무선 센서 네트워크에서 슬라이딩 윈도우 개념이 적용된 Self-healing을 사용하는 그룹키 관리

이재원, 김형찬, R.S. 라마크리시나
광주과학기술원 정보통신공학과

Group Key Management with Self-healing Applying the Concept of Sliding-window 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 기법은 불안정한 네트워크 환경에서 그룹 키를 설정할 수 있게 하며, 그룹을 가입하거나 탈퇴하는 멤버 노드들에 의한 공모 공격에 대한 안전성으로 인하여, 센서 네트워크 환경에 적합한 방식이다. 하지만 기존에 제안된 Self-healing 키 분배 기법들은 브로드캐스트 되는 메시지의 통신량과 그룹 멤버의 그룹 키 복원을 위한 정보 저장량 측면에서 비효율적인 문제가 있다. 본 논문에서는 슬라이딩 윈도우(Sliding Window) 개념을 도입함으로써 향상된 Self-healing 키 분배 기법을 제안하여, 브로드캐스트 되는 메시지의 크기를 줄이고 멤버 노드 단위의 메모리에 대한 효율성을 향상시킨다.

I. 서론

센서 네트워크는 노드 그룹의 규모와 구성이 동적인 특성으로 인한 보안 문제를 내제하고 있다[1]. 그리고 네트워크 환경에 따라 키 분배 과정이 성공적으로 이루어지지 않는 경우도 발생할 수 있다. 이러한 문제를 해결할 수 있는 방법으로써, Self-healing 키 분배 기법[2][3]은 노드가 몇몇 키 정보들을 분실하더라도 베이스 스테이션에게 추가적인 전송을 요청하지 않고 그룹 키를 복원할 수 있으며, 센서노드들은 단지 키와 관련된 정보가 담긴 브로드캐스트 메시지만 수신하면 되기 때문에 노드의 계산량에 부담을 주지 않는 장점이 있다[4].

그러나 적은 메모리, 제한된 배터리 용량과 컴퓨팅 성능의 제약 등 제한된 하드웨어 자원을 사용하는 센서 네트워크 환경에서 기존의 Self-healing 키 분배 기법을 그대로 도입한다면, 통신비용 및 노드 단위의 저장량 측면에서 효율적이지 못한 단점이 있다. 그리고 기존의 Self-healing 키 분배 기법은 모든 세션에 대하여 브로드캐스트 메시지가 공정하게 전달되지 못하는 문제점을 가지고 있기 때문에, 초반부 세션이나 후반부 세션에는 그룹 키 복원의 기회가 상대적으로 줄어드는 문제점이 있다.

본 연구에서는 센서 네트워크 환경에 보다 적합하고 효율적인 키 분배 및 관리를 위하여, 기존의 Self-healing 키 분배 기법을 센서네트워크 환경에 맞게 개선하고자 한다. 이를 위하여 슬라이딩 윈도우(Sliding-window) 개념을 도입함으로써 브로드캐스트 메시지의 크기를 최소로 줄이고 각 멤버노드가 저장해야할 그룹 키 복원 정보의 양 또한 상당히 줄일 수 있는 효율적이고 신뢰성 있는 Self-healing 키 분배 기법을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 2절에서는 Self-healing 키 분배 기법에 적용할 슬라이딩 윈도우 개념의 도입 및 개선책을 제안한다. 3절에서는 2절에서 제안한 내용을 바탕으

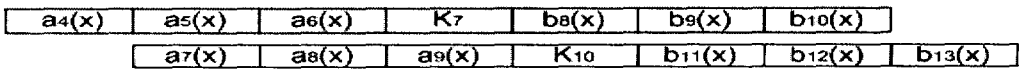


그림 1: δ = 3일 때, 세션7과 10에서 전송되는 브로드캐스트 메시지

로, 발전된 Self-healing 키 분배 기법을 서술한다. 4절에서 제시한 기법의 효율성을 검증한 후에 5절에서 향후과제와 함께 결론을 맺는다.

II. Sliding-window 개념의 도입 및 개선

기존의 Self-healing 키 분배 기법[2][3]에서 브로드캐스트 메시지를 분석해보면, 메시지 내부에 키를 복원하는데 사용되는 그룹 키 복원 정보가 필요 이상으로 많이 포함되어 있다. 다중 세션 환경으로 확장하여 고려해 볼 때, 특정한 세션에 대한 그룹 키 정보의 일부가 과다한 반복전달이 이루어지고 있음을 알 수 있다. 또한 기존의 방식은 그림 2에서 볼 수 있듯이, 초반부 세션과 후반부 세션에서는 그룹 키 복원 정보의 일부가 편중되어 전송 및 저장이 되고 있음을 알 수 있다. 이는 Self-healing 키 분배 과정이 특정한 세션에서 그룹 키를 복원하는데 필요한 구성요소의 부재로 인하여 그룹 키를 복원할 수 없는 상황으로 이어질 수 있다.

본 절에서는 Sliding-Window Self-Healing [4]에서 제시한 방법을 토대로 위의 단락에서 제시한 문제점들을 보완할 수 있는 방법을 살펴보고자 한다.

