 감지할 수 있는 다른 센서의 거리를 1홉으로 정의하며 선출된 대표 노드는 하위 노드들의 정보 집합을 모두 대변할 수 있다.

[2]는 대칭키 알고리즘을 이용한 비밀분산기법을 제안하고 있다. 비밀분산기법은 하나의 비밀키를 n개의 다수의 키로 나누어 각 노드에게 전송하게 되고 t개의 키가 조합되면 원래의 키 값을 복원할 수 있는 알고리즘이다. 이 알고리즘을 사용하면 악의적인 목적을 가진 사용자가 침입하였을 경우 $(t-1)$개의 키를 찾고 조합하였을 때 비밀키가 유출되는 일을 방지할 수 있다.

[3]은 경량의 TESLA인 μ-TESLA 기법을 적용한 센서 네트워크 보안 방안을 제시하였다. 이 방법은 시간당 키 체인으로 이루어지며 항상 시간 동기화가 이루어져야 한다. 키분배는 송신자가 바뀔 때 마다 전송되며 단방향 함수로 키가 생성

된다.

[1]과 [3]의 경우 오프라인의 센서 네트워크 상에서는 효율적인 키관리 기법을 제시하고 있으나 실시간 환경에서는 키갱신이 주기적으로 이루어지지 않으므로 실시간 데이터 흐름의 인증이 이루어지기 어렵다.

따라서 본 논문에서는 실시간 센서 네트워크의 계층적인 인증키관리 기법에 대해서 제안한다.

3. 센서 노드의 인증기법

센서 노드는 센서 노드의 특성상 공개키 암호화 알고리즘을 위한 다양한 정보 및 성능을 수행하기 어렵다. 또한 Gennaro & Rohatgi에 의해 제시되는 대칭키 방식은 패킷 당 필요인증정보가 1Kbyte로서 센서 네트워크에 적용하기에는 부적절하다[4]. 따라서 기존의 비밀분산기법[2]을 이용한 효율적인 계층적 키관리 방법에 대해 제시하도록 한다. 본 논문에서 제안하는 키관리 기법은 센서 노드와 싱크 노드의 통신에 있어서 어떠한 배치상황에서도 적용될 수 있으며, 특히 실시간으로 자료가 이동되는 센서 네트워크 환경에서 효율적인 키관리 기법을 제안한다.

3.1 신뢰적인 통신을 위한 키관리 기법

센서 네트워크가 구성되고 자료 요청이 이루어지면, 먼저 싱크 노드에서 각 센서 노드들에게 최초의 인증을 위한 인증키 값을 브로드캐스팅 한다. 그 다음으로 대표 노드를 선출하기 위한 방안으로 [1]에서 제안한 알고리즘을 이용한다. 대표 노드는 각 센서 노드의 모든 센서를 감지할 수 있는 고유집합 노드로써 이 노드들을 대표 노드라 명명한다. 싱크 노드에서 센서 노드들의 대표 노드들이 선출되면 싱크 노드는 Mac 함수를 이용하여 인증키를 생성한 후 얻어진 공계수 값 a_i를 비밀분산기법을 적용하여 각 대표 노드에게 전달하고 대표 노드들끼리의 인증을 위한 인증키 값을 전달한다. 그림1은 싱크 노드와 대표 노드의 인증키 교환방법을 설명한다.

