센서네트워크에서 평면 그리드 기반의 키 선 분배 기법

맹 영 재[†] · Abedelaziz Mohaisen[††] · 양 대 헌[†††] · 이 경 희[††††]

요 약

무선 센서 네트워크에서는 센서 노드의 제한된 자원이 보안 기법을 디자인 하는데 많은 영향을 미치기 때문에 적은 자원을 요구하는 보안 연구가 주로 이루어지고 있다. 대칭키 암호는 키 선 분배를 필요로 하지만 요구하는 연산 량이 적기 때문에 센서 네트워크를 위한 보안 연구로 주목받고 있다. 키 선 분배는 전체 네트워크의 통신채널 보안을 위해서 노드를 배치하기 전에 키 또는 키의 재료를 각 노드에 할당하는 것이다. 이와 관련하여 다양한 연구가 이루어 졌지만 연결성과 탄력성은 아직 풀어야할 과제로 남아있다. 따라서 이 논문에서는 무선 센서 네트워크의 연결성 향상과 높은 탄력성을 제공하면서도 적은 자원을 요구하는 그리드 기반의 키 선 분배 기법을 보인다. 제안하는 기법은 평면 기반의 그리드를 이용하여 다항식을 할당하고 키를 생성한다. 제안하는 기법과 다른 키 선 분배 기법들의 네트워크 연결성, 자원의 사용량, 보안성의 비교 분석을 통하여 제안하는 기법의 효율성을 분석하였다.

키워드 : 센서 네트워크, 키 선 분배, 평면 그리드

Plat-Based Key Pre-Distribution Scheme in Sensor Network

YoungJae Maeng[†] · Abedelaziz Mohaisen[††] · DaeHun Nyang[†††] · KyungHee Lee[††††]

ABSTRACT

The security of wireless sensor networks is a challenging research area where the resources constraints are a bottleneck for any successful security design. Due to their computational feasibility, symmetric key algorithms that require key pre-distribution are more desirable for use in these networks. In the pre-distribution scheme, keys or keying materials are assigned to each node prior deployment to guarantee a secure communication within the entire network. Though several works are introduced on this issue, yet the connectivity and resiliency are imperfectly handled. In this paper, we revisit the grid based key pre-distribution scheme aiming to improve the connectivity, introduce a higher resiliency level, simplify the logic of key establishment and maintain same level of used of resources usage. The core of our modification relies on introducing the novel plat-based polynomial assignment and key establishment mechanism. To demonstrate the advantageous properties of our scheme over the revisited one, details of consumed resources, resulting connectivity, security and comparisons with relevant works are introduced.

Key Words : Sensor Network, Key Pre-Distribution, Plat-Based, 3D-Grid

1. 서 론

무선 센서 네트워크는 마이크로 전자공학, 반도체, 네트워크, 신호처리 등의 복합체이다[1]. 이 네트워크는 제한적인 자원을 가진 다수의 센서노드들로 이루어져 있으며 센서노드들은 무선 환경에서 $peer-to-peer$ 방식으로 통신하기 때문에 $Man-In-The-Middle$[3], $Sybil$[3,4], 노드 복제공격[5]등에 노출되어 있는 환경에서 서로 협력하여 주어진 임무를 수행한다[2]. 꾸준히 증가하고 있는 센서 네트워크의 응용프로그램들은 다양한 공격에 노출되어 있기 때문에 노드간의 통신에 높은 보안성을 요구한다. 현존하는 센서노드 플랫폼[1,6]에서는 제한된 자원을 근거로 연산비용이 적은 대칭키 암호기법이 효율적이지만 대칭키를 이용한 보안솔루션을 구성하는데 있어서 키 의 분배와 관련한 문제가 풀어야 할 과제중 하나로 남아있다[6,7,8]. 키를 분배하는 방법으로는 이미

※ 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10614-0)지원으로 수행되었음.
† 준 회 원 : 인하대학교 정보통신대학원 석사
†† 정 -회 원 : 한국전자통신연구원 정보보호연구단 연구원
††† 정 회 원 : 인하대학교 정보통신대학원 조교수(교신저자)
†††† 정 회 원 : 수원대학교 전기공학과 조교수
논문접수 : 2007년 10월 1일, 심사완료 : 2008년 1월 7일

DOI: 10.3745/KIPSTC.2008.15-C.1.1

Trusted Third Party, 키 분배 서버를 이용하는 기술들이 존재하지만, 센서 네트워크에서 실제로 구현하기에는 어려움이 따르기 때문에[9] 네트워크가 구성되기 전에 키를 사전에 분배하는 것을 통하여 대칭키의 단점을 극복하기 위한 연구가 이루어져왔다. 2장 에서는 이와 관련한 연구들을 소개한다.

