# 무선 센서 노드의 강한 보안 강도를 위해 이중 해쉬 체인을 적용한 키 사전 분배 기법

정회원 정 윤 수*, 김 용 태**°, 박 길 철***, 이 상 호****

# A Key Pre-distribution Scheme Using Double Hash Chain for Strong Security Strength of Wireless Sensor Node

Yoon-Su Jeong*, Yong-Tae Kim**°, Gil-Cheol Park***, Sang-Ho Lee**** ***Regular Members***

요 약

무선 센서 네트워크에서는 물리적인 접근과는 무관하게 jamming이나 eavesdropping과 같은 공격이 쉽게 발생하기 때문에 무선 센서 네트워크에서의 보안은 중요한 요구 사항 중에 하나이다. 무선 센서 네트워크에서 보안을 향상시키기 위해 최근 키 관련 기법들이 활발히 연구되고 있지만 현재까지 연구된 기법들은 노드가 공유하고 있는 공유키의 발견을 위하여 시간과 에너지가 많이 소요되므로 무선 네트워크 환경에 적합하지 않다. 특히, 무선 센서 네트워크를 구성하고 있는 구성 요소 중 게이트웨이 역할을 담당하는 노드의 안정성은 여러 보안 공격에 취약하다. 따라서, 이 논문에서는 확률적 키에 의존하지 않으면서 게이트웨이 역할을 담당하는 노드의 안전성을 향상시키기 위해 랜덤 키 사전 분배 기술과 이중 해쉬 체인을 조합한 키 사전 분배 기법을 제안한다. 제안 기법은 기존 기법보다 적은 저장 공간과 강한 보안 강도를 유지할 수 있기 때문에 동일 보안 강도를 가지고 있는 기존 기법들보다 효율성이 좋고, 작은 크기의 키 생성 키 셋을 사용하기 때문에 네트워크 확장성에 효율적이며 센서 노드의 저장 오버헤드를 크게 줄일 수 있다.

**Key Words** : 무선 센서 네트워크(Wireless Sensor Networks), 이중 해쉬 체인(Double Hash Chain), 키 사전 분배(Key Pre-distribution), 보안강도(Security Strength)

ABSTRACT

Since WSNs encounter attacks, such as jamming or eavesdropping without physical access occurs, security is one of the important requirements for WSNs. The key pre-distribution scheme that was recently researched for advance of security in WSNs distributes the keys and probability with the use of q-composite random key pre-distribution method, but there is a high probability that no key shared between sensor nodes, and it takes a lot of time and energy to find out the shared key. Therefore,it is not suitable for WSNs. In order to enhance stability of a node that plays a role of gateway without depending on probabilistic key, this paper proposesa key pre-distribution scheme combined with random key pre-distribution scheme and double hash chain. Since the proposed scheme can maintain a small storage place and strong security strengths, it is more efficient than the existing schemes with the same security strengths. In addition, since it uses a small size of key generation key set, it can reduce a great deal of storage overhead.

※ 본 연구는 지식경제부 지역혁신센터 사업인 민군겸용 보안공학연구센터 지원으로 수행되었음
* 충북대학교 전자계산학과 네트워크보안 연구실(bukmunro@gmail.com)
** 한남대학교 멀티미디어공학부 강의전담 교수(ky7762@hannam.ac.kr)(° : 교신저자)
*** 한남대학교 멀티미디어공학부 교수(gcpark@hnu.kr), **** 충북대학교 전기전자컴퓨터공학부 교수(shlee@chungbuk.ac.kr)
논문번호 : KICS2007-12-545, 접수일자 : 2007년 12월 6일, 최종논문접수일자 : 2008년 7월 15일

## Ⅰ. 서 론

최근 무선 센서 네트워크는 기기의 소형화, 센싱 능력의 향상, 안전하고 효율적인 라우팅, 파워 관리 등의 연구를 중심으로 확대되고 있다[11,12]. 그러나, 센서 노드가 군대 센싱과 추적, 환경 모니터링, 환자 감시와 스마트 환경 등의 응용 분야에 적용되면서 보안 문제가 점점 대두되고 있다[1,2]. 특히, 센서 네트워크는 상호간 통신을 위해 무선 매체를 사용하기 때문에 네트워크를 구성하는 센서는 물리적 한계로 인해 기존 유·무선 기술보다 보안이 더욱 취약할 수 밖에 없다. 무선 센서 네트워크에서의 공격자는 센서 노드간 트래픽을 쉽게 엿볼 수 있고, 주변 노드에게 잘못된 정보를 제공함으로써 센서 노드의 흉내를 낼 수 있다. 이러한 문제는 센서 노드 간의 안정적인 통신을 위하여 비밀키를 설정하도록 함으로써 부분적인 해결이 가능하지만 공통의 단일 세션키가 갖는 보안 취약점 또한 존재한다[3,4,13,14,15].

BROSK(BROadcast Session Key Negotiation Protocol)에서는 센서 네트워크의 공통 단일 세션키가 갖는 보안 취약점을 개선하여 센서 네트워크에 있는 모든 센서 노드들에게 공통의 비밀키(secret key)(마스터 키)를 부여하고, 각 센서 노드는 마스터키로 암호화된 키 협상 메시지를 방송하여 이웃 노드와 세션키를 설정하는 방법을 제안하였다[5]. 그러나, 마스터키를 이용한 세션키를 형성하는 BROSK 기법은 마스터키가 모든 센서들에게 공통으로 사용되므로 마스터키의 노출이 모든 세션키의 노출로 연결되는 보안적 문제점을 가진다.

