WSN에서의 효율적 통신을 위한 인증서 폐지 목록 표현 기법

맹 영 재[†] · 아 지 즈[†] · 양 대 헌[††] · 이 경 희[†††]

요 약

WSN의 보안 알고리즘은 센서노드의 제한된 자원을 근거로 비교적 적은 연산과 적은 메모리를 필요로 하는 대칭키를 이용하여 주로 연구되어 왔다. 하지만 공개키와 관련한 최근의 연구들은 실제 측정을 통해 센서노드가 가진 적은 자원으로도 공개키가 사용 가능하다는 것을 보였으며 WSN에서 공개키의 사용을 가정한다면 자원 절약적인 키 관리 방법이 필요하다. 이 논문에서는 공개키의 중요한 키 관리 작업 중 하나인 인증서 폐지를 위한 두 가지 효율적인 인증서 폐지 목록 표현 기법을 소개한다. 첫 번째는 broadcast encryption에서 사용되는 CS(Complete Subtree)를 이용하는 기법이고 두 번째는 인증서의 유효성을 이진벡터로 표현한 새로운 기법인 BVS(Bit Vector Scheme)이다. BVS 및 CS를 이용하여 통신 오버헤드를 얼마나 줄일 수 있는지 보이고 관련된 방법들의 비교로 결론을 내린다.

키워드: 인증서 폐지, 키 선분배, 센서 네트워크, 공개키, RLE, Bit Vector

Communication-Efficient Representations for Certificate Revocation in Wireless Sensor Network

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

ABSTRACT

In this paper, we introduce a set of structures and algorithms for communication efficient public key revocation in wireless sensor networks. Unlike the traditional networks, wireless sensor network is subjected to resources constraints. Thus, traditional public key revocation mechanisms such like the ordinary certificate revocation list is unsuitable to be used. This unsuitability is due to the huge size of required representation space for the different keys' identifiers and the revocation communication as the set of revoked keys grow. In this work, we introduce two communication-efficient schemes for the certificate revocation. In the first scheme, we utilize the complete subtree mechanism for the identifiers representation which is widely used in the broadcast encryption/user revocation. In the second scheme, we introduce a novel bit vector representation BVS which uses vector of relative identifiers occurrence representation. We introduce different revocation policies and present corresponding modifications of our scheme. Finally, we show how the encoding could reduce the communication overhead as well. Simulation results and comparisons are provided to show the value of our work.

Key Words: Certificate Revocation, Key Pre-Distribution, Run Length Encoding, Cover Set Problem, Sensor Networks.

1. 서 론

WSN는 메모리, 연산, 통신 등의 자원이 제한된 많은 수의 작은 센서 노드로 이루어져 있다. 센서 노드에서 통신을 위한 연산은 디바이스 내부의 명령어 처리보다 더욱 많은 양의 자원을 필요로 하는데 실례로, 기존의 센서노드 플랫폼의 100미터 링크에서 1k 비트를 전송하는데 약 3백만 개의 명령어를 필요로 한다[11]. 이렇게 자원이 제한적인 WSN의 특성 때문에 센서노드에서 감지된 데이터를 보증하기 위한 많은 보안 프로토콜과 기법 그리고 오버헤드를 측정하는 접근들은 주로 대칭키 암호로 연구되어 있다. 센서노드에서 대칭키 암호는 공개키 암호에 비해 필요로 하는 연산이 적으며 저장 공간과 통신량도 상대적으로 적게 든다. 8비트 환경을 위한 대칭키 암호의 짧은 키와 간단한 프로토콜 디자인 때문에 요구사항 역시 제한적이다. 대칭키 암호가 불리한 점은 통신하려는 양쪽 모두 반드시 키를 안전하게 교환해야 한다는 것이다. 이 문제에 관련된 많은 연구들 중 키 선분배 기법이 가장 효과적인 해결법으로 알려져 있으며[1-4] 키 선분배 기법에서는 안전한 통신을 위해 미리

※ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-C1090-0603-0028)
† 준 회 원 : 인하대학교 정보통신대학원 석사
†† 정 회 원 : 인하대학교 정보통신대학원 조교수(교신저자)
††† 정 회 원 : 수원대학교 전기공학과 조교수
논문접수 : 2007년 2월 28일, 심사완료 : 2007년 9월 27일

분배된 키 묶음이나 키의 재료가 센서노드의 메모리에 저장된다. 키 선분배의 문제는 연결성과 확장성인데 공개키 암호는 이 두 문제를 효과적으로 해결한다. 공개키 암호는 센서노드가 사전절차 없이도 통신할 수 있으며 손상된 노드의 공개/비밀키가 노출되어도 다른 노드에게는 영향을 주지 않는다.

