情報保護學會論文誌
第 21 卷 第 3 號, 2011. 6

무선센서네트워크 환경에서 안전한 멀티캐스트를 지원하는 신속한 그룹키 갱신 기법*

남 궁 완,[1†] 조 관 태, 이 동 훈[2‡]
고려대학교 정보보호대학원

Fast Group Rekeying Scheme for Secure Multicast in Wireless Sensor Networks*

Wan Nam-Goong,[1†] Kwan-tae Cho, Dong Hoon Lee[2‡]
Graduate School for Information Security, Korea University

요 약

센서네트워크 환경에서 멀티캐스트는 베이스스테이션이 다수의 센서노드에게 명령 또는 쿼리를 전송할 때 사용된다. 멀티캐스트 메시지를 효율적으로 안전하게 전송하기 위하여 그룹키를 이용한 암호화 통신이 요구되며, 포획당한 노드로 인한 그룹키 노출에 강건한 그룹키 갱신기법이 필요하다. 이를 위하여 애드 혹 네트워크 환경에서 안전한 그룹키 갱신 기법이 오랫동안 연구되었다. 하지만 기존에 연구된 기법들은 센서네트워크에 적합하게 설계되지 않았으며, 안전한 그룹키 갱신하기 위한 효과적인 방법이 제안되지 못하였다. 따라서 본 논문에서는 그룹에 속한 센서노드만 새로운 그룹키 생성할 수 있는 방법을 통해서 기존의 기법에 비해 높은 안전성을 가지는 멀티캐스트 그룹키 갱신 기법을 제안한다.

ABSTRACT

Messages need to transmit to the neighbors securely in wireless sensor network, because a sensor node is deployed in hostile area. Thus it is necessary to support secure communication. One of the most important communication part is secure multicast. Especially, group rekeying is a big problem for multicast key management. So, group rekeying must be proceed securely when secrete information is exposed by attacker. Many group rekeying schemes have been studied for ad hoc networks. However, these schemes are undesirable in WSNs. In this paper, we proposed a novel group rekeying scheme in WSNs that it has very powerful security.

Keywords: Sensor networks, Multicast security, group-key, rekey

I. 서 론

일반적으로 센서노드는 공격자에 의해 쉽게 노출되는 장소에 배치되며, 물리적 접근이 용이하지 않기 때문에 관리자는 원격으로 감시/통제하면서 정보를 수집한다. 따라서 다수의 센서노드를 효율적으로 관리하기 위하여 일대다 통신을 위한 멀티캐스트 기법이 사용된다. 멀티캐스트 기법은 특정지역에 있는 센서노드에게

접수일(2010년 12월 4일), 수정일(2011년 2월 14일), 게재확정일(2011년 6월 8일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI002113, Car-헬스케어 보안 기술개발]
† 주저자, ngw5608@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

쿼리 또는 제어 명령을 전송하여 네트워크가 원활하게 구성되도록 관리하며, 필요한 정보를 수집하는데 사용된다. 멀티캐스트 기법은 단일 메시지를 여러 목적지에 전달하는 방식으로, 복수 메시지를 전송하는 유니캐스트 기법에 비해 매우 효율적이다. 하나의 메시지를 동시에 여러 목적지에 전송함으로써 네트워크의 효율성을 높이고, 혼잡성을 줄이기 때문에 네트워크 자원을 절약하는 장점을 가지고 있다. 따라서 멀티캐스트 기법은 제한된 자원을 가지는 센서네트워크 환경에 매우 적합하다. 멀티캐스트 환경에서 메시지를 안전하게 전파하는 방법 중 가장 쉬운 접근은 그룹키를 이용하는 것이다. 필드에 배치된 센서노드들은 작동되는 애플리케이션의 종류, 또는 위치정보를 근거로 그룹을 맺고, 관리자는 이 그룹을 이용하여 네트워크를 좀 더 효율적으로 통제한다.

무선센서네트워크 환경에 그룹키를 적용하기 위하여 몇 가지 중요한 고려사항이 존재한다. 첫 번째 고려사항은 그룹키 갱신이 안전하게 이루어져야 한다는 점이다. 센서노드는 쉽게 포획가능하기 때문에 공격자는 포획한 센서노드를 통해 사용되고 있는 그룹키 및 비밀정보를 얻을 수 있으며, 획득한 정보를 통해 네트워크상에 흘러가는 모든 메시지를 도청하거나 공격에 이용할 수 있다. 따라서 센서노드가 공격자에게 포획되었을 경우, 포획된 노드를 제외한 나머지 센서노드에게 안전하게 그룹키를 갱신해 주는 것이 매우 중요하다. 그룹키를 안전하게 전파하기 위해서는 정당한 센서노드들은 베이스스테이션과 사전에 맺은 비밀키를 통하여 갱신되는 그룹키를 전달받아야 한다. 만약 노드포획공격등과 같이 공격자에게 현재 사용되는 비밀키가 노출되었을 경우, 노출된 비밀키는 네트워크 내에서 사용되지 않아야 한다. 또한 노출된 비밀키를 통하여 공격자는 다음에 사용되는 그룹키에 대한 어떠한 정보도 얻을 수 없어야 한다.

두 번째 고려사항은 그룹키 갱신 시 요구되는 시간과 비용이 적어야 한다는 점이다. 그룹키 갱신은 네트워크 확장에 따라 센서노드가 추가될 때 또는 공격자에 의해 특정 그룹키가 노출되었을 때 이루어지며, 그룹키를 생성하는 조건에 따라 새로운 그룹키를 갱신해 주어야 한다. 만약 그룹키 갱신에 요구되는 지연시간이 길 경우, 그룹키를 갱신하는 동안 공격자에 의하여 또 다른 센서노드가 포획됨으로써 갱신되는 그룹키가 다시 노출될 가능성이 생긴다. 또한 그룹키 갱신에 소모되는 에너지가 클 경우 전체 네트워크 수명에 영향을 주기 때문에 안전하고 효율적인 그룹키 갱신 기법이 요구된다.

오래전부터 애드 혹 네트워크 환경에서 안전한 멀티캐스트 기법에 대한 연구가 진행되었다[1][2][3][4][5][6]. 하지만 기존에 연구된 기법들은 그룹키 갱신이 네트워크 전체에 이루어져 통신오버헤드가 매우 크거나, 공격자에 의한 선택적 포획공격에 매우 취약하다. 따라서 본 논문에서는 무선센서네트워크 환경에 적합한 안전한 멀티캐스트 그룹키 갱신 기법을 제안한다.

제안한 기법의 장점을 요약하면 다음과 같다.

- 신속한 그룹키 갱신 : 기존의 기법에 비하여 그룹키 갱신에 요구되는 시간이 짧다.
- 높은 안전성 : 공격자에게 센서노드가 포획되어 비밀정보가 노출되더라도, 공격자는 갱신되는 그룹키에 대한 어떠한 정보도 획득할 수 없다.
- 효과적인 메모리 사용 : 기존 기법에 비하여 센서노드에 저장되는 키의 개수가 적다.
- 유연한 기법 : 간결한 프로토콜 구성으로 센서네트워크 뿐만 아니라 애드혹 네트워크 환경의 그룹 기반 멀티캐스트 애플리케이션에도 적용 가능하다.

본 논문에서는 기존의 연구되었던 멀티캐스트 동향에 대해 살펴보고, 대표적인 그룹키 갱신 기법을 소개한다. 이어서 제안하는 기법에 대해 소개하고, 안전성 분석과 시뮬레이션을 통한 성능 분석을 통해 기존의 대표적인 기법들과 본 논문에서 제안한 기법을 비교분석한다.

II. 관련연구

그룹키 관리 프로토콜은 접근방법에 세 가지로 분류할 수 있다. 하나의 키 분배 센터를 통해 멀티캐스트 그룹키를 관리하는 중앙 집중형 방식, 멀티캐스트 그룹을 여러 개의 하위 그룹으로 나누어 관리하는 비중앙 집중형 방식, 그룹 내 모든 멤버를 통해 키를 생성하는 분산형 방식이 존재한다.