BROSK 기법의 문제점을 해결하기 위해 랜덤 키 사전 분배 기법은 두 노드가 공통으로 배분된 키를 통해 세션키를 형성하고, 동일한 세션키가 여러 노드의 세션키로 사용될 수 있는 특징이 있다. 그러나, 한 세션키의 노출이 다른 노드들 사이의 보안에 영향을 주는 문제점과 두 노드사이에 공유되는 세션키가 없을 수 있다는 단점이 있다. 이러한 취약점들을 개선하기 위해 현재까지 여러 개의 공유키를 결합하여 세션키를 생성하는 다양한 기법들이 제안되었다[5,9,10]. 그러나 이 기법들은 노드 개개의 보안성에 초점을 맞추어 대부분 연구가 진행되어왔기 때문에 데이터의 전달과정에서 데이터를 처리하고 송·수신하는 게이트웨이 역할을 하는 노드의 보안성이 매우 취약하다[13,14,15].

따라서, 이 논문에서는 무선 센서 네트워크 환경에 적합한 센서 노드의 키 저장 공간과 게이트웨이 역할을 하는 노드의 안전성을 위해 랜덤 키 사전 분배 기술과 이중 해쉬 체인을 조합한 키 사전 분배 기법을 제안한다. 제안 기법은 네트워크 사전 배치 정보 없이 게이트웨이 역할을 하는 중간 노드가 이중 해쉬 체인을 사용하여 jamming이나 eavesdropping과 같은 공격을 예방하는 랜덤 키 사전 분배를 수행하는 것을 목표로 한다. 제안된 기법의 키들은 키 풀을 설계함으로써 매우 작은 크기를 가지는 키 생성 키 셋에 표현하고 저장한다. 제안 기법은 노드 캡처에 대한 회복력을 요구하는 이전 기법보다 적은 크기의 키 링(key ring) 크기를 요구하기 때문에 적은 에너지를 사용하는 센서 네트워크에 적합하다.

이 논문의 구성은 다음과 같다. Ⅱ장에서는 지금까지 연구된 무선 네트워크 환경에서의 키 사전 방식을 분석하고, Ⅲ장에서는 무선 센서 네트워크의 중간 게이트웨이 역할을 하는 노드의 안정성을 향상시키기 위한 이중 해쉬 체인 기반의 키 사전 분배 기법을 제안한다. Ⅳ장에서는 제안된 기법에 대한 보안평가와 성능 평가 결과를 기술하고 마지막으로 Ⅴ장에서 결론을 내린다.

## Ⅱ. 관련연구

무선 센서 네트워크에서는 센서 노드를 필드에 배치하기 이전에 모든 센서 노드들에게 세션키(session key)를 형성하는데, 이러한 과정에서 사용될 키 정보를 미리 센서 노드에게 분배하고, 이를 이용하여 배치 이후에 두 센서 노드들이 공유 비밀키를 스스로 생성하는 센서 노드 협상 방법들이 사용되어 왔다. 그러나, 센서 네트워크의 공통된 단일 세션키가 갖는 단점을 보완하기 위해서 BROSK 기법에서는 모든 센서 노드에게 공통의 마스터 키(세션키가 아닌)가 할당되며, 각 센서 노드는 랜덤 번호를 생성한 후에 마스터 키로 암호화된 키 협상 메시지를 방송하여 이웃 노드와 세션키를 형성한다[5]. BROSK 기법은 통신량이 매우 적고 각 센서 노드 쌍에게 유일한 세션키를 형성할 수 있다는 장점은 있지만, 마스터 키가 모든 센서 노드에게 공통으로 사용되므로 마스터키가 노출된 경우에는 전체 네트워크의 세션키가 노출되는 단점을 가지고 있다.

Eschenhaur와 Gligor는 노드간 비밀키 공유 기법에서 발생한 센서 노드의 저장 부담을 줄이면서 보안 위험을 낮추는 랜덤 키 사전 분배 프로토콜을

제안하였다[6]. Eschenhaur와 Gligor이 제안한 랜덤 키 사전 분배 기법은 네트워크에서 사용될 많은 키들의 집합을 정의하고, 정의된 집합에서 랜덤하게 선택된 소수의 키 집합(이를 키 링이라 한다)을 각 노드가 배치되기 이전에 배분하여 세션키를 형성한다. 이 프로토콜은 배치 이전의 키 사전 분배 단계와 배치 이후의 공유키 발견 단계로 구성되며, 두 노드가 공유한 키가 있는 경우에만 세션키를 형성한다. 그러나, 이 프로토콜은 동일한 세션키가 여러 노드들 사이에서 형성되는 문제점을 가지고 있기 때문에 세션키만을 사용해서는 노드 간 안전성을 보장하지 못한다.

OKS(Overlap-Key-Sharing) 프로토콜은 매우 많은 키들의 집합 대신에 매우 긴 비트열을 이용하여 두 센서 노드가 공유한 비트열로 세션키를 생성하는 프로토콜이다[5]. 이 프로토콜은 센서 노드들에게 네트워크의 긴 비트열의 일부분을 랜덤하게 할당하여 저장하도록 한다. 각 센서 노드는 자신에게 저장된 비트열의 정보를 방송(broadcast)하고, 이웃 노드가 방송한 비트열의 정보를 수신하여 자신이 저장한 비트열과 비교한다. 그리고, 이웃 노드와 공유되는 중복되는 구간의 비트열을 해쉬 함수를 통해 일정 크기의 세션키를 형성한다. 이 프로토콜은 랜덤 키 사전 분배 방법에 비해 저장량 및 통신량은 감소되지만, 두 센서 사이의 세션키를 연결할 확률(연결성)이 줄어드는 단점이 있다.

