(t, n) 임계치 기법을 이용한 센서네트워크에서의 공개키 인증

Public Key Authentication using (t, n) Threshold Scheme for WSN

김 준 엽* 김 완 주* 이 수 진*
Kim, Jun-Yop Kim, Wan-Ju Lee, Soo-Jin

ABSTRACT

Earlier researches on Sensor Networks preferred symmetric key-based authentication schemes in consideration of limitations in network resources. However, recent advancements in cryptographic algorithms and sensor-node manufacturing techniques have opened suggestion to public key-based solutions such as Merkle tree-based schemes. These previous schemes, however, must perform the authentication process one-by-one in hierarchical manner and thus are not fit to be used as primary authentication methods in sensor networks which require mass of multiple authentications at any given time. This paper proposes a new concept of public key-based authentication that can be effectively applied to sensor networks. This scheme is based on exponential distributed data concept, a derivative from Shamir's (t, n) threshold scheme, in which the authentication of neighbouring nodes are done simultaneously while minimising resources of sensor nodes and providing network scalability. The performance advantages of this scheme on memory usage, communication overload and scalability compared to Merkle tree-based authentication are clearly demonstrated using performance analysis.

주요기술용어(주제어) : Wireless Sensor Notwork(무선 센서 네트워크), Public Key Authentication(공개키 인증), Threshold Scheme(임계치 기법), Key Management Protocol(키관리 프로토콜)

1. 머리말

센서네트워크(Wireless Sensor Network, 이하 WSN)는 산불 같은 환경감시, 군사목적의 탐지 · 추적 등을 위하여 특정 지역에 배치되는 대량의 초경량 · 저전력 센서노드로 구성된 네트워크이다[1]. WSN의 각 센서노드는 외부 기반시설의 도움 없이 자체적으로 이웃노드와 무선네트워크를 구축하고 데이터를 주고받게 된다. 그러나 WSN은 기본적인 특성이 기존의 네트워크와 많이 달라서, 안전성 측면에서 기존 네트워크와 다른 상황이 발생한다. 특히 센서 노드의 제한적인 저장 · 통신 · 계산 능력, 무선 매체에 대한 다양한 공격 가능성, 신뢰관계 형성 및 상호 인증의 어려움 등으로 WSN에서는 기존의 보안대책을 그대

† 2008년 7월 2일 접수~2008년 8월 22일 게재승인
* 국방대학교(Korea National Defense University)
교신저자 이메일 : sizipus1@gmail.com

로 적용할 수 없어 WSN의 특성에 맞는 새로운 보안 대책들이 연구되고 있다.

초기의 WSN에서는 대칭키 암호를 이용한 보안대책이 주로 연구되었지만, 최근에는 키 관리가 용이하고 위조와 재연공격 등에 강한 공개키 암호에 대한 연구가 활발히 진행되고 있다. 특히 공개키 암호 중에 타원곡선암호는 WSN에서 실용화가 가능할 만큼 알고리즘의 성능이 개선되었고 센서 제조기술도 발달하였다.

일반적으로 공개키를 인증하기 위해서는 인증기관이 필요하지만, 자원이 제약된 WSN에서 특정 센서에 인증기관의 기능을 구현하는 것은 비현실적인 일이다. 최근에는 Merkle 트리를 이용한 공개키 인증방식이 제안되었지만 메모리 사용량과 통신 오버로드가 네트워크의 크기(N)에 따라 $O(\log N)$으로 증가하고 네트워크의 확장성도 제한되는 단점이 있다.

현재 비밀분산기법 중의 일종인 (t,n) 임계치 기법은 비밀에서 n개의 분산정보를 생성하여 특정 그룹에 속한 n명의 참가자에게 저장한 후, 그 중 $t(<n)$개의 분산정보만으로 원래의 비밀을 복원하는데 주로 사용되어 왔다. 그러나 본 논문에서는 기존의 (t,n) 임계치 기법에 변형된 분산정보의 일종인 지수 분산정보 개념을 새로이 적용하여 WSN에 적합한 공개키 인증방식을 제안한다.

본 논문의 구성은 다음과 같다. II장에서는 기존에 제안된 WSN를 위한 공개키 인증방식과 비밀분산기법에 관해 살펴보고, III장에서는 (t,n) 임계치 기법을 활용한 공개키 인증방법을 제안하며, IV장에서는 제안된 기법을 WSN에 적용하고, V장에서는 제안된 기법의 성능을 분석하며, VI장에서 결론을 맺는다.

2. 관련연구

가. WSN에서 공개키 관리기법

WSN에서는 유선망에서와 같이 인증서를 발급, 분배, 관리하는 인증기관의 문제를 해결하기 위해 중앙 분배방식을 이용할 수 없는 환경이다. 그래서 기반체계가 없는 WSN에서는 일대일 키 관리 문제를 공개키 기반 암호시스템의 분산기법을 이용하여 해결하고자 하는 연구들이 주로 제안되고 있다. 분산방식은 다시 완전분산기법과 분산서브그룹기법으로 구분된다. 하지만 실제적으로 완전분산기법은 수많은 노드로 구성된 WSN에서는 적용하기에 문제점이 있어 분산서브그룹기법을 위주로 주요연구가 진행되고 있다.

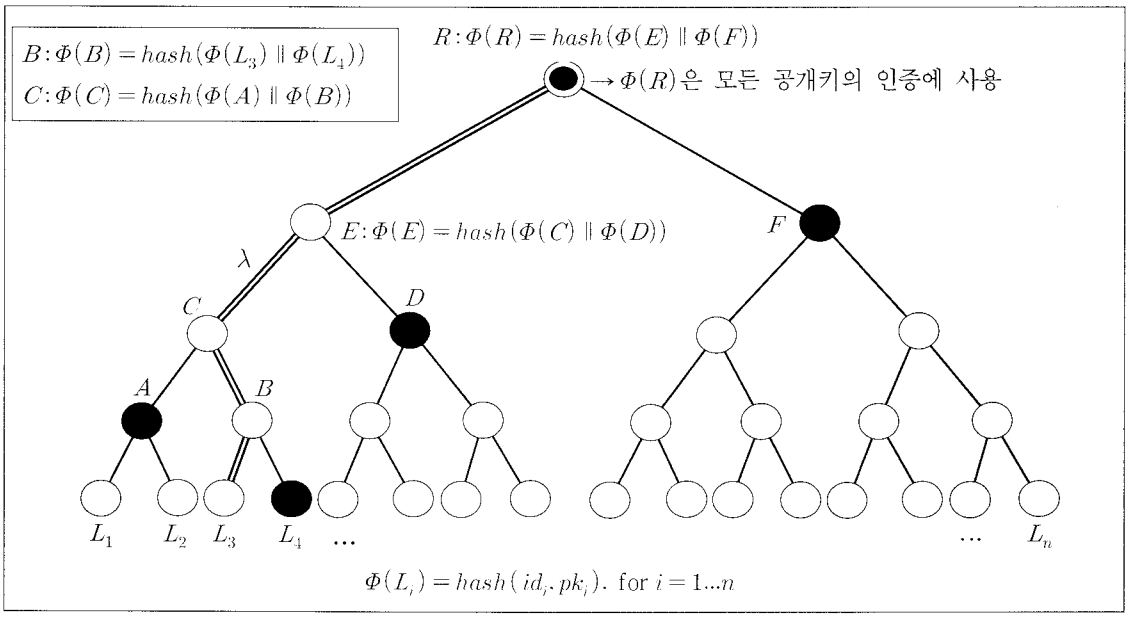
인증기관을 여러 개의 다른 노드들에게로 분산하는 기법[2,3]은 (k,n)임계치 기법을 사용한다. 인증기관의 부분 비밀키를 n개의 노드가 나누어 가지고, 각 노드는 자신이 가지고 있는 비밀키를 이용하여 서명한 부분 인증서를 만들 수 있게 된다. 그리고 이중에서 k개 이상의 노드들이 모인다면, 완전하고 적법한 인증서를 만드는 인증기관의 기능을 수행할 수 있게 된다.

