韓國 컴퓨터情報學會 論文誌
第13卷 第2號, 2008. 3.

2008-13-2-3-1

ECC 기반의 클러스터간 노드들의 안전한 인증 프로토콜

정 윤 수*, 김 용 태**, 이 상 호***

A Secure Authentication Protocol of Nodes between Cluster based on ECC

Jeong Yoon Su *, Kim Yong Tae **, Lee Sang Ho ***

요 약

최근 컴퓨터의 발전을 통해 무선 센서 네트워크 분야가 발전되고 있지만 많은 응용분야에서 보안의 중요성이 증대되고 있다. 특히, 무선 네트워크에서 동작되는 노드의 안전한 통신을 위해서도 보안 메커니즘이나 보안 프로토콜 개발이 필요하다. 이 논문에서는 네트워크에 존재하는 모든 노드가 네트워크 크기에 부합되는 독립된 키들을 소유하면서 노드간 안전한 통신을 보장할 수 있도록 비밀키 방법과 ECC 알고리즘을 조합한 사전 키 분배 방법을 제안한다. 제안된 기법은 노드 캡처에 대해서 탄력적으로 동작하기 때문에 데이터 융합과 집합에 적합하며 네트워크상에 존재하는 타협된 노드들의 탐지를 위해 디지털 시그너처 기능을 적용함으로써 노드간 안전성 문제를 해결하고 있다. 시뮬레이션에서는 제안 기법에서 사용되는 파라미터들의 처리 시간을 평가하여 ECC 키 길이가 증가하더라도 제안 기법이 효율적임을 평가하고 있다.

Abstract

The current pre-distribution of secret keys uses q-composite random key and it randomly allocates keys. But there exists high probability not to be public-key among nodes and it is not efficient to find public-key because of the problem for time and energy consumption. We presents key establishment scheme designed to satisfy authentication and confidentiality, without the need of a key distribution center. Proposed scheme is scalable since every node only needs to hold a small number of keys independent of the network size, and it is resilient against node capture and replication due to the fact that keys are localized. In simulation result, we estimate process time of parameter used in proposed scheme and efficiency of proposed scheme even if increase ECC key length

▸ Keyword : 센서 네트워크(Sensor Network), 클러스터(Cluster), 키 설립(Key Establishment)

• 제1저자 : 정윤수 교신저자 : 김용태
• 접수일 : 2008. 1. 19, 심사일 : 2008. 2. 15, 심사완료일 : 2008. 2. 29.
* 충북대학교 전자계산학과 **한남대학교 멀티미디어학부
***충북대학교 전기전자컴퓨터공학부 컴퓨터전공

Ⅰ. 서 론

최근의 컴퓨터와 통신 기술의 발전은 무선 센서 네트워크의 확대를 용이하게 하고있다[1,2]. 센서 네트워크는 군대 센싱과 추적, 환경 모니터링, 환자 감시와 스마트 환경 등과 같은 분야에서 응용되고 있으며, 센서 노드가 위험 지역에 설치된 경우 보안성은 매우 중요하다. 일반적으로 무선 센서 네트워크의 보안성 제공을 위해서 통신 데이터의 암호화와 인증 절차가 필요하다. 특히, 센서 네트워크의 보안 메커니즘과 프로토콜 개발을 위해서 센서 노드는 센서 노드 간의 비밀키를 설정한다. 센서 네트워크의 사전 키 분배 방식은 모든 정보를 사전에 결정하여 키 정보를 센서에 저장한 후에 센서 노드를 배치한다. 그러나 센서 노드의 설치는 임의적으로 이루어지므로 다양한 사전 지식을 보유하는 것은 불가능하다. 따라서, 센서 노드는 네트워크의 모든 센서 노드들이 공용으로 사용할 수 있는 공용키를 사용해야 한다[3,4].

노드들이 중간 노드들과 통신할 때, 중간 노드가 베이스 스테이션에서 전송하는 비정상적인 메시지를 제거하기 위해 암호화된 데이터를 액세스하기 위한 동작을 수행한다. 이 때 노드간 안전한 통신을 제공하기 위해 센서 노드는 사전에 모든 정보를 결정하고 사전에 정의된 키를 이용하여 노드간 안전하게 통신을 하지만 센서 노드가 사전에 보유하는 키 정보를 많이 소유하지 못하는 단점을 가진다. 이러한 문제점을 해결하기 위해 [5]에서는 센서 네트워크를 위한 하이브리드 키 설립 프로토콜이 제안되었다. 프로토콜은 대칭키 암호 기술을 가지고 표준 ECDH 키 설립을 조합하고 있다. EC 키들의 인증은 오프라인 인증서 권한에 의해 유포된 함축적 인증서를 기반으로 한다. 이 프로토콜은 네트워크의 크기와 상관없이 제한된 키를 가지고 사전 배치되는 센서를 확장하고 있다. 그러나 이 기법은 베이스 스테이션에서 생성한 함축적 인증서를 분실할 경우 안전성이 매우 위협되는 단점을 가진다.