Q 복합키 기법은 두 노드의 공유 세션키가 일정 개수(q) 이상인 경우에만 세션키를 형성하며 키 사전 분배 단계와 공유키 발전 단계로 구성된다[7]. Q 복합키 기법의 키 사전 분배 단계는 랜덤 키 사전 분배 프로토콜과 동일하게 자신의 노드 ID를 방송하고, 자신과 이웃한(통신 범위에 있는)노드 ID를 확인한다. 공유 키 발전 단계에서 각 센서 노드는 자신의 키 링에 있는 키들에 대한 퍼즐(클라이언트 Merkle 퍼즐)을 인접한 노드에게 전송한다. 인접한 노드의 퍼즐을 수신하면, 자신의 키 링에서 퍼즐에 올바른 답을 제공하는 키(이것이 두 센서 노드의 공유키)를 찾아 정답을 퍼즐로 송신한 센서에게 전송한다. 이웃 노드와의 공유키의 수가 일정 개수 이상이면 이들 공유키로부터 해쉬를 통해 두 노드 사이의 세션키를 형성한다. Q 복합키 기법은 서로 다른 센서 노드의 쌍이 동일한 세션키를 가질 확률을 낮추어 안전성을 높이고, 퍼즐을 사용하여 도청 공격에 대비한다. 그러나, 재생 공격에 대비하여 각 퍼즐을 별도의 메시지로 전송하므로 센서 노드의 가장 취약한 전력에 큰 영향을 주는 전송량을 과도하게 증가시킨 문제점이 있으며, 또한 형성된 키에 대한 상호 확인 작업이 생략되어 있다.

모바일 통신에서는 각 노드의 주소로부터 해당 노드의 고유한 공개키를 추출하는 ABK 기법이 도입되었는데, 센서 네트워크에서는 연산이 과도한 공개키 기법을 사용하지 못하므로 ABK와 유사한 개념인 노드 ID 기반의 키 생성 기법이 제안되었다[8]. 노드 ID 기반의 기법은 다중의 공유 키를 결합하여 세션키를 형성하므로 다른 세션키의 노출에도 비교적 안전하고 인접한 노드의 ID만으로 상호 협상 과정 없이 공유키의 발견이 가능하므로 전송량이 감소되는 장점이 있다. 그러나, 노드 ID 기반의 기법은 네트워크내의 어떤 센서 노드라도 두 센서 노드의 세션키를 쉽게 노출되는 보안적인 취약점이 있다. 마지막으로, 배치 이전에 세션키 형성에 필요한 키 정보를 미리 분배하고, 이를 이용하여 배치 이후에 두 센서 노드들이 공유 비밀키를 생성하는 센서 노드 협상 방법들은 미리 분배되는 정보의 공유성으로 인해 각 세션키들이 서로 독립적이지 못하는 문제점이 발생한다. 따라서, 일부 센서 노드가 공격을 받으면 다른 센서 노드의 세션키가 노출된다. 이러한 보안 문제의 해결책으로 Blom의 사전키 분배 기법[9]과 랜덤 키 사전 분배 기법[6]을 결합하여 일정한 개수 이하의 세션 노드가 공격을 받아도 다른 노드의 세션키는 안전함을 보장하는 독립 세션키 사전 분배 기법이 제안되었다[10]. 이 기법에서는 각 센서 노드의 저장량을 줄이면서, 세션키를 형성하기 위해 인접한 노드에게 자신의 ID와 사용할 매트릭스 공간의 ID 및 매트릭스 열의 생성을 위한 기본값(seed)만을 전송함으로써 전송량이 최적화되며 세션키 형성 과정이 완료된다. 하지만 일부 노드에 대한 공격으로부터 다른 세션키의 보호를 위해 Blom의 기법을 수정하여 모든 인접한 노드들 사이의 연결성을 보장하지 못해 경로 키(path key)를 도입하고 있다.

## Ⅲ. 랜덤 키 사전 분배 기술과 이중 해쉬 체인을 조합한 키 사전 분배 기법

이 절에서는 센서 노드의 키 저장 공간과 게이트웨이 역할을 하는 노드의 안전성과 에너지 효율성을 높이기 위해 랜덤 키 사전 분배기술과 이중 해쉬 체인을 조합한 효율적인 키 사전 분배 기법을 제안한다.

### 3.1 용 어

이 절에서는 제안 기법에서 사용하는 주요 용어를 [표 1]과 같이 정의한다.

표 1. 주요 용어 정의

| 개 념 | 정 의 |
|---|---|
| x,y | 센서 노드 |
| n | 센서 노드의 수 |
| S | 키 풀 크기 |
| $G_i$ | $i$ 번째 그룹 |
| $L$ | 키 체인 |
| $K_i$ | 각 센서에 할당된 $i$번째 키 풀 |
| $K_{x,y}$ | 센서 노드 x와 y 사이의 공유키 |
| $c_{x,y}$ | 센서 노드 x와 y 의 랜덤 수 |
| $g_i$ | Unique 생성 키 |
| $r_0$, $r_1$ | 서로 다른 키 체인으로부터 임의로 선택된 키의 수 |
| E() | 암호 함수 |
| h() | 해쉬 함수 |
| ‖ | XOR 동작 |

### 3.2 이중 해쉬 체인 기반의 키 사전 분배

이 절에서는 게이트웨이 역할을 하는 중간 노드의 안전한 통신을 보장하기 위한 랜덤 키 사전 분배 기법을 기술한다. 제안된 키 사전 분배 기법은 크게 키 사전 분배 구문, 클러스터 내 공유키 생성 구문, 연결 키 설립 구문 등의 3가지 구문으로 구성한다. 키 사전 분배 구문에서는 네트워크 배치 이전에 노드의 큰 키 풀과 ID를 생성한다. 각 노드는 m개의 키 링을 할당하고 랜덤하게 풀(pool)에서 추출한다. 네트워크 설정동안 사용되는 클러스터 내 공유키 복구 구문에서는 모든 노드들이 자신의 키 링 상에 존재하는 키의 ID를 브로드캐스트한다. 노드는 이러한 브로드캐스트 과정을 통해 키를 공유하는 인접한 노드에서 검색한다. 마지막으로 연결 키 설립 구문에서는 인접한 노드들과 안전한 통신을 위해 노드의 ID와 키의 쌍을 설정한다.