이 기법은 중앙 분배 방식의 인증기관의 기능을 분산 시켰으므로 WSN 환경에 적합하지만, 이 기법의 변수인 k와 n의 값이 인증기관에서는 기능의 가용성, 전체 시스템의 안전성, 그리고 비용에 큰 영향을 미치므로, 여러 가지 상황들을 고려해서 변수의 값들을 선택하는 것이 중요하다. 그리고 부분 비밀키를 가지고 있는 노드들이 서로 원활하게 통신할 수 있도록 노드들의 위치도 신중하게 고려되어야 한다.

인증기관 없이 노드들이 스스로 인증서의 문제를 해결하는 방법들도 연구되고 있다. 대표적인 방법으로는 유선망의 PGP(Pretty Good Privacy)와 같이 각 노드들이 스스로 인증서를 발급하고 저장하여 자신이 한 노드를 인증하면 그 노드가 인증하는 다른 노드까지 인증서 사슬을 통해 서로를 확인할 수 있는 방법[4]과 주변의 노드들로만 통신할 수 있는 채널로 미리 주고받은 데이터를 이용하여 서로의 공개키에 대한 해쉬 값을 주고받는 과정을 통해 인증하는 방법[5]이 있다. 첫 번째 방법은 발급한 인증서의 수가 많지 않은 초기단계에서 인증이 제대로 이루어지지 않고, 많은 인증서를 갖고 있기 때문에 메모리 한계가 있다. 두 번째 방법은 주변의 노드들과의 완전한 통신채널 필요성으로 국지적 환경에서만 적용이 가능하다는 문제가 있다.

나. Merkle 트리를 이용한 공개키 인증

Du 등은 Merkle의 인증 트리 기법[6]을 이용하여



[그림 1] Merkle 트리를 이용한 공개키 인증

해쉬 함수만으로 효율적인 공개키 인증이 가능한 기법을 제안하였다[7]. Merkle 트리는 할당(assignment) Φ를 통해서 내부 노드 및 루트노드로 구성된 완전이진트리 구조이다. 그림 1에서 보여주는 바와 같이 Merkle 트리를 구축하기 위해 N개의 노드로 구성되는 센서네트워크에서는 N개의 잎 노드(leaf node)로 구성된다.

잎 노드와 그 외의 노드들이 가지게 되는 Φ값은 다음 식에 의해 정의된다.

$$\Phi(L_i)=h(id_i,pk_i),\ \text{for}\ i=1,\cdots,N$$
$$\Phi(V)=h(\Phi(V_{left})\parallel\Phi(V_{right}))$$

$\Phi(L_i)$는 i번째 노드의 식별자와 공개키를 해쉬함수로 매핑한 값이고, 후에 계산될 $\Phi(R')$와 $\Phi(R)$ 값이 동일할 경우, 사용자의 공개키를 인증하는 방식이다. 여기서, V는 전체 Merkle 트리에서 내부 노드를 가리킨다. 부모 노드들은 자식 노드들의 Φ 값의 접합을 다시 해쉬하여 자신의 Φ 값을 구한다. 루트 노드도 다른 부모 노드와 동일하게 자신의 Φ 값을 구한다. Merkle 트리의 생성이 완료되면 모든 노드는 Merkle 트리의 루트인 $\Phi(R)$과 각 노드를 기준으로 루트까지의 경로 λ에 포함되는 노드들의 형제 Φ 값들을 부가인자로 저장한다. 이에 따른 각 노드의 메모리 사용량은 $(log_2 N)+1$이 된다.

다. 비밀분산기법

비밀분산이란 특정 그룹의 참가자들에게 비밀을 분산시키는 것으로서 각 참가자는 분산정보(share)가 할당된다. 이 비밀은 분산정보가 모아져야만 복구될 수 있으며 각각의 분산정보만으로는 비밀에 대해서 아무 것도 알아 낼 수가 없다. 이러한 비밀분산은 비밀키의 안전한 저장, 공개키를 이용한 암호화된 백업 시스템 구축, 여러 통신경로로 비밀 메시지 전송, 권한 분산 등의 용도로 사용되고 있다[8,9].

회사의 중요 정보를 보호하기 위해 정보를 암호화하여 보관할 때 한 사람이 키를 간직하는 경우를 생각해보면, 키를 관리하는 사람의 부주의로 암호 키가 분실되었을 때 그 정보를 복호화 할 수 없어 다시 사용할 수 없게 될 우려가 발생할 뿐만 아니라 혼자 키를 갖고 있는 경우 정보의 오용이 발생할 가능성이

있다. 즉, 혼자 키를 갖고 있는 경우 정보의 접근이 독립적으로 이루어지므로 정보의 오용이 발생할 수 있다.

따라서 특정 그룹에서 n명이 키 정보를 분할해 갖고 있을 때, $t(t<n)$명 이상이 모이면 암호문을 복호화 할 키를 만들 수 있는 방식을 생각할 수 있으며, 이러한 방식은 (t,n) 임계치 기법[10]을 이용하면 실현이 가능하다. 이 때 n명이 갖고 있는 정보를 분산정보(share), 키 정보를 비밀정보(secret)라고 한다. (t,n) 임계치 기법에서 최대 $t-1$명이 모여도 비밀을 알아내는 데에 아무런 정보를 제공하지 않아야 한다. 대표적인 (t,n) 임계치 기법에는 Lagrange의 보간 다항식 기법을 이용한 Shamir 기법[11]이 있으며 효율성과 간편성 등의 이유로 가장 많이 사용되고 있다.

Shamir는 유한체 상에서 다항식을 이용하여 (t,n) 임계치 기법을 실현하였다. n명이 갖고 있는 분산정보보다 큰 소수 p를 선정하고 $t-1$차의 임의의 Lagrange 다항식을 생성한다. 예를 들어 $(3,n)$ 임계치 기법의 비밀분산이라면 다음과 같이 2차 다항식을 선정한다.

$$F(x) = ax^2 + bx + K \bmod p$$

p는 소수로 상수 a,b보다 커야하며 a,b는 무작위로 선정한 값이다. K가 3명 이상이 모여야만 그 값을 알 수 있는 비밀이다. n명의 분산정보를 비밀리에 보관하여 3명 이상이 모여 비밀 K를 확인하고 난 후에는 다시 분산정보를 계산해 n명에게 나누어야 한다. 분산정보 K_i는 임의의 x_i 값에 따라 결정된다.

$$K_i = F(x_i)$$

즉, $x_i = 1,2,3,\cdots$ 임의의 값을 대입하면 K_i가 결정된다. 따라서, n명 중 t명의 사람이 모이면 비밀 K를 복원할 수 있다.

