무선 센서 네트워크에서 Self-healing 방법을 사용한 그룹키 관리

이재원*, 김형찬, R.S. 라마크리시나
광주과학기술원 정보통신공학과
{jwlee80*, kimhc, rsr}@gist.ac.kr

Group Key Management with Self-healing for Wireless Sensor Networks

JaeWon Lee*, Hyung Chan Kim, R.S. Ramakrishna
Department of Information and Communications
Gwangju Institute of Science and Technology

요 약

Self-healing 키 분배 방법은 불안정한 채널에서 규모가 크고 동적인 그룹에 적합하다. 제한된 전력과 컴퓨팅 능력을 가진 다수의 노드들을 기반으로 하는 센서네트워크 환경에서 self-healing 키 분배 방법은 효율적인 키 분배를 제공할 수 있는 접근법이다. 더불어 local collaboration은 같은 그룹에 속한 노드들이 서로 협력하여 그룹 키를 보호하고 침입자에 의해 손상된 노드를 발견할 수 있는 유용한 방법이다. 본 논문에서는 기존의 self-healing 키 분배 방법을 보완하여 센서네트워크 환경에 적용하기 위하여 임의의 변수를 적용한 지역적 협력(local collaboration)을 사용한다. 결과적으로 그룹 단위로 키를 안전하게 분배 및 관리를 할 수 있으며 센서 노드들 간의 통신비용 및 메모리에 대한 효율성 향상을 가져올 수 있음을 실험을 통하여 검증한다.

1. 서론

센서 네트워크 환경에서는 노드 topology 구성이 가변적이어서, 노드 그룹의 크기와 구성이 동적인 특성으로 인한 보안 문제를 내제하고 있다[1]. 그리고 네트워크 환경에 따라 키 분배 과정이 성공적으로 이루어지지 않은 경우도 발생할 수 있다. 기존의 키 분배 방식의 상당수는 키의 재분배 요청 프로토콜에 의존하거나 안전한 키 분배 자체를 위한 메커니즘을 구현해야만 했다. 그로 인한 성능저하와 관련된 문제가 꾸준히 제기되어 왔다.

본 연구에서는 센서 네트워크에서의 효율적인 키 분배를 위하여 self-healing 키 분배 방법을 이용한 스킴을 제안하고자 한다. self-healing 키 분배에서 센서노드는 단지 키와 관련된 정보가 담긴 브로드캐스트 메시지를 수신하면 되기 때문에 노드의 계산량에 부담을 주지 않는 장점이 있다. 하지만 이 방법은 다항식 기반의 키(polynomial -based key)를 그룹 키로 사용하기 때문에 외부 침입자에게 다항식 차수(t) 이상의 키와 관련된 다항식 정보(polynomial share)들이 누출이 되면, 외부 침입자가 해당 그룹의 그룹 키를 유도할 수 있는 문제가 있다. 이에 본 논문에서는 self-healing 키 분배 방법을 적용하는데 있어서 랜덤 변수(Random variance-based)를 기반으로 지역적으로 이웃한 노드들끼리 협력적인 방법(Local collaboration)[2]을 사용하여 효율적이고 안전한 그룹 키 관리 방법을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 센서 네트워크 환경에서의 그룹 키 관리에 관한 연구를 알아보고, 3절에서는 센서네트워크 환경에서의 self-healing 키 분배 방법을 적용한 스킴에 대해 서술한다. 4절에서는 3절에서 기술한 내용을 바탕으로, 랜덤변수 기반의 지역적 협력 개념을 도입하여 확장된 방법을 제안한다. 5절과 6절에서는 제시한 방법의 안전성 및 효율성 분석과 더불어 결론을 맺는

다.