#### 3.2.1 키 사전 분배 구문

키 사전 분배 구문에서는 모든 노드들이 여러 그룹으로 나누어 각 그룹에 최소 $n$개의 노드로 구성한다. 동일 그룹 $G_i$에 포함되는 모든 센서 노드들은 역할 구분과 노드 구성을 제어하는 bootstrapping 프로그램을 사전에 로드한다. 그룹 $G_i$을 구성하는 센서들은 그룹 $G_i$의 키 풀 $K_i$을 가진다. 키 풀 $K$는 키 풀 크기 $S$와 키 체인의 수 $n$으로 구성한다. 센서 노드는 클러스터 대신 signature 키를 사용하여 센서 노드를 합법적으로 인증한다. 이 같은 이유는 악의적인 노드가 센서 노드의 키에 대하여 위조하지 못하게 하며 프로세스를 통해 다양한 환경 서비스에 사용하기 때문이다. 이 구문에서 사용되는 키 풀 $K$는 서로 다른 키 체인 $L$로 구성한다. $K_i$는 $K=_{C_{j,i}} \cup_{C'_{j,n-1+1}} (i=n-1,n-2,...,0,\ j=1,2,..., n)$과 $_{C_i} \cap_{C_{i+1}} = \phi (i \neq j)$로 구성된다. 각각의 키 체인 $L_i$는 유일한 생성키 $g_i$을 통해 생성하고 keyed 해쉬 알고리즘을 반복적으로 적용하여 시드($seed$)을 구한다.

$$c_{j,i}=h(c_{j,i+1};g_{j,i+1}),(i=n-1,n-2,...,0) \quad (1)$$

$$c_{j,0}=h^n(c_{j,n};g_{j,n}) \quad (2)$$

키 체인 $L$의 $i$ 번째 키는 식 (1)과 같이 랜덤 수 $c_{j,i}$을 이용하여 계산한다. 식 (2)의 $c_{j,0}$는 해쉬 함수가 $n$번 $c_{j,n}$에 적용할 때 생성된다. 식 (2)의 $h^n(c_{j,n};g_{j,n})$에서 $g_{j,n}$는 무선 센서 네트워크에서 다른 노드들과 엄격히 유지되는 비밀 정보값이다.

#### 3.2.2 클러스터 내 공유 키 생성 구문

이 절에서 기술하는 클러스터 내 공유 키 생성 구문은 게이트웨이 역할을 하는 중간 노드의 안전성을 향상시키기 위해 이중 해쉬 체인을 기반으로 동작한다. 공유키 생성 구문에서 $j$번째 해쉬 체인의 키는 $k^{j-1}$의 값을 가진다. 만약 인증이 센서 노드에 의해 요구되는 경우, 클러스터 헤드는 센서 노드의 키를 체크하고 이중 해쉬 체인을 생성한다. 이 때, 이중 해쉬 체인 중 한 개의 체인은 센서 노드에 의해 생성하고 다른 체인은 클러스터 헤드에 의해 생성한다. 이중 해쉬 체인 중에서 한 개의 체인에서 생성되는 $i$번째 키는 상호교환 순서에 따라 해쉬 함수 값 ($c'_{j,n-i+1}$)의 쌍으로 구성한다. 이 때, 센서 노드는 임의로 시드 값 $c'_{j,n}$을 선택하고 다른 체인을 생성하여 해쉬 함수에 적용한다.

[그림 1]은 클러스터 헤드와 센서 노드 사이에 이중 해쉬 체인을 생성하는 초기 과정을 나타내며, 이에 대한 세부적인 동작과정은 다음과 같다.

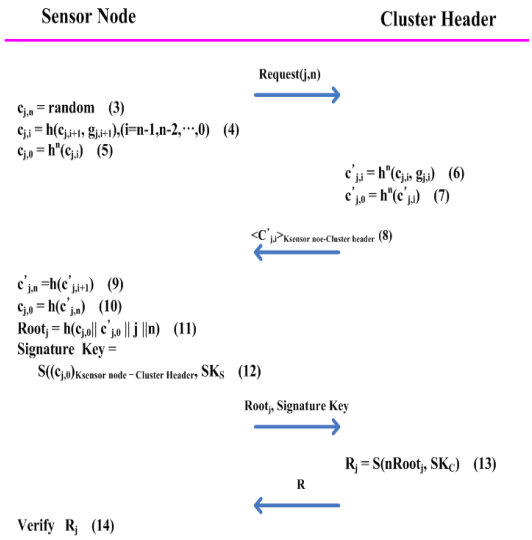


그림 1. 클러스터 내 센서 노드의 키 생성 과정

■ 단계 1 : 센서 노드 → 클러스터 헤드 : 통신 요청 메시지 전달

센서 노드에 의해 인증이 요구될 때 클러스터 헤드는 센서 노드의 정보를 체크한다. 만일 정보가 정확한 경우 키는 센서 노드에게 전달하고 정확하지 않은 경우 프로세스는 종료한다.

■ 단계 2 : 센서 노드 : 이중 해쉬 체인을 위한 정보 생성

센서 노드는 해쉬 체인의 수 $j$에 의해서 일정한 양이 서로 다른 이중 해쉬 체인을 위해 생성한다. 센서 노드는 하나의 해쉬 체인을 생성하기 위해서 식 (3)과 같이 랜덤 수 $c_{j,n}$을 선택한다. 식 (4)에서 센서 노드는 선택된 $c_{j,n}$을 해쉬 함수에 적용하여 $h(c_{j,n+1},g_{j,n+1}),(n=n-1,n-2,...,0)$와 같은 이중 해쉬 체인 중 한 개의 체인을 생성한다. 그리고, 센서 노드는 식 (5)의 루트 값 $c_{j,0}$을 생성하기 위해 해쉬 함수에 $n$번 $c_{j,n}$을 적용한다.