이 논문에서는 노드들이 중간 노드들과 통신하기 위해서 베이스 스테이션과 무관하게 통신 데이터의 인증과 기밀성을 만족하는 ECDSA 기반의 키 설립 기법을 제안한다. 제안 기법은 네트워크에 존재하는 모든 노드가 네트워크 크기에 부합되는 독립된 키들을 소유한 경우 네트워크 확장을 위하여 비밀키 방법과 ECC 알고리즘을 조합한 키를 사용한다. 그리고, 제안 기법은 노드 캡처에 대해서 탄력적으로 동작하기 때문에 데이터 융합과 집합에 적합하다. 또한 네트워크상에 존재하는 타협된 노드의 탐지를 위해 디지털 시그너처 기능을 적용함으로써 노드간 안전성 문제를 해결한다. 그리고 성능 평가를 통해 제안기법에서 사용되는 파라미터의 처리 시간, 노드당 교환되는 메시지 수, 네트워크 밀집도에 따른 클러스터 노드의 평균 수 등을 평가한다.

이 논문의 구성은 다음과 같다. 2장에서는 지금까지 연구된 무선 센서 네트워크 환경에서의 키 분배 방식을 분석하고, 3장에서는 무선 센서 네트워크에서 네트워크의 확장성을 보장하면서 최소 에너지를 가지고 통신할 수 있는 키 설립 기법을 제안한다. 4장에서는 시뮬레이션 환경을 통해 제안 기법의 성능 평가를 기술하고 마지막으로 5장에서 결론을 내린다.

Ⅱ. 관련연구

2.1 타원곡선암호

타원곡선암호(Elliptic Curve Cryptography)는 타원곡선의 이산로그문제의 어려움에 기초한 암호 알고리즘으로 1985년 Koblitz와 Miller에 의해 발표된 이 후 현재까지 암호분야에 많이 적용되고 있다. 타원곡선암호는 유한체의 이산로그문제나 합성수의 인수분해 문제의 어려움에 기반을 둔 공개키 알고리즘보다 효율성과 안전성 측면에서 우수하게 평가받고 있다. 특히 타원곡선 암호는 타원곡선의 이산로그 문제에서 아직 효과적인 공격방법이 발견되지 않고 다른 문제들의 해법을 적용하기 어렵다고 알려져 있어 현재까지 다른 공개키 암호 알고리즘보다 안전성 측면에서 우수하다. 그리고 효율성 측면에서 타원곡선암호는 기존 공개키 암호알고리즘보다 상대적으로 작은 키 길이를 사용하기 때문에 RSA와 DSA 알고리즘보다 빠른 속도로 동작된다.

[표 1]은 안전도에 따른 ECC와 RSA의 키 길이를 비교하고 있다. [표 1]처럼 키 길이 당 안전도가 타원곡선암호가 높게 나타나고 있다. 이 같은 결과는 타원곡선암호가 상대적으로 작은 키 길이를 사용하여도 RSA와 동일한 안전도를 보장할 수 있는 것을 보여주고 있다.

표 1. 안전도에 따른 키 길이의 비교
Table 1. Compare Key Length through Security

Time to break(MIPS years)	RSA Key Size(bits)	ECC Key Size(bits)	RSA/ECC Key Size
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1024	160	7:1
10^{20}	2048	210	10:1
10^{78}	21000	600	35:1

2.2 키 인증 메커니즘

확률적인 키 분배 방법과 랜덤 키 사전 분배 방법[6,7]은 설치 전에 각 센서 노드가 대규모 키 풀로부터 부분 키 집합을 받는 것이다. 통신을 위한 센서 노드들의 임의의 두 노드는 그들의 키 집합 내에서 공통키를 검색하고, 노드간 통신을 위한 공유키로 사용한다. Eschenauer-Gigor 기법을 기반으로 [8]에서는 센서 노드가 배포되기 전에, 노드에의 키 생성에 필요한 정보를 미리 저장하는 키 설립 방법을 제시하였다. 이 기법에서 센서 노드는 분포된 이후 자신이 소유한 몇 개의 키 중에 이웃 노드와 공통된 키가 존재하면 그 키를 사용하여 안전하게 통신할 수 있다. [6]에서는 [8]의 방법을 확장한 q-composite라는 방법을 제시하였다. 이 방법은 각 노드가 하나의 공통된 키가 아닌 최소한 q개의 공통된 키가 존재하는 경우 키 설립이 가능하다. 이 방법은 기존 연구에 비해 보안성을 증가시킬 수가 있지만, 센서 노드에 저장하는 정보가 증가하며, 네트워크 연결성이 감소하는 단점이 있다.

