센서 네트워크 내의 위조된 데이터 삽입 공격 방지를 위한 인증 방법

조 관 태[†] · 김 용 호[††] · 이 동 훈[†††]

요 약

위조된 데이터를 센서 네트워크 내에 삽입하기 위한 공격을 방지하기 위해 센서 노드의 위치 기반 임계값 보증(LTE) 방법이 최근에 제안되었다. 제안된 방법은 이전에 제안된 대칭키 기반 방법보다 필터링 능력이 더 뛰어나며 에너지 절약 측면에 있어서도 더 효율적이다. 본 논문에서는 LTE 방법이 지닌 치명적인 취약성을 증명하고 취약성을 완화시킴과 동시에 LTE 방법이 의도했던 데이터 필터링 능력을 그대로 유지한 채, 본래 이루고자했던 목적에 더 근접한 결과를 보여줄 수 있는 향상된 방법을 제시할 것이다.

키워드 : 보안, 위조된 데이터 공격, 센서 네트워크

An Authentication Scheme for Filtering Injected Bogus Data in Sensor Networks

Cho, Kwan Tae[†] · Kim, Young Ho[††] · Lee, Dong Hoon[†††]

ABSTRACT

Recently, a location-based threshold-endorsement(LTE) scheme is proposed to thwart bogus data injection attacks. The scheme exhibits much greater filtering power than earlier symmetric schemes and results in enhanced energy savings. In this paper, we show that LTE has fatal vulnerabilities. We also propose an improved scheme that mitigates the weakness and thereby achieves the original claims without lessening remarkable filtering power intended in LTE.

Key Words : Security, Bogus Data Injection Attack, Sensor Networks

1. 서 론

유비쿼터스 컴퓨팅 환경의 기반이 되고 있는 무선 센서 네트워크는 일반적으로 초경량, 초전력의 수많은 센서 노드들로 네트워크를 형성한다. 무선 센서 네트워크의 센서 노드들은 무작위로 배치되기 때문에 물리적 공격에 의해 쉽게 노출될 수 있다. 예를 들어 공격자는 단지 센서 노드를 포획함으로써 메모리 안에 있는 비밀 정보를 얻을 수 있다.

본 논문은 무선 센서 네트워크에 악의적인 목적을 가진 공격자가 무선 센서 네트워크 내에 위조된 데이터를 삽입하려 할 때, 그러한 행동을 사전에 발견하고 이를 방지하는 것에 중점을 둔다. 이러한 공격은 위조된 데이터의 삽입으로 인한 잘못된 정보를 전달할 수 있을 뿐만 아니라 센서 노드가 싱크로 정보를 전달하는 경로 내에 있는 센서 노드들의 자원고갈을 야기 시킬 수 있다. 그러므로 위조된 데이터가 싱크 노드에 도착하기 전에 가능한 일찍 위조된 데이터를 발견해야 한다. 위조된 데이터의 파급을 줄이기 위해 몇 가지 방법들이 제안되었다[15, 19]. 제안된 방법들은 위조된 데이터를 발견하기 위해 여러 개의 센서 노드들이 투표를 통해 데이터가 위조되었는지 아닌지 결정한다. 하지만 투표를 통한 방법들은 두 가지 단점을 가지고 있다. 첫 번째 단점은 필터링 능력을 높이기 위해 각 센서 노드들은 많은 키를 저장해야 한다는 것이다. 두 번째 단점은 이웃 노드들 중 미리 정의된 값인 t개 이상의 이웃 노드들이 공격자에 의해 포획 당했을 때 위조된 데이터의 삽입을 발견할 수 없다는 것이다.

최근 Zhang이 위조된 데이터를 발견하고 위조된 데이터를 무시할 수 있는 위치 기반 임계값 보증(LTE) 방법을 제안하였다[17]. LTE 방법에서 합법적인 데이터를 보고하기 위해서는 t개 이상의 인증된 센서 노드들에 의해 공동 서명

※ 본 논문은 SSDU 2007 "Bogus Data Filtering in Sensor Networks"의 확장 버전이다.
※ 본 연구는 정보통신부 및 정보통신 연구진흥원의 대학 IT연구센터 지원 사업으로 수행되었음
† 정 회 원 : 고려대학교 정보경영공학전문대학원 석사과정
†† 준 회 원 : 고려대학교 정보경영공학전문대학원 박사과정
††† 정 회 원 : 고려대학교 정보경영공학전문대학원 교수
논문접수 : 2007년 5월 28일, 심사완료 : 2007년 8월 20일

을 받아야 한다. 이전의 방법들[15,19]과 비교해 볼 때, LTE 방법은 원거리에 있는 싱크 노드에 데이터를 전송하기 위해 요구되는 통신 에너지를 효과적으로 줄임과 동시에 필터링 능력을 높였다는 것이 특징이다. LTE 방법이 통신 에너지를 효과적으로 줄일 수 있게 된 가장 큰 이유는 기존의 방법들[3, 5-7]처럼 대칭키 기반 방법이 아닌 공개키 기반 방법을 적용했기 때문이다. 요구되는 계산 에너지는 증가하지만 반면에 요구되는 통신 에너지를 현저히 줄일 수 있기 때문에 전체적으로 보았을 때 무선 센서 네트워크의 수명을 연장시킬 수 있다는 점이 큰 장점이다.