중앙 집중형 방식에서 그룹키를 생성하고, 모든 노드에게 전달하는 역할은 키 서버 혹은 그룹 리더에 의해 이루어진다. 대표적인 기법으로 지리학적 위치정보를 기반으로 트리 형식의 그룹을 이용하는 LKH (logical key hierarchy) 기법[5]이 있으며, 이 기법을 향상시킨 LKHW(LKH wireless) 기법[7],

Kaya 등의 기법[8], Lazos 등의 기법[9]이 존재한다. 또한 위 기법과 달리 사전에 각각의 노드에 여러 개의 키들을 저장시키고, 그룹키를 생성할 때 사용하는 GKMPAN 기법[6]이 있다. 이러한 중앙 집중형 방식은 노드의 포획 및 추가로 인한 그룹키 갱신 시 네트워크 전체에 갱신되는 그룹키가 전달되어야 하기 때문에 통신오버헤드가 크다는 단점을 가진다.

비 중앙 집중형 방식은 그룹을 클러스터라고 불리는 여러 개의 하위 그룹들로 이루어져있다. 각각의 하위 그룹들은 LC(location controller)에 의해 관리되며, 정적 클러스터링 방식과 동적 클러스터링 방식으로 나뉜다. 정적 클러스터링 방식은 사전에 정의된 그룹에 각각의 그룹키를 지정하며, 대표적인 기법으로는 IOLUS 기법[10]가 있다. 동적 클러스터링 방식은 노드가 필드에 배치된 후 동적으로 그룹을 생성하며, 중앙 집중형 방식이 가지는 단점을 해소하는 장점을 가진다. 대표적인 기법으로는 BAAL 기법[11], OMCT(optimized multicast cluster tree) 기법[12], BALADE 기법[13]가 있다.

분산형 방식은 키를 관리하는 주체가 없이 그룹 내 모든 노드들이 스스로 그룹키를 생성하는 방식이다. Chiang 등의 기법[14]에서는 각각의 노드들이 가지고 있는 GPS 장치를 이용하여 MANET 환경에 적합한 그룹키를 생성하는 기법을 제안하였지만, 그룹키 생성 시 공개키 기반 암호화 및 인증서를 사용하기 때문에 자원의 제약을 가지는 센서네트워크 환경에 적합하지 않다. PCGR(predistribution and local collaboration-based group rekeying) 기법[15]은 센서네트워크 환경에서 정보 수집을 통한 그룹키 갱신 기법을 제안하였다. 하지만 이 기법은 선택적 포획 공격에 취약하다는 단점을 가진다.

그밖에 GPLD(grobal-partition, local-diffusion) 기법[16]는 여러 타입의 그룹을 지정하여 여러 애플리케이션 타입이 존재하는 센서네트워크 환경에서 안전한 멀티캐스트를 지원하는 기법을 제안하였다.

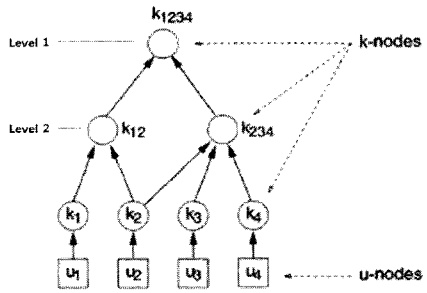
2.1 LKH

LKH 기법[5]은 멀티캐스트 환경에 적합한 트리 기반 그룹키 관리 기법을 제안하였다. 각각의 그룹은 [그림 1]와 같이 여러 개의 서브 그룹을 가지고 있으며, 계층적 트리 구조를 가진다. 키 생성 및 분배는 키 서버(key distribute center)에 의해 이루어지며, 모든 사용자의 비밀키 및 그룹키를 관리한다. 이 기법에서는 그룹을 (U, K, R)로 정의한다. U는 비밀키를 가지고 있는 각각의 사용자, K는 사용자가 가지고 있는 비밀키와 그룹키, R은 사용자와 비밀키의 관계를 나타낸다. 네트워크 구조가 [그림 1]과 같을 때 다음과 같이 정의할 수 있다.

$$U=(u_1,u_2,u_3,u_4)$$

$$K=(k_1,k_2,k_3,k_4,k_{12},k_{234},k_{1234})$$

$$R=((u_1,k_1),(u_1,k_{12}),(u_1,k_{1234}),\\(u_2,k_2),(u_2,k_{12})(u_2,k_{234}),(u_2,k_{1234}),\\(u_3,k_3),(u_3,k_{234}),(u_3,k_{1234}),\\(u_4,k_4),(u_4,k_{234}),(u_4,k_{1234}))$$



[그림 1] LKH 트리 구조의 예

새로운 사용자가 그룹에 추가될 경우 그룹에 포함되는 모든 사용자에게 갱신되는 그룹키를 재분배해야 한다. k_{12}를 그룹키로 가지는 u_1, u_2를 그룹 1이라하고, k_{234}를 그룹키로 가지는 u_2, u_3, u_4를 그룹 2이라할 때, 만약 u_5가 level-2 의 그룹2 에 추가될 경우, 키 분배는 다음과 같다.

$$KeySever \rightarrow u_5 : (k_{12345}, k_{2345})_{k_5},$$

$$KeySever \rightarrow (u_2,u_3,u_4) : (k_{12345}, k_{2345})_{k_{234}},$$

$$KeyServer \rightarrow u_1 : (k_{12345})_{k12}$$

또한 특정 사용자가 가지고 있는 비밀키 정보가 노출되었거나 사용자 이탈로 인하여 트리에서 삭제될 경우, 사용자 추가와 동일하게 삭제된 사용자가 속한 그룹의 그룹키를 갱신한다. 따라서 사용자의 가입 또는 탈퇴에 따라 갱신되는 그룹키 메시지는 네트워크 전체에 전달되어야 하기 때문에 통신오버헤드가 매우 크다.

2.2 GKMPAN

GKMPAN 기법[6]은 애드 혹 네트워크 환경에서 멀티캐스트를 위한 효율적인 그룹키 재분배 기법을 제안하였다. 제안된 기법에서는 노드가 네트워크에 배치되기 전에 각각의 노드는 l개의 키로 이루어진 키 풀 안에서 랜덤하게 m개의 키를 선택하여 저장하며, 이 키들은 추후에 그룹키를 업데이트하는데 사용된다. 또한 각각의 노드는 초기 그룹키 k_g를 저장하며, TESLA[4]를 통해 키를 인증하기 위하여 키 체인의 초기 검증 값(commitment)를 저장한다.

그룹키 갱신은 키 서버에 의해 사전에 정의한 키 풀(key pool)안에서 포획된 노드가 가지고 있는 키를 제외한 나머지 중 임의로 하나를 선택한다. 선택된 키의 ID를 M이라 하고, 폐기할 노드의 ID를 u라 하였을 때 브로드캐스트 메시지는 다음과 같다.

$$KeyServer \rightarrow *: u, M, f_{k'_g}(0), MAC(k_i^T, u|M|f_{k'_g}(0))$$

이때 $MAC(k_i^T, u|M|f_{k'_g}(0))$은 k_i^T의 키를 이용하여 $u|M|f_{k'_g}(0)$에 대한 MAC(Message Authentication Code)값을 의미한다. k_i^T는 MAC인증에 사용되는 TESAL 키로 차후에 KeyServer를 통해 전파된다. 메시지를 전송받은 노드는 TESLA 기법을 이용하여 전송되는 MAC값을 인증하고, 자신이 가지고 있는 키 셋에서 M이 있는지 체크하여 만약 존재한다면 다음과 같이 그룹키를 생성한다.

M을 가지고 있는 노드는 $k_{im} = f_{k_M}(k_g)$과 같이 중간 값을 생성하고, 폐기된 노드를 제외한 나머지 모든 노드들에게 이전에 설립한 비밀키로 암호화하여 전송한다. k_{im}을 전송받은 노드들은 새로운 그룹키 k'_g를 $k'_g = f_{k_{im}}(0)$와 같이 생성하고, 자신이 가지고 있는 모든 키들은 k_{im}를 이용하여 갱신한다.