[3]에서는 두 통신 주체 사이에 키를 공유하기 전에 클러스터 헤드가 자신의 멤버 호스트들을 대신하여 인증을 수행하는 방법이 제안되었다. 이 방법에서는 임의의 두 클러스터 헤드가 각자 상대편 클러스터 헤드의 공개키를 이용하여 상호 인증을 수행한다. 따라서 클러스터 헤드의 공개키가 먼저 모든 클러스터 헤드에 분배되어 한다. 클러스터 헤드 간 인증 후에 대칭키 기반의 세션키가 분배되고, 이는 다시 통신 주체인 멤버 호스트에게 분배된다. 이 방법은 클러스터 헤드들이 자신의 공개키를 모든 클러스터 헤드에게 분배하므로 통신 오버헤드가 크다. 또한 두 멤버 호스트 간 비밀키인 세션키 분배 시 헤드의 개인키로 암호화되어 해당 노드에 분배함으로써 세션키가 클러스터내의 모든 호스트들에게 노출 될 수 있다.

Khalili는 ID 기반 암호화 기법의 편리성과 효율성, 임계치 암호화 기법의 유연성 및 안전성의 이점을 결합하여 Ad Hoc 네트워크에서 각 노드의 공개키와 개인키를 생성하는 기법을 제안하였다. 이 방식은 노드가 네트워크에 참여할 때 공통적으로 분배받는 마스터 공개키와 공개되어 있는 호스트의 ID로 해당 노드의 공개키를 유도하고 임계 개수만큼 주변 노드들로부터 ID에 해당하는 부분 개인키를 추출하여 완전한 개인키를 획득하지만 비밀키를 요청하는 주체를 분명히 인증하지 못하므로 중간자 공격에 매우 취약하다.

Blundo는 노드 사이의 충돌에 대해서 안전한 공통키 계산을 위해서 t 파티 그룹으로 여러 기법들을 제안했다[9,10]. 이러한 기법들은 메모리 소비가 그룹 멤버에 있지 않도록 통신 비용을 줄이는데 초점을 가진다. Perriget에 의해 제안된 SPINS는 센서 네트워크에 대해 특별하게 설계된 보안 구조이다[11]. SPINS에서 각 센서 노드는 베이스 스테이션과 함께 비밀키를 공유한다. 두 센서 노드들은 직접 비밀키를 만들지 못한다. 그러나 비밀키를 설정하기 위해서는 신뢰할만한 제3자의 베이스 스테이션을 사용해야 한다. Tatebayashi, Matsuzaki와 Newman은 이동 환경에서의 자원 소비를 위해 키 분배를 생각했으며, Park의 방식보다 더 향상된 방식이다[12]. 그러나 공유키를 발견하는데 시간과 에너지가 많이 소요되어 효율적이지 못하다.

위에서 제시된 방법들은 모두 무선 센서 네트워크에 적합한 키 설립 방법을 제공하지만, 배치되는 센서 노드와의 키 설립을 위해 유지하는 정보의 양이 많은 단점이 있다. 이러한 특징은 무선 센서 네트워크에서 사용할 수 있는 자원이 극히 제한되어 있는 센서 노드에 있어 과부하가 발생하며, 실제 구현도 어렵다.

III. ECC 기반의 키 설립 기법

제안된 키 설립 프로토콜은 균일한 자가 구성 모델에 안전한 다중 구문 배치를 지원하기 위해 대칭키 암호 기술과 함께 ECC 기반의 알고리즘을 조합하고 있다. 노드들은 네트워크에 임의로 배치되고 배치 전까지 이웃 노드들을 인지하지 못한다. 네트워크 초기화 후에 노드들은 동일한 생성 키들을 가지고 동작 기간 동안 네트워크에 참여한다. [그림 1]은 제안기법의 전체 메커니즘 흐름도를 보여주고 있다. 제안기법의 전체 메커니즘은 초기화과정, 키 인증 과정, 키 복구과정 등의 3가지 과정으로 구성된다.

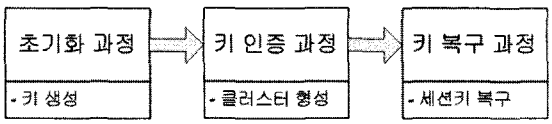

그림 1. 제안기법의 전체 메커니즘 흐름도
Fig 1. The Whole Mechanism Flowchart of Proposed Scheme

3.1 용어 정의

제안 기법에서 사용하는 주요 용어를 정의하면 [표 2]와 같다. [표 2]에서 사용된 용어는 타원곡선 암호에 사용되는 파라미터들과 노드들의 좌표값에 해당하는 용어들이다.