2. 관련연구

2.1 일반적인 기법

키 선 분배와 관련한 연구 중 *Blom*등의 연구[10]에서는 전체 네트워크의 안전한 통신을 위해서 N이 네트워크 크기라고 했을 때 $N \times N$크기의 대칭행렬을 사용하고 N^2개의 키들을 각각의 노드에 저장하는 방법을 사용하였다. 노드 $s_i \in N$는 행렬에서의 열과 행 정보를 이용하여 노드 s_i와 노드 s_j가 통신하기 전, 노드 s_i가 가지는 원소 E_{ij}와 s_j가 가지는 원소 E_{ji}가 같은지 확인하여 같을 경우에만 통신이 가능하도록 한다(예, 대칭행렬이기 때문에 E_{ij}와 E_{ji}는 같다). *Du*등은[12] 키를 저장하는데 요구되는 메모리를 줄이기 위해서 보안 파라미터에 따른 공개된 행렬과 비공개 대칭행렬을 이용한 방법을 소개하였다. 이 방법 역시 대칭행렬에 기초하기 때문에 두 노드사이에 안전한 채널을 생성하기 위해서 그 노드들이 공유하고 있는 행렬 원소의 정보를 이용하였다. *Blundo*의 두 번째 연구[11]에서는 2변량 다항식(Symmetric Bivariate Polynomial)을 이용하여 노드들에 키를 분배하고 공유된 다항식의 정보를 이용하여 키를 생성하도록 하였다.

2.2 랜덤 키 선 분배 기법

무선 센서 네트워크를 위한 초기 키 선 분배 기법은 *ESCHENAUER-GLIGOR(EG)*등이 소개하였다[13]. 각각의 노드들은 키 풀(예, 2^{17}-2^{20}개의 키)에서 임의적으로 미리 정해진 수만큼의 키를 선택한다. 통신하고자 하는 두 노드가 공유된 키를 가진다면 그 키를 비밀 키로 사용하고 공유된 키가 없을 경우에는 중개노드를 통한 경로 찾기를 수행하여 키를 찾도록 한다. 이 연구에서는 메모리 사용량은 줄였으나 탄력성이 약하다는 단점을 가진다(예, 손상된 노드의 수가 적더라도 다른 노드들의 통신 문제를 야기한다). 탄력성을 향상시키기 위해서 *Chan*등이 제안한 *Q-COMPOSITE*[14]은 [13]에서 제안된 기법과 기본적으로 같은 프로시저를 이용한다. 두 노드사이에 공유된 키가 미리 정해진 개수 이상일 때만 그 개수만큼의 키를 해시하고 이 해시값을 두 노드의 통신을 위한키로 사용한다. 그렇지 않을 경우에는 중개노드들이 사용된다. 확률적인 기법의 더 나아간 분석은 [15]에서 보였다.

2.3 대칭 행렬에 기반을 둔 키 선 분배 기법

*Blom*의 기법[10]을 향상시키기 위해서 *Du*등은 [16,12]기법을 제안했다. 그 중 하나는 *Blom*의 기법[10]에 비해 불필요한 메모리, 통신, 연산을 피하면서 적합한 연결성을 보이는 지식분배 기반의 기법을 보였다[16]. [12]에서는 [10,13]에 기초하는 *multi-space* 행렬 기법이 소개되었다. 두 노드 사이에서 적어도 하나의 *space*를 공유시키기 위한 방법으로 미리 만들어진 행렬들 중에서 임의의 비공개 행렬들을 선택한다. 이 비공개 행렬들을 이용하여 생성한 행렬의 임의의 열들을 노드들에 할당하고 통신하고자 하는 두 노드가 공통된 *space*를 가진다면 *Blom*의 나머지 과정을 수행하도록 한다. 공통된 *space*를 찾을 수 없다면 키 경로를 설정하기 위해서 중개 역할을 하는 *space*를 찾는다. 이 방법은 메모리 사용량과 통신량을 많이 요구하면서도 낮은 연결성을 제공하지만 [13,14]의 연구에서보다 높은 탄력성을 보인다. *Ito*[17]는 [16]에 기초하여 확률적인 분배함수를 이용한 방법을 소개하였으며 여러 분배기법들의 실제 에러 비율을 측정해 보였다.

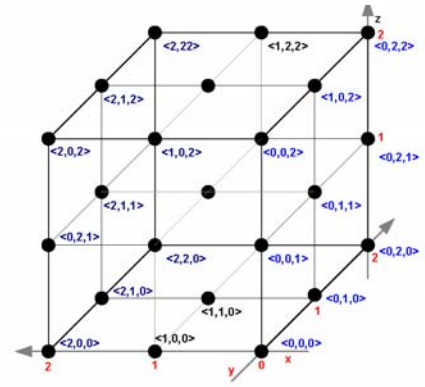
2.4 대칭 Bivariate 다항식 기반의 기법

같은 시기에 *Liu*는 주로 [11]에 기반을 두는 기법들[9,18]을 보였다. *Blundo*의 기법[19]에서는 EG기법[13]과 비슷하게 각 노드에 다항식을 할당하는 방법과 네트워크 크기가 N일 때, $N^{1/2} \times N^{1/2}$ 그리드를 이용한 2차원 분배환경을 제공하는 방법을 소개하였다. 이 기법에서, 노드들은 그리드상의 교차점에 분배되고 그리드의 열과 행에 따라 다항식들이 할당된다. 두 노드가 같은 SBP를 공유하고 있다면, [11]에서와 같은 직접적인 키 생성이 수행되며 같은 SBP를 공유하고 있지 않을 경우에는 간접적인 키 생성을 위해 중개노드를 이용한다. 이 방법은 손상된 노드의 수가 네트워크의 절반을 차지하더라도, 중개노드를 이용하여 키를 찾을 수 있기 때문에 네트워크는 안전한 채널을 생성하여 통신할 수 있다. n차원의 기법은 [18]에서 소개되었다.