최근의 연구들은 공개키 암호를 사용하는데 효율적인 연산 성능을 보였지만[6-9] 여전히 센서노드에게는 부담이 되어 WSN에서 공개키 암호를 사용하는 것은 아직은 시기상조이다. 하지만 효율적인 공개키 암호의 계속적인 연구와 발전하는 성능의 센서노드를 고려하면 가까운 미래에 WSN에서 공개키 암호가 사용될 것으로 보이며 공개키가 적용된 WSN에서는 공개키를 관리하기 위한 효율적인 기법이 필요하게 될 것이다. 기존의 네트워크에서의 전자서명은 키 분배와 인증을 목적으로 사용되고 여러 이유들에 의해 인증서를 무효화하기 위한 방법으로 인증서 폐지가 사용된다. X.509와 같은 전자서명은 인증서 ID, 공개키(1024 RSA, 320 ECC), 인증서 정보와 이들에 대한 전자서명을 포함한다. 인증서 폐지가 필요하게 됨에 따라 폐지할 인증서에 해당하는 ID의 인증서 폐지 목록CRL(Certificate Revocation List)을 각 노드에 전달해야 하지만 이에 따른 통신 오버헤드는 기존의 많은 유/무선 네트워크에서는 가능 할 수 있으나 센서네트워크에서 이러한 통신 오버헤드는 부담이 아닐 수 없다.

본 논문에서는 센서노드에서 공개키가 사용될 것을 고려하여 효율적인 인증서 폐지 목록 표현 기법을 보인다. 2장은 WSN에서의 공개키 연구들에 대해 알아보고 3장은 제안하는 기법에 적용한 기존 기법들의 정의를 소개한다. 4장은 집합 ID(set identifier)를 통해 폐지된 인증서 ID의 집합을 이용한 CS(Complete Subtree)와 BVS(Bit Vector Scheme)를 소개하며 이 중 BVS는 한 노드에 발급된 인증서의 폐지를 한번으로 제한하는 정적인 인증서 폐지 목록 표현 기법(BVS-S)과 한 노드에 대한 인증서 폐지가 여러 번 가능한 동적인 폐지 목록 표현 기법(BVS-D)으로 나누어 보인다. 5장에서는 분석과 모의실험 결과를 담았으며 6장은 관련된 모든 연구와의 비교로 결론을 내린다.

2. WSN에서의 공개키 암호연구

최근 연구에서 공개키 암호 프로토콜은 센서노드에서 적절한 연산효율을 보였다. Gura 등은 ECC와 RSA 서명 확인에 소요되는 시간을 실제로 측정해 보였다.[6] ECC 서명확인은 8Mhz로 작동하는 8비트의 ATmega128 프로세서에서 1.62초가 소요되고 다른 환경(14.7456 Mhz으로 동작하는 CC1010)에서도 서명확인에 필요한 코드와 데이터가 감소하였다. 공개키 암호 프로토콜의 에너지 소비를 연구한 [6]의 확장된 연구결과는 [7]에서 보였다. Watro은 TinyPK에서 센서노드마다 소비하는 자원의 실제적인 측정을 바탕으로 제한적인 공개키 암호구조를 개발했다[8]. 타원곡선 암호의 실제 측정과 평가를 바탕으로 한 TinyOS에서의 키 분배는 Malan의 연구[9]에서 보였다. 공개키 인증은 다른 방법으로도 연구가 진행되어 왔다. Du등은 Merkle Authentication Trees를 이용하여 메모리/통신 사이에 트레이드오프가 있는 공개키를 인증하기 위한 deployment knowledge를 연구했다[10]. DaeHun Nyang 등은 보안 레벨과 요구되는 리소스 사이의 트레이드오프 관계가 존재하는 MAC 계층에서의 공개키 인증 기법들을 보였다[12]. 이처럼 센서노드에서 공개키를 사용하기 위한 연구들이 점차 이루어지고 있으며 점차 향상되는 센서노드의 성능을 고려하면 머지않아 센서노드에서 공개키가 사용될 것으로 기대한다. 하지만 센서노드에서 공개키가 사용된다 하더라도 제한된 자원의 센서노드에서 통신을 위해 소요되는 비용은 여전히 부담이 되므로 통신 절약적인 기법들이 요구된다. 따라서 본 논문에서는 공개키 사용에 필요한 키 관리 방법 중 하나인 인증서 폐지를 위한 효율적인 인증서 폐지 목록 표현기법에 대해서 소개한다.