표 2. 용어 정의
Table 2. Notation

개념	설명
E	$GF(p)$상의 타원곡선
n	가장 큰 수
P	큰 소수
Q_x	x의 공개키
d_x	[2,n-2]에서 선택한 x의 개인키
t_x	x의 인증 만기 시간
I_x	x의 임시 인식자
Q_{xy}-Z	x와 y사이에 상호 동의된 키
e_x	h(Q_{xy}-Z,x, t_x, I_x)에서 선택한 값
S_x	x의 전자서명
R_x	x의 타원곡선 점
r_x	타곡곡선상의 x 좌표값
(r, S)	메시지에 대한 인증서 쌍

3.2 키 설립 기법

이 절에서는 키 설립을 위해 초기화 과정, 키 인증 과정, 키 복구 과정 등의 3가지 과정에 대해서 기술한다.

3.2.1 초기화 과정

클러스터를 구성하는 클러스터 헤드와 노드는 초기화 과정을 통해 유한체 상에 정의된 타원 곡선의 강한 보안 알고리즘을 이용하여 키를 생성한다. 이 때, 초기화 과정은 오프라인에서 동작하며, 노드는 자가 처리 가능한 에너지를 가진다. [그림 2]은 센서 노드와 클러스터 헤드 사이의 키 설립 과정을 나타내고 있다.

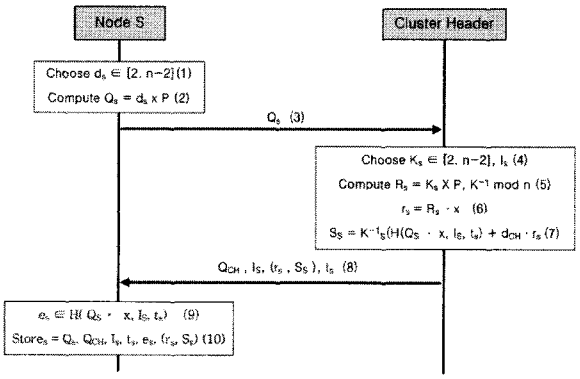

그림 2. 키 설립 초기화 과정
Fig 2. Initial Process of Key Establishment

노드는 (1)처럼 $d_S \in [2,n-2]$ 중에 선택된 임의의 정수를 선택하고, (2)와 같이 $Q_S = d_S \times P$을 계산하여 비밀/공개키 쌍을 생성한다. 노드는 (2)에서 생성한 공개키를 (3)과 같이 클러스터 헤드에게 Q_S을 전달한다. 클러스터 헤드는 센서 노드로부터 Q_S을 수신하고, 센서 노드에게 전달하기 위한 디지털 전자 서명을 만들기 위해 (4)~(7)의 과정을 수행한다. 특히, (7)에서는 노드들의 원활한 관리를 위해 노드의 임시 인식자 I_S, 클러스터 주기 시간과 동일한 값을 나타내는 인증서 만기 시간 t_S 등이 사용된다. (6)에서는 사전에 노드와 동의한 키 $R_S \cdot x$를 r_S로 대치하여 디지털 전자 서명 S_S와 함께 인증서 (r_S, S_S) 쌍으로 표현한다. 그리고, (8)에서는 클러스터 헤드가 클러스터 헤드의 공개키 Q_{CH}와 함께 I_S, (r_S, S_S) 그리고 t_S를 노드에게 전달한다. 노드가 수신한 인증서 정보 중 $Q_S \cdot x$, I_S, t_S의 정보를 해쉬한 값에서 추출한 e_S 값을 노드의 다른 정보와 함께 (10)처럼 저장한다.

3.2 키 인증 과정

이 절에서는 클러스터를 구성하고 있는 노드 사이에서 안전하게 메시지를 송·수신하기 위한 키 인증 과정을 기술한다. 클러스터 그룹을 형성하는 각 노드는 클러스터 헤드가 네트워크에 HELLO 메시지를 브로드캐스트하기 전까지 임의 시간을 기다린 후 클러스터가 형성된 이후에 응답 메시지를 수신한다. 이 때, 클러스터 헤더로부터 전달된 메시지가 신뢰적이지 못한 중간 매체를 통해 최종 센서 노드까지 안전하게 전달하기 위해서 센서 노드간 인증이 필요하다. [그림 3]은 키 인증 과정의 전체적인 동작 흐름도를 나타내고 있다. 키 인증 과정의 동작 과정은 크게 7가지 과정으로 구성된다.