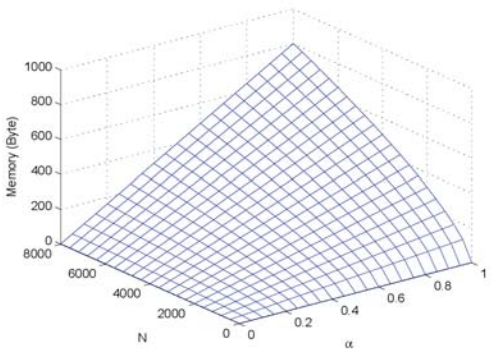
이 논문에서는 [9, 18]의 연구에서 보인 3차원 그리드 기반의 키 선 분배 기법을 향상시키기 위해서 평면에 기반을 두는 다항식과 확장된 차수의 그리드를 이용한 기법을 소개한다. 또한 3차원 그리드 상에서 노드/다항식의 분배, 연결성과 보안 성능 향상의 성능분석을 포함하며 자원 사용량의 명세와 요구된 자원에서의 통신 트래픽 모델링의 효과에 대해서도 보인다. 3장에서는 제안하는 기법의 상세를 보이고 4장에서는 연결성과 자원 사용량, 성능과 보안성에 대해 분석한다. 5장에서는 제안하는 기법과 다른 기법들의 비교를 보이고 6장에서는 결론을 담는다.

3. 평면에 기반을 두는 다항식과 그리드 기반의 키 선 분배 기법

제안하는 기법은 (그림 1)에서와 같이 3차원 그리드를 이용한다. 네트워크 크기가 N이라고 가정했을 때 3차원 그리드는 각각 $N^{1/3}$길이의 x,y,z축을 가지며 각 축에 따른 좌표는 C_x, C_y, C_z로 표현한다. 노드들은 그리드의 교차점에 따라 배치되고 배치된 i번째의 노드 s_i는 세 축의 좌표정보



(그림 1.a) 평면에 기반을 두는 다항식을 적용한 그리드의 구조



(그림 1.b) 네트워크 크기와 보안 파라미터에 따라 다항식을 저장하기 위해 요구되는 메모리

(C_x, C_y, C_z)를 가진다. 노드들이 배치된 후, 같은 축(평면)에 해당하는 노드들은 동일한 다항식을 공유하도록 노드가 위치한 그리드의 축에 따라 다항식을 할당한다. 각 노드는 그 노드가 위치한 축의 좌표에 대응하는 세 개의 다항식을 가지기 때문에 네트워크에 필요한 전체 다항식의 개수는 $3(N^{1/3})$가 된다. 아래에서 키 재료 생성과 안전한 키 설정 과정을 보인다.

3.1 키 재료의 할당과 식별자 구조

키 관리 서버에서는 다음과 같은 프로시저가 한번 실행된다.

- (그림 1)의 그리드를 만들기 위해서 $m=[N^{1/3}]$을 정한다. 이때 N은 유연한 확장성을 보이기 위해 실제 네트워크의 사이즈보다 크게 정하여 노드들의 참여와 탈락을 자유롭게 한다.
- 그리드 상에 위치한 센서노드 s_i는 $\lg N$비트의 식별자 $i=<c_x \| c_y \| c_z>$를 가진다.
- 키 관리 서버는 $3\times m$개의 대칭 다항식을 생성한다. 각 다항식은 함수 $f(x,y)$가 $finite\,field$ F_q(q는 충돌을 피하고 더 나은 보안성을 위해서 N보다 크게 정함)상에서 계수들이 랜덤하게 선택되었을 때, $f(x,y)=f(y,x)$를 만족한다.
- 모든 다항식들은 세 개씩 짝을 지어 m개의 그룹을 구성하며 각 그룹은 $<f_{c_x}; f_{c_y}; f_{c_z}>$와 같이 표기한다.
- [19]와는 다르게, 식별자 $<c_x \| c_y \| c_z>$를 가지는 각 노드는 식별자와 대등한 인덱스(c_x, c_y, c_z)를 가지는 세 개의 다항식을 선택한다(i.e. 같은 평면에 있는 노드들은 동일한 다항식을 갖는다).
- 서버는 각 센서 노드 s_i(i는 노드 식별자, 다항식 $<f_{c_x}; f_{c_y}; f_{c_z}>$를 가짐)의 공유정보$g_{c_x}=f_{c_x}(i,y), g_{c_y}=f_{c_y}(i,y), g_{c_z}=f_{c_z}(i,y)$를 확인한 후에 이 공유정보들을 센서 노드 s_i의 메모리에 저장한다.

이러한 과정을 통해 같은 축(예, 같은 차원의 같은 평면에 속한)에 속한 노드들은 같은 다항식을 가지게 된다.

3.2 키 생성

제안하는 기법은 손상된 노드의 수가 제한 수이하라면 두 노드가 공유하고 있는 다항식을 통해 직접적으로 통신하는 것이 가능하다. 손상된 노드의 수가 그 이상이라면, 중개노드를 이용하여 키를 생성하도록 한다. 아래에서 여러 경우들을 보인다.