하지만 LTE 방법은 치명적인 약점을 지니고 있다. LTE 방법은 필터링 능력을 높이기 위해 셀 서명을 할 때, 각 노드에 공통으로 할당된 키를 사용한다. 어떠한 셀이라도 이벤트가 발생하였을 경우 이벤트를 발견한 노드들 사이에서 선출된 데이터 집합 노드(AP)는 데이터를 보고하기 위해 서명값을 생성한다. 그렇지만 LTE 방법을 한번 실행한 후에는 일반적으로 AP는 셀 키와 셀 서명 키를 생성하는 데 필수적인 비밀 정보들의 일부분을 획득할 수 있게 된다. 따라서 LTE 방법에서 의도하지 않았지만 하나의 셀에 대한 정보의 일부분이 공격자에게 노출되고 이로 인해 또 다른 셀의 안전성 또한 위협받게 된다.

논문의 나머지는 다음과 같이 구성된다. 2절에서는 본 논문과 관련된 연구들을 소개하고 3절에서는 LTE 방법에 대한 내용과 LTE 방법이 지닌 취약성을 분석한다. 그리고 4절에서는 발견된 취약성을 수정한 향상된 방법을 제안하고 5절에서 제안한 방법의 실행 능력과 안전성을 분석한다. 6절에서는 마지막으로 결론을 내린다.

2. 관련 연구

2.1 Bilinear 그룹과 Pairing

p, q을 두 개의 큰 소수로 정의하고 G_1, G_2는 q을 소수인 위수로 갖는 그룹으로 정의한다. G_1은 타원 곡선 E/F_p위에 있는 점들의 집합을 의미한다. G_2는 적절한 α에 대해 유한 필드 $F_{p^\alpha}^*$의 곱셈 그룹의 서브 그룹을 의미한다. Pairing은 다음과 같은 특성[2]를 가진 $\hat{e}: G_1 \times G_1 \rightarrow G_2$에 기반 한다.

(1) Bilinearity : 모든 P와 Q에 대해 $P, Q \in G_1$과 $a, b \in Z_q^*$을 만족할 때, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$을 만족한다.

(2) Non-degenerancy : P가 G_1의 생성자일 때, $\hat{e}(P, P)$는 G_2의 생성자이다.

(3) Computability : 모든 P와 Q에 대해 $P, Q \in G_1$을 만족할 때, $\hat{e}(P, Q) \in G_2$을 계산하는데 효과적인 알고리즘이 존재한다.

2.2 ID 기반 공개키 암호

전통적인 공개키 기반 암호(PKI)는 너무 복잡하고 느리며 많은 에너지가 소모된다. 이러한 특성들은 무선 센서 네트워크에 적절하지 않기 때문에 대부분의 센서 키 연구는 대칭키 위주로 진행되었다[3, 5-7]. 대칭키 기반 방법은 적은 계산 오버헤드를 가지고 있는 반면에 대체적으로 많은 통신 오버헤드가 존재하거나 각 노드에게 상당한 메모리를 요구한다. 이러한 이유로 많은 연구자들은 최근에 센서 네트워크에서 실행 가능한 PKI를 연구하기 시작했다[8, 9, 11, 13, 14].

인증서 기반 시스템에서 사용자들은 인증기관으로부터 장기간 사용할 수 있는 인증서를 획득하여야 한다. 그리고 인증서는 사용자를 인증하기 위해 다른 사용자들에게 주어진다. 반면 ID 기반 시스템에서 사용자들은 이메일 같은 것을 통해 사용자의 공개 아이디를 알 수 있다. 그러므로 인증서 기반 시스템과는 달리 ID 기반 시스템에서는 인증서 전송이 요구되지 않는다. 무선 센서 네트워크에서 이러한 차이점은 무선 센서 네트워크의 수명에 있어서 커다란 영향을 준다. 왜냐하면 1 비트를 전송하는 데 요구되는 통신 에너지는 32 비트를 계산하는 데 필요한 계산 에너지보다 훨씬 많은 에너지를 요구하기 때문이다[1]. 에너지 소비에 관한 실험 결과, 계산에 요구되는 에너지는 전체 에너지 소비의 3%미만인 반면에 통신에 요구되는 에너지는 대략 97%정도이다[12]. 이러한 이유로 몇 개의 ID 기반 AKE 방법들[16-18]이 무선 센서 네트워크를 위해 제안되었다.

2.3 위치 기반 키 관리 방법

이 절에서는 LTE 방법과 본 논문에서 제안한 방법이 공통으로 사용한 위치 기반 키(LBK) 관리 방법에 대해 간단히 설명할 것이다. 노드 배치에 앞서 다음과 같은 기능을 하는 믿을 수 있는 개체(TA)가 존재한다고 가정한다.