이 기법에서 그룹키는 키 서버로부터 선택된 비밀키를 가지고 있는 센서노드는 그룹키를 계산할 수 없는 센서노드에게 계산된 그룹키를 암호화하여 각각 전달하며, TESLA 인증 기법을 이용하기 때문에 추가적인 통신오버헤드가 발생한다. 또한 선택적 포획공격에 취약하다는 단점을 가진다.

2.3 GPLD

GPLD 기법[16]은 다중 애플리케이션이 존재하는 무선 센서 네트워크 환경에 적합한 멀티캐스트 모델을 제시하였다. 이 기법에서는 네트워크를 구성하기 위하여 지리학적 가상 그리드 시스템을 이용하여 각각의 노드가 속한 위치의 ID를 획득한다. 위치 ID는 앞으로 안전한 통신을 위하여 사용될 비밀키를 생성하는데 사용된다. 모든 노드들은 총 6개의 그룹(개인, 이웃, 클래스, 지역, 클래스&지역, 전체)을 가지며, 세분화된 그룹을 바탕으로 원하는 목적지에 효과적으로 메시지를 전달하는 기법을 제안하였다.

싱크노드는 멀티캐스트 메시지를 전송하기 위하여 새로운 그룹키 k_g를 생성한다. 생성된 그룹키 k_g를 전송하기 위하여 이웃 센서노드들이 가지는 가장 큰 그룹을 선택하여, 해당 그룹의 그룹키로 k_g를 암호화하여 전송하는 방식으로 네트워크 전체 센서노드에게 전파한다.

위와 같은 과정이 이루어진 후 메시지 헤더인 Hdr를 목적지에 전송한다. Hdr은 목적지 그룹에 대한 위치정보 및 클래스 정보, 암호화된 그룹키가 포함되어 있다. 메시지를 전송받은 목적지 내 선택된 그룹에 속한 센서노드는 헤더를 복호화하여 k_g를 얻을 수 있다.

k_g를 획득한 센서노드는 k_g를 계산할 수 없는 인접 센서노드에게 전송하기 위하여 인접노드를 가장 많이 포함하고 있는 그룹을 선택하고, 해당 그룹키로 k_g를 암호화 하여 이전과 동일한 방식으로 Hdr를 재구성하여 인접노드에게 전송한다. 싱크노드에서 지정한 목적지 지역의 모든 센서노드가 k_g를 획득할 때까지 위 과정을 반복하여 수행하며, 완료 시 $E_{k_g}(Msg)$을 전송한다.

GPLD 기법은 다양한 애플리케이션이 존재하는 센서네트워크 환경에서 효과적으로 그룹키 분배 기법에 중점을 두고 있다. 그룹키 갱신은 싱크 노드로부터 새로 생성된 마스터키를 모든 노드에게 그룹키를 전파하는 방식과 동일하게 전파되고, 새로운 마스터키를 전송받은 모든 노드들은 자신이 속한 모든 그룹키를 업데이트한다. 하지만 포획된 센서노드를 제외하고 안전하게 전파하기 위해서는 포획된 센서노드가 가지고 있는 그룹키를 사용할 수 없기 때문에 추가적인 통신비용 및 연산비용이 요구된다. 또한 모든 그룹키는 하나의 마스터키를 통해서 생성되므로, 공격자에 의한 포획공격으로 인하여 마스터키가 노출될 우려가 매우 크다.

III. 제안하는 기법

공격자에 의한 포획 및 기계적 결함으로 인하여 센서노드가 폐기될 경우, 중앙 집중형 방식은 베이스스

테이션에서 폐기명령 및 새로운 그룹키를 전송한다. 이때 전송되는 메시지는 폐기된 노드가 알 수 없도록 안전하게 전파되어야 한다. 하지만 대표적인 중앙 집중형 방식 기법들[5][6]에서 공격자에 의한 포획 및 도청 공격을 통하여 네트워크 내에서 사용되는 비밀정보가 누출될 수 있기 때문에 안전하게 그룹키를 갱신하는 것은 매우 어려운 문제이다. 따라서 본 논문에서는 무선센서네트워크 환경에서 가장 취약한 포획공격에도 높은 안전성을 제공하는 멀티캐스트 기법을 소개한다.

3.1 용어 정리

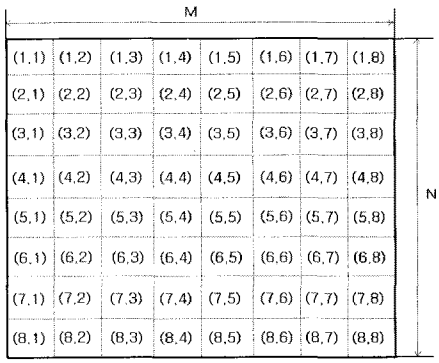
본 논문에서 사용되는 용어는 [표 1]과 같다.

[표 1] 용어 정리

표기	정의
k_i	센서노드 i의 비밀키
G_i	센서노드 i의 위치정보
K_{g_i}	그룹 i의 그룹키
K'_{g_i}	갱신된 그룹 i의 그룹키
N	160 bit 길이의 모듈러값
q	그룹의 센서노드 수
f	그룹키 계산에 사용되는 다항식 함수
c_i	다항식 계수값
s	광범위 멀티캐스트 지역에 포함되는 셀의 수

3.2 가정

센서 네트워크 환경에서 센서노드로부터 획득하는 정보들을 수집하고, 각각의 센서노드를 통제하는 노드를 베이스스테이션이라고 정의한다. 데이터를 수집하고자 하는 장소에 센서노드가 배치된 후 이웃노드와 안전한 통신을 위하여 상호간 쌍방향(pair-wise)키를 맺는다. 베이스스테이션은 공격자에 대하여 강건하며, 다른 센서노드에 비하여 강력한 성능을 지닌다고 가정한다. 공격자는 포획당한 센서노드의 모든 비밀정보를 얻을 수 있으며, 포획한 센서노드 또는 획득한 비밀정보를 이용하여 네트워크 전체에 심각한 영향을 끼칠 수 있다. 따라서 본 논문에서는 이웃노드들을 통해 포획당한 센서노드를 탐지할 수 있다고 가정한다. 포획당한 노드를 탐지하는 기법은 기존에 많은 연구가 이루어져 왔다. 변경된 기기를 탐지하는 기법에 대한 연구[17], watchdog 기법[18] 및 협동적 탐지 기법



[그림 2] 제안한 기법의 그리드 구성

[19]을 이용하여 포획된 센서노드를 탐지할 수 있다. 또한 기기에서 작동하는 소프트웨어의 변경을 탐지할 수 있는 기법[20]을 통해 센서노드의 포획여부를 검증할 수 있다[15]. 기존의 많은 연구[16][21][22][23][24]에서 센서노드의 위치정보를 획득하기 위하여 GPS 기능을 가진 비콘(beacon) 노드 또는 이동식 로봇을 이용하였다. 따라서 본 논문에서도 GPS기능을 가진 비콘 노드를 이용하여 각각의 센서노드들의 위치정보를 획득할 수 있다고 가정한다. 또한 센서 노드는 필드에 배치되기 전에 랜덤하게 생성된 유일한 비밀키 k_i를 저장한다고 가정한다.

3.3 그리드 구성

센서노드를 필드에 배치하기 전, 베이스스테이션은 센서가 배치되는 장소를 [그림 2]와 같이 그리드형태로 구성한다. 본 논문에서는 M×N 크기의 2차원 사각형 그리드를 적용한다. 각 셀의 크기는 센서의 밀집정도에 따라 유동적으로 조정하며, 각 셀의 최대 센서노드 수를 50개로 제한한다[1]. 각각의 센서노드는 필드에 랜덤하게 배치되며, 센서노드는 GPS기능을 이용하여 위치정보를 획득한다. 위치정보를 $G_i=(m,n)$라 하였을 때, 이 값을 센서노드 내에 저장한다. 본 논문에서는 베이스스테이션을 통하여 효율적으로 센서노드를 통제할 수 있도록 중앙집중형 방식을 이용한다. 따라서 센서노드는 자신의 위치정보인 $G_i=(m,n)$를 베이스스테이션에 전송하며, 베이스스테이션은 수집한 위치정보를 통하여 센서노드들의 그룹을 지정한다.