3.2.1 직접적인 키 생성

식별자 $i=<c_x \| c_y \| c_z>$, $j=<c_x \| c_y \| c_z>$를 가지는 두 노드 s_i와 s_j가 $i.c_x=j.c_x$ 또는 $i.c_y=j.c_y$ 또는 $i.c_z=j.c_z$일 때, s_i와 s_j는 하나이상의 동일한 차원에 속해있다는 것을 뜻하고 이는 적어도 하나의 다항식을 공유하고 있다는 것으로, 공통된 키를 생성하기 위해 공유된 다항식 $g^*(y)$를 이용한다. 만약 $i.c_x=j.c_x$와 $i.c_y=j.c_y$ 또는 $i.c_x=j.c_x$와 $i.c_z=j.c_z$ 또는 $i.c_y=j.c_y$와 $i.c_z=j.c_z$이면 손상이 적은 것을 택하고 공통된 다항식을 이용하여 키를 생성한다(모든 좌표정보가 동일하다면 자기 자신을 뜻한다). 마지막으로 두 노드가 동일한 평면에 존재하지 않다면 하나 또는 그 이상의 중개노드들이 간접적인 키 생성을 위해 이용될 수 있다.

3.2.2 간접적인 키 생성

만약 두 노드가 위치한 평면을 찾을 수 없다면 중개 노드들을 통하여 키 경로를 생성해야 한다. 식별자 i, j를 가지는 노드 s_i, s_j는 다음 중 어느 것이라도 만족하는 $s_\varnothing$를 뽑는다($\varnothing$는 식별자).

- $\varnothing.c_x=i.c_x$이고 $\varnothing.c_y=j.c_y$또는$\varnothing.c_z=j.c_z$
- $\varnothing.c_y=i.c_y$이고 $\varnothing.c_x=j.c_x$또는$\varnothing.c_z=j.c_z$
- $\varnothing.c_z=i.c_z$이고 $\varnothing.c_x=j.c_x$또는$\varnothing.c_y=j.c_y$

위와 같은 방법으로 $\varnothing$안에 상응하는 공유들은(적어도 두 개) 노드 $s_\varnothing$를 중개노드로 이용한다. 예로, 첫 번째의 경우 아래와 같이 키를 생성할 수 있다.

$$k_{\varnothing i}=g_{cx}^{\varnothing}(i), k_{i\varnothing}=g_{cx}^{i}(\varnothing), k_{\varnothing j}=g_{cx}^{\varnothing}(j), k_{j\varnothing}=g_{cx}^{j}(\varnothing) \quad (1)$$

다른 경우에 있어서도 같은 방식으로 키를 생성한다.

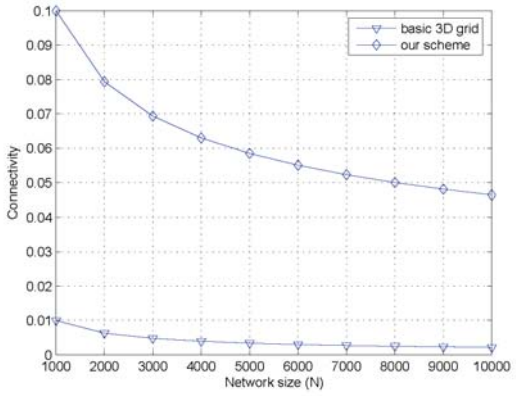
4. 분석

4.1 통신의 분배

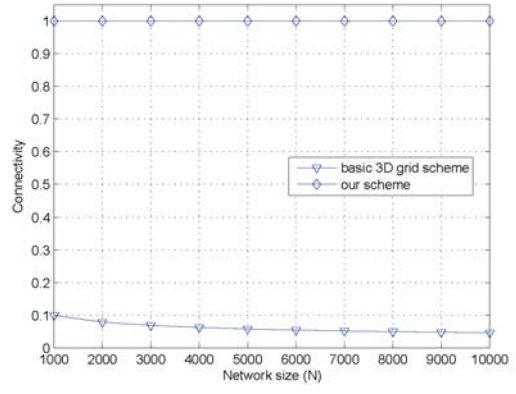
무선 네트워크에서의 통신은 지역 R의 확률적인 분배 함수 f_R에서의 통신 트래픽 함수를 이용하여 분배하도록 디자인하였다. 이 장점을 이용하기 위해서 노드들이 연관되어 있는 영역과 평면들에 정의된 $f_R(n)$을 이용한다. 다시 말해서, n은 공격자가 존재하지 않는 환경에서의 홉의 수를 뜻한다.

4.2 연결성

일반적으로 연결성은 부분적인 네트워크의 노드들이 자신의 키 재료를 가지고 단일 홉으로 통신할 수 있는 확률로 정의된다. 제안하는 기법에서는 3차원 그리드에서 노드들이 위치한 축의 평면에 따라 할당된 다항식이 실제 연결성을 향상시키는데 중요한 역할을 한다. $m=N^{1/3}$이라 할 때, 제안하는 기법의 실제 연결성은 $\frac{3}{m+1}$에 근접한 $C_{actual}=3(\frac{m^2-1}{m^3-1})$이다. 제안하는 기법보다 간단한 그리드 기법에서의 단일 홉 연결성은 제안하는 기법보다 작은 $C_{actual}=3(\frac{m-1}{m^3-1})=(\frac{3}{m^2+m+1})$[18]이다. (그림 2.a)(단일 홉)와 (그림 2.b)(두 단계 홉)는 제안하는 기법과 이전 기법의 비교를 보여준다. 제안하는 기법은 $\frac{3}{m+1}>\frac{3}{m^2+m+1}$ $(N>0)$이기 때문에 언제나 [18]에서의 연결성 보다 좋은 결과를 보인다. 실제로 그리드가 구성될 수 있는 최소의 네트워크 크기보다 적은 사이즈 $m=2$인 $N=8$네트워크에서도 제안하는 기법의 연결성이 더 높게 나타났다.