Lagrange 보간 다항식은 $(x_1, y_1 = f(x_1))$, $(x_2, y_2 = f(x_2))$, …, $(x_t, y_t = f(x_t))$의 t개의 점을 지나는 $(t-1)$차 다항식으로서 다음과 같이 나타낼 수 있다.

$$F(x) = \sum_{j=1}^{t} F_j(x)$$

여기에서

$$F_j(x) = y_j \prod_{k=1, k\neq j}^{t} \frac{x - x_k}{x_j - x_k}$$

이를 풀어서 쓰면

$$\begin{aligned} F(x) = & \frac{(x-x_2)(x-x_3)\cdots(x-x_t)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_t)} y_1 \\ & + \frac{(x-x_1)(x-x_3)\cdots(x-x_t)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_t)} y_2 \\ & + \cdots \\ & + \frac{(x-x_1)(x-x_2)\cdots(x-x_{t-1})}{(x_t-x_1)(x_t-x_2)\cdots(x_t-x_{t-1})} y_t \end{aligned}$$

이 공식은 Waging(1779)에 의하여 처음 발표되었으며 1783년에 Euler에 의해서 재발견되었고, 1795년에 Lagrange에 의해 발표되었다. 이 Lagrange 보간 다항식 기법의 의미는 특정 다항식을 임의의 서로 다른 t개의 (x,y) 값을 이용하면 원래 다항식을 완벽하게 나타낼 수 있다는 것이다.

3. (t, n) 임계치 기법을 이용한 공개키 인증

본 장에서는 Shamir의 (t,n) 임계치 기법을 이용하여 공개키 인증을 위한 기본 스킴을 제안하고, Elgamal 암호시스템[12]과 지수 분산정보 등을 이용하여 기본 스킴의 보안 취약성을 보완한 확장된 스킴을 제안한다.

가. 기본 스킴

현재 (t,n) 임계치 기법은 비밀(secret)에서 n개

의 분산정보(share)를 생성하여 특정 그룹 n명의 참가자에게 각각 저장한 후, 그 중 $t(<n)$개의 분산정보로 원래의 비밀을 복원하는 용도로 사용되어 왔다. 그러나 본 논문에서 제안한 공개키 인증방식에서는 특정 그룹 n명의 참가자가 하나의 비밀을 공유하고 이 비밀의 분산정보(share)를 각각 따로 저장한다. 나중에 신원이 확인되지 않은 상대방이 인증을 요구할 때에는 상대방이 동일한 비밀의 분산정보를 소유했는지 여부에 따라 상대방을 인증하는 것이다.

본 절에서는 비밀분산 기법 중에서 Shamir의 $(t.n)$ 임계치 기법을 이용하여 공개키를 인증하는 방식을 제안한다. 우선 Shamir의 $(t.n)$임계치 기법에서 사용되는 Lagrange 보간 다항식 기법에 대하여 자세히 알아보고, 이후 이 기법을 이용하여 특정 비밀에 대한 분산정보(share)를 생성하여 공개키를 인증하는 방법에 대하여 설명한다.

1) 인증정보 생성 및 저장

Shamir의 (t,n) 임계치 기법에서는 Lagrange 보간 다항식 기법(interpolating polynomial scheme)을 이용하여 비밀에 대한 분산정보(share)를 생성한다. 특정 그룹 n명의 참가자들에게 비밀에 대한 분산정보를 배포하는 배포자(distributor)는 아래와 같은 $t-1$차 Lagrange 다항식 $F(x)$를 임의로 생성한다. $a,b,c,\cdots$는 임의의 상수, K는 비밀, p는 분산정보보다 큰 소수이다.

$$F(x) \equiv ax^{t-1} + bx^{t-2} + cx^{t-3} \cdots + K \bmod p$$

배포자는 타원곡선 암호방식 등의 공개키 암호 시스템을 이용하여 i번째 참가자($1 \leq i \leq n$)의 공개키(pk_i)와 개인키(sk_i)의 공개키 쌍(pk_i, sk_i)을 생성하고 각 참가자에게 한 쌍씩 할당한다. 각 참가자의 공개키(pk_i)를 Lagrange 다항식 $F(x)$의 x값에 대입하여 다음 식과 같이 각 참 가자의 분산정보 K_i를 계산한다.

$$K_i = F(pk_i)$$

각 참가자들은 동일한 비밀 K, 각각의 공개키 쌍 $(pk_i,\ sk_i)$과 분산정보 K_i를 저장한다.

2) 공개키 인증

위와 같이 공개키 인증정보를 저장하고 있는 참가자는 신원 미상의 상대를 인증할 필요가 있을 경우 상대방의 공개키 pk_i, 분산정보 K_i 정보를 요청한다. 본 논문에서 제안하는 공개키 인증방식은 한 번에 특정 상대방 한명만을 인증하지는 못하고 $t-1$명의 상대방을 동시에 인증한다. 그러므로 인증작업을 수행하기 위해서는 최소한 t개의 (pk_i, K_i) 정보가 필요하다. 참가자 본인의 (pk_i, K_i)와 다른 참가자 $t-1$명의 (pk_i, K_i) 정보를 가지고 있으면 다음과 같은 식을 이용하여 Lagrange 다항식 $F'(x)$를 생성할 수 있다.

$$F'(x) = \sum_{s=1}^{t} K_s \prod_{j=1.j\neq s}^{t} \frac{(x-pk_j)}{(pk_s - pk_j)} \pmod p$$

$F'(x)$가 배포자가 그룹의 참가자들에게 분산정보를 배포할 때 사용하던 Lagrange 다항식 $F(x)$와 동일한 지를 알아보기 위하여 $F'(x)$의 상수항 K'가 다항식 $F(x)$의 비밀 K와 동일한 값인지 확인하면 된다. 만약에 $K'=K$ 이라면 이 다항식 $F'(x)$를 생성하기 위하여 사용된 $t-1$명의 상대방이 자신과 동일한 다항식 $F(x)$를 사용하여 (pk_i, K_i) 정보를 생성했다고 확인할 수 있는 것이다. 이와 같이 $t-1$명의 정보가 정상적인 공개키와 분산정보임을 확인함으로써 $t-1$명의 공개키(pk_i)를 동시에 인증할 수 있다.

만약에 (pk_i, K_i) 정보를 제공한 $t-1$명이 상대에 대한 공개키 인증작업에 실패한다면, 이는 한명 이상의 상대를 신뢰할 수 없다는 것을 의미한다. 이 경우 (pk_i, K_i) 정보를 제공한 기존 $t-1$명의 상대방 외에 추가로 (pk_i, K_i) 정보를 제공하는 상대가 필요하다. 신뢰할 수 없는 상대방이 1명이라고 가정한다면 기존 (pk_i, K_i) 정보 중에 임의의 1개를 새로운 정보로 교환하여 다시 인증작업을 진행한다. 이와 같이

인증이 성공할 때까지 인증 정보를 교환하여 인증하는 작업을 반복적으로 수행함으로써 신뢰할 수 없는 상대방을 제외한 나머지를 인증할 수 있게 된다.

3) 취약점

기본 스킴에서 제안한 Shamir의 (t,n) 임계치 기법을 이용한 공개키 인증방식은 아주 간단하고 효율적이지만 보안적인 측면에서 문제점을 가지고 있다.