(1) TA는 2.1절에서 명시한 두 개의 그룹 G_1, G_2 그리고 $\hat{e}$을 설계한다.

(2) TA는 두 개의 암호 해쉬 함수 H와 h을 선택한다. 단 해쉬 함수는 G_1내의 0이 아닌 임의의 입력 값에 대해 일정한 길이의 출력 값과 맵핑시킨다.

(3) TA는 네트워크 마스터 비밀 값으로 $k \in Z_q^*$을 만족하는 k을 임의로 선택한다. W가 G_1의 무작위 생성원인 때, $W_{pub} = kW$을 만족한다.

(4) 식별 정보인 ID_A을 가지고 있는 노드 A에 대해, TA는 ID 기반 키인 $IK_A = kH(ID_A)$을 계산한다.

각 센서 노드는 공개키 시스템의 매개 변수들 $(p, q, G_1, G_2, \hat{e}, H, h, W, W_{pub})$과 ID 기반 키인 IK_A을 배치 전에 미리 저장한다. 일단 센서 노드가 배치되면 각 센서 노드에게 센서 노드의 위치 정보가 제공된다. Zhang은 이동 가능한 로봇과 주요지점을 사용하여 위치 정보를 제공하는 두 개의 센서 위치 기반 기술을 고려하였다[17]. 위치 측정 후, 노드 A는 노드 A의 위치 정보 l_A와 $LK_A = kH(ID_A \| l_A)$을 저장하게 된다.

마지막으로 서로 이웃 노드인 센서 노드 A와 B는 위치 정보와 식별 정보를 교환한 후에 공유키를 생성한다.

$$K_{A,B} = \hat{e}(LK_A, H(ID_B \| l_B)) = \hat{e}(H(ID_A \| l_A), kH(ID_B \| l_B)) = \hat{e}(LK_B, H(ID_A \| l_A)) = K_{B,A}$$

3. LTE 방법에 대한 분석

이 절에서는 Zhang이 제안한 LTE 방법을 간단히 소개한다. 좀 더 자세한 내용은 그의 논문[17]에 언급되어 있다.

3.1 셀 키의 생성과 분배

r을 각 변의 길이로 하는 정사각형 모양의 $M \times N$으로 센서 필드를 나눈 후, $1 \le m \le M$, $1 \le n \le N$을 만족하는 m, n에 대해 각 셀을 정수 쌍 $<m,n>$으로 이름 짓는다. LTE 방법의 기본 개념은 비밀 공유 방식[17]을 사용하여 셀 $<m,n>$안에 있는 각 노드에 $K_{m,n}$에 대한 공유 정보를 할당하는 것이다. $ID^i_{m,n}$은 셀 $<m,n>$안에 있는 위치 정보 $l^i_{m,n}$을 가진 i번째 노드를 나타낸다. 다음 두 가지 방법이 셀 키를 공유하기 위해 사용된다.

3.1.1 범위 기반 셀 키 분배

이동 가능한 로봇이 $K_{m,n}$에 대한 공유 정보를 분배하는 데 결정적인 역할을 한다. 로봇이 $(t-1)$차 다항식 $\rho(x) = \sum_{j=1}^{t-1} F_j x^j$을 가지고 있다고 가정한다. 여기서 F_j는 G_1^*에서 무작위로 선택한 계수이다. 이동 가능한 로봇은 우선 $K_{m,n} = kH(m \| n)$과 인증자 벡터 $\overrightarrow{V_{m,n}} = \{v^{(j)}_{m,n} | 0 \le j \le t-1\}$을 계산한다. 여기서 $v^{(j)}_{m,n}$와 F_0은 각각 $v^{(j)}_{m,n} = \hat{e}(F_j, W)$와 $F_0 = K_{m,n}$을 의미한다. 다음으로 이동 가능한 로봇은 $K_{m,n}$과 센서 노드의 식별 정보인 $ID^i_{m,n}$을 사용하여 $K^i_{m,n} = \rho(ID^i_{m,n} \| l^i_{m,n}) + K_{m,n} \in G_1$을 계산한다. 마지막으로 이동 가능한 로봇은 센서 노드 $ID^i_{m,n}$와의 공유키인 IK_1을 사용하여 $K^i_{m,n}$와 $\overrightarrow{V_{m,n}}$을 노드 $ID^i_{m,n}$에게 안전하게 전송한다. $K_{m,n}$은 t개 이상의 공유 정보로부터 다시 만들어 질 수 있는 반면에, $(t-1)$개 이하의 공유 정보로부터는 만들어 질 수 없다. 논문에서는 다음과 같은 방법으로 t차 선형 방정식에 의해 셀 키를 생성한다. Ω는 셀 $<m,n>$안의 모든 센서 노드들의 t-order 서브셋이라고 정의한다.

$$K_{m,n} = \sum_{i \in \Omega} \lambda_i K^i_{m,n}$$

위 방정식에서 λ_i는 다음과 같다.

$$\lambda_i = \prod_{j \in \Omega \setminus \{i\}} \frac{(ID^j_{m,n} \| l^j_{m,n})}{(ID^j_{m,n} \| l^j_{m,n} - ID^i_{m,n} \| l^i_{m,n})}$$

공격자의 노드 포획으로 인한 공유 정보 유출에 대한 저항력과 노드 밀도는 트레이드오프 관계이기 때문에 중 어느 성질이 더 중요한 가에 따라 매개 변수 t값을 결정해야 한다.