(그림 2.a) 단일 홉의 연결성



(그림 2.b) 두 단계 홉의 연결성

4.3 메모리 오버헤드

메모리 사용량은 요구되는 보안 레벨에 의존한다. $0\le\alpha\le1$일 때 (α)를 공유된 다항식[15]을 가진 노드의 보안 레벨을 결정하는 파라미터라고 했을 때 다항식 $x^0,x^1,...,x^t$의 계수 $a_0,a_1,...,a_t$를 저장하는데 필요한 메모리는 $(t+1)\lg(q)$비트이며 이는 $(\alpha\times m+1)\times\lg(q)$와 같다. N_c를 손상된 노드의 수라고 보았을 때 요구되는 메모리 M은 아래와 같다.

$$M=3((N_c+1)\lceil\lg(N^{1/3})\rceil+(t+1)\lg(q)) \quad (2)$$

4.4 통신 오버헤드

보안과 관련된 통신 오버헤드는 두 노드의 식별자를 교환할 때 발생한다. 노드들이 손상되었을 때, 키 생성은 크게 두 경우로 나눌 수 있다. 첫 번째의 경우는 단일 식별자 교환을 요구하는 직접적인 키 생성이며 두 번째 경우는 두 개의 식별자와 한 개의 중개노드를 필요로 하는 방법이다. 앞서 언급한 식별자 구조에 따라 표현하는 데는 $3\lg(N^{1/3})$비트가 요구된다. 평균적으로 요구되는 비트단위의 통신 오버헤드는 다음과 같이 식별자들을 교환하는 두 경우와 같다.

$$C_{com_{avg1}}=\frac{1+2}{2}\times3\lceil\lg(\sqrt[3]{N})\rceil=4.5\lceil\lg(\sqrt[3]{N})\rceil \quad (3)$$

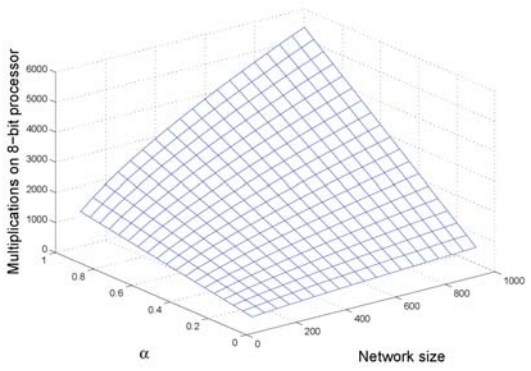
통신 트래픽 함수의 사용을 고려한 실용적인 모델에서는 통신 오버헤드가 다음과 같다.

$$C_{com_{avg2}}=3\lceil\lg(\sqrt[3]{N})\rceil\sum_{i=1}^{n}if_R(i) \quad (4)$$

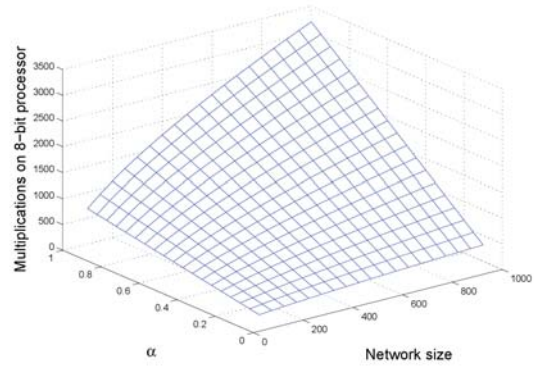
4.5 연산 오버헤드

두 노드가 같은 평면에 위치할 경우 차수 t의 다항식 확인이 필요하다. 그렇지 않을 경우 두 번 또는 그 이상의 다항식 확인이 요구된다. 일반적인 경우에 $f_R(n)$은 네트워크 수명의 $running-time$동안에 요구되는 평균적인 연산량을 결정하는데 쓰인다. 첫 번째의 경우 $m=N^{1/3}$일때 $t=\alpha\times m^2$ 차수의 다항식을 확인하기 위해 큰 정수의 곱하기 연산이 $C_m=2t-3$번 요구되며 두 번째의 경우에 요구되는 연산은 아래와 같다.

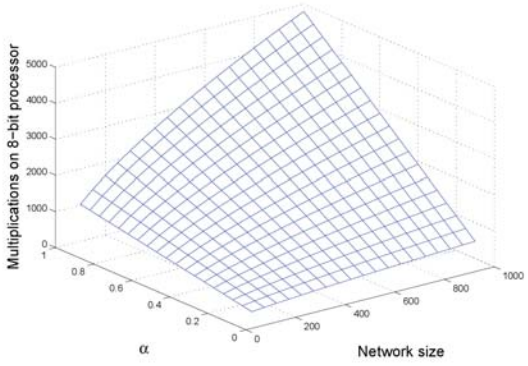
$$C_c=C_m\sum_{i=1}^{n}if_R(i) \quad (5)$$



(그림 3.a) q = 64의 연산 오버헤드 ($F(n)=\frac{c}{2^n-1}$)