2. 관련 연구

LEAP(Localized Encryption and Authentication protocol)[3]은 개인키, 대칭키(pair-wise key), 클러스터 키(cluster key), 그룹 키의 4가지 암호 키를 사용한다. 이 방식에서 공격노드는 개인키를 알 수 없으며, 대칭 키와 클러스터 키는 지역적으로 이웃한 노드들을 인증하기 위해서 사용된다. 그룹 키는 노드가 배치되기 전에 각 노드들에게 할당되어서 브로드캐스트 되는 데이터를 복호화 하는데 사용된다. LEAP의 장점 중 한 가지는 위협 노드에 의해 주변 이웃 노드들이 위험한 상황에 노출되는 경우라도 보안유지가 가능하다는 것이다. 하지만 LEAP의 그룹 키 분배 방식은 노드가 배치되기 전에 할당되기 때문에 위의 4가지 키들은 제대로 갱신될 수 없다는 단점이 있어 센서네트워크에서 사용되는 다중 세션(multi-session)환경에 적용될 수 없다는 단점이 있다.

지역적인 협력(Local Collaboration)을 통한 Group Key Distribution[4]에서는 그룹 키를 분배 및 관리를 할 때, 베이스 스테이션(base station)으로부터 브로드캐스트 되어 전송되는 그룹 키의 정보와 노드가 배치되기 전에 미리 할당되어진 다항식 구성 정보(share)들을 바탕으로 한다. 이를 가지고 노드들 사이의 지역적인 협력을 통하여 하나의 그룹 키를 생성 및 갱신을 하는 키 관리 메커니즘을 소개하고 있다. 그러나 이 방법에서 사용하고 있는 그룹 키 생성이 다항식을 기반으로 하고 있기 때문에 다항식 차수(t개) 이상의 키와 관련된 polynomial share가 누출될 경우 해당 그룹 키를 외부 침입자가 유도해 낼 수 있는 단점이 존재한다. 또한 이 방법은 self-healing 키 분배 시, 브로드캐스트 단계에서 베이스 스테이션으로부터 할당받은 키 생성과 관련된 정보를 노드 상에 저장할 때 저장 공간의 효율성을 고려하지 않은 문제가 있다.

본 논문에서는 센서 네트워크상에서 self-healing 키 분배를 위하여 브로드캐스트와 지역적 협력을 통한 방법을 개선하여 랜덤 변수를 기반으로 하는 효율적인 self-healing 키 분배 방법을 제안한다.

3. Self-healing 키 분배 기법의 적용

본 절에서는 잃어버린 세션의 그룹 키 정보를 노드 스스로 복원해 낼 수 있는 self-healing 키 분배 방식[1, 5]을 센서 네트워크 환경에 맞게 적용시켜 보고자 한다. 그리고 그룹에 속하지 않는 센서 노드들의 빠른 감지 및 추적을 위하여 그룹에 속하는 노드들 사이의 지역적 협력(Local collaboration)[4] 개념을 도입한다.

제안하는 self-healing 키 분배 방식의 절차는 다음과 같다.

1. 설정 단계

a. 베이스 스테이션(base station)은 m개의 2t차수의 다항식 $\{h_i(x)\}_{i=1,\cdots,m}$를 랜덤한 방법으로 선택한다. 그리고 t차수의 다항식 $\{d_i(x)\}_{i=1,\cdots,m}$와 $\{a_i(x)\}_{i=1,\cdots,m}$를 각각 m개씩 선택한다.

b. 세션 i마다의 다항식 $f_i(x)$를 다항식 $a_i(x)$와 $b_i(x)$($b_i(x)=f_i(x)-a_i(x)$)의 형태로 나타낸다.

c. 각 센서 노드 U_v에게 $\{h_i(v), d_i(v)\}_{i=1,\cdots,m}$를 분배한다.

2. 브로드캐스트 단계

(1) $g(x)=(x-r_1)(x-r_2)\cdots(x-r_{w_i})$, $1\le i\le j$

(2) $\{R_i\}_{i=1,\cdots,j} || \{ w_i(x) = g(x)a_i(x)+h_i(x) \}_{i=1,2,\cdots,j} || \{ w_i'(x) = b_i(x) + d_i(x) \}_{i=j,j+1,\cdots,m}$

베이스 스테이션은 메시지 (1), (2)를 모든 그룹 멤버 노드들에게 브로드캐스트 한다.

3. 각 노드의 개인키 복원 단계

각각 멤버노드 u는 $a_i(x)$와 $b_i(x)$를 측정하여 세션 j의 비밀 키 $f_j(u)$를 얻어낸다. 그리고 아래와 같은 secret-share들을 저장한다.