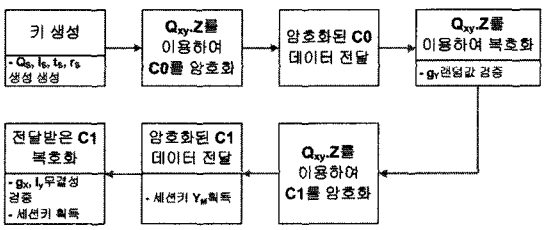

그림 3. 키 인증 과정의 동작 흐름도
Fig 3. Operation Flowchar of Key Authentication Process

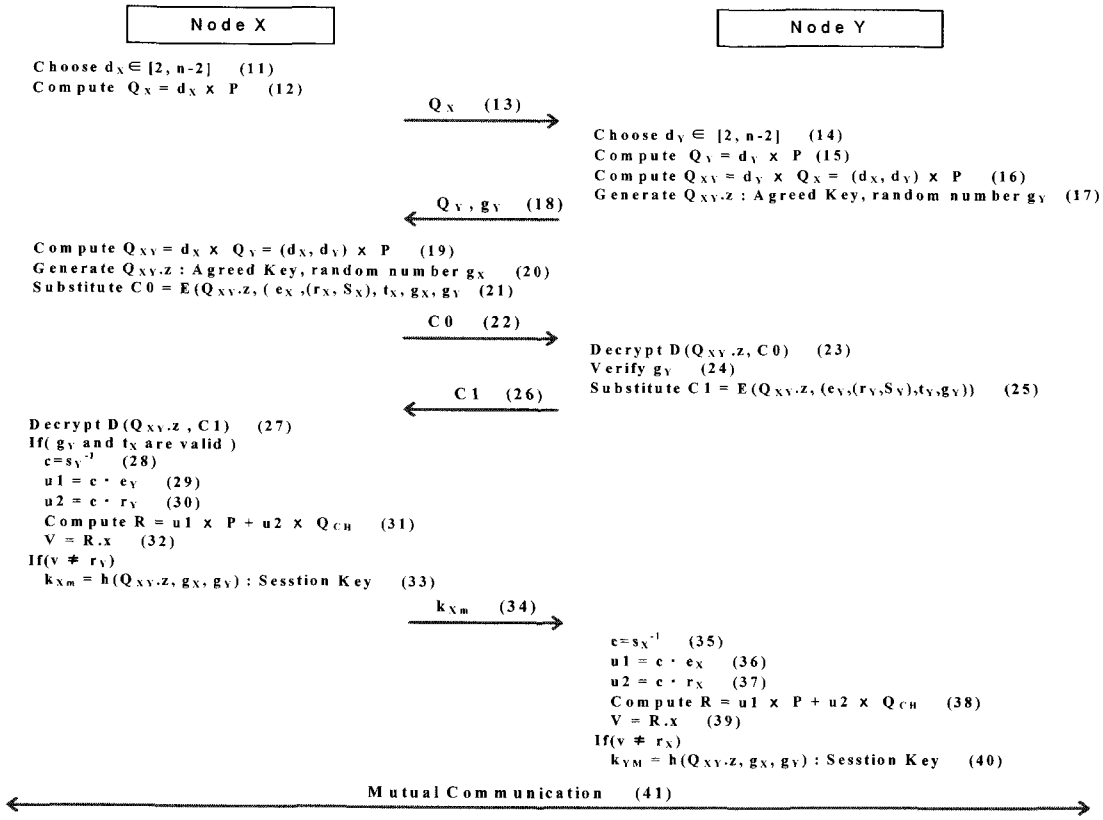

그림 4. 노드간 상호 인증 절차
Fig 4. Mutual Authentication Process between Nodes

[그림 4]은 클러스터 그룹을 형성하는 각 노드 사이의 상호 인증 과정을 기술한다.

- 단계 1 : 노드 X와 노드 Y는 초기화 과정과 동일한 방법을 수행하여 키 인증을 위해 필요한 키를 생성한다.

- 단계 2 : 노드 X는 큰 소수 P와 비밀값 d_X와 d_Y를 이용하여 키 복구 정보 Q_{XY}를 계산한 후, 사전 동의 키 $Q_{XY}.Z$를 이용하여 C0로 암호화한다.

- 단계 3 : 노드 X는 사전 동의 키 $Q_{XY}.Z$로 암호화 한 C0를 노드 Y에게 전송한다.

- 단계 4 : 노드 Y는 수신된 C0를 사전 동의된 키 $Q_{XY}.Z$를 이용하여 복호화한 후 노드 Y의 랜덤 값 g_Y의 존재 여부를 검증한다.

- 단계 5 : 노드 Y는 자신이 생성한 e_Y, (r_Y, S_Y), t_Y 그리고 g_Y를 사전 동의 키 $Q_{XY}.Z$로 암호화하여 C1을 생성한다.

- 단계 6 : 노드 Y는 사전 동의 키 $Q_{XY}.Z$로 암호화 한 C1를 노드 X에게 전송한다. C1을 노드 X에게 전송한 후 노드 Y는 타원곡선 상의 점 $R.x$를 획득하고 노드 X 좌표값과 비교한다. 만일 타원 곡선 상의 점 $R.x$와 노드 X의 좌표값이 일치하지 않으면 $h(Q_{XY}.Z, g_X, g_Y)$를 이용하여 세션키 k_{Y_M}을 획득한다.

· 단계 7 : 노드 X는 전달받은 C1을 사전 동의 키 $Q_{XY}Z$를 이용하여 복호화한다. 노드 X는 전송된 정보를 이용하여 g_X와 t_Y의 무결성을 검증한 후, 타원곡선 상의 점 $R.x$를 획득하고 노드 Y 좌표값과 비교한다. 만일 타원곡선 상의 점 $R.x$와 노드 Y의 좌표값이 일치하지 않으면 h($Q_{XY}Z$, g_X, g_Y)를 이용하여 세션키 k_{X_M}을 획득한다.