$$c_{j,n} \ : \ \text{random} \tag{3}$$

$$c_{j,i} = h(c_{j,i+1},g_{j,i+1}),(i=n-1,n-2,...,0) \tag{4}$$

$$c_{j,0}=h^n(c_{j,i}) \tag{5}$$

■ 단계 3 : 클러스터 헤드 → 센서 노드 : $<C'_{j,i}>_{K_{Sensor\ node-Cluster\ header}}$ 전송

이중 해쉬 체인의 또 다른 체인을 생성하기 위해서 클러스터 헤드는 식 (6)과 같이 $h^n(c_{j,i},g_{j,i})$을 이용하여 랜덤 수 $c'_{j,i}$을 선택한다. 그리고 식 (7)과 같이 n번 동안 선택된 $c'_{j,i}$을 해쉬 함수에 적용하여 $c'_{j,0}=h^n(c'_{j,i})$을 계산한다. 생성한 해쉬 체인의 시드 값은 클러스터 헤드와 공유된 센서 노드의 $K_{Sensor\ node-Cluster\ header}$ 키를 가지고 암호화한 식 (8)의 $<C'_{j,i}>_{K_{Sensor\ node-Cluster\ header}}$를 센서 노드에게 전송한다.

$$c'_{j,n} \ = \ h^n(c_{j,i},g_{j,i}) \tag{6}$$

$$c'_{j,0}=h^n(c'_{j,i}) \tag{7}$$

$$<C'_{j,i}>_{K_{Sensor\ node-Cluster\ header}} \tag{8}$$

■ 단계 4 : 센서 노드 → 클러스터 헤드 : 시그너처 키 $s((c_{j,0})_{CH-s},SK_S)$ 생성

센서 노드는 전달받은 $c'_{j,n}$을 이용하여 식 (9) ~ 식 (10)와 같이 루트 값 $c'_{j,0}$을 구한 후에 $h(c_{j,0}||c'_{j,0}||j||n)$을 이용하여 식 (11)과 같이 $Root_j$을 구한다. 식 (12)의 $Signature\ Key$는 클러스터 헤드와 센서 노드 사이의 공유된 키를 사용하여 $c_{j,0}$을 암호화한 값과 센서 노드의 비밀키를 이용하여 시그너처(signature) 키 $s((c_{j,0})_{CH-s},SK_S)$을 생성한다.

$$c'_{j,n}=h(c'_{j,i+1}) \tag{9}$$

$$c'_{j,0} \ = \ h(c'_{j,n}) \tag{10}$$

$$Root_j= \ h(c_{j,0}||c'_{j,0}||j||n) \tag{11}$$

$$Signature\ Key=S((c_{j,0})_{K_{Sensor\ node-Cluster\ header}},SK_S) \tag{12}$$

■ 단계 5 : 클러스터 헤드 → 센서 노드 : $R_j=S(n \cdot Root_j,SK_C)$

센서 노드는 생성된 $Root_j$와 $Signature\ Key$를 클러스터 헤드에게 전달한다. 전달된 값을 클러스터 헤드가 검증하고 나면, 클러스터 헤드는 식 (13)처럼 $R_j=S(n \cdot Root_j,SK_C)$을 센서 노드에게 전송한다. 여기서 $Root_j$에 표시된 값은 센서 노드에 의해 전달받은 값을 의미한다. 이 처럼 키들이 클러스터에서 분할될때, 베이스 스테이션의 프록시 시그너처 키들의 쌍들은 베이스 스테이션 대신 클러스터 헤드에게 보내지게 된다. 클러스터 헤드가 프록시 시그너처 키들의 쌍을 사용함으로써 키들에 대한 클러스터 헤드의 공정성을 검증한다.

$$R_j = S(n \cdot Root_j, SK_C) \quad (13)$$

$$Verify \quad R_j \quad (14)$$

그리고, 클러스터 헤드는 $R_j$를 센서 노드에게 전달하여 식 (14)처럼 $R_j$를 센서 노드가 검증하여 클러스터 헤드에서 전달된 키 값의 부인방지를 제공한다.

3.2.3 연결 키 설립 구문

이 절에서는 네트워크 브트스트래핑 구문동안 각 센서 노드가 인접한 노드의 키 정보를 얻기 위해서 키 링 $R_j$의 키 인덱스 정보를 브로드캐스트한다. 이 과정을 통해 각 센서 노드는 이웃 노드의 키를 인식한다. 그리고, 각 노드는 이웃 노드와 공유하는 키를 계산하거나 찾기 위해서 자신의 키 링의 키 인덱스 정보를 조사한다. 센서 노드는 $c_{j-1,0}=c_{j,n} \cdot s_{BS}$과 랜덤 수 $c_{j-1,n}$을 선택하고 n번 동안 해쉬 함수에 적용하기 위해 식 (15)과 같이 계산한다.

$$c_{j-1,0}=h^n(c_{j-1,n}), c'_{j-1,0}=h^n(c'_{j-1,n}) \quad (15)$$

그리고, 센서 노드는 BS의 프록시 시크너처 키를 사용하여 새로운 키에 대한 식 (16) ~ 식 (17)을 동의한다.

$$Root_{j-1}=h(c_{j-1,0}\|c'_{j-1,0}\|j-1\|n) \quad (16)$$

$$R_{j-1}=S(n \cdot Root_{j-1}, PSK_{BS}) \quad (17)$$

센서 노드 A는 클러스터간 통신을 위해서 다른 클러스터안에 포함된 센서 노드 B에게 다음 식 (18)을 전송한다.

$$S(c_{j-1,0}, c'_{j-1,0}, j-1, n, R_{j-1}, r_{BS}, SK_S), Cert_s \quad (18)$$

다른 지역의 클러스터내에 존재하는 센서 노드 B는 전달받은 $Cert_s$을 체크하고 BS의 공유키를 사용하여 식 (19)을 검증한다.

$$V(Root_{j-1},\ R_{j-1}, r_{BS}) = \text{true} \quad (19)$$

식 (19)의 검증 과정이 종료되면 센서 노드 B는 센서 노드 A에게 생성된 키를 전달함으로써 상호간 통신이 이루어진다.