만약 신뢰할 수 없는 상대방이 인증 대상자에 포함되어 있을 경우 여러 가지 경우의 수가 발생할 수 있으며, 이 경우 정보 교체 대상 선정 등의 방법에 대한 최적화는 별도의 추가 연구가 필요하다. 공격자가 고의적으로 위조된 인증정보를 가지고 인증작업을 방해하는 서비스 거부 공격(DoS : Denial of Service)에 대한 대응도 앞으로 고려되어야 할 것이다.

인증작업에 인증정보를 제공하는 각 참가자의 인증정보가 평문으로 브로드캐스팅 되는 경우 p, t값을 미리 알고 있다면 누구나 평문으로 수신한 t개의 인증정보를 이용하여 Lagrange 다항식 $F(x)$를 쉽게 알아낼 수 있다. 또한 인증정보를 비밀리에 전달하였다고 하더라도 t명이 모의하면 $F(x)$를 쉽게 알아 낼 수 있기 때문에 인증체계가 무너질 수 있다.

이와 같이 제안한 기본 스킴은 참가자들이 인증정보를 상대방에게 전달하는 과정이 제 3자에게 노출되지 않아야 된다는 가정이 전제된다. 이는 WSN와 같이 필드 배치 초기에 인증정보를 브로드 캐스팅해야 하는 환경에서는 추가로 암호통신이 지원되어야 한다는 문제점이 발생한다. 따라서, 이를 해결하기 위해서는 각 참가자의 분산정보가 상대방 및 제 3자에게 노출되지 않으면서도 인증작업을 할 수 있는 방법이 필요하며 이에 대한 해결방안으로 지수 분산정보와 Elgamal 암호시스템을 이용한 확장된 스킴을 제안한다.

나. 확장된 스킴

앞 절에서 제안한 기본 스킴은 분산정보 값이 외부에 공개될 경우 전체 네트워크의 공개키 인증체계가 와해될 수 있어 보안상 취약하므로 이를 해결하기 위한 확장된 스킴을 제시한다.

1) 변형된 분산정보와 Elgamal 암호시스템

변형된 분산정보는 분산정보의 다른 형태이며 이러한 변형된 분산정보를 이용해서도 원래의 비밀을 복원할 수 있다. Shamir (t,n) 임계치 기법에서 변형된 분산정보를 정의하고 사용하는 방법은 다음과 같다[8].

Shamir의 (t,n) 임계치 기법에서 $t-1$차 다항식 F에서 $F(0)$는 비밀 K이다. 특정 그룹의 각 참가자 i의 분산정보는 $K_i = F(i)$로 주어진다. n명 중 t명의 참가자로 이루어진 부분집합을 B라고 하면 $\pi_B : B \rightarrow \{1,2,\cdots,n\}, |B| = t$ 이다. t개의 분산정보($K_{\pi_B(1)}$, $K_{\pi_B(2)}$, $\cdots$, $K_{\pi_B(t)}$)로 이루어진 임의의 부분집합 B를 이용하여 다항식 F를 다음과 같이 복원할 수 있다. 여기에서 계산은 $GF(p)$ 상에서 이루어진다.

$$F(x) = \sum_{s=1}^{t} K_{\pi_B(s)} \prod_{j=1, j \neq s}^{t} \frac{(x - x_{\pi_B(j)})}{(x_{\pi_B(s)} - x_{\pi_B(j)})} \pmod p$$

여기에서 x_i는 공개된 값이며 변형된 분산정보, $a_{\pi_B(s)}$는 다음과 같이 정의된다.

$$a_{\pi_B(s)} = K_{\pi_B(s)} \prod_{j=1, j \neq s}^{t} \frac{(0 - x_{\pi_B(j)})}{(x_{\pi_B(s)} - x_{\pi_B(j)})} \pmod p$$

변형된 분산정보 $a_{\pi_B(s)}$를 다른 사람에게 전달하는 것은 분산정보 $K_{\pi_B(s)}$를 전달하는 것과 동일한 효과를 갖는다. 그러므로 각 참가자의 변형된 분산정보는 실제 분산정보와 동일한 안전성을 유지해야 한다.

Elgamal 암호시스템은 Diffie와 Hellman이 제안한 공개키 암호기법[13]을 확장한 것이다. 이 암호시스템의 안전성은 이산대수문제에 기초한다. 이 암호시스템을 사용하기 위해서는 유한체(finite field) F_p상에서 발생자(generator) g를 선택한다. 특정 그룹의 비밀 관리자는 $0 < a < p-1$범위에서 임의의 정수값 a를 발생시켜 비밀키로 사용하고 g^a를 공개키로 공개한다. 메시지 M을 전송하기 위하여 전송자는 임의

의 정수값 k를 생성하고 암호문 $C=(g^k, Mg^{ak})$를 전송한다. 이 메시지를 복원하기 위해 수신자는 암호문 첫 번째 인자인 g^k를 a승 한다. 이 결과 값의 곱셈에 대한 역수인 g^{-ak}를 Mg^{ak}와 곱해주면 메시지 M을 복원하게 된다.

2) 확장된 스킴을 이용한 공개키 인증

Elgamal 암호시스템과 변형된 분산정보를 이용하여 암호문을 생성하고 복원하는 과정을 설명한 후 이 과정에서 지수 분산정보를 새로 정의하고 이를 이용하여 공개키를 인증하는 방식을 제시하겠다. 전송자는 참가자들에게 메시지를 전송하고 각 참가자는 메시지를 암호화하여 분산 저장한 후 필요시에 이 정보를 이용하여 메시지를 복호하려고 한다. 수신자는 t명의 참가자가 변형된 분산정보와 Elgamal 암호문을 이용하여 생성한 부분결과(partial result)를 전송받아서 원래의 메시지를 복원한다.

우선 Elgamal 암호시스템 초기 설정 단계에서 비밀 관리자는 비밀키 a를 선정한 후, 각 참가자에게 a의 분산정보 a_i를 할당한다. 암호화 과정은 Elgamal 암호시스템과 동일하며 복호화 과정은 다음과 같은 절차를 통해 수행된다.

① 메시지가 도착하면 t명의 참가자 $\pi_B(s)$로 이루어진 부분집합 B는 3.2.1에서와 같이 변형된 분산정보 $a_{\pi_B(s)}$를 계산한다. 이렇게 계산된 변형된 분산정보의 합은 3.2.2에서의 비밀키 $a \bmod \phi(p)$와 합동이다.

② 각 참가자 $\pi_B(s)$는 g^k에 $-a_{\pi_B(s)}$승을 하여 각각의 부분결과 $g'_{\pi_B(s)}$를 얻는다. 이 부분결과 값이 메시지를 복원할 수신자에게 전송된다.

③ 수신자는 메시지 M을 얻기 위해서 모든 $g'_{\pi_B(s)}$를 곱한다. 이 결과 값인 g^{-ak}를 암호문의 2번째 인자인 Mg^{ak}에 곱하여 메시지 M을 얻게 된다.