3.3 키 복구 과정

이 절에서는 클러스터 내부에서 동작하는 특정 노드가 클러스터를 벗어나 세션키를 분실하였을 경우 클러스터를 이탈한 노드가 세션키를 다시 복구하는 과정을 기술한다. [그림 5]은 키 복구 과정의 전체적인 동작 흐름도를 나타내고 있다. 키 복구 과정은 크게 4가지 동작으로 구성된다.

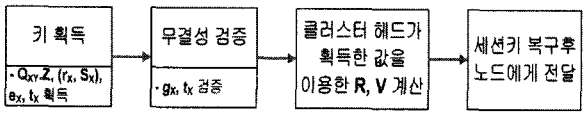

그림 5. 키 복구 과정의 동작 흐름도
Fig 5. Operation Flowchar of Key Recovery Process

키 복구 과정의 구체적인 동작은 다음과 같다.

· 단계 1 : 클러스터 헤드는 적법한 과정을 통하여 무선 인증 및 키 설립 프로토콜에서 전송되는 노드 X의 $Q_{XY}Z$, (r_x, S_X), e_X, t_X를 획득한다.

· 단계 2 : 클러스터 헤드는 적법한 과정을 통하여 노드 X와 비밀리에 공유하고 있는 g_X를 획득하고 획득한 g_X와 t_X의 무결성을 검증한다.

· 단계 3 : 클러스터 헤드는 획득한 값들을 이용하여 $R(= u1 \times P + u2 \times Q_{CH})$과 $V = R.x$를 차례로 계산한다.

· 단계 4 : 클러스터 헤드는 세션키 $K_{X_m} = h(Q_{XY}Z, g_X, g_Y)$을 복구하여 노드 X에게 전달한다.

Ⅳ. 분석 및 평가

4.1 실험 환경

이 절에서는 제안 기법의 실험을 위하여 [표 3]의 실험 시나리오를 통해 임의적으로 생성되는 모델을 사용하여 시뮬레이션된 키 설정 구문을 동작시킨다[13]. 실험을 위해 사용되는 시뮬레이터는 NS-2로 하고, 실험에 사용되는 노드수는 15,000~20,000로 한다. 실험을 위해 크기는 1,000m × 1,000m으로 하여 노드의 초기 에너지를 0.5줄로 설정한다. 또한 실험 환경의 동작시간은 노드들의 잔존 에너지가 0줄이 모두 될 때까지 동작한다.

표 3. 실험 시나리오
Table 3. Experiment Scenario

노드의 수	15,000 ~ 20,000
크기	1000m X 1000m
초기 에너지값	0.5 joules
무선 범위	200 m
버퍼	50 packet
소스 수	100
트래픽	4 pkts/s

4.2 성능 분석

제안 프로토콜에서 사용되는 대칭 키와 해쉬 알고리즘에 대한 에너지 비용을 구하기 위해 128bit 키를 가지는 AES와 해쉬에 사용되는 SHA-1에 대한 에너지량을 [1,14]과 동일한 방법으로 [표 4]과 [표 5]로 나타낸다.

표 4. AES와 SHA-1을 위한 에너지량
Table 4. Energy numbers for AES and SHA-1

Algorithm	Energy
SHA-1	5.9 uJ/byte
AES-128 Enc/Dec	1.62/2.49 uJ/byte

표 5 ECC기반의 전체 프로세스에 의해 소비된 에너지
Table 5. Energy consumed by the entire process based on ECC

Algorithm	Sensor	Server
ECC	93.7 uJ	93.9 uJ

[그림 6]에서는 다양한 네트워크 밀집도에 따른 클러스터 당 노드의 평균수를 나타낸다. [그림 6]의 결과처럼 동일 클러스터내의 노드들은 공용 클러스터 키를 공유하고 노드와 타협하는 공격자가 클러스터 노드의 나머지 통신 링크를 제어한다. 그리고 클러스터수가 작을수록 타협 노드에 대한 위험을 최소화하고 네트워크에 전파되는 것을 예방한다.

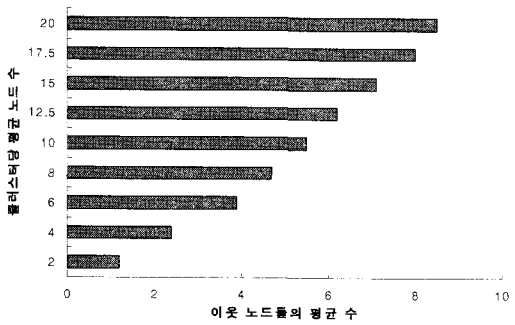

그림 6. 네트워크 밀집도에 따른 클러스터 노드의 평균 수
Fig. 6. A Number of Cluster Node in Network Density

네트워크 환경에서 사용되는 키를 설정하기 위해서 [그림 7]는 노드 당 요구되는 메시지의 평균 수를 나타낸다. [그림 7]의 결과처럼 노드 수가 증가함에 따라 노드당 요구되는 메시지의 수는 감소하고 키 설립에 필요한 전체 시간 또한 material의 복호화 시간을 추가한 메시지 시간만큼만 더 소비된다.