1) 본 논문에서 제안하는 기법은 그룹의 크기가 증가할수록 그룹키를 계산하는데 요구되는 시간과 전송되는 메시지의 길이가 늘어나기 때문에 통신 및 계산의 최적화를 위하여 단일 그룹에 속하는 센서노드의 수를 제한한다.

3.4 그룹키 생성 및 분배

베이스스테이션은 지역의 그룹키 K_{g_i}를 랜덤하게 생성한다. q개의 센서노드를 구성원으로 가지는 그룹의 다항식 f를 다음과 같이 구성한다.

$$f(x) = K_{g_i} + \prod_{i=1}^{q}(x - k_i) \bmod N, (q \geq 5)$$

예를 들어 [그림 3]과 같이 그룹B의 구성원이 {A,B,C,D,E,F} 일 때 생성된 $f(x)$는 6차방정식인 $f(x) = x^6 + c_1x^5 + c_2x^4 + c_3x^3 + c_4x^2 + c_5x + c_6$형태를 가진다. 생성된 다항식의 계수를 해당 그룹에게 전송하기 위하여 다음과 같이 그룹키 메시지를 구성하며, 헤더에 해당 그룹의 정보 및 다항식 차수를 포함하여 전송한다.

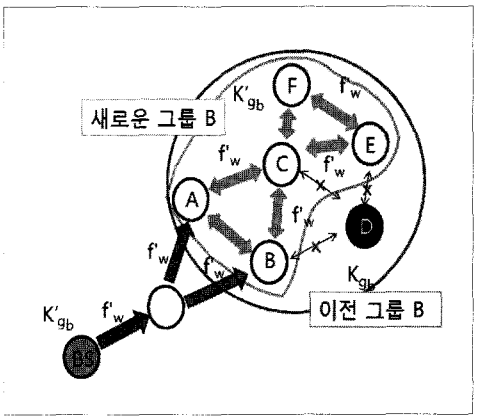
$$c1\|c2\|c3\|c4\|c5\|c6, MAC_{K_{g_i}}(c1\|c2\|c3\|c4\|c5\|c6)$$

이때, ‖은 메시지를 연결시키는 것을 의미하며, $MAC_{K_{g_i}}(\bullet)$은 K_{g_i}를 키로 사용하는 MAC 인증을 나타낸다. 베이스스테이션으로부터 그룹키 메시지를 받은 센서노드는 메시지 헤더로부터 $f(x)$의 차수를 파악하고 전달받은 $c1, c2, c3, c4, c5, c6$을 6차방정식의 계수로 사용하여 다항식을 구성한다. 만약 헤더에 정의한 그룹 구성원일 경우, 다항식에 자신의 비밀키 k_i를 대입하면 $\prod_{i=1}^{q}(x - k_i)$의 결과값이 0이 되기 때문에 K_{g_i} 값을 얻어낼 수 있다. 하지만 그룹에 속하지 않은 센서노드는 자신의 비밀키 $k'_j (k_j \neq k_i,\ 1 \leq i \leq q)$를 다항식에 대입할 경우, 임의의 값 $R(R \neq K_{g_i})$생성되기 때문에 그룹키를 얻을 수 없다. 마지막으로 MAC인증을 통해 계산된 그룹키 K_{g_i}가 올바른지 검증하고, 검증 실패 시 베이스스테이션에게 그룹키 요청 메시지를 전송한다.

3.5 그룹키 갱신

그룹키 갱신이 필요 시 베이스스테이션은 새로운 그룹키 K'_{g_i}를 생성한다. 이때 K'_{g_i}는 이전에 사용되지 않은 랜덤한 값을 사용한다. 그룹키 갱신 메시지는 폐기된 센서노드를 제외한 나머지 구성원의 비밀키를 이용하여 4.4와 동일한 방식으로 다항식 $f'(x)$을 생성하여 전송한다. 그룹키 갱신이 완료되면 이전에 사용했던 K_{g_i}는 삭제한다.

[그림 3]은 폐기된 센서노드로 인해 그룹키 갱신이



[그림 3] 제안한 기법을 통한 그룹 키 갱신 예

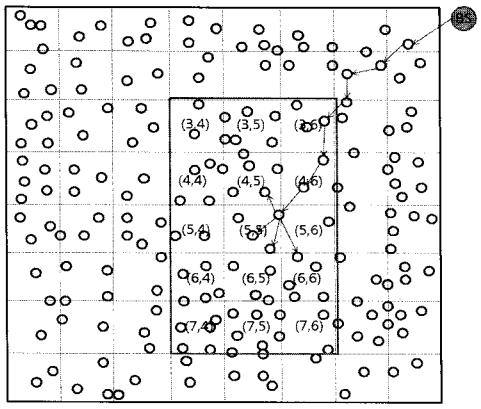
이루어지는 모습을 나타낸 것이다. 폐기된 센서노드D를 제외한 나머지 A,B,C,E,F는 각각의 비밀키를 다항식 $f'(x)$에 대입하여 새로운 그룹키 K'_{g_i}를 얻을 수 있다. 하지만 폐기된 센서노드인 D는 자신의 비밀키를 $f'(x)$에 대입할 경우 K'_{g_i}와 다른 값을 얻기 때문에 그룹키 갱신 이후의 멀티캐스트 통신에 참여할 수 없다.

따라서 본 기법에서는 특정 센서노드의 폐기명령이 이루어지지 않더라도 안전한 그룹키 갱신이 가능하다. 갱신된 그룹키는 새롭게 정의된 그룹에 포함된 센서노드만 생성가능하며 폐기된 노드를 포함하여 그룹에 속하지 않은 센서노드는 고차방정식의 해를 구하지 못하기 때문에 K'_{g_i}를 계산할 수 없다.

3.6 광범위 지역에 대한 멀티캐스트 전송

베이스스테이션은 각각의 그룹에 대해 이전에 생성된 그룹키로 안전하게 멀티캐스트 메시지를 보낼 수 있다. 하지만 베이스스테이션은 하나의 그룹에 국한되지 않고, 특정 지역에 존재하는 센서노드를 통제할 수 있어야 한다. 본 논문에서 제안한 기법을 응용하여 광범위한 지역에 멀티캐스트 메시지를 안전하게 전파할 수 있다.

[그림 4]는 광범위한 지역에 대해 멀티캐스트 메시지를 전송하는 예를 보여준다. 각각의 센서노드는 8×8 크기의 필드에 무작위로 배치되었으며, 3.4과 동일한 방법으로 그룹키 생성 및 분배가 이루어졌다고 가정하자. 베이스스테이션은 모든 센서노드가 배치현황과 각각의 그룹키들을 알고 있기 때문에 메시지를 보내고자 하는 지역을 새로운 그룹으로 지정하여 다항식을 구성한다. 이때 선택된 지역에 포함된 모든 센서



〔그림 4〕 광범위 지역에 대한 멀티캐스트 전송

노드의 비밀키로 다항식을 구성할 경우 차수가 너무 높기 때문에 비효율적이다. 하지만 선택된 지역에 모두 포함되는 그룹에 대해서 센서노드의 비밀키 대신 그룹키를 사용함으로써 다항식을 단순하게 변형시킬 수 있다. 즉, a를 선택된 지역의 셀 수라 하였을때, 광범위 지역 멀티캐스트를 위한 새로운 그룹키 다항식은 다음과 같다.

$$f(x) = K_{g_{red}} + \prod_{i=1}^{a}(x - K_{g_i}) \bmod N$$

베이스스테이션은 3.4절과 동일한 방식으로 그룹키 메시지를 구성하여 베이스스테이션과 가장 최단거리의 라우팅 경로를 가지는 선택된 지역 내 센서노드에게 전송하며, 메시지를 전달받은 센서노드는 이웃노드에게 브로드캐스트하여 전파한다. 그룹키 전송이 완료되면, 베이스스테이션은 새로 분배한 그룹키 $K_{g_{red}}$를 이용하여 멀티캐스트 메시지를 안전하게 전송할 수 있다.