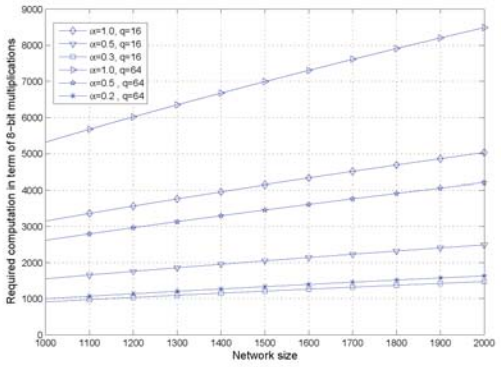


(그림 3.b) q' = 16의 연산 오버헤드 ($F(n)=\frac{c}{2^n-1}$)



(그림 3.c) q' = 16의 연산 오버헤드

[19]에 기초하여, 16 또는 64비트의 *finite field*에서 두 정수의 곱하기는 각각 16 또는 27번의 8비트 곱하기 연산이 요구된다. (그림 3)과 (그림 4.a)는 16비트와 64비트의 *finite field*에서 보안 파라미터의 수치에 따라 요구되는 연산의 비교를 보인다. (그림 3.c)는 $F_R(n)$를 제외한 연산이며 (그림 3.(a,b))와 비교했을 때 연산량이 확연히 증가한 것을 볼 수 있다.



(그림 4.a) 8비트 워드 프로세서에서의 곱셈 연산량

4.6 보안성 분석

다항식에 기반을 두는 기법의 보안성은 $t+1$보다 적은 수의 노드들이 손상되었을 때에도 다항식이 안전하다는 사실에 기초한다. 아래에서 제안된 기법의 다양한 상황에 따른 보안성을 분석한다.

4.6.1 한 개 노드의 공격

하나의 노드는 하나의 다항식을 생성하는데 필요한 공유정보 중 하나만을 가진다(나머지 두 개의 공유정보는 각각 다른 2개의 다항식을 생성하는데 필요하다). 그러므로 한 개의 노드가 손상되었다 하여도 해당 센서가 저장하고 있는 공유정보 이상의 정보 누출을 초래하지 않는다.

4.6.2 한 평면의 공격

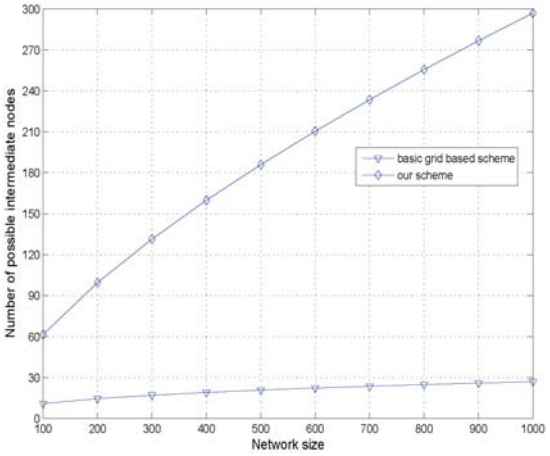
$\alpha=1$일 때, 같은 한 평면에 있는 노드들이 공유하고 있는 공유정보들은 다항식을 복구하기 위해 사용될 수 있다. 이러한 경우에 대한 확률 p_c는 아래와 같다(N_c가 손상된 노드의 수).

$$p_c = 1-\sum_{i=0}^{t}\left(\frac{(N^{2/3})!}{i!(N^{2/3}-i)!}\right)(F_c)^i(1-F_c)^{N^{2/3}-i} \qquad (6)$$

F_c는 부분적인 N_c를 뜻하고, i는 주어진 다항식의 공유 중 손상된 공유의 수, N은 네트워크 사이즈이다. 예로, $N=1000$이고 $F_c=0.5$일때 제안된 기법에서는 $p_c \approx 0.2$이고 같은 조건의 [18]에서는 $p_c \approx 0.4$로 나타났다.

4.6.3 네트워크를 통한 공격

위와 같은 접근으로 전체 네트워크를 공격하여 모든 다항식을 손상시킨다면 노드들 사이의 통신 보안을 무너트릴 수 있다. 하지만 손상된 노드들에 의해 노출된 공유정보의 상당수가 겹치는 것으로 많은 다항식을 계산해 낼 수 있다 하여도 이것은 손상된 노드들의 연결에만 영향을 주기 때문에 그 외의 네트워크는 안전할 것이고 노출된 공유정보의 수가 a에 의해 결정되는 임계값보다 적으면 노출된 공유정보는 무시될 것이다.