◦ $\{ a_1(u),\cdots,a_{j-1}(u),b_{j+1}(u),\cdots, b_m(u) \}$

4. self-healing의 적용

특정한 세션 j에서 멤버노드 u가 브로드캐스트 메시지를 받지 못하여 세션 비밀 키를 얻지 못한 경우, 직전의 세션 j_1의 share들 중에서 $a_j(u)$와 직후의 세션 j_2의 share들 중에서 $b_j(u)$를 가지고 세션 j의 비밀 키 $f_j(u)$를 복원하게 된다.

$$f_j(u) = a_j(u) + b_j(u)$$

이와 같이 각 노드마다 개인 비밀 키를 보유하게 되면, 그룹 키를 얻기 위한 협력 과정을 수행하기 위하여 각 멤버 노드를 중심으로 주변의 멤버 노드들과 하나의 소규모 그룹을 구성한다. 각 노드는 이웃 멤버노드들과 개인 비밀 키를 서로 교환한다. 이 과정을 거친 후, 각 노드는 이웃으로부터 획득한 비밀 키들을 가지고 세션 j의 그룹 키를 유도한다. 여기서 중요한 것은 주변 노드가 자신의 그룹에 속하는지를 구분하는 것이다. 이를 판별하는 방식은 크

게 두 가지로, (i) 그룹 키를 분배하는 주체인 베이스 스테이션이 그룹멤버가 아닌 노드를 추적하는 방법과 (ii) 주변 노드들이 추적하는 방법이 있다. 본 연구에서는 후자를 기반으로 하여 주변 노드들이 서로 협력하도록 함으로써 그룹에 속하지 않는 멤버를 추적하는 방법을 택하였다[6][7]. 이것은 전복되거나 그룹에 속하지 않는 노드를 찾을 때, 후자의 경우가 전자의 경우보다 거리상 훨씬 가까워 주변 노드의 변화를 신속히 파악할 수 있기 때문이다. 그리고 베이스 스테이션이 일괄적으로 추적을 수행할 때보다 주변 노드들이 병렬적으로 수행할 때 더 효율적이기 때문이다.

4. 랜덤 변수 기반의 지역적 협력

그룹의 멤버 노드들 사이에 공유하는 그룹 키는 다항식을 기반으로 하기 때문에 외부 침입자가 해당 다항식의 차수 t만큼의 비밀 키를 획득할 수 없도록 하는 것이 필요하다. 더욱이 본 논문에서 제시하는 기본 골격이 노드들끼리 소그룹을 이루어서 협력하는 체제이기 때문에, local collaboration에 적합한 방식을 도입할 필요성이 대두된다.

이에 본 절에서는 Random Variance-based PCGR (RV-PCGR) scheme[2]에서 제시한 방법을 토대로 각 노드마다 주어진 보조키를 가지고 그룹 키를 보호하는 방법을 살펴본다.

여기서 보조키는 그룹 멤버들이 지역적 협력을 할 때 노드들끼리 공유하는 그룹 키 성격을 지니고 있으며 노드가 미리 배치될 때 할당된다. 보조키는 주위의 이웃 센서노드들과 주기적으로 협력하여 키 갱신을 하게 된다.

그림 2에서 볼 수 있듯이, 각 노드 u는 보조키의 share 부분인 g(i)를 본래의 크기 L에서 2L로 늘린 후 보조키의 share를 암호화할 다항식의 share e(i)와 L 크기의 랜덤변수 $б_i$를 덧붙여서 임의의 연산들(XOR연산, 덧셈, 곱셈 등)을 거친 결과인 $g^r(i)$을 보조 개인키로 보관하게 된다. 이로 인해, 외부침입자는 어떤 멤버노드로부터 탈취하게 될 보조키는 $g^r(i)$이다. 결국 외부침입자는 보조키 g(i)이 아닌 $g^r(i)$을 가지고 보조키를 유도하려 할 것이다. 그러나 실제 보조키는 지역적 협력을 하는 노드들은 $g^r(i)$의 앞부분인 g(i)을 가지고 유도된다.