## Ⅳ. 성능평가

이 절에서는 키 공유 확률 $P_m$가 주어졌을 때 센서 노드의 키 링 크기와 보안 강도의 관계를 평가한다. 이 절에서는 초기에 각 센서 노드가 이웃 노드와 보안 협상을 설립한 것으로 가정한다.

### 4.1 Performance Analysis

성능 평가의 수치적 평가는 [4]와 동일하게 Mathlab을 사용하여 수행한다. 제안 기법의 단순성을 위해 이 절에서는 모든 그룹 키 사전 분배에 대하여 동일한 속성 함수의 보유를 가정한다. 이 가정은 동일 저장 공간, 그룹 크기 그리고 keying material 크기를 할당하는 [4]의 모든 키 사전 분배 기술과 동일하다.

이 절에서는 키 공유 확률 $p_m$을 이용하여 센서 노드에 요구되는 저장 공간을 평가한다. 특히, 저장 공간 평가를 위해 임의 두 노드 $n_i$와 $n_j$는 최소 하나의 키에서 q개의 키까지를 공유한다고 가정하고, 키 사전분배 기법을 위해 $p_m$을 식 (18)과 같이 계산한다.

$$p_m = 1-(1-\frac{1}{s})^m \quad (20)$$

$$\Pr ob\{\hat{d}=j\}=(\frac{d-1}{j-1})P_m^{j-1}(1-p_m)^{d-j} \quad (21)$$

$$\Pr ob\{\hat{d}=j\}=(\frac{d}{j})P_m^{j}(1-p_m)^{d-j} \quad (22)$$

식 (20)에서 s 는 키 링의 크기를 의미하고 m은 키 풀(pool)의 크기를 의미한다. 또한, 식 (21) ~ 식 (22)의 $\hat{d}$는 키 풀에 할당된 셋의 수를 카운트하는 것을 의미한다. 확률 $\hat{d}$는 키 풀에서 $m$을 선택하고, 이 값은 $1 \le j \le d$를 만족하는 $j$와 같다. 따라서, $j$값을 이용하여 키 풀의 셋 수를 구하면 $1+(d\text{-}1)_{p_m}$와 같다. 키 링이 다른 노드에 할당되는 동안 확률 $\hat{d}$는 키 풀내에 $m$을 얻어 $0 \le j \le d$를 만족하는 $j$와 같다. 위 식 (18)~ 식 (20)을 기반으로 키 풀 설정의 예상 수는 $d_{p_m}$와 같다.

이 절에서 성능평가를 위해 사용되는 값은 $K$, $L$과 $(r_0, r_1)$ 쌍의 다양한 값으로 표현이 가능하다. 제안 기법에 $K$와 $L$의 큰 수가 주어졌을 때 노드 캡쳐에 대한 더 나은 의존(resilience) 속성 관찰이 가능하다. 예를 들어 제안 기법은 보안 길이를 비교하기 위해서 210개의 키가 Eschenauer 기법에서 요구된 $K$=100,000을 가지는 100개의 키보다도 더 낮게 요구된다. 비록 제안 기법이 노드 캡쳐에 대한 보안

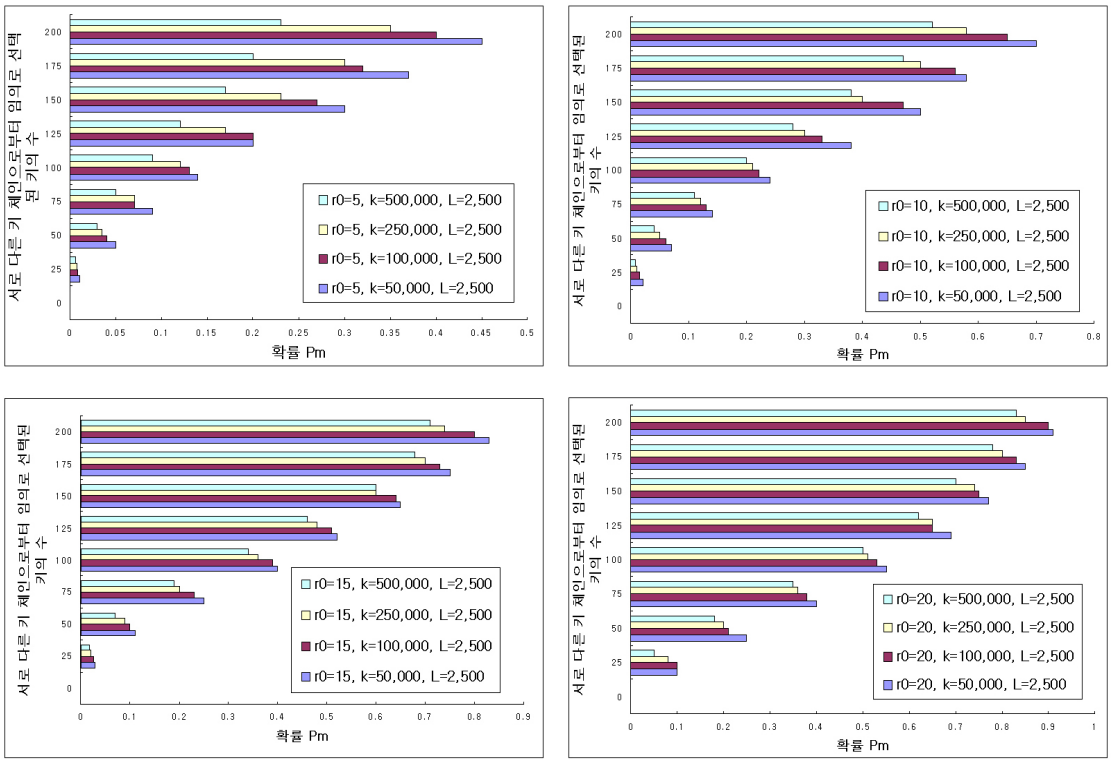


그림 2. 네크워크 크기가 n=10,000일 때, 서로 다른 키 체인으로부터 임의로 선택된 키의 수($r0$, $r1$)와 확률 $p_m$ 사이의 관계