3. 기술 관련 정의

이 절에서는 연구와 관련된 두 가지 정의를 소개한다. 그 첫 번째로 집합 표현방법을 이용하는 CS(Complete Subtree)[13,14]이다. CS는 $N=2^k$개의 리프노드가 네트워크의 노드를 나타내는 완전이진트리 T를 이용하고 k비트의 식별자로 가능한 값은 $0 \sim 2^k-1$ 이므로 리프노드들의 ID는 k비트로 표현될 수 있다. 또한 한 개의 네트워크 노드의 인증서를 한번만 폐지하는 것을 고려하므로 각 리프노드의 ID를 인증서 ID로 대신할 수 있다. 루트에서부터 리프노드까지의 다른 경로(부모노드로부터 왼쪽은 0, 오른쪽은 1로 표현)는 리프노드의 식별자(ID)를 나타내며 폐지될 노드들의 식별자는 $R=v_1, v_2 \ldots v_r : |R|=r$로 표기한다. Broadcast encryption에서 원래의 CS는 키를 각 노드에 어떻게 할당할 것인가에 의의가 있으나, 여기서는 임의의 노드를 최소 개수의 집합으로 표현하는 방법에 초점을 맞춘다. 아래 정의에서 폐지된 식별자들의 ID가 어떻게 줄여지는지 보인다.

정의 1: Complete Subtree(CS) Cover 위의 완전 이진트리 T에서 리프들의 그룹 $R \subset T$의 CS $V_1 \ldots V_t \subset T$ (루트에서부터 시작된 ID로 표현)의 집합을 찾는 방법인데 노드 $v_{i1} \ldots v_{it}$는 i가 $0 < i < t$, $V_i \cap V_j = \varnothing (i \neq j$그리고 $V_1 \cup V_2 \ldots V_t = R)$일 때 V_i의 자식노드들을 나타낸다. V_i의 ID는 루트로부터 V_i까지의 경로를 나타내는 이진 문자열이므로 ID의 길이는 언제나 $\lceil \lg N \rceil$ 이다.

정의 2: Run-length encoding RLE 이진 문자열 P를 인코딩된 스트링 C로 만드는 데이터 인코딩 알고리즘이다. 예로, 1RLE-4b는 {1, 01, 001, 0001, 00001, 000001, 0000001, 00000001, 00000000} → {0, 1, 2, 3, 4, 5, 6, 7, 8}과 같이 $P \rightarrow C$로 매치되는데 여기서 각각의 C는 단일표현

'1'(1RLE-4b에서는 8)을 제외하고 4비트의 코드워드로 인코딩된다. 인코딩 전의 '1' 이나 '0'은 평문의 비트를 표현하며 1-RLE는 P에서의 '1'을, 0-RLE는 P에서의 '0'을 run-length로 표현하는데 사용한다.

4. 효율적 통신을 위한 인증서 폐지

N개의 노드가 있는 네트워크에서 r개의 인증서(인증서의 ID는 $\lceil \lg N \rceil$ 비트)가 폐지된 CRL에서의 통신 오버헤드는 $C = r \times \lceil \lg N \rceil$ 비트이다. 이와 같이 간단한 CRL을 Naive라 하고, 아래에서 CRL의 크기를 줄이는 방법들을 소개한다.