예를 들어, $(3,n)$ 임계치 기법을 이용하면 다음과 같다. $\pi_B(1)=1$, $\pi_B(2)=2$, $\pi_B(3)=3$이고 $a_1+a_2+a_3 = a \bmod \phi(p)$이라고 한다면, 각 참가자들은 각자의 $g'_{\pi_B(s)}$를 목적지에 전송한다. 목적지에서는 다음과 같이 계산을 하여 메시지 M을 복원한다.

$$\begin{aligned} Mg^{ak}\prod_{i=1}^{3} g'_{\pi_B(i)} &= Mg^{ak}g^{k(-a_1-a_2-a_3)} \\ &= Mg^{ak}g^{-ak} \\ &= M \end{aligned}$$

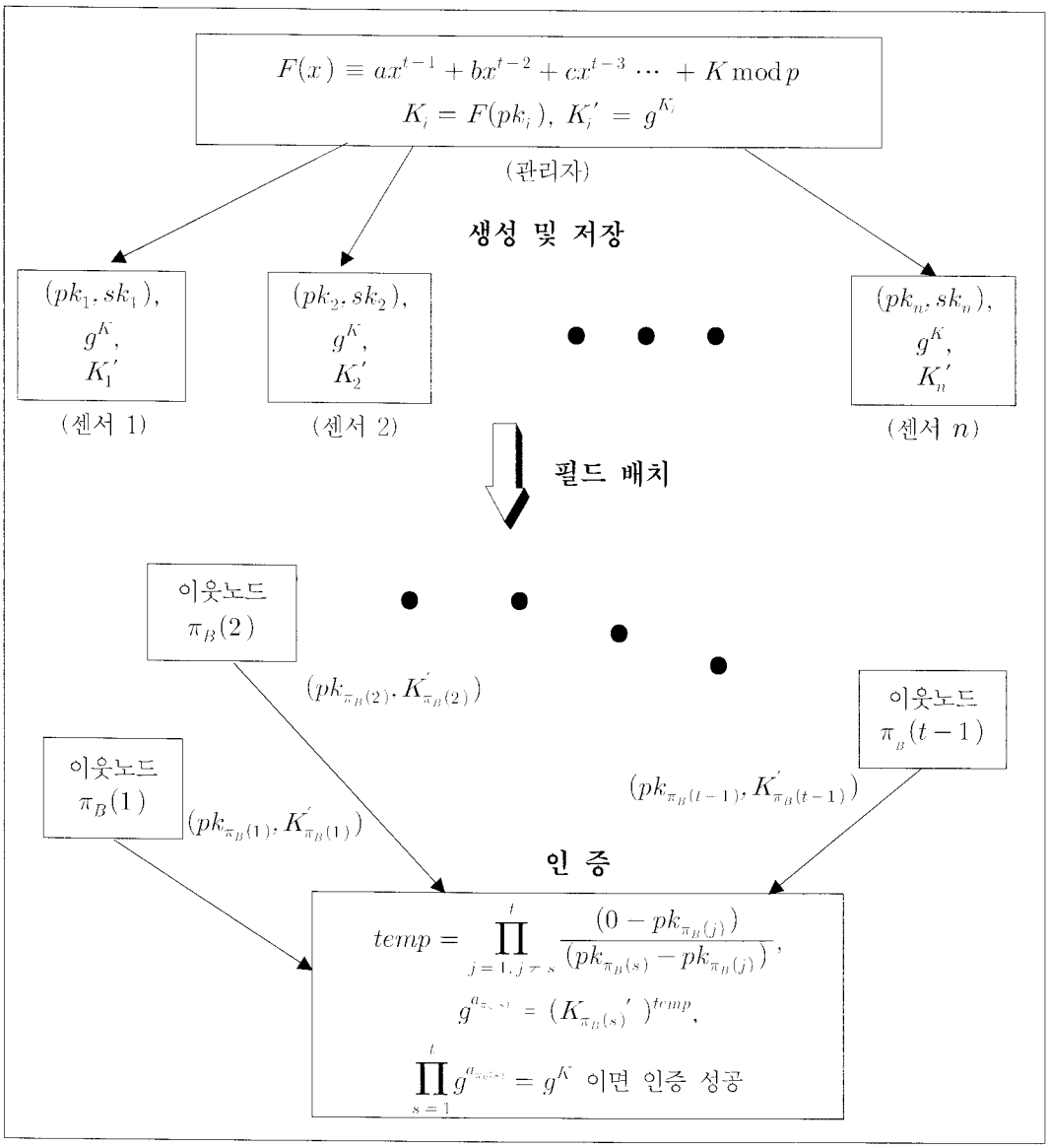
WSN에서는 필드에 배치된 센서가 상호 인증 이전에 통신이 불가능한 상황이다. 그러나 각 센서가 변형된 분산정보 $a_{\pi_B(s)}$를 계산하기 위해서는 주변의 센서와 분산정보 $K_{\pi_B(s)}$와 $x_{\pi_B(s)}$를 교환해야 한다. 이러한 문제를 해결하기 위해서는 위 알고리즘을 완전한 비대화형(non-interactive)으로 만들어야 한다. 이를 위해 각 참가자는 $(g^{kK_{\pi_B(s)}}, x_{\pi_B(s)})$를 목적지에 전송하도록 하면 된다. 이 경우 목적지에서는 첫 번째 인자 $g^{kK_{\pi_B(s)}}$를 $\prod_{j=1, j\neq s}^{t} \frac{(0-x_{\pi_B(j)})}{(x_{\pi_B(s)}-x_{\pi_B(j)})}$ 승 하여 부분결과인 $g^{ka_{\pi_B(s)}}$를 얻게 된다.

위의 메시지 M의 암·복호화 과정에서 M을 1로 설정하고 g^{ak}를 모든 센서가 공유하고 기본 스킴에서와 마찬가지로 각 참가자는 자신의 공개키 값으로 $x_{\pi_B(s)}$를 설정함으로써 공개키 인증작업을 수행할 수 있다. 결과적으로 각 노드의 분산정보 $K_{\pi_B(s)}$ 대신에 $g^{kK_{\pi_B(s)}}$를 전송함으로써 분산정보 값이 공개되는 것을 방지하면서도 공개키를 인증할 수 있게 된다. 이 경우 k값이 항상 일정해도 무방하므로 $k=1$로 설정하고 공개키 인증에 사용되는 $g^{K_{\pi_B(s)}}$를 지수 분산정보라고 정의한다.

4. WSN에서 (t, n) 임계치 기법을 이용한 공개키 인증

가. 전체적인 인증과정

WSN에서 (t,n) 임계치 기법을 이용한 공개키 인



[그림 2] (t,n) 임계치 기법을 이용한 공개키 인증 과정

증과정은 그림 2와 같다. 즉, 공개키를 생성 및 저장하는 단계, 센서 노드를 필드에 배치하는 단계, 인증의 단계를 수행한다.

나. 인증정보 생성 및 저장

네트워크 관리자는 센서를 필드에 배치하기 전에 다음과 같은 과정을 통하여 각 센서노드에 공개키 쌍 (pk_i, sk_i), 지수 비밀(g^K), 지수 분산정보(K_i')를 생성하여 저장한다. 그리고 기본적으로 발생자(g), 분산정보 보다 충분히 큰 소수(p), 임계치(t), ID(센서 식별자) 등 연산에 필요한 정보도 필요하다.

① 네트워크 관리자는 ECC 등의 공개키 방식을 이용하여 각 센서노드에 공개키 쌍 (pk_i, sk_i)을 할

당한다. 또한 다음과 같이 임의의 $t-1$차 다항식을 생성한다.