3.1.2 범위 제한 없는 셀 키 분배

각 센서 노드는 배치 전에 다항식 $\rho(x)$와 마스터 키 k을 저장한다. 각 노드는 먼저 LBK를 계산한 후에 노드 $ID^i_{m,n}$는 k을 사용하여 $K_{m,n}$와 공유 정보인 $K^i_{m,n}$을 생성한다. 또한 인증자 벡터 $\overrightarrow{V_{m,n}}$을 계산한다. 이러한 모든 과정을 마친 후에 반드시 센서 노드의 메모리에 저장되어 있는 k, $F(x)$ 그리고 셀 키 $K_{m,n}$을 안전하게 지워야 한다.

3.2 라우팅 경로에서의 데이터 필터링

먼저 셀 $<m,n>$안에서 이벤트가 발생하였을 경우, 이벤트를 $s \ge t$ 개의 노드가 감지했다고 가정한다면 이벤트를 발견한 센서 노드들은 싱크에게 전달할 최종 보고서 Λ을 작성하여야 한다.

우선 센서 노드들은 그들 사이에서 AP 역할을 할 센서 노드를 선출한다. Λ의 각 센서 노드에 대한 서명을 획득하기 위해 AP는 무작위로 $\alpha \in Z_q^*$을 선택하고 $\theta = \hat{e}(W, W)^\alpha$을 계산한다. 그리고 AP는 θ을 주위의 이웃 노드들에게 브로드캐스트 한다. θ값을 수신하는 즉시, 이벤트를 감지했던 노드 $ID^i_{m,n}$는 $U^i_{m,n} = h(\Lambda \| \theta) K^i_{m,n}$을 계산함으로써 보고서 Λ에 대한 자신의 서명값을 생성한다. 그리고 AP와 공유하는 pairwise 키를 사용하여 $U^i_{m,n}$을 AP에게 전송한다. 이웃 노드들로부터 t개 이상의 서명값을 수신한 AP는 서명값을 전송한 이웃 노드들 중 임의로 t개를 선택한다. 이 때 이웃 노드들은 Ω에 언급되어 있는 노드들이다. 그리고 AP는 $U_{m,n} = \sum_{i \in \Omega} \lambda_i U^i_{m,n} = h(\Lambda \| \theta) K_{m,n}$과 $\gamma_{m,n} = U_{m,n} + \alpha W$을 계산한다. Λ의 최종 서명값은 $(\gamma_{m,n}, h(\Lambda \| \theta))$이다. 따라서 AP에 의해 싱크로 보내어지는 최종 보고서의 구성은 $<\Lambda, \gamma_{m,n}, h(\Lambda, \theta)>$가 된다.

AP에서 싱크로 보내어지는 경로 상에 있는 중간 노드들이 최종 보고서를 수신할 때, 최종 보고서는 견본 추출 확률[17]이라 불리는 확률 p_s에 의해 검증된다.

3.3 보안 측면에서 LTE 방법의 결점

3.3.1 악의적인 AP에 의한 영향

LTE 방법에서 Zhang은 AP가 악의적인 노드일 경우를 고려하였고 새로운 AP를 재선출함으로써 문제를 간단히 해결하였다. 하지만 LTE 방법을 한번 실행한 후, 악의적인 AP는 셀 키와 다수의 공유 정보를 알아낼 수 있다. 이벤트를 감지한 각 센서 노드들로부터 서명값을 획득한 후에 AP는 최종 보고서를 전송한 각 센서 노드들의 $U^i_{m,n} = h(\Lambda \| \theta) K^i_{m,n}$을 획득할 수 있고 이를 이용해서 $U_{m,n} = \sum_{i \in \Omega} \lambda_i U^i_{m,n} = h(\Lambda \| \theta) K_{m,n}$을 계산할 수 있다. 그리고 $h(\Lambda \| \theta)$을 사용하여 역함수 $h(\Lambda \| \theta)^{-1} \in Z_q^*$을 쉽게 계산할 수 있기 때문에 AP는 셀 키와 적어도 t개의 공유 정보를 획득할 수 있다. 참고로 공유 정보 $K_{m,n}$과 $K^i_{m,n}$은 각각 $K_{m,n} = h(\Lambda \| \theta)^{-1} U_{m,n}$, $K^i_{m,n} = h(\Lambda \| \theta)^{-1} U^i_{m,n}$을 통해 알아낼 수 있다.