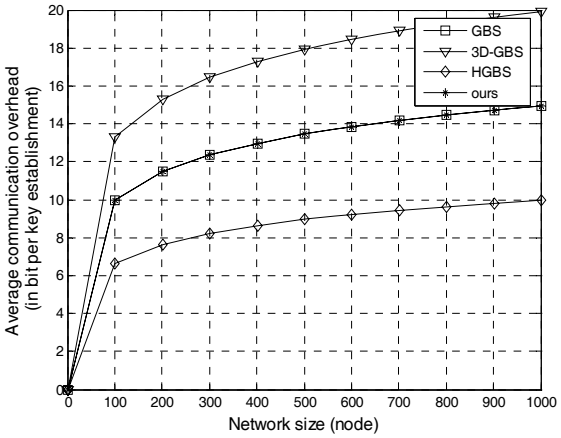
(그림 4.b) 두 단계 홉에서 중개노드 발견 확률

4.6.4 키 패스 생성을 위한 중개노드 가능성

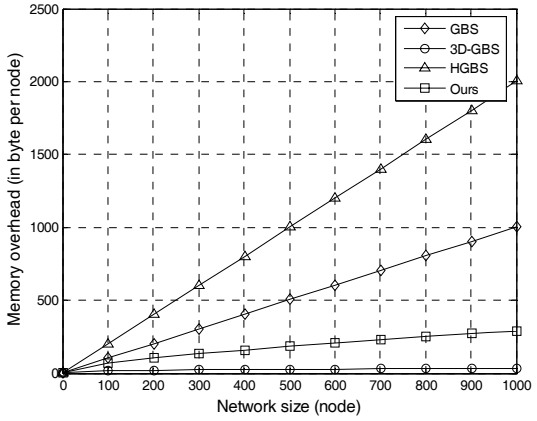
제한된 수의 노드가 손상되었다고 가정했을 때, 두 단계 홉을 통해 키 경로를 생성할 수 있는 중개노드의 가능성은 이전의 그리드 기법[18]이 보이는 $3\sqrt[3]{N}$과는 다르게, 제안하는 기법은 $(3\sqrt[3]{N})^2$ 을 제공한다. (그림 4.b)는 제안하는 기법과 [18]의 비교를 나타낸다.

5. 다른 기법들과의 비교

제안하는 기법의 보안수준은 [9]연구에서의 보안수준과 같다. 제안하는 기법과 다른 기법들의 비교는 4장에서의 자원 사용량에서 보였으며 <표 1>에서는 센서 네트워크에서의 다른 키 선 분배 기법들과의 비교를 보인다. 이 비교는 그리드 기반의 기법과 3차원 그리드 기반의 기법[9], 계층적 그리드 기법[20], Du등의 기법[12], 제안하는 기법을 포함한다. 제안하는 기법은 상대적으로 [9,18]과 비교 할만하다. 또한 연결성과 관련한 장점은 위에서 보였다. (그림 5-8)에서는 네트워크 크기 N이 1에서 1000, $q=14$, $a=0.5$라고 했을 때, 제안하는 기법과 다른 기법들과의 통신량, 메모리 사용량, 연산량, 연결성의 비교를 보여준다.



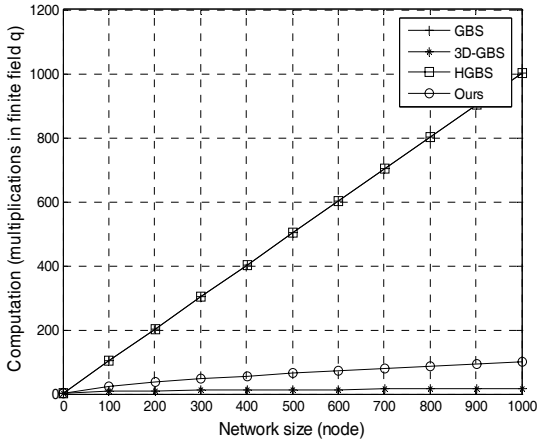
(그림 5) 키 생성에 필요한 비트단위의 평균적인 통신량 비교



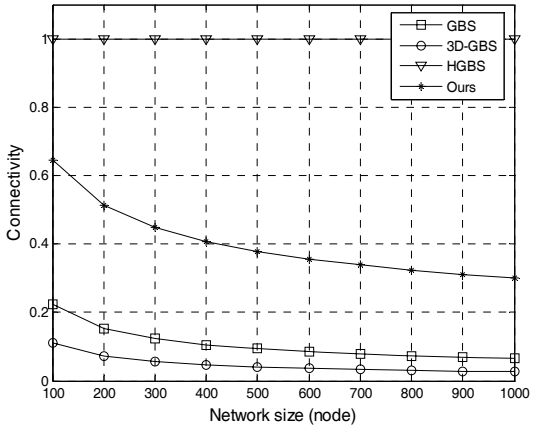
(그림 6) 각 노드에 필요한 바이트단위의 메모리 사용량 비교

<표 1> 제안하는 기법과 다른 기법들과의 자원 사용량과 연결성 비교.

Scheme	Communication	Computation	Memory	Connectivity
GBS [18]	c	SBP Evaluation	ID + 2 SBP	$\frac{2}{N^{1/2}-1}$
3D-GBS [18]	c	SBP Evaluation	ID + 3 SBP	$\frac{3}{N^{2/3}+N^{1/3}+1}$
our scheme	c	SBP Evaluation	ID + 3 SBP	$\frac{3}{N^{1/3}}$
EG [13]	$Cg(S_k)$	$\frac{(2C+p-p_k)}{2}lg(C)$	S_k keys	$1-\frac{((P-k)!)^2}{(P-2k)!P!}$
CPS [14]	Constant	c	S_k keys	$\frac{m}{N}$
DDHV [12]	$Cg(n\times\tau)$	2 vectors mult.	τ+1 vectors	$1-\frac{((\omega-\tau)!)^2}{(\omega-2\tau)!\omega!}$
HGBS [20]	c	SBP Evaluation	ID + n SBP	1



(그림 7) finite field q 에서의 곱하기 연산량 비교



(그림 8) 제안하는 기법과 다른 기법들과의 연결성 비교

6. 결 론

이 논문에서는 센서 네트워크에서의 연결성 향상을 위해서 대칭 2변량 다항식을 이용하고 그리드 구조상에 배치된 노드들의 대칭키를 생성하는 평면 그리드 기반의 키 선 분배 기법을 소개하였다. 논문에서 보인 기법에서는 평면에 기반을 두는 다항식을 이용하여 보안성을 유지함과 동시에 연결성을 향상시켰음을 다른 키 선 분배 기법들과의 요구되는 연산과 통신, 메모리의 성능을 분석, 비교하였다. 제안하는 기법은 한층 향상된 연결성을 제공하고 큰 네트워크를 포함하는 전망 있는 응용프로그램들에 실현가능한 기법이 될 것이다.