위의 과정으로 유도된 보조키는 앞서 언급한 실제적인 그룹 키의 근간이 되는 비밀 키를 센서 노드들끼리 주고받을 때 암호화 및 복호화 하는 과정에서

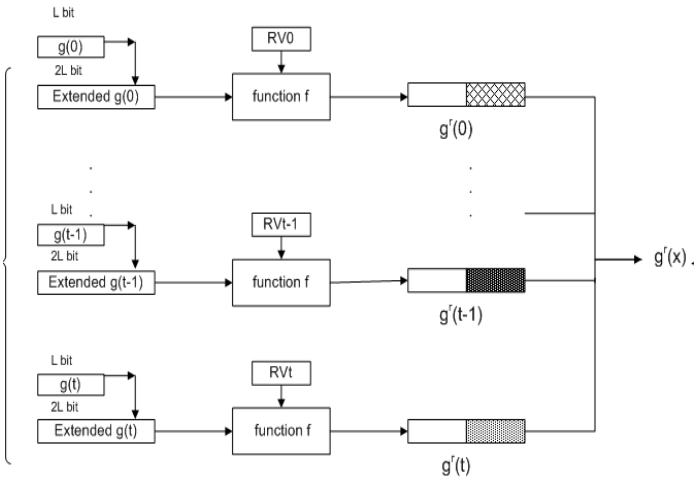

그림1. 랜덤변수 기반 보조키 생성과정

사용된다. 이 절에서 사용된 방식은 외부침입자가 원래의 보조키를 획득하기 위해서는 랜덤변수 $б_u$를 찾아내는 것이 필요한데, $б_u$는 0에서 2^L - 1사이에 속하는 임의의 숫자이기 때문에 침입자가 이 랜덤변수를 찾기 힘들다는 점과 이러한 랜덤변수를 t+1 만큼 더 찾아야 한다는 점을 이용하여 다항식을 기반으로 하는 키의 약점을 극복하고 있음을 알 수 있다.

5. 평가 및 실험

본 절에서는 제시한 방법들의 타당성을 검증하기 위하여 안전성과 효율성 분석을 한다. 안전성 측면은 수학적인 모델에 근거하여 분석하였고, 효율성 측면은 TinyOS 1.1.10 버전에서 구현하여, 기존의 방법과 제시한 방법을 비교하여 분석하였다.

5-1. 안전성 분석

개인키의 분배 및 그룹 키의 유도를 할 때, 그룹 키의 보안 유지는 랜덤변수를 기반으로 하는 보조키의 안전성에 의존하게 된다. 이 절에서는 보조키의 안전성을 아래와 같이 분석해 보고자 한다.

먼저, 외부침입자가 t +1개의 $g^r(i)$를 획득하였다고 가정을 하자. 그러면 외부침입자는 g(x)를 유도하기 위해 아래의 수식을 사용하려 한다[2].

$$g(x) = \sum_{i=0}^{t} a_i x^i$$

$б_u \in \{0,1, \ldots ,2^L-1\}$ (i=0,...,t)에서

a. $$f(g^r(0), б_i) = \sum_{i=0}^{t} 0^i a_i'$$

$$f(g^r(1), б_i) = \sum_{i=0}^{t} 1^i a_i'$$

. . .

$$f(g^r(u),\sigma_i)=\sum_{i=0}^{t}u^i a_i'$$

a의 수식에서 알 수 있듯이, 외부침입자는 g(x)를 유도해내기 위해서는 t +1개의 항으로 이루어진 t + 1 개의 등식을 풀어야 함을 알 수 있다.

b. $f(g^r(u),\sigma_v)=E_{\sum_{j=0}^{t}e_{v,j}(c)\oplus\sigma_v'}[g^r(c)]$

그리고 b의 수식에서 외부침입자는 0부터 2^L-1사이에서 랜덤변수를 정확히 찾아낼 확률이 $\frac{1}{2^L}$이고, 이러한 확률을 고려하여 t + 1개에 해당하는 share를 암호화하는 다항식의 랜덤변수를 모두 찾을 확률은 $\frac{1}{2^{2(t+1)}}$임을 알 수 있다.

위의 a와 b에서 드러난 안전성을 바탕으로 만들진 보조키를 가지고 3절에서 언급한 개인키를 암호화하게 되므로, 개인키 그 자체와 그것을 바탕으로 만들어지는 그룹 키에 대한 안전성이 더욱 견고해진다는 점을 명확하게 알 수 있다.