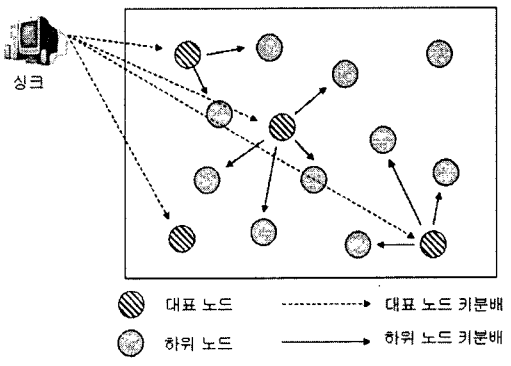

그림 1. 각 노드의 인증키 교환과정

공계수 값과 대표 노드 인증키 값을 전송 받은 대표 노드는 이 공계수 값 a_i를 처음 싱크 노드로부터 받은 인증키 값으로 단방향 암호화를 하여 나온 값을 버퍼에 저장한다. 그 후 원래의 공계수 값 a_i를 하위 노드에게 전달하고 a_i값을 받은 하위노드는 자신이 수집한 정보와 함께 대표 노드로부터 받은 a_i값을 처음 싱크에게 받은 인증키 값으로 똑같이 단방향 암호화를 한 후 그 값을 대표 노드에게 보낸다. 이렇게 하여 하위 노드에게 정보를 전달 받은 대표 노드는 자신의 버퍼에 있는 암호화된 키 값과 하위 노드에게 받은 암호화된 키 값을 비교하여 하위 노드의 인증을 할 수 있게 된다. 이 때, 대표 노드와 하위 노드의 한계 범위는 1홉으로 한정하고 여러 대표 노드를 갖는 하위 노드는 대표 노드들의 게이트웨이적인 역할을 담당하며 먼저 수신된 대표 노드에게 소속된다.

이렇게 단계적인 절차가 진행되는 동안 처음 싱크 노드에게 받은 대표 노드 인증키 값으로 대표 노드들 간의 신뢰적인 통신이 이루어지며 비밀분산기법으로 나누어진 a_i값으로 대표 노드들이 수집한 자료의 인증이 이루어질 수 있다. 또한 대표 노드와 하위 노드 간에는 단방향 암호 알고리즘을 이용하여 신뢰성이 제공된다. 그림2는 각 노드에서 이루어지는 인증키 관리 방법에 대해 설명한다.

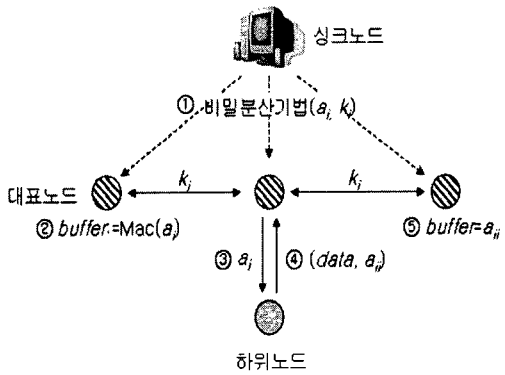

그림 2. 각 노드의 키관련 메커니즘

싱크 노드와 대표 노드 사이에서는 비밀분산기법 방식을 사용하기 때문에 모든 대표 노드들의 인증 값 a_i들을 사용하지 않고, t개의 a_i들만 사용하여 키 값을 도출해 낼 수 있다. 이것은 귀납적으로 $t-1$개의 a_i값들이 모였을 경우에는 대표 노드의 인증키 값을 얻어낼 수 없다는 뜻이 된다. 따라서 그 만큼 신뢰성 있는 통신이 가능하게 되고 각 노드의 임의적인 고장을 허용할 수 있는 효과와 신뢰성 있는 통신을 제공하여주는 효과를 얻을 수 있다. 또한 한 개의 센서 노드는 일반적으로 저용량의 메모리와 낮은 프로세싱 능력을 갖고 있기 때문에 단방향 암호 알고리즘을 한번만 사용하여 신뢰적인 통신을 제공할 수 있다. 그림3은 대표 노드에서 이루어지는 키관리 기법에 관한 알고리즘이고 표1은 알고리즘에 쓰인 함수를 설명한다.

입력 : 싱크에서 보내진 인증키와 해쉬키
출력 : 싱크에서 보내진 해쉬키

Procedure *leaf node authentication*
If receive k_i, a_i from *sink node* **then**
Begin
buffer:= **Mac**(a_i)
Send a_i **to** *leaf node*
  If receive *data*, a_{ii} from *leaf node* **then**
  Begin
    If *buffer* = a_{ii}
    Begin
      Authenticate *leaf node*
      Send *data* **to** *next representation node*
    Else
    Listen *data*, a_{ii}
    End
  End
End
Else
Listen k_i, a_i

그림 3. 대표 노드의 키분배 알고리즘

표 1. 알고리즘에 사용된 함수와 변수의 기능

정의된 함수 및 변수	설명
k_i	단방향 암호화된 대표 노드 인증키 값
a_i	비밀분산기법을 이용한 대표 노드 인증키
receive	메시지나 데이터 수신하는 함수
Mac	단방향 암호화 함수
a_{ii}	하위 노드에서 전달된 단방향 암호화된 하위 노드 인증키 값
buffer	센서 노드안의 임시저장 공간
Authenticate	노드를 인증하는 함수
Listen	데이터나 변수를 기다리는 함수
sink node	센서 노드의 데이터와 인증을 담당하는 총괄 노드
next represe-ntation node	이웃한 센서 노드의 부분집합을 대표하는 노드
leaf node	대표 노드에 속한 하위 노드
Send	데이터가 키 값을 전송하는 함수
data	센서 노드가 수집한 정보