IV. 안전성 분석

센서네트워크 환경에서 안전한 멀티캐스트를 지원하기 위하여 그룹키 갱신은 네트워크를 위협하는 공격에 대해 강건해야 한다. 특히 센서네트워크는 노드 분포의 특성상 포획공격에 매우 취약하기 때문에 공격자는 포획한 노드로부터 획득하는 비밀정보를 이용하여 전송되는 메시지를 도청하거나, 악의적인 목적으로 삽입 또는 위조된 메시지를 전송할 수 있다. 따라서 포획공격에 대한 강건성은 안전한 통신 프로토콜을 구성함에 있어 중요한 요소 중 하나이다.

기존에 제안된 대표적인 기법들[5][6][16]은 "그룹키 갱신을 위하여 공격자에 의해 포획된 센서노드를 제외한 나머지 노드에게 안전한 방식으로 그룹키 갱신 메시지를 전파한다."고 단순히 언급되어 있다. 하지만 안전한 방식으로 나머지 노드들에게 전파하는 것은 결코 간단한 방법이 아니며, 보다 구체적인 기법이 제시되어야 한다. 더구나, 기존 기법들은 안전하게 그룹키 갱신 메시지를 전송하기 위해서 폐기할 센서노드에 대한 정보를 별도로 네트워크 전체에 전파해야 하며, 그룹키 갱신 메시지는 포획된 노드가 존재하는 그룹 내에서 포획된 노드 이외의 합법적인 노드들에게 각각의 비밀키로 암호화되어 유니캐스트 방식으로 전송해야 하는 등 매우 높은 통신 오버헤드를 요구한다.

본 논문에서 제안한 기법은 이러한 기존 기법들이 단순히 가정으로 그친 안전한 그룹키 갱신 전파 방법에 대하여 포함하고 있으며, 공격자의 포획 및 도청 공격에 높은 안전성을 제공한다. 예를 들어, 본 논문에서 제안한 기법에서 공격자가 포획된 센서 노드로부터 얻을 수 있는 비밀정보는 베이스스테이션과의 비밀키와 그룹 안에서 사용되는 그룹키이다. 이때 베이스스테이션은 해당 그룹의 그룹키를 갱신하기 위하여 포획된 노드를 제외한 나머지 센서노드의 그룹을 재지정하여 새로운 그룹키를 갱신한다. 이때 새로운 그룹키는 해당 그룹의 포획된 센서 노드이외의 노드의 비밀키를 이용하여 하나의 메시지 안에 암호화되기 때문에, 공격자에 의해 포획된 센서노드는 갱신된 그룹키를 제대로 도출할 수 없다. 따라서 본 논문에서 제안한 기법은 공격자가 그룹키 갱신 전파 관련 메시지를 도청할지라도, 새로운 그룹키를 생성하는데 필요한 정보를 얻을 수 없기 때문에 높은 안전성을 제공한다.

V. 시뮬레이션 분석

5.1 시뮬레이션 환경

제안한 기법과 그룹키 기반 멀티캐스트 기법인 LKH 기법, GKMPAN 기법, GPLD 기법을 성능을 분석하기 위하여 대표적인 시뮬레이션 도구인 NS-2[25]를 이용하였다. 네트워크는 2,000m× 2,000m 크기로 구성하였고, 라우팅 프로토콜은 AODV를 적용하였다. 센서노드의 밀집도에 따른 변화를 살펴보기 위하여 센서 노드를 필드에 1000개부터 3,000개까지 무작위로 배치하였다. 또한 각각의 센서노드는 100m의 전파범위를 가지며, 초기 에너지량은 1,000mJ이다. 시뮬레이션에서 사용되는 모든 에너지 파라미터들은

MICA2를 기준으로 [26][27][28][29]을 참조한다.

동일한 시뮬레이션 환경을 구성하기 위하여 제안하는 기법과 [5][6][16]기법에 [그림 2]와 같이 8×8 크기의 동일한 그리드를 적용한다. 또한 시뮬레이션은 네트워크에서 임의의 노드가 공격자에게 노출되어, 해당노드의 폐기 명령과 그룹에 속한 센서노드에게 새로운 그룹키를 전파하는데 필요한 시간과 에너지를 측정하기 위하여 100번 반복하여 평균치를 계산한다. 시뮬레이션 결과는 메시지를 주고받을 때 사용되는 에너지, 메시지 인증 및 갱신되는 그룹키 계산에 사용된 에너지, 그리고 라우팅 계산에 사용된 에너지를 포함한다.

그룹키 갱신 방법은 다음과 같다.

LKH 기법은 하나의 셀 단위로 트리를 구성한다고 가정한다. 또한 트리는 최대 level-4형태를 가지며, 각 레벨에 속하는 그룹은 최대 4개로 가정하며, 각 셀에 속하는 센서노드의 수에 따라서 최적화된 트리를 이용한다. 그룹키 갱신을 위하여 키 서버는 폐기된 노드가 속한 최하위 그룹 내 센서노드에게 각각의 비밀키로 암호화된 그룹키 갱신 메시지를 유니캐스트 전송하며, 나머지 센서노드에게 노출되지 않은 각각의 그룹키로 암호화된 그룹키 갱신 메시지를 브로드캐스트 전송한다. 또한 광범위 지역에 대한 멀티캐스트에 대하여 본 논문에서 제안한 기법과 비교하기 위하여 각 셀마다 유지하는 트리의 최상위 그룹키를 이용하여 광범위한 지역에 대한 멀티캐스트를 위한 그룹키를 암호화 하여 전송한다.

GPLD 기법은 위치기반 정보를 통해 각각의 센서가 총 6개의 그룹을 가진다. 메시지를 전송받은 센서노드는 이웃노드와 공통으로 가지고 있는 가장 상위 그룹의 그룹키로 암호화하여 메시지를 전달한다. 이와 같은 방식으로 폐기된 센서노드가 속한 그룹에게 그룹키 갱신 메시지를 전달하며, 안전한 그룹키 갱신을 위하여 최초로 그룹키 갱신 메시지를 전송받은 그룹 내 센서노드가 그룹 구성원들에게 이전에 맺은 쌍방향키로 메시지를 암호화하여 유니캐스트 전송한다.

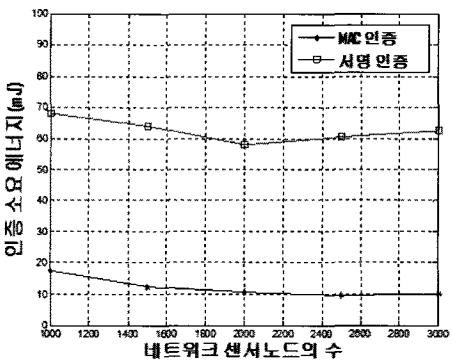
GKMPAN 기법은 키 풀(key pool)의 크기가 2,000이고, 각각의 센서노드에 저장되는 키의 수를 100라 가정하며, 폐기된 노드가 가지고 있는 키를 제외한 나머지 키 중 무작위로 선택된 키 아이디를 전송하며, 전송되는 키 아이디를 검증하기 위하여 TESLA 기법을 이용한다. 이때 해당 선택된 키를 가지고 있는 센서노드만 그룹키를 생성할 수 있으며, 그룹키를 생성할 수 있는 노드를 통해 그룹 내 모든 센서노드에게 이전에 맺은 쌍방향키로 메시지를 암호화하여 유니캐스트 전송한다.

본 논문에서 제안한 기법은 폐기된 센서노드가 속한 그룹의 임의의 센서노드에게 그룹키 갱신 메시지를 전송하고, 메시지를 전송받은 센서노드를 통해 브로드캐스트 방식으로 해당 그룹 내 모든 센서노드에게 그룹키 갱신 메시지를 전파한다. 또한 3.6절에서 제안한 광범위한 지역에 대한 멀티캐스트 환경을 고려하기 위하여 그룹키 분배 및 갱신에 요구되는 에너지량과 시간을 측정한다.