4.1 인증서 폐지에서의 Complete Subtree

정의 1에서 소개된 CRL과 CS개념을 기본으로 두고, CS는 CRL ID들의 통신 오버헤드를 줄이는데 바로 적용될 수 있다. 이후에 소개될 실험에서 볼 수 있듯이, CS는 오버헤드가 $r < 5\%$일 때 효율을 보이기 시작하고 오버헤드가 충분히 클 때($r > 20\%$) 상당한 압축 효과를 보인다. (그림 1)을 보면 효율 정도를 알 수 있다. 정의 1의 과정은 아래와 같다.

```
for (i = depth; i > 0; i--) {
    for (j = 0; j < N; j += 2) {
        if (CS[j][i] == 1 && CS[j + 1][i] == 1) {
            CS[j / 2][i - 1] = 1;
            CS[j][i] = NULL;
            CS[j + 1][i] = NULL;
        }
    }
}
```

여기서의 depth는 인증서 ID의 비트길이와 같다. (즉, $\lceil \lg N \rceil$ 비트)

4.2 효율적인 인증서 폐지를 위한 Bit Vector Scheme

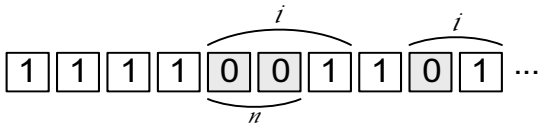
4.2.1 BVS-S

BVS(Bit Vector Scheme)은 인증서 폐지 목록을 줄이는데 사용될 수 있다. N개의 노드를 N개의 비트로 표현한 비트 벡터에서, i번째 비트가 '0'이라면 폐지되지 않은 인증서를 나타내고 '1' 이라면 폐지된 인증서를 나타내도록 한다. 노드는 이 비트벡터에서 '1'의 위치를 보고 어느 인증서가 폐지되었는지 알 수 있다. 여기서와 같이 폐지를 한번만 고려한 BVS를 BVS-S(Static)라고 하며 BVS-S의 길이는 N 비트이다.

대부분의 시스템에서 한번 인증서가 폐지 되면 다른 ID를 가진 인증서가 그것을 대체하는데(같은 ID에 다른 파라미터를 가질 수 도 있다) BVS-S는 폐지를 한번만 고려하여 실제 시스템에서 사용하기에는 다소 무리가 있다. 각 센서마다 폐지 횟수를 고려하여 미리 고정된 공간(예, 10)을 만들어 놓고 폐지될 때마다 한자리씩 '1'로 채우는 방법을 생각할 수 있지만 이 방법은 폐지된 인증서의 수가 적을 때는 효율적이지 않다.

4.2.2 BVS-D

WSN에서는 공격자가 노드를 물리적으로 취할 수 있기 때문에 비밀키가 노출될 수 있다. 공격으로 비밀키가 노출되었다 하더라도 해당 노드가 코드인증(Code Attestation) 등을 통해 성공적으로 인증을 받은 후 네트워크에 재참여하는 것을 고려하면 인증서가 재발급 되어야 할 필요가 있으며 키 업데이트 또한 고려되어야 한다. 이러한 사항들은 동적인 인증서 폐지의 필요성을 나타낸다. 앞서 언급한 방법인 동적인 폐지를 위한 공간을 미리 할당하는 기법의 낭비를 줄이기 위해 BVS-D는 미리 공간을 할당하지 않아도 동적인 폐지가 가능하도록 한다. 먼저, 인증서에서 노드와 관련된 정보는 i번 노드의 $n+1$번째 발급된 인증서라고 표시할 수 있도록 한다. 초기의 비트벡터는 네트워크 크기인 N만큼 '1'로 설정해 놓고 i번째 노드의 인증서가 폐지될 때마다 비트벡터에서 i번째 '1' 앞에 '0'을 추가한다. 이렇게 i번째 '1' 앞에 추가된 '0'의 개수(n)는 i번째 노드에 대한 인증서가 폐지된 수를 의미하기 때문에 노드 i에게 발급된 $n+1$번째 인증서가 유효한지 여부를 확인하려면 비트벡터의 i번째 '1'에서 $i-1$번째 '1' 사이의 '0'의 개수 n를 확인하면 된다. 예로 (그림 1)에서 5번째 '1' 앞에 2개의 '0'이 있으므로 노드 5의 인증서는 두 번 폐지되었고 노드 5에 대해서 세 번째로 발급된 인증서가 유효하다는 것을 뜻한다. 결국, 인증서가 폐지될 때마다 전체 비트벡터의 길이는 1씩 늘어난다. 앞서 언급된 아이디어는 폐지의 횟수에 제한을 두어야 했지만 이 방법은 폐지의 횟수에 제한이 없다. 참고로 원래의 CRL에서는 더 큰 범위의 ID가 10번의 폐지를 가능하게 한다. (Naive-D: 10,000개의 인증서를 표현하기 위해 14비트가 필요하지만 각각 최대 10번의 폐지를 고려하여 4비트를 추가한 18비트의 ID를 사용한다.)