길이가 낮아 Eschenauer 기법보다 좋지 않더라도 $R$ 값은 Eschenauer 기법보다 30 이상 낮게 나타난다. 이와 같이 유사한 보안 길이가 보장될 때 제안기법에서 요구되는 키 링 크기는 Eschenauer 기법보다 약 20% 더 낮다. 이것은 네트워크 크기가 $n$만큼 커질 경우 제안 기법이 다른 기법보다 성능 향상하는 것을 의미한다.

[그림 2]는 n=10,000이고 $p_m$=0.5 일 때, 임의로 선택된 키의 수 ($r_0$,$r_1$)와 확률 $p_m$ 사이의 보안 길이를 나타내고 있다. [그림 2]의 결과에서 제안 기법은 Eschenauer 기법의 타협된 통신 fraction이 100% 수행될 경우보다 동일 환경에서 28% 낮은 값을 가진다. 결과적으로 이런 결과는 네트워크 크기가 커질 경우 더 낮은 수치 값을 얻을 수 있어 동일 보안 강도측면에서 더 좋을 저장 공간의 효율성을 얻는다.

[그림 3]은 다양한 크기의 네트워크에서 임의로 선택된 키의 확률 $p_m$을 나타내고 있다. [그림 3]에서 나타난 것과 같이 임의로 선택된 키의 확률이 지역의 크기와 반대로 증가한다. 이러한 결과는 서로 다른 $K$,$L$과 ($r_0$,$r_1$) 쌍의 값 분석을 통해 얻은

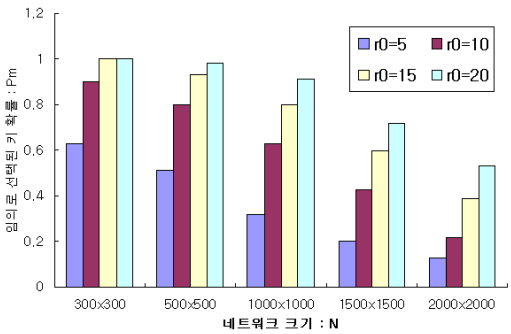


그림 3. 네트워크 크기에 따라 임의로 선택된 키 확률 $p_m$

수치 선에서 검색이가능하다. [그림 3]에서 임의로 선택된 키의 확률 $p_m$은 $\frac{2}{N}$와 비례적이다. 여기서 $N$은 센서 노드가 이동한 지역의 크기와 같다.

### 4.2 Security Analysis

제안 기법에서 키를 생성하는 해쉬 함수는 키를 생성하는 측면에서만 만족된다. 이것은 루트의 시드 값으로부터 키를 생성하거나 검증이 가능하지만 역

으로 계산이 불가능하기 때문이다. 만일 $(c_i, c_{n-i}),...,(c_{i+k},...,c'_{n-i-k})$이 인증을 위해 사용하면 제3자는 $j > i+k$인 $c_j$의 해쉬값 생성이 불가능하다. 그러므로 키 위조를 수행하기가 불가능하다. 특히, 이중 해쉬 함수를 사용하는 제안 기법은 한 개의 해쉬 함수를 사용하는 기존 기법보다 키를 구성하는 것이 더 안전하다. 만일 센서 노드가 정당하다는 것을 증명하려면 분할된 키가 체인의 시드 값인 $c'_{j-1}=c'_{j,n}$로 계산되도록 생성한 후에 인증되어야 한다. 만일 센서 노드가 $c'_{j,n} \cdot s_{BS}$로 분할되기 위해서 키의 시드 값을 설정하지 않았다면 클러스터 헤드는 센서 노드의 시드 값을 체크하거나 분할된 정당성을 검증함으로써 센서 노드의 정당성의 결정이 가능하다. 인증을 위해 센서 노드의 정보를 가지고 있는 BS는 센서 노드가 위조된 키를 생성할 때 추적이 가능하다.

센서 노드가 $(c_{j,j+1}, c'_{j,n-i})$을 이중 사용할 경우 베이스 스테이션은 키의 루트 값을 계산한 후 키를 생성한 센서 노드를 찾는다. 이것은 키 분할을 위해 사용된 한 개의 키 체인을 위해 베이스 스테이션의 루트 값을 이용하여 이전의 사용한 키의 시트 값 계산이 가능하고 그렇게 함으로써 키를 생성한 센서 노드를 찾는다. 만일 센서 노드가 키를 분할하고 분할된 키를 재사용하는 경우는 베이스 스테이션은 분할되고 생성된 키를 사용하여 생성된 키의 시드 값을 만들고 프록시 시그너처가 주어졌을 때 저장된 센서 노드 정보를 사용하여 센서 노드를 추적한다.

[그림 4]는 $n$= 10,000, $p_m$=0.5 그리고 키 링 크기 R이 168으로 고정되었을 때 제안기법의 보안 강도를 나타내고 있다. [그림 4]에서 Eschenauer이 100% 수행될 때 타협된 통신의 fraction이 동일할 경우, 제안기법이 Eschenauer 기법보다 38% 더 좋은 효율성을 나타내고 있다. 또한 [그림 4]의 결과에서는 제안 기법이 네트워크의 크기와 상관없이 보안 강도가 좋기 때문에 소규모 공격에만 보안 강도가 좋은 Chan et.al 기법보다 효율적이다.