5-2. 효율성 비교

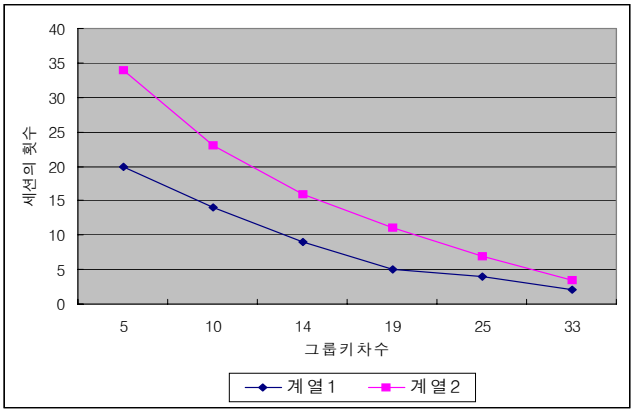

그림2. 서로 다른 self-healing 스킴에 따른 브로드캐스트 패킷의 효율성 비교

본 논문에서 제시한 방법을 평가하기 위하여 하나의 브로드캐스트 메시지 단위가 수용할 수 있는 그룹 키의 차수와 세션의 횟수를 기준으로 효율성 분석[5]을 하였다.

그림 2에서 계열1의 경우는 기존의 self-healing 방법을 TinyOS에서 실험한 경우이며 계열2의 경우는 본 논문에서 제시한 발전된 self-healing 방법과 그와 관련된 보조 기법들을 적용하여 TinyOS에서 실험한 결과이다.

그림2에서 볼 수 있듯이, 제시한 방법이 하나의 패킷 단위당 다양한 세션의 횟수와 더 큰 그룹차수를 수용할 수 있다는 것을 알 수 있다. 수치상으로는 대략 2배에 가까운 효율성을 보인다. 그러므로 본 논문에서 제시한 방식이 브로드캐스트 메시지의 양을 효율적으로 줄일 수 있으며 이로 인해 그룹 멤버노드의 저장량 또한 줄일 수 있다는 것을 확인할 수 있다.

6. 결론 및 추후과제

본 논문에서는 센서 네트워크 환경을 위하여 기존의 self-healing 키 분배 방법을 보완하였으며 이를 TinyOS 상에서 구현하였다. self-healing 키 분배 방식이 다항식 기반의 키를 사용함으로써 발생 할 수 있는 한계점에 대한 방안을 제시하였다.

추후 과제로는 침입 탐지와 관련된 연구를 수행할 예정이고, sliding-window 개념을 도입하여 저장 공간과 통신비용에 좀 더 효율성을 기하는 방향으로 연구를 진행할 것이다. 이번 연구에서는 3절에 해당하는 부분만 TinyOS에서 실험 하였으나, 추후에는 아직 구현하지 않은 나머지 부분과 추후 연구 과정 중에 추가될 방법들도 고려하여 TinyOS에서 실험을 할 예정이다.

참고문헌

[1] M. Franklin, D. Balfanz, M. Malkin, J. Staddon, S. Miner and D. Dean, "Self-healing key distribution with revocation" in Preceedings of IEEE Symposium and on Security and Privacy, Oakland, CA, 2002.

[2] W. Zhang, G. Cao, "Group rekeying for filtering false data in sensor networks: a predistribution and local collaboration-based approach" in IEEE INFOCOM 2005, 2005.

[3] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", The 10th ACM Conference on Computer and Communications Security, 2003.

[4] A. Chadha, Y. Liu, and S. K. Das "Group Key Distribution via Local Collaboration in Wireless Sensor Networks", 2005 Second Annual IEEE Communications Conference, 2005.

[5] D. Lui, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability" in Proceedings of ACM CCS, Washington D.C., WA, 2003.

[6] G. Itkis, D. Micciancio, M. Naor, R. Canetti, J. Garay and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions", in IEEE INFOCOMM '99, 1999.

[7] S. Marti, T. J. Giuli, K. Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proceedings of ACM Mobicom, Boston, MA, 2000.