3.3.2 $\rho(x)$의 취약성

공격자는 다른 셀에서 발생하는 이벤트를 성공적으로 위조하기 위해 획득한 t개의 공유 정보들을 남용할 수 있다. 악의적인 AP나 t개의 센서 노드들을 획득함으로써 셀에서 t개의 공유 정보를 얻을 수 있고, 공격자는 셀 키와 t-가변 선형 방정식에 의해 $(t-1)$차 다항식 $\rho(x)$의 모든 계수를 계산할 수 있다. 공격자가 다른 셀$<m',n'>$에 있는 추가적인 공유 정보 $K_{m',n'}^{i}$을 획득했다고 가정했을 때, 공격자는 $K_{m',n'}=K_{m',n'}^{i}-F(ID_{m',n}^{i}\|l_{m',n'}^{i})$을 계산하여 또 다른 셀 키를 얻을 수 있다. 결과적으로 임의의 $\alpha'\in Z_q^*$을 선택하고 $\theta'=\hat{e}(W,W)^{\alpha'}$을 계산한 후에 공격자는 최종 보고서 Λ의 서명값 $<\gamma_{m',n'}=h(\Lambda\|\theta')K_{m',n'}+\alpha' W, h(\Lambda\|\theta')>$을 위조할 수 있다.

4. 제안된 방법

4.1 셀 키의 생성과 분배

하나의 다항식과 인증자 벡터가 아닌 각 셀에 대한 셀-다항식 $\rho_{m,n}(x)=\sum_{j=1}^{t-1}H(F_j\|m\|n)x^j$과 셀-인증자 벡터 $V_{m,n}=\{v_{m,n}^{(j)}|0\le j\le t-1\}$을 정의한다. $v_{m,n}^{(j)}$, $v_{m,n}^{(0)}$은 각각 $v_{m,n}^{(j)}=\hat{e}(H(F_j\|m\|n),W)$, $v_{m,n}^{(0)}=\hat{e}(K_{m,n},W)$을 의미한다. 각 노드의 셀 $<m,n>$을 결정한 후에 다항식 $\rho(x)$로부터 $\rho_{m,n}(x)$을 유도한다. 셀 키의 생성과 분배는 각 셀마다 셀-다항식 $\rho_{m,n}(x)$와 셀-인증자 벡터 $V_{m,n}$가 존재한다는 점만 제외하고 나머지 과정은 LTE 방법의 과정(3.1절 참고)과 같다.

4.2 라우팅 경로에서의 데이터 필터링

LTE 방법에서 이벤트가 발생하면 이벤트를 발견한 센서 노드들은 그들 사이에서 AP를 선출한다. 이벤트를 발견한 모든 센서 노드 $ID_{m,n}^{i}$은 Λ에 대한 서명값을 생성하기 위해 임의로 $\alpha_i\in Z_q^*$을 선택하고, $\theta_i=\hat{e}(W,W)^{\alpha_i}$을 계산한 후, 서명값 θ_i을 AP에게 전송한다. 이웃 노드들로부터 t개 이상의 서명값을 받은 AP는 이웃 노드들 중 임의로 t개를 선택한다. 서명값을 전송한 센서 노드는 Ω에 포함되어 있는 센서 노드이다. 다음으로 AP는 $\theta=\prod_{i\in\Omega}\theta_i^{\lambda_i}$을 계산하고 θ을 이웃 노드들에게 브로드캐스트 한다. θ을 수신하는 즉시 센서 노드 $ID_{m,n}^{i}$는 $\gamma_{m,n}^{i}=h(\Lambda\|\theta)K_{m,n}^{i}+\alpha_i W$을 계산함으로써 보고서 Λ에 대한 자신의 서명값을 생성한다. 그리고 각 센서 노드는 AP와 공유한 pairwise 키를 사용하여 AP에게 $\gamma_{m,n}^{i}$을 송신한다. 다음으로 AP는 $\gamma_{m,n}=\sum_{i\in\Omega}\lambda_i\gamma_{m,n}^{i}$을 계산한다. Λ의 최종 서명값은 $(\gamma_{m,n},h(\Lambda\|\theta))$이다. 따라서 AP에 의해 싱크로 보내어지는 최종 보고서의 구성은 $<\Lambda,\gamma_{m,n},h(\Lambda,\theta)>$가 된다.

다수의 센서 노드가 공격자에 의해 포획되었다고 가정했을 때, AP는 $\gamma_{m,n}$을 계산한 후, $\hat{e}(\gamma_{m,n},W)=(v_{m,n}^{(0)})^{h(\Lambda\|\theta)}\cdot\theta$을 검사함으로써 타당성을 검증할 수 있다. 세부 과정은 다음과 같다.