(그림 1) BVS-D의 비트벡터

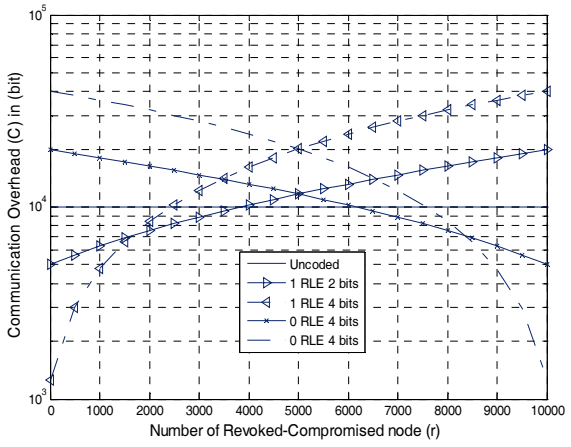
4.3 인코딩 / 압축

제안된 방법들의 비트벡터에서 '0' 또는 '1'이 연속해서 나타난다면 정의 2의 RLE와 같은 인코딩 방법을 이용하여 비

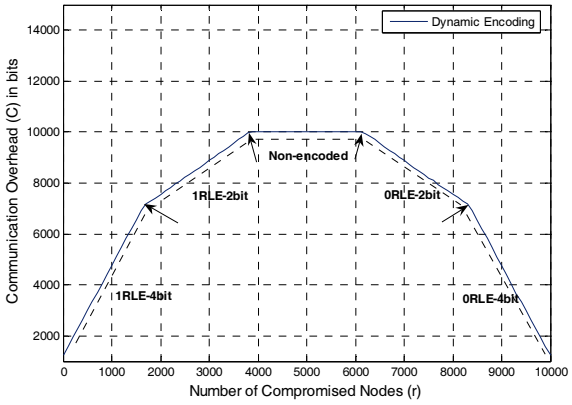
〈표 1〉 10,000개의 노드가 있는 네트워크에서 다른 CRL 기법을 적용한 비트단위의 통신 오버헤드. r은 전체 네트워크에서의 인증서 폐지율을 뜻하고 그 아래의 수치들은 해당 인증서 폐지율에 따른 비트 단위의 통신 오버헤드를 뜻한다. '-C'는 RLE를 나타낸다. RLE를 이용해서 Naive, CS, SD 기술들을 인코딩 하는 것은 효율적이지 않다. Dynamic Scheme에서의 표현 I는 노드의 수(정적인 기법에서 인증서 폐지 수)를 뜻하고 II는 최대 가능한 인증서 폐지 수를 고려한 수치이다.

Scheme	$r=01\%$	$r=05\%$	$r=10\%$	$r=20\%$	$r=40\%$	$r=50\%$
Naive	1,400	7,000	14,000	28,000	56,000	70,000
Naive-C	2,595	12,876	26,132	52,104	103,403	130,070
CS	1,355	6,805	13,310	25,004	42,850	49,408
Naive-D-I	1,800	9,000	18,000	36,000	72,000	90,000
Naive-D-II	18,000	90,000	180,000	360,000	720,000	900,000
BVS-S	10,000	10,000	10,000	10,000	10,000	10,000
BVS-S-C	1,597	2,994	4,753	7,569	10,000	10,000
BVS-D-I	10,100	10,500	11,000	12,000	14,000	15,000
BVS-D-II	11,000	15,000	20,000	30,000	50,000	60,000
BVS-D-II-C	3,756	13,778	20,000	27,508	37,498	41,320