3.2 키갱신 주기

실시간 센서 네트워크에서는 싱크 노드로부터 받은 인증 키 값이 주기적으로 갱신 되어야 한다. 이는 센서 네트워크의 특성상 각 센서 노드들의 짧은 수명주기와 이동성, 낮은 프로세싱 능력, 인증되어지지 않은 노드의 침입과 실시간으로 자료를 주고받는 환경에서 신뢰적인 통신을 하기 위해 꼭 필요한 요소이다.

키갱신 주기의 요소로는 첫 번째, 대표 노드의 변화이다. 대표 노드는 싱크로부터 비밀분산기법을 이용한 키분배를 받는데 이런 대표 노드가 어떠한 이유로 제 기능을 수행하지 못 할 경우 센서 노드들은 다시 새로운 대표 노드를 선출한다. 그 후 싱크 노드는 기존의 인증키 값을 해쉬 알고리즘을 이용해 새로운 인증키 값을 생성한 후 그 값을 다시 비밀분산기법을 사용하여 새로 선출된 대표 노드에게 전송한다. 이때 새로 선출된 대표 노드는 기존의 인증키 값을 해쉬한 후 싱크 노드에게 전송해 싱크로부터 인증을 받게 된다. 이렇게 인증 받은 대표 노드는 밑단의 하위 노드에게 제안된 메커니즘을 이용하여 새로운 키 값을 전송한다.

두 번째, 센서 노드의 변화와 상관없이 주기적으로 키 값을 갱신해주어야 한다. 만약 최초의 인증이 이루어진 후 키 값의 갱신이 이루어지지 않으면 허가 없이 침입한 악의적인 노드가 라우팅 과정이나 정보 수집 과정에서 허용되지 않은 정보를 유출할 수 있게 된다. 더불어 실시간 환경에서의 키갱신은 데이터의 흐름을 인증하기 위해 꼭 필요하다. 따라서 키갱신 주기는 전체 데이터가 수집되는 시간을 대표 노드의 수 값으로 나눈 시간만큼의 주기로 키갱신을 한다. 위와 같은 주기로 키갱신이 이루어지게 되면 전체 센서 네트워크의 범위가 대표 노드 집단을 주기로 변화되므로 최소한의 인증키 값을 얻기 위한 라우팅 과정보다 인증키 값의 갱신이 먼저 일어나게 된다. 따라서 악의적인 노드가 침입하여 한 집단의 대표 노드 인증키 값을 알게 되더라도 다음 키를 얻기 전에 키가 갱신되어 이미 얻은 인증키 값의 효용이 없어지게 된다.

4. 결론 및 향후 연구과제

본 논문은 실시간 센서 네트워크에 적용될 수 있는 키관리 기법에 대해 제안하였다. 각 노드의 인증을 위해 두 계층으로 나눈후 싱크 노드가 각 센서 노드를 인증한다. 이와 함께 대표 노드를 선출하고 비밀분산기법을 사용하여 비밀키를 분산하며 각각의 하위 노드와는 단방향 암호화 알고리즘을 사용하여 인증을 제공한다. 이와 같은 메커니즘을 이용하여 낮은 프로세싱과 저전력을 요구하는 센서 네트워크에서의 인증키 관련 키관리 기법을 충족시켜줄 수 있다. 향후에는 하위 노드들끼리의 인증 방안과 갱신 주기의 다양화, 메시지 오버헤드 등의 분석이 이루어질 예정이다.

참고문헌

[1] 윤미연, 이광겸, 손상철, 신용태: 센서 네트워크에서 고장을 허용하는 견고한 인증기법, 한국 통신 학회, 2004.

[2] Adi Shamir: How to Share a Secret, Communications of the ACM, November 1979.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar: Spins: Security protocols for sensor networks. Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom). Rome. Italy(2001) 189--199.

[4] Rosario Fennaro & Pankaj Rohatgi: How to sign Digital Streams. In CRYPTO'97, pages 180--197, 1997.