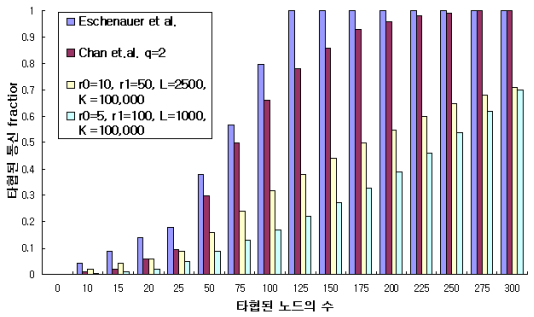


그림 4. n=10,000, $p_m$=0.5 그리고 R = 168을 가지는 보안 강도

## V. 결 론

무선 센서 네트워크에서는 유선보다 무선상에서 jamming 이나 eavesdropping이 더 쉽게 발생하기 때문에 보안은 무선 센서 네트워크에서 중요한 평가 요소 중에 하나이다. 무선 센서 네트워크에서 사용되었던 기존 키 사전 분배 기법은 각 노드들이 동작하기 위해서 많은 수의 키를 로드하기 때문에 대규모의 센서 네트워크에서는 적합하지 않다. 이 논문에서는 네트워크의 크기에 영향을 미치지 않으면서 중간 노드의 안전성을 보장하는 해쉬 체인 기반의 키 사전 분배 기법을 제안했다. 제안 기법은 센서 노드들이 모든 키들을 할당받지 않는 대신에 동일 보안 길이를 유지하면서 저장 공간을 줄이기 위해 키 풀을 이용하여 키 생성 셋에 중요 키 값을 저장하여 효율성을 극대화하였다. 특히, 제안 기법은 네트워크 크기가 클 경우 보안 공격측면에서 Eschenauer 기법과 Chan et.al 기법 보다 보안 강도 길이 측면에서 평균 13% 향상하였다. 또한, 제안기법은 네트워크 크기가 커질 경우 더 낮은 수치 값을 얻을 수 있어 Eschenauer 기법보다 동일 보안 강도 측면에서 28% 더 좋은 저장공간의 효율성을 얻었다. 향후 연구에서는 최적화된 크기에서 임의로 노드를 캡처할 경우 active 공격 종류에 따른 보안 강도를 평가할 계획이다.

## 참 고 문 헌


〔1〕 J. D. Richard and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Network", Proc. of ACM Workshop on SASN, pp.83-93, 2003.

〔2〕 S. Doshi and A. Eswaran, "A Hierarchical Security Architecture for Group Communication in Sensor Network," Project Report, 2003.

〔3〕 S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Network," Proc. of WETICE, pp.139-144, 2002.

〔4〕 H. Chan and A. Perrig, “PIKE: Peer intermediaries for key establishment in sensor networks,” Proc. of IEEE INFOCOM, 2005.
〔5〕 B. Lai, D. Hwang, S. Kim and I. Verbauwhede, “Reducing Radio Energy Consumption of Key Management protocols for Wireless Sensor Networks,” Proc. of ISLPED’04, pp.351-356, 2004.
〔6〕 L. Eschenhaur and V. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. of CCS’02, pp.41-47, 2002.
〔7〕 H. Chan, A. Perrig and D. Song, “Random Key Predistribution Schemes for Sensor Networks, Proc. of 2003 IEEE Symposium on Security and Privacy(SP’03), pp.197-213, 2003.
〔8〕 R. Pietro, L. Mancini and A. Mei, “Random Key Assignment for Secure Wireless Sensor Networks,” Proc of 1st Workshop Security of Ad Hoc and Sensor Networks, pp.62-71, 2003.
〔9〕 R. Blom, “An Optimal class of symmetric key generation systems,” Proc. of EUROCRYPT84, Lecture Notes in Computer Science, Springer-Verlag 209, pp.335-338, 1984.
〔10〕 W. Du, J. Deng and J. Katz, “A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks,” Proc. of CCS’03, pp.27!31, 2003.
〔11〕 M. Horton, et al., “Mica: The commerciatlization of microsensor motes,” Sensors Online Magazine, April 2002.
http://www.sensorsmag.com/articles/0402/40/main/shtml
〔12〕 A-S. K. Pathan, H. W. Lee, C. S. Hong, Security in Wireless Sensor Networks: Issues and Challenges, ICACT 2006, Vol.2, pp.1043-1048, Feb, 2006.
〔13〕 Xiao Chen, Jawad Drissi, “An Efficient Key Management Scheme in Hierarchical Sensor Network,” Mobile Adhoc and Sensor Systems Conference 2005 IEEE International Confercence, pp.6, Nov. 2005.
〔14〕 H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges and Solutions“, IEEE Wireless Communications, Volume 11, Issue 1, pp.38 - 47, Feb. 2004.
〔15〕 L. B. Oliveira, H. C. Wang, A. A. Loureiro, “LHA-SP:secure protocols for hierarchical wireless sensor networks,” In 9th IFIP/IEEE International Symposium on Integrated Network Management, pp.31-44, 15-19. May. 2005.

**정 윤 수** (Yoon-Su Jeong) 정회원

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** (Yong-Tae Kim) 정회원

1988년 숭실대학교 석사
2008년 2월 충북대학교 전자계산학 이학박사
2006년 3월-현재 한남대학교 멀티미디어 학부 강의전담교수
<관심분야> 모바일 웹서비스, 정보보안, 센서 웹, 모바일 통신 보안, 멀티미디어

**박 길 철** (Gil-Cheol Park) 정회원

1986년 숭실대학교 전자계산학과 석사
1998년 성균관대학교 전자계산학과 박사
2006년 UTAS, Australia 교환교수
1998년 8월-현재 한남대학교 멀티미디어학부 교수
<관심분야> multimedia and mobile communication, network security

**이 상 호** (Sang-Ho Lee) 정회원

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