$$\begin{aligned}\hat{e}(\gamma_{m,n},W)&=\hat{e}(\sum_{i\in\Omega}\lambda_i\gamma_{m,n}^{i},W)\\&=\hat{e}(\sum_{i\in\Omega}(\lambda_iK_{m,n}^{i}h(\Lambda\|\theta)+\lambda_i\alpha_iW),W)\\&=\hat{e}(h(\lambda\|\theta)K_{m,n}+\sum_{i\in\Omega}\lambda_i\alpha_iW,W)\\&=\hat{e}(K_{m,n},W)^{h(\lambda\|\theta)}\cdot\prod_{i\in\Omega}\hat{e}(W,W)^{\alpha_i\lambda_i}\\&=(v_{m,n}^{(0)})^{h(\lambda\|\theta)}\cdot\prod_{i\in\Omega}\theta_i^{\lambda_i}\\&=(v_{m,n}^{(0)})^{h(\lambda\|\theta)}\cdot\theta\end{aligned}$$

검증을 통과하면 AP는 최종 보고서가 타당하다고 믿고 싱크로 보낸다. 하지만 검증을 통과하지 못한다면 AP는 악의적은 센서 노드를 찾기 위해 다음과 같은 과정을 통해 각각의 센서 노드로부터 수신한 $\gamma_{m,n}^{i}$을 검증한다.

$$\begin{aligned}&\hat{e}(\gamma_{m,n}^{i},W)\\&=\prod_{j=0}^{t-1}(v_{m,n}^{(j)})^{(ID_{m,n}^{i}\|l_{m,n}^{i})^{j}h(\Lambda\|\theta)}\cdot\theta_i\end{aligned}$$

세부 과정은 다음과 같다.

$$\begin{aligned}&\hat{e}(\gamma_{m,n}^{i},W)\\&=\hat{e}(h(\lambda\|\theta)K_{m,n}^{i}+\alpha_iW,W)\\&=\hat{e}(K_{m,n}^{i},W)^{h(\Lambda\|\theta)}\cdot\hat{e}(W,W)^{\alpha_i}\\&=\hat{e}(\sum_{j=1}^{t}H(F_j\|m\|n)(ID_{m,n}^{i}\|l_{m,n}^{i})^{j}\\&\qquad+K_{m,n},W)^{h(\Lambda\|\theta)}\cdot\theta_i\\&=\prod_{j=0}^{t-1}(v_{m,n}^{(j)})^{(ID_{m,n}^{i}\|l_{m,n}^{i})^{j}h(\Lambda\|\theta)}\cdot\theta_i\end{aligned}$$

AP와 싱크 노드 경로 상에 있는 중간 노드가 최종 보고서 $<\Lambda,\gamma_{m,n},h(\Lambda\|\theta)>$을 수신할 때, 중간 노드는 확률 p_s로 최종 보고서를 검증한다.

중간 노드는 먼저 $H(\Lambda\|\theta')$을 계산한 후, 이를 검증한다. 여기서 θ'는 다음과 같다.

$$\theta'=\hat{e}(\gamma_{m,n},W)\cdot\hat{e}(H(m\|n),-W_{pub})^{h(\lambda\|\theta)}$$

최종 보고서가 타당하다면 다음을 만족시킨다.

$$\begin{aligned}\theta'&=\hat{e}(\gamma_{m,n},W)\cdot\hat{e}(H(m\|n),W_{pub})^{-h(\Lambda\|\theta)}\\&=\hat{e}(K_{m,n},W)^{h(\Lambda,\theta)}\cdot\prod_{i\in\Omega}\theta_i^{\lambda_i}\\&\qquad\cdot\hat{e}(K_{m,n},W)^{-h(\Lambda\|\theta)}\\&=\theta\end{aligned}$$

만일 $h(\Lambda\|\theta)=h(\Lambda\|\theta')$을 만족한다면 중간 노드는 최종 보고서를 다음 중간 노드로 보낸다. 그렇지 않으면 최종 보고서는 위조된 것으로 판단되어 중간 노드에서 무시된다.

5. 분 석

5.1 악의적인 AP에 대한 저항력

악의적인 AP의 영향력은 거의 없다. 하지만 LTE 방법에서는 한 번 실행 과정을 거친 후, 공격자는 이벤트가 발생

한 셀에 대한 셀 키와 적어도 t개의 공유 정보를 획득할 수 있다[17]. 이유는 LTE 방법의 보고서 생성 과정이 안전하지 않기 때문이다. 본 논문에서 제안한 방법은 이벤트를 발견한 각 센서 노드 $ID^i_{m,n}$가 임의로 α_i을 선택하기 때문에 AP가 각 센서 노드의 α_i을 알아낼 수 없다. AP가 $\gamma^i_{m,n}=h(\Lambda\|\theta)K^i_{m,n}+\alpha_i W$와 $\gamma_{m,n}=h(\Lambda\|\theta)K_{m,n}+\sum_{i\in\Omega}\lambda_i\alpha_i W$을 알아냈다고 하더라도, 공격자는 α_i없이 $K^i_{m,n}$와 $K_{m,n}$을 결코 획득할 수 없다.