5.2 소모 에너지

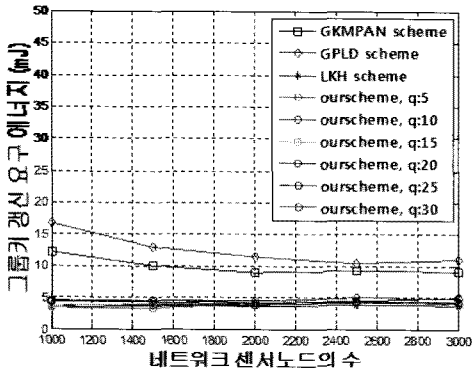
기존에 제안된 기법들에서는 포획된 노드를 제외하고 그룹키를 전파하기 위하여 모든 노드에게 포획된 노드에 대한 폐기 명령을 전파해야 한다. 따라서 베이스스테이션에서 폐기되는 노드의 ID 등을 브로드캐스트전송하며, 메시지 인증을 위하여 MAC 또는 서명기법을 이용한다. [그림 5]는 폐기명령 인증 시 소모되는 에너지의 양[2]을 나타내고 있으며, MAC인증에 비하여 서명 검증에 필요한 에너지가 매우 크다는 것을 볼 수 있다. 하지만 본 논문에서 제안한 기법은 폐기 노드에 대한 명령이 이루어지지 않더라도 그룹키 갱신이 안전하게 이루어지기 때문에 폐기명령에 요구되는 통신 및 계산에 대한 비용을 절감할 수 있다.

[그림 6]은 하나의 센서노드가 포획되었다고 가정하였을 때 그룹키 갱신에 소모되는 센서노드의 평균 에너지를 나타낸다. GPLD 기법에서는 그룹키 갱신

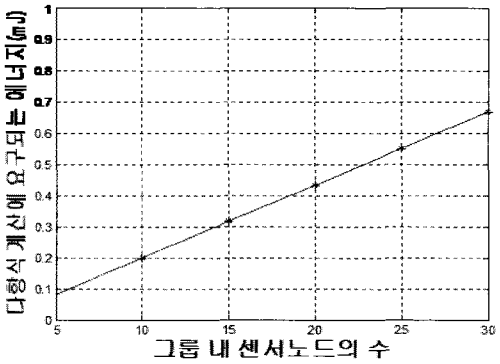


[그림 5] 인증기법에 따른 요구 에너지량

2) MICA2에서 SHA-1은 0.0059mJ/byte, ECDSA_160 서명은 22.82mJ, ECDSA_160 검증은 45.09mJ의 에너지가 요구된다[29].



〔그림 6〕 단일 셀에 대해 그룹키 갱신에 요구되는 에너지량



〔그림 7〕 다항식 계산에 요구되는 에너지량

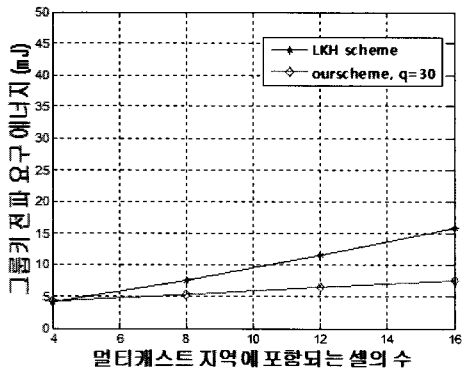
메시지가 네트워크 전체 센서노드에게 전파된다. 특히 메시지를 안전하게 전파하기 위하여 이웃 노드와 사전에 정의된 6개의 그룹 중 공통으로 가지는 가장 큰 그룹을 이용하여 암호화 통신한다. 따라서 다른 기법들에 비하여 그룹키 갱신에 요구되는 에너지가 매우 높다. GKMPAN 기법에서는 그룹키 갱신 메시지 이외에 메시지 인증을 위한 TESLA키의 전파가 이루어지며, 확률적으로 그룹키를 계산할 수 있는 센서노드를 통해 이웃노드에게 암호화하여 전파하기 때문에 추가적인 통신이 이루어진다. 하지만 폐기된 노드가 속한 그룹에만 영향을 미치기 때문에 〔16〕에 비해 적은 에너지가 소모된다. LKH 기법에서는 폐기된 노드가 속한 셀에만 영향을 주기 때문에 그룹키 갱신에 요구되는 에너지가 가장 적다.

본 논문에서 제안한 기법에서 주된 에너지 소모[3]는 다항식 계산에 의존한다. 그룹키 다항식의 차수는 그룹 내 센서노드의 수와 동일하다. 따라서 그룹 내 센서노드의 수를 t라고 할 때, 생성되는 t차 방정식으로부터 그룹키 K_{g_i}를 계산하기 위하여 (t-1)번의 지수승 연산과 (t-2)번의 곱셈이 요구된다. 8 bit CPU를 가지는 MICA2에서 활성화 에너지 소비량은 30mW이며〔27〕, 160bit × 160bit 곱셈에 걸리는 시간이 0.39ms〔28〕이므로 곱셈에 요구되는 에너지량은 0.0117mJ이다. 〔그림 7〕은 그룹 내 센서노드의 수에 따라 요구되는 다항식 계산 에너지량을 나타낸 것이다. 160bit의 AES 암/복호화에 요구되는 에너지가 0.0324mJ/0.0598mJ〔29〕임을 고려해보았을 때, 다항식 계산이 상대적으로 많은 에너지를 요구하지만, 센서노드의 수명에 큰 영향을 주지 않는다. 또한 그룹키 갱신 메시지는 폐기된 노드가 속한 그룹에만 영향을 미치기 때문에 〔그림 6〕에서 보이는 것과 같이 그룹키 갱신에 요구되는 평균 에너지량이 적다는 것을 알 수 있다.

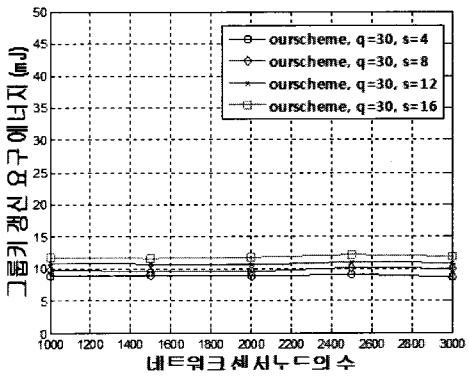
하나의 셀에 대하여 그룹키 갱신이 이루어질 경우 본 논문에서 제안한 기법보다 LKH기법이 적은 에너지를 소모하기 때문에 광범위 지역에 대한 그룹키 분배 및 갱신에 요구되는 에너지량을 비교분석하였다. 〔그림 8〕은 3.6절에서 제안한 광범위지역에 대해 그룹키를 분배하는데 요구되는 에너지량을 나타낸다. LKH 기법에서는 각 셀마다 트리를 유지하기 때문에 여러 셀을 포함하는 광범위한 지역에 대해 멀티캐스트하기 위하여 각 셀에 해당하는 그룹키로 광범위한 지역에 대한 멀티캐스트를 위한 그룹키를 분배하였다. 하지만 〔그림 8〕에서 보이는 바와 같이 멀티캐스트 지역에 포함되는 셀의 수가 증가할수록 통신 오버헤드가 증가하여 그룹키 전파에 요구되는 에너지가 증가함을 볼 수 있다. 본 논문에서 제안한 기법 역시 멀티캐스트 지역에 포함되는 셀의 수가 증가할수록 그룹키 전파에 요구되는 에너지가 증가하지만, LKH 기법과 비교해보았을 때 멀티캐스트 지역에 포함되는 셀의 수가 증가할수록 요구되는 에너지가 상대적으로 매우 적다.