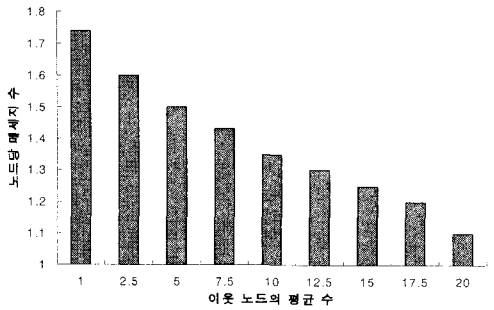

그림 7. 노드당 교환되는 메시지 수
Fig. 7. A number of message changed per Node

[그림 8]는 제안 기법에서 사용하는 대표적인 파라미터들에 대한 ECC 키 길이에 따른 처리 시간을 나타낸다. [그림 8]에서처럼 (r,s)와 $Q_{X,Y}$ 파라미터는 ECC 키 길이가 160에서부터 256까지 증가할수록 최대 8.9%와 5.3%의 처리 시간이 더 필요하였고, $e_{X,Y}$, t 그리고 g 파라미터 등은 ECC 키 길이가 160에서부터 256까지 증가할 때까지 1% 이내로 변화가 거의 없었다. 제안 기법에서 사용되는 파라미터 중 (r,s) 파라미터는 디지털 시그너처와 노드의 좌표값을 포함하기 때문에 다른 파라미터 $e_{X,Y}$, t, g에 비해 1.5~5배 이상의 처리 시간이 더 필요하다. 그러나 제안 기법에서 사용하는 ECC는 다른 알고리즘 DSA, RSA보다 처리 시간이 낮기 때문에 효과적이다.

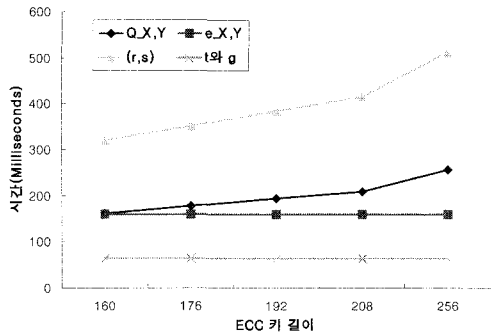

그림 8. ECC 키 길이에 따른 파라미터 처리시간
Fig 8. Process Time of Parameter through ECC Key Length

4.3 보안 분석

노드간 인증은 센서 네트워크의 많은 응용 분야에서 중요한 보안 요구 사항이다. 제안 기법에서는 데이터를 중간 노드를 통해 베이스 스테이션으로 포워딩하는 경우 홉-대-홉 방법으로 인증 단계를 수행한다. 이 때, ECC 기반의 ECDSA 알고리즘을 통해 노드간 인증을 수행하기 때문에 일부 타협된 노드를 통해 특정 패킷을 선택적으로 포워드하는 Selective forwarding 공격에 대해서 제안 기법이 안전하다. 센서 네트워크에서 무결성은 노드간의 전송 메시지에 대한 무결성과 객체간의 무결성이 있다. 데이터의 무결성은 일반적인 보안의 무결성과 같은 의미를 가진다. 그리고 객체에 대한 무결성은 노드 자체를 공격자가 다른 것으로 변경하는 것을 말한다. 이러한 공격을 예방하기 위해서 제안 기법에서는 홉-대-홉 방법의 인증을 수행한다. 데이터 신성성은 예전에 보낸 데이터에 대한 재사용을 방지하기 위한 기수로서 가장 최근에 보낸 데이터임을 보장하는 보안 서비스이다.

제안기법에서 사용한 t_X와 t_Y는 네트워크 상의 타임 동기화를 제공하기 때문에 수신된 메시지가 이전에 수신자가 보낸

요청 메시지에 대한 응답 확인이 가능하다. 네트워크에 참여한 이웃 노드는 새로운 비밀 키를 생성하고 상위 노드의 키들을 수정하기 위해 연속적인 해쉬 동작을 사용한다. 새로운 키들은 그룹에 전송하기 전에 동일 그룹내에서 익명된 노드의 키에 의해 암호화된다. 파생된 모든 키들이 수정되기 때문에 새로운 노드는 이미 이전에 사용된 키들의 액세스가 불가능하다. 네트워크를 빠져나온 노드는 익명된 키들의 이웃 노드의 정보가 부족하다. 모든 키들은 네트워크를 빠져나온 후에 이웃 노드에 의해 새로워지기 때문에 네트워크를 빠져 나오게 된 노드는 향후 암호 키들의 액세스가 불가능하다. 그룹에 참여하기 위해서 새로운 노드는 신뢰된 비밀키 q_X을 획득해야 한다. 새로운 노드는 그룹에 참여하기를 원하는 클러스터 헤드에게 네트워크 참여 메시지 요구를 전송한다. 클러스터 내의 노드는 새로운 노드에게 랜덤 값 r_X를 전송한다. 새로운 노드는 노드간 상호 인증 기법을 사용함으로써 네트워크에서 사용 가능한 현재 키를 획득하고 클러스터의 일원이 된다.