참 고 문 헌

[1] Culler, D., Estrin, D., Srivastava, M.B.: Overview of sensor networks, pp.41-49 IEEE Computer Society Press, Los Alamitos (2004)

[2] Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks (2002)

[3] Newsome, J., Shi, E., Song, D.X., Perrig, A.: The sybil attack in sensor networks: analysis & defenses. In: IPSN, pp.259 - 268 (2004)

[4] Zhang, Q., Wang, P., Reeves, D.S., Ning, P.: Defending against sybil attacks in sensor networks. In: ICDCS Workshops, pp.185 - 191 (2005)

[5] Parno, B., Perrig, A., Gligor, V.D.: Distributed detection of node replication attacks in sensor networks. In: IEEE Symposium on Security and Privacy, pp.49 - 63 (2005)

[6] Pietro, R.D., Law, Y.W., Etalle, S., Hartel, P.H., Havinga, P.: State of the art in security of wireless sensor networks. IEEE Computer 35, 1 - 10 (2002)

[7] Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Commun. ACM 47, 53 - 57 (2004)

[8] Tillet, J., Ziobro, J., Sharma, N.K.: Secure wireless sensor networks: Problems and solutions. Journal on Systemic, Cybernetics and Informatics 1, 1 - 11 (2004)

[9] Liu, D., Ning, P.: Establishing pairwise keys in distributed sensor networks. In ACM CCS, pp.52 - 61 (2003)

[10] Blom, R.: An optimal class of symmetric key generation systems. In: Proc. of the EUROCRYPT 1984 workshop on Advances in cryptology: theory and application of cryptographic techniques, Paris, France, pp.335 - 338. Springer, Heidelberg (1985)

[11] Blundo, C., Santis, A.D., Herzberg, A., Kutten, S., Vaccaro, U., Yung, M.: Perfectly-secure key distribution for dynamic conferences. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol.740, pp.471 - 486. Springer, Heidelberg (1993)

[12] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur. 8, pp.228 - 258 (2005)

[13] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: ACM CCS, pp.41 - 47 (2002)

[14] Chan, H., Perrig, A., Song, D.X.: Random key predistribution schemes for sensor networks. In: IEEE Symposium on Security and Privacy, p. 197 (2003)

[15] Hwang, J., Kim, Y.: Revisiting random key pre-distribution schemes for wireless sensor networks. In: SASN, pp.43 - 52 (2004)

[16] Du,W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor

networks using deployment knowledge. In: INFOCOM (2004)
[17] Ito, T., Ohta, H., Matsuda, N., Yoneda, T.: A key pre-distribution scheme for secure sensor networks using probability density function of node deployment. In: SASN, pp.69 - 75 (2005)
[18] Liu, D., Ning, P., Li, R.: Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur. 8, pp.41 - 77 (2005)
[19] Liu, D., Ning, P.: Establishing pairwise keys in distributed sensor networks. In: ACM CCS, pp.52 - 61 (2003)
[20] Mohaisen, A., Nyang, D.: Hierarchical grid-based pairwise key pre-distribution scheme for wireless sensor nets. In: EWSN, pp.83 - 98 (2006)

맹 영 재
e-mail : brendig@seclab.inha.ac.kr
2006년 8월 인하대학교 컴퓨터 공학과
2006년 9월～현재 인하대학교 정보통신 대학원(석사)
관심분야 : 인터넷 보안, 네트워크 보안

아 지 즈
e-mail : asm@seclab.inha.ac.kr
2005년 2월 가자대학교 컴퓨터공학과
2007년 8월 인하대학교 정보통신대학원(석사)
2007년 9월～현재 한국전자통신연구원 정보보호연구단 연구원
관심분야 : 네트워크 보안, 암호프로토콜

양 대 헌
e-mail : nyang@inha.ac.kr
1994년 2월 한국과학기술원 과학기술 대학 전기 및 전자 공학과
1996년 2월 연세대학교 컴퓨터 과학과(석사)
2000년 8월 연세대학교 컴퓨터 과학과(박사)
2000년 9월～2003년 2월 한국전자통신 연구원 정보보호연구본부 선임연구원
2003년 2월～현재 인하대학교 정보통신대학원 조교수
관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희
e-mail : khlee@suwon.ac.kr
1989년 서울대학교 식품영양학과(학사)
1993년 연세대학교 전산과학과(학사)
1998년 연세대학교 컴퓨터과학과(석사)
2004년 연세대학교 컴퓨터과학과(박사)
1993년 1월～1996년 5월 LG소프트(주) 연구원
2000년 12월～2005년 2월 한국전자통신연구원 선임연구원
2005년 3월～현재 수원대학교 전기공학과 조교수
관심분야 : 영상처리, 컴퓨터비전, 인공지능, 패턴인식, 생체인식, 얼굴인식, 다중생체인식