〔그림 9〕는 광범위한 지역에 대한 멀티캐스트 그룹키가 분배된 이후, 하나의 센서노드가 포획되어 그룹키를 갱신하는데 요구되는 에너지를 측정한 것이다. 멀티캐스트 지역의 그룹키를 갱신하기 위하여 포획된 노드가 속하는 셀의 그룹키를 갱신한 후, 멀티캐스트 지역에 포함되는 모든 센서노드에게 각 셀의 그룹키로

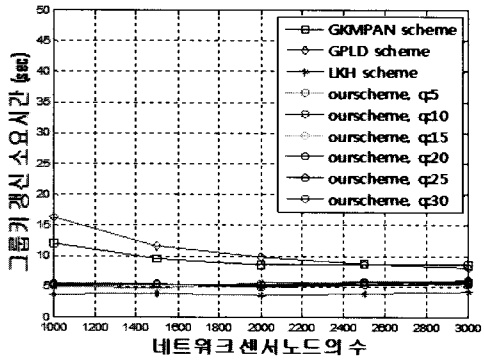
3) 다항식 계산에서 곱셈과 지수승 연산이 대부분을 차지하기 때문에 제안한 기법의 다항식 계산에 요구되는 에너지량은 곱셈과 지수승 연산만을 고려한다. 또한 지수승 연산은 차수가 높아질수록 최적화 기법을 통해 곱셈보다 적은 에너지를 소모하지만, 곱셈과 지수승 연산에 요구되는 에너지량을 동일하게 적용한다.



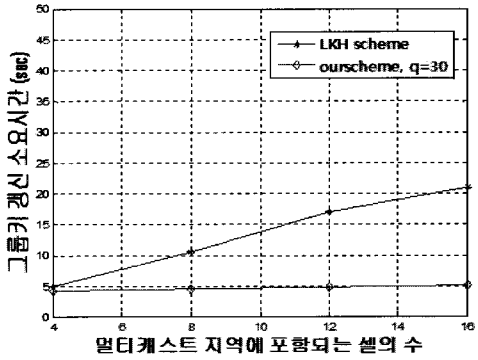
〔그림 8〕 광범위 지역에 대한 그룹키 분배에 요구되는 에너지량, 네트워크 센서노드의 수=2000



〔그림 9〕 광범위 지역에 대한 그룹키 갱신에 요구되는 에너지량



〔그림 10〕 단일 셀에 대해 그룹키 갱신에 요구되는 시간



〔그림 11〕 광범위 지역에 대한 그룹키 분배에 요구되는 시간, 네트워크 센서노드의 수=2000

광범위지역에 대한 멀티캐스트 그룹키를 암호화 하여 전송하기 때문에 〔그림 8〕에서 보이는 바와 같이 비교적 적은 에너지가 소모된다.

5.3 소요 시간

〔그림 10〕은 그룹키 갱신에 요구되는 시간에 대한 시뮬레이션 결과를 나타낸 것이다. GKMPAN 기법은 전송하는 메시지를 인증하기 위하여 TESLA를 이용하며, 확률적 기반의 그룹키 생성 기법을 이용하기 때문에 그룹키가 전파되는데 추가적인 지연시간이 발생한다. GPLD 기법은 그룹키 갱신에 필요한 정보를 폐기된 노드를 제외한 네트워크 전체 센서노드에게 전달하기 때문에 그룹키 갱신에 요구되는 시간이 매우 높은 것을 볼 수 있다. 이에 반해 LKH 기법은 단일 셀에만 영향을 미치기 때문에 그룹키 갱신에 요구되는 시간이 가장 적다. 본 논문에서 제안한 기법 역시 폐기된 센서 노드가 속한 그룹에만 영향을 미치기 때문에 네트워크 크기에 크게 상관없이 그룹키 갱신이 빠르게 이루어진다.

하지만 광범위 지역에 대한 멀티캐스트가 이루어질 경우 본 논문에서 제안한 기법은 LKH 기법보다 뛰어난 성능을 보인다. 〔그림 10〕에서 보이는 바와 같이 LKH 기법은 멀티캐스트 지역에 포함되는 셀의 수가 증가할수록 그룹키 분배에 요구되는 시간이 급격히 증가한다. 하지만 본 논문에서 제안한 기법은 멀티캐스트 지역에 포함되는 셀의 수에 상관없이 그룹키 분배가 신속하게 이루어짐을 볼 수 있다. 또한 〔그림 11〕에서 보이는 바와 같이 광범위 지역에 대한 그룹키 분배 이후 하나의 센서노드의 포획으로 인하여 광범위 지역에 대한 그룹키 갱신이 발생하더라도 그룹키 갱신이 비교적 신속하게 이루어진다.

5.4 확장성

센서노드는 물리적인 접근이 어려운 네트워크 환경

에 배치되기 때문에 네트워크의 확장에 따른 센서노드 추가가 쉽게 이루어져야 한다. 센서노드가 필드에 추가되었을 경우, 추가가 이루어진 그룹에 해당하는 센서노드의 그룹키를 갱신해주어야 한다. GPLD 기법의 경우, 모든 센서노드들이 동일한 비밀값을 이용하여 여러 개의 그룹키를 갱신하기 때문에 네트워크 전체에 그룹키 갱신이 이루어진다. LKH기법은 트리를 구성하는 방식에 따라 차이를 보인다. 만약 네트워크 전체에 하나의 트리로 구성할 경우, 그룹키 갱신은 네트워크 전체에 영향을 미친다. 하지만 각 셀 단위로 트리를 구성할 경우, 센서노드가 추가된 셀에만 영향을 미치기 때문에 높은 확장성을 가진다. GKMPAN 기법 역시 추가되는 센서노드가 속한 그룹에만 영향을 미친다.

본 논문에서 제안한 기법은 추가되는 센서노드의 추가가 이루어질 경우, 센서노드가 속한 그룹에만 영향을 미친다. 하지만 단일 그룹 내 센서노드의 추가가 지속적으로 이루어질 경우, 그룹의 크기가 증가하여 다항식 계산에 요구되는 에너지량 및 전송되는 메시지의 길이가 증가하는 단점을 가진다. 하지만 센서노드를 배치하기 이전에 사전에 그룹의 크기를 조정하여 다항식 계산에 요구되는 에너지 및 메시지의 길이를 최적화 시킬 수 있다. 또한 새로운 영역에 대한 센서노드의 추가로 인하여 네트워크 범위가 확장될 경우, 새로운 그룹을 지정하여 제안한 기법을 적용할 수 있기 때문에 확장성에 큰 제한을 가지지 않는다.

5.5 저장 공간

〔표 2〕는 제안된 기법을 비롯하여 대표적인 기존 기법들에 대한 저장 공간을 비교하여 나타낸 것이다. LKH 기법은 센서노드의 트리 레벨을 L이라 할 때, 각각의 센서노드는 L개의 그룹키를 저장한다. GPLD 기법은 그룹키 이외에 타입에 따라 분류된 6개의 그룹에 대한 비밀키를 저장한다. GKMPAN 기법은 그룹키 이외에 각각의 센서노드에 저장된 m개의 비밀키와 TESLA 초기 인증키 1개를 저장한다. 본 논문에서 제안한 기법은 기존의 기법들과 비교하였을 때 네트워크 크기에 상관없이 비교적 적은공간을 사용한다. 각각의 센서노드에는 셀단위의 그룹키 1개, 광범위한 지역에 대한 멀티캐스트를 지원하는 그룹키 α개 이외에 1개의 비밀키와 다항식 계산에 사용되는 모듈러 N값이 저장된다.

제안한 기법과 기존의 대표적인 기법〔5〕〔6〕〔16〕을 보다 명확히 비교하기 위하여 본 논문에서 수행한 시뮬레이션 시나리오를 그대로 적용한다. LKH 기법에서 각 셀에 포함되는 센서노드의 수에 따라 최적화 트리를 사용할 경우, 평균 트리의 레벨이 4이며, GKMPAN 기법 역시 논문에서 제안한 최적화 기법에 따라 각 센서노드에 저장되는 비밀키는 200개이다, 따라서 본 논문에서 제안한 기법은 광범위 지역에 대한 그룹키를 1개를 지원한다고 하였을 때, 〔표 2〕에서 보이는 바와 같이 본 논문에서 제안한 기법과 LKH 기법이 가장 작은 저장공간을 사용하는 것을 알 수 있다.