5.2 각 셀의 독립적인 안전성

공격자가 하나의 셀에 대한 정보를 획득했다고 하더라도 공격자는 획득한 셀 키나 공유 정보를 다른 셀에 대한 이벤트를 위조하기 위해 사용할 수 없어야 한다. 하지만 LTE 방법에서는 각 셀에 대한 독립적인 안정성을 제공하지 못하기 때문에 하나의 셀이 공격자에게 노출된다면 다른 셀의 안전성에도 직접적인 영향을 준다. 이것은 LTE 방법이 오직 하나의 다항식 $\rho(x)=\sum_{j=1}^{t-1}F_j x^j$만을 사용하기 때문이다. 이러한 취약성을 개선하기 위해 본 논문에서는 모든 셀에 대해 별개의 셀-다항식을 사용한다. 예를 들어 공격자가 셀 $<m,n>$에 대한 t개의 공유 정보를 획득했다고 가정했을 때, 공격자가 t-가변 선형 방정식을 계산함으로써 $(t-1)$차 다항식 $\rho_{m,n}(x)$의 모든 계수 $\{H(F_j\|m\|n)\}$을 유도해낼 수 있다고 하더라도, 공격자는 다른 셀 $<m',n'>$에 대한 어떠한 정보도 획득할 수 없다. H가 단방향 성질을 지닌 암호학적 해쉬 함수이기 때문에 $H(F_j\|m\|n)$으로부터 $H(F_j\|m'\|n')$을 이끌어내는 것은 상당히 어렵다. 결과적으로 공격자가 공격한 셀의 셀-다항식이 공격자에게 노출되었다 하더라도 다른 셀의 안전성에는 영향을 주지 못한다.

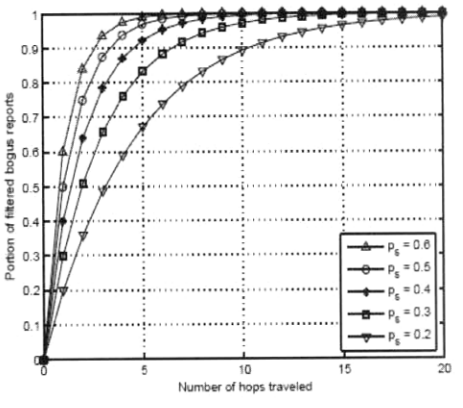
5.3 라우팅 경로에서의 데이터 필터링

논문에서 제안한 방법은 중간 노드가 확률 p_s에 의해 수신한 보고서를 검증한다. 중간 노드가 l홉 이내에 위조된 보고서를 발견하고 그것을 무시할 기대 확률은 다음과 같다.

$$1-(1-p_s)^l$$

(그림 1)은 홉 수가 증가함에 따라 위조된 보고서를 발견할 확률을 보여준다. (그림 1)에서 보듯이, 필터링 능력을 높이기 위해 p_s을 0.6으로 높게 책정했을 경우 단지 다섯 홉 이내면 위조된 데이터를 발견할 확률이 99%가 된다. 하지만 p_s을 높인 만큼 무선 센서 네트워크 내의 계산 오버헤드는 증가한다. 그렇지만 계산 오버헤드를 낮추기 위해 p_s을 0.2로 낮게 책정했을 경우 다섯 홉 이내의 필터링 능력은 68%로 밖에 되지 않는다. 이와 같이 계산 오버헤드와 필터링 능력은 트레이드오프 관계이기 때문에 p_s은 필요에 따라 적절한 값을 책정해야 한다.

많은 수의 위조된 데이터가 발견되었을 때, 필터링 능력을 높일 필요가 있다. 이를 위해 추가적인 메모리 오버헤드



(그림 1) 증가하는 홉 수에 따라 위조된 보고서가 발견될 확률

없이 p_s을 증가시켜 필터링 능력을 높일 수 있다. 그렇지만 기존의 방법들[15, 19]은 p_s을 증가시키기 위해 배치 전에 각 노드의 메모리에 미리 저장되는 키의 수를 증가시키므로 그에 따른 메모리 오버헤드도 증가하게 된다. 기존의 방법과 본 논문에서 제안된 방법의 이러한 차이점은 매우 중요하다. 그 이유는 제안된 방법은 배치 전에 미리 저장되는 키의 수 증가 없이 라우팅 경로 상에서 충분한 필터링 능력을 발휘할 수 있기 때문이다.

5.4 통신 오버헤드와 계산 오버헤드

제안된 방법과 LTE 방법은 비슷한 통신 오버헤드와 계산 오버헤드를 갖는다. 일반적으로 G_1안의 점은 170비트[2]이고 SHA-1이 사용하는 해쉬 함수의 크기는 160비트이기 때문에 전체 통신 오버헤드는 330비트이다. 이 정도의 크기는 RSA 서명 사이즈의 절반 이하이다. 보고서의 타당성을 검증하기 위해, 중간 노드는 LTE 방법과 같이 두 개의 pairing과 한 개의 지수 연산이 필요하다. G_2에 사용되는 해쉬 함수, 대칭 암호 그리고 곱셈과 같은 암호학적 요소의 계산 오버헤드는 pairing과 지수 연산에 비해 무시할 만한 수준이다.