$F(x) \equiv ax^{t-1} + bx^{t-2} + cx^{t-3} \cdots + K \bmod p$

② 각 센서노드의 분산정보(K_i)는 다음과 같은 식을 이용하여 생성하고

$K_i = F(pk_i)$

③ 지수 분산정보(K_i')를 다음과 같이 계산한다.

$K_i' = g^{K_i}$

다. 공개키 인증

필드에 배치된 센서노드는 다음과 같은 과정을 통하여 이웃센서노드의 공개키를 인증한다.

① 각 센서노드는 이웃센서노드에 자기의 공개키 값(pk_i), 지수 분산정보(K_i'), ID를 포함하는 인증정보를 브로드캐스팅 한다.

② 각 센서 노드는 이웃 노드에서 $t-1$개 이상의 인증정보를 수신하고, 센서노드 자신과 이웃노드의 $t-1$개의 ($pk_{\pi_B(s)}$, $K'_{\pi_B(s)}$) 정보로 이루어진 부분집합 B를 설정($\pi_B : B \rightarrow \{1, 2, \cdots, n\}, |B| = t$) 한다.

③ 각각의 $K'_{\pi_B(s)}$에 $\prod_{j=1, j\neq s}^{t} \frac{(0 - pk_{\pi_B(j)})}{(pk_{\pi_B(s)} - pk_{\pi_B(j)})}$ 승을 하여 부분결과 $g^{a_{\pi_B(s)}}$를 얻는다.

④ 아래 식과 같이 t개의 부분결과를 모두 곱하여 얻은 결과가 지수 비밀(g^K)과 동일하면 $t-1$개의 센서노드의 공개키를 동시에 인증한다.

$$\prod_{s=1}^{t} g^{a_{\pi_B(s)}} = g^K$$

⑤ 인증에 실패할 경우 $t-1$개 이웃노드들 내에서 임의의 이웃노드를 새로운 이웃노드와 교체한 후 ③, ④의 인증작업을 반복적으로 수행한다.

⑤에서 교체할 이웃노드 선정방식의 최적화에 대한 방법과 공격자에 의한 악의적인 인증정보 브로드캐스팅 에 대응하는 방법 등에 대해서는 추가적인 연구가 필요하다. 이웃노드 중에서 최소한 $t-1$개 이상이 정상이라면 위와 같은 방법을 통하여 정상적인 이웃노드를 모두 인증할 수 있게 된다. 본 논문에서는 각 센서노드는 최소한 $t-1$개 이상의 이웃노드를 가지도록 관리자는 센서노드를 배치시 적절한 이웃노드의 밀집도(d)를 설정하고 배치한다는 가정을 하였다.

이와 같이 하여 이웃노드를 모두 인증한 후에는 인증한 이웃노드의 인증정보에 포함된 공개키로 데이터를 암호화하여 송신하면 그 이웃노드는 자신의 비밀키로 데이터를 복호화 함으로써 이웃노드간 암호통신이 가능하게 된다. 또한 각 노드가 브로드캐스팅한 지수 분산정보만으로는 원래의 분산정보를 알아낼 수가 없으므로 인증정보를 위조할 수 없어 안전성을 보장하게 된다.

5. 성능분석

가. 효율성

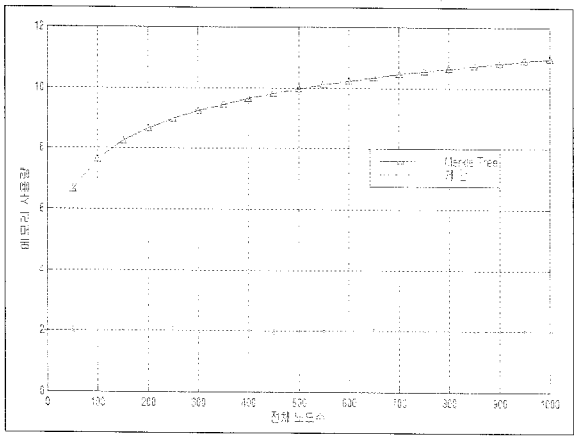
일반적으로 센서 네트워크를 구성하는 센서 노드들은 에너지, 메모리, 통신 반경 및 연산능력 면에서 제한적인 특성을 가진다. 그러므로 이들 자원을 효율적으로 사용하는 것이 매우 중요한 문제이다. 특히 상호인증과정에서 자원을 최소로 사용함으로써 센서노드가 본연의 임무에 보다 많은 자원을 활용할 수 있어야 할 것이다. 본 절에서는 제안한 공개키 인증방식에서의 센서 자원 사용 효율성을 현재까지 최고의 성능을 보여주고 있는 Merkle 트리 공개키 인증방식과 비교 · 분석한다.

1) 메모리 사용량

각 센서노드는 필드에 배치되기 전에 공개키 인증을 위한 정보를 저장하는데 자원이 제약된 센서노드에서 인증에 소요되는 메모리 사용량을 최소화하는 것은 중요한 일이다. 전체 네트워크의 노드 수가 n이면 (t,n) 임계치 기법을 이용하여 공개키 인증을 할 때 한 번의 인증 작업에 필요한 이웃노드의 수는 $t-1$이다. 어느 센서노드 주변의 이웃노드 개수를 밀집도 d라고 하며 d는 t보다 충분히 큰 값이어야 한

다. Merkle 트리 공개키 인증방식에서 한 노드가 이웃노드를 인증하기 위해서 사용하는 메모리 공간은 $(log_2 n)+1$이다. 이에 반해 제안한 공개키 인증방식의 메모리 사용 공간은 2로 항상 일정하다. 즉 모든 센서노드가 공유하는 지수 비밀과 센서노드 각각이 할당받은 지수 분산정보만이 필요하다.

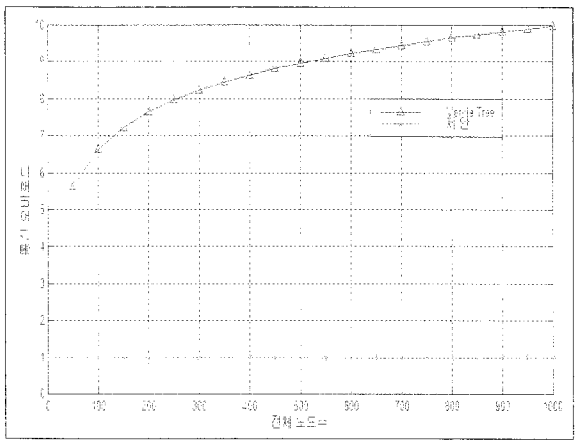
결과적으로 본 논문에서 제안하는 공개키 인증방식은 인증시 필요한 각 센서의 메모리 공간이 Merkle 트리 공개키 인증방식의 $O(log_2 n)$에서 상수로 줄어든 것을 알 수 있다. 그림 3에서 알 수 있는 바와 같이 네트워크의 크기에 상관없이 일정한 메모리 용량만이 필요하여 이는 Merkle 트리방식에 비해 상당한 성능 향상을 이룬 것이다. 즉, 소수 p값을 충분히 크게 해주면 네트워크의 크기와 상관없이 인증에 필요한 메모리 공간의 크기가 일정함을 알 수 있다.