Ⅵ. 결론

이 논문에서는 클러스터 간 노드들의 안전한 인증을 제공하기 위해서 노드들이 사용하고 있는 키를 베이스 스테이션과 무관하게 인증과 기밀성을 만족하는 ECC 기반의 키 설립 기법을 제안하였다. 제안 기법은 디지털 시그너처와 노드의 인증 만기 시간 t를 사용하여 기존 기법보다 키 관리를 효과적으로 처리하였고, 노드간 공유하는 세션키를 생성하여 네트워크 확장성 및 보안성을 향상시켰다. 제안 기법의 실험 결과에서 (r,s)와 $Q_{X,Y}$ 파라미터는 ECC 키 길이가 160에서부터 256까지 증가할수록 최대 8.9%와 5.3%의 처리 시간이 더 필요하였고, $e_{X,Y}$, t 그리고 g 파라미터는 등은 ECC 키 길이가 160에서부터 256까지 증가할 때까지 1% 이내로 변화가 거의 없었다. 이 결과에서 제안 기법은 메시지에 대한 전체 처리 시간이 다른 기법보다 낮아 효율성이 좋다.

향후 연구에서는 중간 노드의 공격 유형에 따른 에너지 소비 비율을 평가하여 평가된 에너지 소비 비율을 줄이면서 효과적으로 재클러스터링이 이루어질 수 있는 연구가 필요하다.

참고문헌

[1] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," In Proceedings of the 5th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking(MobiCom). pp.483-492, 1999

[2] I. F, Akyildiz, W. Su, Y. Sankarasubramaniam, and E . Cayirci, "A survey on sensor network," IEEE Communications Magazine 40, pp. 102-114, 8(August), 2002

[3] T. Dimitriou, I. Krontiris, and F. Nikakis, "Key establishment in sensor networks with resiliency against node capture and replication," December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (MobiHoc) 2004.

[4] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti, "Secure pebblenet," in proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking & Computing, MobiHoc 2001, pp. 156-163, October 2001.

[5] M. Abdalla and M. Bellare, "Increasing the lifetime of a key:A comparativeanalysis of the security of the security of rekeying techniques," In T. Okamoto, editor, Advances in Cryptology ASIACRYPT2000, volume 1976 of LNCS, pages 546-565, Springer-Verlag, 2000.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistributio schemes for sensor networks," In proceedings of the IEEE Symposium on Security and Privacy, 2003

[7] R. Di Pietro, L. V. Mancini, and A. Mei, "random key assignment for secure wireless sensor networks," In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN '03), 2003.

[8] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM conference on Computer

and communications Security(CCS "02), 2002.

[9] L. Echenauer and V. D. Gligor, "A Key-Management scheme for Distributed sensor networks," In Proceedings of the 9th Computer Communication Security, Nov. 2002, pp.41-47.

[10] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for Sensor networks," In IEEE Symposium on Research in Security and Privacy, May, 2003, pp.197-213.

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

[12] G. Gupta, M. Younis, "Performance Evaluation of Load-Balanced Clustering in Wireless Sensor Networks" In the proc. of 10th International Conference on Telecommunications (ICT 2003), Tahiti, French Polynesia, Feb. 2003.

[13] C. Ulmer, Wireless sensor probe networks SensorSimII, http://www.craigulmer.com/research/sensorsimii.

[14] R. di Pietro, L. V. Mancini, and S. Jajodia, "Providing secrecy in key management protocols for large wireless sensors networks,"Journal of AdHoc Networks, 1(4), 2003.

저 자 소 개

정 윤 수

1998년 2월 : 청주대학교 이학사
2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
2008년 2월 : 충북대학교 대학원 전자계산학 박사
관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태

1984년 한남대학교 학사
1988년 숭실대학교 석사
2008년 2월 충북대학교 전자계산학 이학박사
2006.3 ~ 현재 한남대학교 멀티미디어학부 강의전담교수
관심분야: 모바일 웹서비스, 정보보안, AAA, 모바일 통신보안, 멀티미디어

이 상 호

1989년 2월 : 숭실대학교 대학원 컴퓨터네트워크 공학박사
1981년 6월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수
관심분야: Protocol Engineering, Network Security, Network Management, Network Architecture