6. 결 론

Zhang의 위조된 데이터 필터링 방법은 필터링 능력을 증가시키기 위해 비대칭 임계값 서명 기술을 적용하였다는 것에 의미가 있다. 본 논문에서는 Zhang이 제안한 LTE 방법을 간단히 소개하였고, LTE 방법이 치명적인 두 가지 취약성을 지니고 있다는 것을 보여주었다.

첫 번째 취약성은 센서 노드가 이벤트를 감지한 후 서명값을 생성하기 위해 AP와 데이터를 송수신하는 과정에서 악의적인 AP에 의해 셀 키와 그에 대한 다수의 공유 정보가 공격자에게 노출된다는 것이다. 그리고 두 번째 취약성은 하나의 셀에 대한 정보가 공격자에게 노출되었을 경우, 각 셀에 대한 독립적인 안전성을 보장할 수 없다는 것이다.

이러한 치명적인 취약성을 수정하기 위하여 논문에서는 AP가 아닌 각 센서 노드가 비밀 정보를 생성하고 각 셀에

독립적인 셀-다항식과 셀-인증자 벡터를 사용하여 향상된 방법을 설계하였다. 그 결과 LTE 방법이 의도한 필터링 능력의 손실없이 취약성을 수정할 수 있었다.

참 고 문 헌

[1] K. Barr and K. Asanovic, "Energy aware lossless data compression," pp.231-244, 1st Int. Conf.Mobile Syst., Applicat., Services, May 2003.

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," pp.514-532, in Proc. Asiacrypt' 01, Lecture Notes in Computer Science, vol. 2248, Dec. 2001.

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

[4] "Digital Hash Standard," federal information processing standards publication 180-1, Apr. 1995.

[5] W. Du, J. Deng, Y. S. Han, S. Chen, and P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," pp.586-597, IEEE INFOCOM 04, Mar. 2004.

[6] W. Du, J. Deng, Y. S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," pp. 228-258, ACM Transactions on Information and System Security, Aug. 2005.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," pp.41-47. 2002, ACM CCS 02, Nov. 2002.

[8] G. Gaubatz, J. Kaps, and B. Sunar, "Public keys cryptography in sensor networks?revisited", pp.2-18, ESAS 04, Aug. 2004.

[9] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUS," pp.119-132, CHES 04, Lecture Notes in Computer Science, vol. 3156, Aug. 2004.

[10] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," pp.41-77, ACM Transactions on Information and System Security, Feb. 2005.

[11] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," pp.71-80, IEEE SECON 04, Oct. 2004.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," pp. 189-199, ACM/IEEE Internation Conference on Mobile Computing and Networking, Jul. 2001.

[13] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Chang, "Energy analysis for public-key cryptography for wireless sensor networks," IEEE PERCOM 05, Mar. 2005.

[14] R. Watro, D. Kong, S. fen Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," pp.59-64, ACM SASN 04, Oct. 2004.

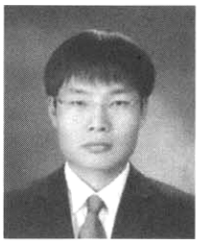
[15] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," vol.23, no.4, pp.839-850, IEEE JSAC, Special Issue on Self-Orgazing Distributed Collaborative Sensor Networks, Apr. 2005.

[16] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing sensor networks with location-based keys," pp.1909-1914, IEEE WCNC 05, Mar. 2005.

[17] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks,", vol.24, no.2, pp.247-260, IEEE JSAC, Special Issue on Security in Wireless Ad Hoc Networks, Feb. 2006.

[18] Y. Zhang, W. Liu, W. Lou, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," vol.24, no.4, pp.829-835, IEEE JSAC, Special Issue on UWB Wireless Communications - Theory and Applications, Apr. 2006.

[19] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," pp.259-271, Proc. IEEE Symp. Security Privacy, May 2004.



조 관 태

e-mail : ckt27@korea.ac.kr

2005년 2월 고려대학교 컴퓨터학과 (학사)

2005년 3월~현재 고려대학교 정보경영 공학전문대학원 석사과정

관심분야 : 키 교환, USN 데이터베이스 보안, USN 위치 기반 프라이버시

김 용 호

e-mail : optim@korea.ac.kr

2000년 2월 고려대학교 수학과 (학사)

2002년 2월 고려대학교 수학과 (이학석사)

2005년 3월~현재 : 고려대학교 정보경영 공학전문대학원 박사과정

관심분야 : 정보보호 프로토콜, 암호이론, RFID/USN 보안 이론, 키 교환

이 동 훈

e-mail : donghlee@korea.ac.kr

1983년 8월 고려대학교 경제학과 (학사)

1987년 12월 Oklahoma University 전산학 (공학석사)

1992년 5월 Oklahoma University 전산학 (공학박사)

1992년 8월 단국대학교 전자계산학과 전임강사

1993년 3월~1997년 2월 고려대학교 전산학과 조교수

1997년 3월~2001년 2월 고려대학교 전산학과 부교수

2001년 2월~현재 고려대학교 정보경영공학전문대학원 교수

관심분야 : 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술