[그림 3] 메모리 사용량 비교

2) 통신 오버로드

각 센서노드는 필드에 배치된 후에 이웃노드끼리 상호 인증을 위하여 ID, 공개키, 분산정보 등으로 이루어진 인증정보를 교환한다. Merkle 트리방식에서 공개키 인증을 위해서 필요한 통신 오버로드는 $\log_2 n$이다. Merkle 트리방식에서 각 센서노드는 자신의 공개키 이외에, 필드에 배치되기 전에 공개키 인증을 위해 저장한 경로 λ상의 형제노드의 Φ값을 전송한다. 이에 반해서 제안한 공개키 인증방식의 통신 오버로드는 1로 항상 일정하다.



[그림 4] 통신 오버로드 비교

즉 제안한 공개키 인증방식에서 각 센서노드는 자신의 공개키 이외에, 필드 배치되기 전에 할당받은 지수 분산정보를 이웃노드에 브로드캐스팅하면 된다.

결과적으로 본 논문에서 제안하는 공개키 인증방식은 인증시 필요한 각 센서의 메모리 사용량이 Merkle 트리방식의 $O(log_2 n)$에서 상수로 줄어드는 것을 알 수 있다. 이는 네트워크의 크기에 상관없이 일정한 통신 오버로드만이 필요한 것으로 Merkle 트리방식에 비해 상당한 성능 향상을 이룬 것이다. 즉 모든 계산에 사용되는 공통 모듈러 소수 p값을 충분히 크게 해주면 네트워크의 크기와 상관없이 인증에 사용되는 통신오버로드의 크기가 일정함을 알 수 있다. 그림 4와 같이 제안한 공개키 인증방식의 통신 오버로드는 Merkle 트리 공개키 인증방식 보다 네트워크 크기가 커질수록 상대적으로 효율적임을 알 수 있다.

3) 연산성능

Merkle 트리 인증방식에서 각 센서노드는 이웃센서노드에 대해 한 개씩 순차적으로 인증을 수행하는 반면, 제안한 인증방식에서는 $t-1$개의 이웃노드를 동시에 인증한다. 두 방식에서 한 번 인증을 수행하는 데에 동일한 계산량이 소요된다면 제안한 인증방식이 최고 $t-1$배 연산 성능이 우수하다고 할 수 있다. 센서의 이웃노드 밀도가 d이고 오류 분산정보가 포함되어 있지 않을 경우 $\lceil d\%(t-1)\rceil$회의 인증 작업만으로 주변 센서노드의 모든 공개키를 인증할 수

있다.

그러나 인증에 관여한 분산정보에 오류가 포함되어 있을 경우 이를 제거하기 위해서는 추가적인 연산이 필요하여 연산성능을 크게 떨어뜨릴 수 있다. 또한 Merkle 트리 인증방식에서는 주로 해쉬 연산이 수행되고 제안한 인증방식에서는 지수연산이 수행되므로 두 방식에 대한 연산 성능을 단순히 비교할 수가 없어 이에 대한 추후 연구가 필요하다.

나. 안전성

이 절에서는 센서노드가 필드에 배치되기 전에 내부 공격자에 의해서 발생할 수 있는 공격이나 공개키 방식 자체의 안정성 위해요인에 대한 분석은 생략하고 센서노드가 필드에 배치된 이후 발생할 수 있는 보안 취약점에 대해서만 분석한다. 기본적으로 공개키 암호방식을 사용하면 공개키 쌍이 노출되지 않는 이상 메시지 위조·도청 등의 공격이 불가능하므로 여기에서는 공개키 인증과정에서의 안전성에 대하여 중점적으로 분석한다. 또한 필드에 배치된 노드가 외부의 악의적인 공격자에 의해 포획되거나 손실되었을 경우에 발생할 수 있는 보안 문제점에 대해서도 기존 방식과 비교·분석 한다.

1) 인증서 위조 가능성

센서노드가 필드에 배치된 이후 ID, 지수 분산정보, 공개키 등으로 이루어진 인증정보를 평문으로 브로드캐스팅 했을 때 이를 도청한 외부의 공격자가 지수 분산정보 등을 이용해서 위조된 인증정보를 생성할 가능성이 있다. 공격자가 목표 네트워크에서 공개키 인증을 위하여 Shamir의 보간 다항식을 이용한 (t,n) 임계치 기법을 사용한다는 것을 알고 있다고 가정하고, 공격자는 t개의 지수 분산정보를 감청하였으며, 연산에 사용되는 모듈러 소수 p, 생성자 g를 알고 있다면, 공격자는 이러한 정보를 이용하여 모든 노드가 공유하고 있는 인증을 위한 지수 분산정보까지는 알아 낼 수 있을 것이다.

공격자는 자신이 정상적인 노드인 것처럼 위장하여 네트워크에서 인증을 받기 위해서는 자기의 공개키가 포함된 인증서가 주변노드에서 인증을 받도록 해야 할 것이다. 이를 위해서는 자기의 공개키와 연결된 지수 분산정보를 생성해야만 한다. 하지만 이는 Shamir의 보간다항식을 아는 자만이 만들 수 있고 이 다항식을 생성하기 위하여 t개의 분산정보를 알아야 한다. 그러므로 공격자가 지수 분산정보에서 원래의 분산정보를 계산해 낼 수 있다면 그 다항식을 계산해 내고 그의 공개키 값을 대입하여 그만의 지수 분산정보를 위조할 수 있는 것이다.

분산정보가 K_i일 때 지수 분산정보는 g^{K_i}이므로 g 와 g^{K_i}를 알고 있을 때 K_i를 계산하는 것은 이산대수문제를 해결하는 것과 동일한 난이도를 갖는 것으로서 매우 어려운 일이다. 그러므로 공격자는 위에서 언급한 정보를 모두 입수하였다고 하더라도 위조된 인증서를 만들어 내는 것은 불가능하다.

2) 노드 포획시 안전성

필드에 배치된 센서가 악의적인 공격자에 의해서 포획되었을 경우 센서 내에 저장된 공개키 쌍 등이 노출된다. 공격자는 포획한 센서 노드의 비밀키를 이용하여 위조된 메시지를 송신하거나 수신한 암호 메시지를 복호해 낼 수 있을 것이다. 여기까지는 공개키 시스템에서 키가 노출되었을 때 일반적으로 발생하는 문제로 이 논문에서 제안하는 방식과 직접적인 관련이 없으므로 따로 설명하지 않겠다. 그리고 포획된 센서노드의 발견 및 조치에 대하여서도 따로 언급하지 않겠다.

한 개의 센서 노드가 포획되었을 경우 모듈러 소수 p, 생성자 g, 임계치 t 등의 정보가 노출될 것이다. 그러나 앞에서 설명한 바와 같이 이러한 정보의 노출은 인증서 위조 등의 전체시스템 인증체계의 안전성 위해상황이 발생하지는 않는 것을 알 수 있다.

일반적으로 (t,n) 임계치 기법을 사용할 경우 t개 이상의 분산정보가 노출되었을 경우 100% 안전성이 깨진 것으로 간주되지만 본 제안방식에서는 지수 분산정보를 사용함으로써 t개 이상의 노드가 포획되더라도 전체 시스템의 인증체계가 와해되는 경우는 발생하지 않는다.