트벡터의 길이를 더욱 압축될 수 있다. 비트벡터에서 연속성을 판단할 비트('0' 또는 '1')에 따라 0RLE 또는 1RLE로 표현하고 RLE에서 사용할 코드워드(cordword)에 따라 -2b(bit) 또는 -4b 로 나눈다. 상대적으로 폐지된 인증서의 수가 적은 경우($r<35\%$) 비트벡터에서의 '1' 역시 상대적으로 적으므로 1RLE-4b 또는 1RLE-2b를 이용하여 CRL을 줄이는 것이 효율이 좋으며 폐지된 인증서의 수가 많은($r>65\%$) 경우에는 '1'대신 '0'의 연속성을 고려한 인코딩(0RLE-2b, 0RLE-4b)을 택하는 것으로 인증서 폐지의 수가 많을수록 압축효율이 떨어져 인코딩 결과의 길이가 길어지는 것을 대체한다. 그 외($35\% \le r \le 65\%$)구간에서는 N비트의 BVS-S를 사용하여 모든 경우에 N비트 이하의 길이를 유지할 수 있게 한다. (그림 2)는 동적인 인코딩의 변환점은 폐지된 인증서의 비율에 따라 다양한 종류의 RLE를 적용하여 실험한 결과를 보여주며 (그림 3)은 앞의 실험 결과의 교차점에 따라 수동으로 지정한 변환점을 보여준다.



(그림 2) 다른 종류의 RLE를 적용한 통신 오버헤드



(그림 3) 수동으로 조절한 파라미터에 따른 통신 오버페드

5. 분석 & 모의실험 결과

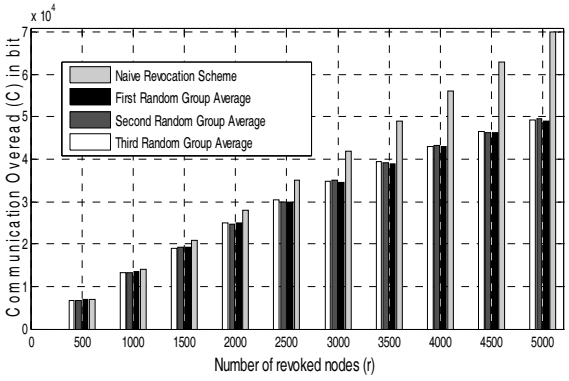
5.1 분석

각 노드별로 한 번 이상의 인증서 폐지를 지원하는 경우에, BVS-S와 BVS-D를 이용한 인코딩은 비트로 표현된 인증서 폐지 목록에서 '0' 또는 '1'의 연속성과 압축 효율은 비례한다. 반면에 CS와 Naive기법에서 사용된 ID는 비트로 표현되었을 때의 연속성을 고려하지 않았기 때문에 압축 효율이 좋지 않아 인코딩을 적용할 경우 인증서 폐지 목록이 더욱 길어질 수 있다. CS 알고리즘은 폐지된 인증서들이 서브트리(subtree)를 구성할수록 압축 효율이 좋아진다. 따라서 폐지된 인증서가 많을수록 이진트리 상에서 폐지된 ID가 연속적으로 존재할 가능성이 커지고 인증서 목록을 줄이기가 더욱 수월하다. 이는 집합 ID가 큰 집합을 표현할 가능성이 커져 효율적인 집합 표현을 제공할 것이고 이것은 전체 통신량을 감소시킨다. 폐지된 인증서가 연속적이지 않으면 Naive CRL에서와 같이 좋지 않은 성능을 보여줄 것이다. <표 1>은 임의적으로 폐지될 ID들을 선택한 결과이다.

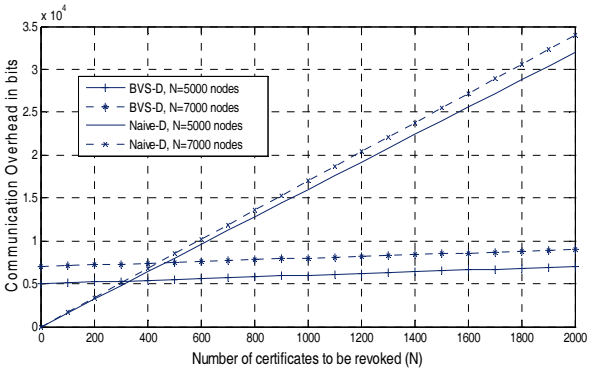
r개의 폐지된 인증서(같은 엔티티에 대해 중복도 포함)가 있는 BVS-D에서의 통신 오버헤드는 N이 노드의 수라고 했을 때, $f_r = r + N$이다. Naive-D의 경우 먼저 언급한대로 다수의 폐지를 고려한 ID의 수를 N'이라고 하면 통신 오버헤드는 $f_r = r \times \lg N'$이다. 즉, BVS-D는 $r \geq \frac{N}{\lg N' - 1}$크기의 어떠한 폐지집합에서도 적은 통신량과 좋은 성능을 보인다.