〔표 2〕 그룹키 갱신에 요구되는 저장 공간

기법	센서노드에 저장되는 키의 수	시뮬레이션 환경에서 저장되는 키의 수
제안한 기법	$3+\alpha$	4
LKH〔5〕	L	4
GKMPAN〔6〕	m+2	202
GPLD〔16〕	7	7

VI. 결 론

본 논문에서는 무선 센서 네트워크 멀티캐스트환경에서의 새로운 그룹키 갱신 기법을 소개하였다. 이 기법에서는 폐기명령을 내리지 않더라도 그룹키를 안전하게 갱신할 수 있으며, 정당한 센서노드만 올바른 그룹키를 계산할 수 있기 때문에 공격자에 의한 도청/포획 공격에 안전하다. 특히 하나의 그룹키 갱신 메시지를 통하여 광범위한 지역에 브로드캐스트함으로써 통신오버헤드를 줄이는 장점을 가진다.

시뮬레이션 결과를 살펴보면, 본 논문에서 제안한 기법은 그룹키 갱신에 필요한 에너지가 셀에 포함되는 센서노드의 수에 비례하여 증가하는 단점을 가지고 있기 때문에, 셀 단위의 그룹키를 갱신하는데 요구되는 비용과 시간은 LKH 기법이 보다 뛰어나다. 반면, 광범위한 지역에 대한 멀티캐스트 환경에서는 지역의 크기가 커질수록 본 논문에서 제안한 기법이 LKH 기법에 비해 효율성이 매우 높다. 따라서 셀 단위 그룹키를 제공하는 LKH 기법과 본 논문에서 제안하는 광범위 지역에 대한 멀티캐스트 기법을 혼합 적용한다면 보다 효율적인 멀티캐스트를 지원하는 센서네트워크를 구성가능하다.

또한 본 논문에서 제안한 기법의 계산의 양을 줄이기 위하여 센서노드를 필드에 배치하기 전에 각각의

센서노드에게 비밀키에 대한 지수승 계산을 사전에 미리 저장시킨다면, 그룹키 갱신 시 필요로 하는 에너지의 양을 감소시킬 수 있다. 따라서 본 논문에서 제안하는 기법은 다양한 애플리케이션을 지원하는 그룹 기반 네트워크 환경에서 안전한 그룹 통신을 제공할 것이다.

참고문헌

[1] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Construction," IEEE INFOCOM, pp. 708-176, Mar. 1999

[2] K. Ren, W. Lou, and Y. Zhang, "Multi-user Broadcast Authentication in Wireless Sensor Networks," IEEE Communications Society Conference, pp. 223-232, June 2007

[3] A. Perrig, D. Song, and D. tyhar, "ELK, A New Protocol for Efficient Large Group Key Distribution," IEEE Signal Processing, pp. 247-262, May 2001

[4] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. Culler, "SPINS : Security Protocols for Sensor Networks," Wireless Network, vol.8, no.5, pp. 521-534, Sep. 2002

[5] C. Wong, M. Gouda, and S. Lam, "Secure Group Communications Using Key Graphs," IEEE/ACM Transactions on networking, vol. 8, no. 1, Feb. 2000

[6] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN : An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks," ACM Mobiquitous, pp. 42-51, Aug. 2004

[7] R.D. Pietro, L. Mancinim, Y. Law, S. Etalle, and P, Havinga, "LKHW:A Directed Diffusion-based Secure Multicast Scheme for Wireless Sensor Networks," International Conference on Parallel Processing Workshops, pp. 397-406, Oct. 2003

[8] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure Multicast Groups on Ad Hoc Networks," ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 94-102, 2003

[9] L. Laxos and R. Poovendram, "Energy -Aware Secure Multicast Communication in Ad Hoc Netwroks Using Geographical Location Information," IEEE International Conference on Acoustics Speech and Signal Processing, vol. 4 pp. IV-201-4, 2003

[10] S. Mittra, "Iolus : A framework for scalable secure multicasting," ACM Special Interest Group on Data Communication, pp. 277-288, 1997

[11] M. Bouassida, I. Chrisment and O. Festor, "An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks," NETWORKING LNCS 3042, pp. 725-742, 2004

[12] M. Bouassida, I. Chrisment and O. Festor, "Efficient Clustring for Multicast Key Distribution in MANET," NETWORKING LNCS pp. 138-153, 2005

[13] M. Bouassida, I. Chrisment and O. Festor, "Group Key Management in Manets," International Journal of Network Security, pp. 67-79 2008

[14] T. Chiang and Y. Huang, "Group Keys and the Multicast Security in Ad Hoc Networks," International Conference on Parallel Processing Workshops, pp. 385-390, Oct. 2003

[15] W. Zhang, S. Zhu, and G. Cao, "Predistribution and Local Collaboration -based Group Rekeying for Wireless Sensor Networks," Ad Hoc Network, vol. 7, pp. 1229-1242, Aug. 2009

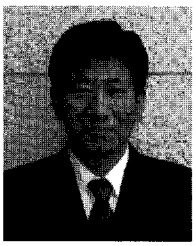
[16] K. Ren, W. Lou, B. Zhu, and S. Jajodia "Secure and Efficient Multicast in Wireless Sensor Networks Allowing Ad Hoc Group Formation," IEEE Transactions on vehicular technology, vol.58, no.

4, pp. 2018-2029, May 2009
[17] J. Hall, M. Barbeau, and E. Kranakis, "Detection of Transient in Radio Frequency Fingerprinting Using Phase Characteristics of Signals," IASTED International Conference on Wireless and Optical Communication (WOC), pp. 13-18, May 2003
[18] S. Marti, T. Giuli, T. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," ACM MobiCom, pp. 255-265, Aug. 2000
[19] G. Wang, W. Zhang, and G. Cao, T. La Porta, "On Supporing Distribued Collaboration in Sensor Networks," IEEE Military Communications Conference (MILCOM), pp. 752-757, Oct. 2003
[20] A. Seshadri, A. Perrig, L.V. Doorn, and P. Khosla, "SWATT : Software-based Attestation for Embedded Devices," IEEE Symposium on Security and Privacy, May 2004
[21] T Shi-Chun, T Wen-Guey, and Z Kun-Yi, "Key establishment schemes against storage-bounded adversaries in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 8, no. 3, pp. 1218-1222, Mar. 2009
[22] M. Jadliwala, Z. Sheng, S.J. Upadhyaya, Q. Chunming, and J.P. Hubaux, "Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes," Mobile Computing, IEEE Transactions on, vol. 9, no. 6, pp. 810-823, Apr. 2010
[23] F. Anjum, "Location dependent key management in sensor networks without using deployment knowledge," Wireless Networks, vol. 16, no. 6, pp. 1587-1600, Oct. 2008
[24] T.V. Srinath, "Localization in resource constrained sensor networks using a mobile beacon with in-ranging," Wireless and Optical Communications Networks, pp.5, Apr. 2006
[25] "The Network Simulator, ns-2," available at http://www.isi.edu/nsnam/ns
[26] A. Liu and P. Ning, "TinyECC : A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks," Information Processing in Sensor Networks(IPSN), pp. 245-256, 2008
[27] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," The International Workshop on Scalable Ad Hoc and Sensor Networks(SASN), pp. 169-176, 2006
[28] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C.Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," IEEE International Conf. Pervasive Computing and Communications (PerCom), pp. 324-328, Mar. 2005
[29] Y. Wang, G. Attebury, and B. Ramamurthy "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, 2006.

〈著者紹介〉

남 궁 완 (Wan Namgoong) 학생회원
2006년 2월: 단국대학교 컴퓨터과학 학사
2009년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심 분야〉 무선센서네트워크, VANET, 스마트그리드

조 관 태 (Kwantae Cho)
2005년 2월: 고려대학교 컴퓨터학과 학사
2005년 3월~2008년 2월: 고려대학교 정보보호대학원 석사
2008년 2월~현재: 고려대학교 정보보호대학원 박사과정
〈관심 분야〉 무선센서네트워크, VANET, 스마트그리드



이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 졸업(학사)
1987년 12월: Oklahoma University 전산학 대학원 공학석사
1992년 5월: Oklahoma University 전산학 대학원 공학박사
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 2월~현재: 고려대학교 정보보호대학원 교수
〈관심 분야〉 암호프로토콜, 암호이론, 키 교환, 익명성 연구, USN 이론, PET 기술