다. 기 타

제안한 방식은 Merkle 트리 공개키 인증 방식에

비하여 확장성이 뛰어나다. Merkle 트리 방식에서는 네트워크의 크기가 정해지고 인증 정보가 계산된 이후에는 네트워크 크기를 확장하는 것이 불가능하다. 하지만 제안한 방식의 네트워크의 크기는 소수 p의 크기로 제한되지만 실제로 p는 아주 큰 값으로 설정되어 있으므로 네트워크 크기에 무관하게 인증정보를 계속적으로 생성할 수 있다고 할 수 있다.

제안한 방식에서 (t,n) 임계치 기법을 이용하여 공개키 인증할 때 t는 노드의 밀집도 d보다 충분히 작게 설정해야 한다. 만약에 이웃노드의 수가 부족해서 인증작업을 하지 못하는 경우가 발생하면 전체 네트워크의 연결성을 보장할 수 없는 것이다. 물론 필드의 변두리에 배치된 센서노드는 밀집도가 필드 중심부의 노드보다 낮을 확률이 크므로, 변두리 센서노드와 이의 이웃센서노드는 필요에 따라 인증작업 동안 송신 출력을 높일 필요가 있을 것이다. 변두리 센서노드는 중심부의 센서노드보다 메시지를 중계하는데 소모되는 전원이 적으므로, 인증작업 동안 더 많은 전원을 소모하는 것은 큰 문제가 되지 않을 것이다. 다른 해결 방안으로는 한 개의 센서노드에 여러 개의 인증정보를 저장하게 할 수도 있지만 이것은 메모리의 효율성을 떨어지게 하므로 몇 개의 인증정보를 한 개의 센서 노드에 저장하는 게 적당한 지에 대한 최적화 방안도 추후 연구되어야 할 것이다.

지금까지의 성능 비교 · 분석 결과를 표 1로 요약하였으며 각 값은 1개의 노드가 d개의 이웃노드를 인증하는 데 필요한 자원의 수를 나타낸다. 표 1에서 알 수 있는 바와 같이 제안한 공개키 인증방식이 Merkle 트리 공개키 인증방식보다 연결성을 제외한 나머지 분야에서 우수한 특성을 나타낸다.

6. 맺음말

본 논문에서는 WSN에서 효과적으로 사용될 수 있는 (t,n) 임계치 기법을 이용한 공개키 인증방식을 제안하였다. 제안한 인증방식은 기존의 (t,n) 임계치 기법에 변형된 분산정보의 일종인 지수 분산정보 개념을 도입하였으며 제한된 자원의 센서노드, 대규모의 네트워크 등이 특징인 WSN에서 효율적인 공개키 인증방식을 제공하는 것을 목표로 하였다.

제안한 공개키 인증방식과 Merkle 트리 공개키 인증방식을 비교 · 분석한 결과 각 센서노드가 인증작업에 필요한 메모리 사용량과 통신 오버로드가 $O(log_2 n)$에서 각각 2와 1의 상수로 급격히 줄어드는 것을 알 수 있었으며, 또한 센서노드를 무제한으로 네트워크에 추가할 수 있는 확장성을 제공하고 연산성능도 우수하였다.

기존의 (t,n) 임계치 기법에서는 t개의 분산정보가 노출될 경우 전체 비밀시스템이 와해되지만 본 논문에서 제안한 (t,n) 임계치 기법과 지수 분산정보를 이용한 공개키 인증방식에서는 원래의 분산정보가 노출되지 않으므로 t개 이상의 노드가 포획되더라도 전체 네트워크의 공개키 인증체계가 와해되는 경우는

[표 1] 공개키 인증성능 비교

성 능 \ 인증방식	Merkle 트리방식	제안한 인증방식
메모리 사용량	$log_2 n + 1$	2(지수 비밀, 지수 분산정보)
통신 오버로드	$log_2 n$	1(지수 분산정보)
인증작업 회수	d <hashing>	$\lceil d/(t-1) \rceil$ <exponentiation, multiplication>
확 장 성	제 한	보 장
연 결 성	보 장	제한($t-1$개 이상의 이웃노드 필요)

발생하지 않아 안전성이 우수하였다.

이와 같이 제안한 공개키 인증방식은 비밀분산기법을 단지 비밀 분산보관만이 아니라 인증에도 사용할 수 있음을 최초로 보여 주었으며, 앞으로 이 분야에 대한 추가적인 연구가 계속되리라고 생각된다.

또한 WSN과 같이 센서의 자원이 제약된 네트워크에서 초기에 동시 다발적인 대규모 인증이 필요한 경우 제안한 공개키 인증방식은 기존의 어느 공개키 인증방식보다 유용하게 사용될 수 있는 주요 보안기술이 될 것이다.

향후연구에서는 임계치 t와 센서노드의 밀집도 d의 관계($t < d$)의 최적화 방안, 포획된 노드 존재 시 보안대응 방안, 연산성능에 대한 객관적인 분석 및 이웃노드 t의 가변적 변화에 따른 제안기법의 안전성 및 Shamir의 (t,n) 임계치 기법 이외의 비밀분산기법을 이용한 공개키 인증방식에 대한 연구도 수행할 것이다.

참 고 문 헌

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks : A Survey", Computer Networks 38(4), pp. 393~422, 2002.

[2] G. Gaubatz, J. Kaps and B. Sunar, "Public Keys Cryptography in Sensor Networks - Revisited", In The Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks(ESAS), 2004.

[3] L. Zhou and Z. J. Haas, "Securing Ad Hoc Network", IEEE Network, 13(6) : pp. 24~30, Nov/Dec 1999.

[4] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux, "Small Worlds in Security Systems : An Analysis of the PGP Certificate Graph", In Proceedings of the ACM New Security Paradigms Workshop 2002, p. 2, 2002.

[5] Dirk Balfanz, D. K. Smetters, Paul Stewart and H. Chi Wong, "Talking To Stranger : Authentication in Ad-Hoc Wireless Networks", In Proceedings of the Network and Distributed System Security Symposium 2002, 2002.

[6] R. Merkle, "Protocols for Public Key Cryptosystems", In Proceedings of the IEEE Symposium on Research in Security and Privacy, Apr 1980.

[7] Wenliang Du, Ronghua Wang and Peng Ning, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc), 2005.

[8] Y. Desmedt and Y. Frankel, "Threshold Cryptosystems", In Advances in Cryptology - Crypto '89, Proceedings, Lecture Notes in Computer Science 435, G. Brassard, Ed., Santa Barbara : Springer-Verlag, pp. 307~315, 1990.

[9] Y. Desmedt. "Society and Group Oriented Cryptography : A New Concept", In C. Pomerance, Editor, Advances in Cryptology, Proc. of Crypto '87(Lecture Notes in Computer Science 293), pp. 120~127, Springer-Verlag, Santa Barbara, California, U.S.A., August 16~20, 1988.

[10] G. R. Blakley, "Safeguarding Cryptographic Keys", In Proc. Nat. Computer Conf. AFIPS Conf, Proc., pp. 313~317, Vol. 48, 1979.

[11] A. Shamir, "How to Share a Secret", Commun. ACM, 22 : pp. 612~613, November 1979.

[12] T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Inform. Theory, 31 : pp. 469~472, 1985.

[13] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, IT-22(6) : pp. 644~654, November 1976.