5.2 모의실험 결과

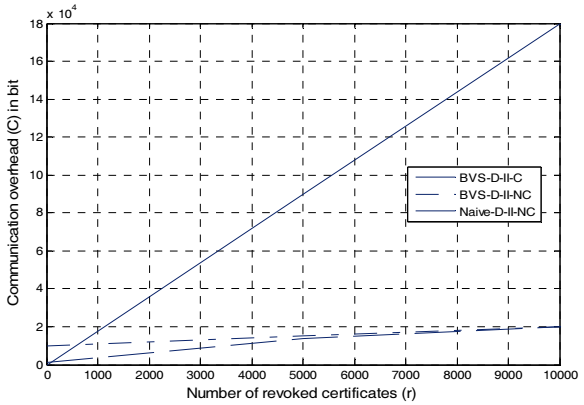
이 절에서는 제안한 알고리즘들(Naive, Naive Encoded, CS, BVS-S, BVS-D, BVS-S encoded, BVS-D encoded)의 성능을 모의실험을 통해 보였다. 펜티엄4 2G CPU와 1G메모리의 컴퓨터에서 C와 C++을 이용하여 코드를 작성하였으며 인증서 폐지 ID를 랜덤하게 하기위해 랜덤 함수를 이용한 ID 선택기(random identifier selector)를 이용하였다. 모의실험에서 네트워크 사이즈 N은 10,000으로 정하고(정적인 기법들에서는 같은 수의 인증서) r은 전체 네트워크에 대한 인증서 폐지율을 뜻하고 한 노드에 가능한 인증서 폐지 횟수는 10번으로 제한하였다. 인코딩의 교환점은 (그림 2), (그림 3)과 같이 폐지된 인증서의 비율에 따라 다양한 종류의 RLE 인코딩의 교차점으로 설정했다. <표 1>은 제안한 알고리즘들의 비트단위의 통신 오버헤드를 보여준다. (그림 4)는 CS와 Naive의 CRL 교환에 따른 통신 오버헤드를 보인다. 폐지된 인증서의 ID가 Subtree를 구성하는 것은 확률상의 문제이기 때문에 CS를 같은 조건에서 여러 번(e.g. 100번) 시도하여 평균을 구하였다. (그림 5)는 주어진 네트워크 크기에 따라(N=5000, N=7000) 동적인 인증서 폐지를 고려한 BVS-D와 Naive에 요구되는 통신 오버헤드의 차이를 보인다. (그림 6)과 (그림 7)은 RLE 허용 가능한 최대 인증서 폐지 수(10번)를 고려한 동적인 인증서 폐지 기법(D-II)에 RLE 인코딩을 적용(-C)한 BVS-D-II-C와 Naive-D-II-C에 요구되는 비트단위 통신 오버헤드의 차이를 보였다. 모의실험에서 $N/2$의 인증서가 폐지되었을 경우 제안하는 정적인 기법의 CRL 길이는 기존의 기법에 비해 최대 1/7로 줄었으며 동적인 기법은 기존의 CRL보다 최대 1/20이하로 그 길이를 줄였다.



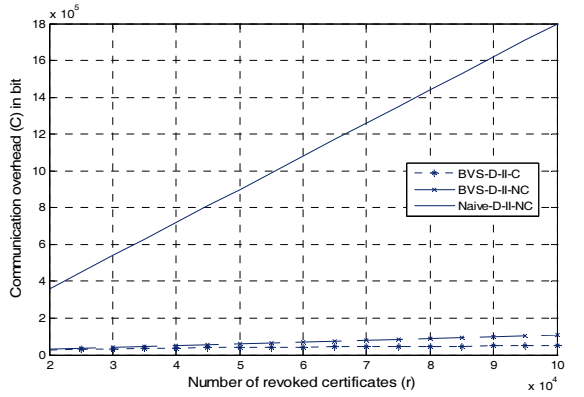
(그림 4) CS와 Naive의 통신 오버헤드



(그림 5) Naive-D와 BVS-D의 통신 오버헤드



(그림 6) BVS-D-II-C와 Naive-D-II-C의 통신 오버헤드



(그림 7) BVS-D-II-C와 Naive-D-II-C의 통신 오버헤드

6. 결 론

본 논문에서는 WSN에서 통신 효율을 높이기 위해 인증서 폐지 목록의 길이를 줄이는 방법을 소개했다. 첫째는 Broadcast encryption에서 사용 되는 CS(Complete Subtree)를 이용한 방법이고, 두 번째는 새롭게 정의한 BVS(Bit Vector Scheme)이다. 두 가지 방법 모두 인증서 폐지 목록의 길이를 매우 높은 비율로 감소시켰다.

본 논문에서 제안한 기법들은 WSN에서 통신에 사용되는

자원을 절약하기 위해서 다른 응용프로그램들에 적용될 수 있으며 제안한 기법이 적용된다면 결과적으로 센서네트워크의 수명을 연장시킬 수 있을 것으로 기대한다. 제안하는 기법들에 다른 종류의 인코딩/압축 기법을 적용해 보는 것은 앞으로 연구할 과제이며, 센서 노드들의 배치 방법(Deployment knowledge)를 고려해서 CRL 표현 방법을 설계하는 것도 좋은 연구 주제가 될 것이다.

참 고 문 헌

[1] Eschenauer, L., Gligor, V. D.: A key management scheme for distributed sensor networks, *In Proc. of the ninth ACM CCS'02*, pp.41-47, 2003

[2] Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks, *IEEE Symp on S&P*, pp.197-213, May 2003.

[3] Du, W., Deng, J., Han, Y. S., and Varshney, P.: A pair-wise key pre-distribution scheme for wireless sensor networks, *ACM CCS'03*, pp.42-51, 2003.

[4] Liu, D., Ning, P.: Establishing Pair-wise keys in distributed sensor networks, *ACM CCS'03*, pp.52-61, 2003.

[5] Rivest, R. L., Shamir, A., Adleman, L. M.: A method for obtaining digital signatures and public-key cryptosystems, *Com. of the ACM, 21(2)*: pp.120-126, 1978.

[6] Gura N., Patel A., Wander A., Eberle A., Shantz S. C.: Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, *CHES* pp.119-132, 2004

[7] Wander A., Gura N., Eberle H., Gupta V., Shantz S.C.: Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks, *PerCom'05*, pp.324-328.

[8] Watro R.J., Kong D., Cuti S.F., Gardiner Ch., Lynn Ch., Kruus P.: TinyPK: securing sensor networks with public key technology, *SASN'04*, 59-64, pp.10-2004.

[9] Malan D.J., Welsh A., Smith M.D.: A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Crypt., *IEEE SECON'04*, pp.71-80.

[10] Du W., Wang R., and Ning P.: An Efficient Scheme for Authenticating Public Keys in Sensor Networks. *Proc. of The sixth ACM MobiHoc*, pp.58-67.

[11] Pottie G. J. and Kaiser W. J. Wireless integrated network sensors. *Communications of the ACM*, pp. 51-58, May 2000.

[12] Nyang D., Mohaisen A.: Cooperative Public Key Authentication Scheme for Wireless Sensor Networks, *To appear in proceeding of UIC06*, LNCS, Sep 2006

[13] Naor D., Naor M., Lotspiech J.: Revocation and Tracing Schemes for Stateless Receivers. *CRYPTO* : pp.41-62, 2001

[14] Fiat A., Naor M.: Broadcast Encryption. *CRYPTO* : pp.480-491, 1993.

[15] Koblitz N., Menezes A., Vanstone S.: The State of Elliptic Curve Cryptography, *Designs, Codes and Cryptography*, 19, 173-193, 2000.

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
2005년~9월 현재 인하대학교 정보통신 대학원(석사)
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