세션들의 횟수를 m이라 하고, 그림 2와 3에서 다항식 $a_i(x)$와 $b_i(x)$의 미지수 x에 대입된 숫자 2를 노드 ID라 하자.

그림 1에서 볼 수 있듯이 슬라이딩 윈도우 메커니즘을 적용하면, 브로드캐스트 메시지는 모든 세션에 해당하는 그룹 키 복원 정보를 포함하지 않고 현재 세션 j를 기준으로 이전의 δ 만큼의 세션과 이후의 δ 만큼의 세션에 해당하는 복원 정보들을 메시지에 포함한다. 즉, 현재 세션 j에서 브로드캐스트 메시지는 $a_i(x)$($i \in [j-\delta, \cdots, j-2, j-1, j]$), $b_i(x)$($i \in [j, j+1, \cdots, j+\delta]$), 세션 j의 그룹 키 K_j($K_j = a_j(x) + b_j(x)$)들로 구성되어 있다. 예를 들면, 그림 1에서 위의 메시지 두 개를 가지고 세션 7, 10의 키를 획득할 수 있으며 동시에, 세션 8, 9에서 브로드캐스트 메시지를 받지 못하였을지라도 세션 8, 9에 해당하는 그룹 키 또한 복원할 수 있다.($\because K_8 = a_8(x) + b_8(x)$, $K_9 = a_9(x) + b_9(x)$)

$K_1(2), \ldots, b_{i-1}(2), b_i(2), b_{i+1}(2), \ldots, b_m(2)$
$\cdots$
$a_1(2), \ldots, K_{i-1}(2), b_i(2), b_{i+1}(2), \ldots, b_m(2)$
$a_1(2), \ldots, a_{i-1}(2), K_i(2), b_{i+1}(2), \ldots, b_m(2)$
$a_1(2), \ldots, a_{i-1}(2), a_i(2), K_{i+1}(2), \ldots, b_m(2)$
$\cdots$
$a_1(2), \ldots, a_{i-1}(2), a_i(2), a_{i+1}(2), \ldots, K_m(2)$

그림 2: 기존의 Self-healing 키 분배 방식을 적용할 경우, 각 노드가 저장하게 될 그룹 키와 그룹 키 정보들

$a_{m-2}(2), a_{m-1}(2), a_m(2), K_1(2), b_2(2), \underline{b_3(2)}, b_4(2)$
$a_{m-1}(2), a_m(2), a_1(2), K_2(2), \underline{b_3(2)}, b_4(2), b_5(2)$
$\cdots$
$a_1(2), a_2(2), \underline{a_3(2)}, K_4(2), b_5(2), b_6(2), b_7(2)$
$a_2(2), \underline{a_3(2)}, a_4(2), K_5(2), b_6(2), b_7(2), b_8(2)$
$\underline{a_3(2)}, a_4(2), a_5(2), K_6(2), b_7(2), b_8(2), b_9(2)$
$\cdots$
$a_{m-3}(2), a_{m-2}(2), a_{m-1}(2), K_m(2), b_1(2), b_2(2), \underline{b_3(2)}$

그림3: Sliding-Window 개념의 도입 후, 각 노드가 저장하게 될 그룹 키와 그룹 키 정보들(δ =3인 경우)

이 방식은 현재 세션을 기준으로 그룹 키 복원이 발생할 가능성이 있는 세션들에 한해서만 그룹 키 복원 정보들만 전송한다. 즉, 각 세션마다 전송되는 브로드캐스트 메시지들은 모든 세션에 해당하는 그룹 키 복원 정보들을 모두 포함할 필요가 없다. 그러므로 그림 2와 3에서 볼 수 있듯이, 각 세션마다 노드가 획득하는 그룹 키 정보의 개수는 슬라이딩 윈도우 개념을 도입하기 전에는 m-1개이며, 도입 후에는 $2*\delta$ 까지 줄일 수 있다($\delta < m/2$).

그림 2에서 보면, i번째 세션을 기준으로 과거 세션의 키 정보 방향으로 이동할수록 b(x) 다항식의 개수가 줄어들고 a(x) 다항식의 개수는 늘어나고 있다. 이는 각 세션의 그룹 키를 구성하는 정보인 a(x)와 b(x)의 분배가 불균형을 이루고 있음을 의미한다. 초반부 세션에서 그룹 키를 획득하지 못하여, 이를 복원하고자 할 때, 소수의 b(x)마저도 획득하지 못한다면 이 세션에 해당하는 키를 복원할 방법은 전혀

없을 것이다. 뿐만 아니라 후반부 세션에서도 비슷한 현상이 발생하고 있다. 따라서 본 연구에서는 슬라이딩 윈도우 개념을 도입할 때, 그림 3과 같이 그룹 키 정보들이 순환적인 구조를 이루도록 슬라이딩 윈도우 방식을 개선하였다. 이를 브로드캐스트 메시지에 적용하여, 각 세션마다 두 종류의 그룹 키 복원 정보에 대하여 충분한 횟수의 전송과 고른 분배를 가능하게 함으로써 이러한 문제점을 해결하였다.

III. 슬라이딩 윈도우 개념이 적용된 Self-healing 키 분배 방식

본 절에서는 기존의 Self-healing 키 분배 기법[3][5]을 기본으로 하되 위의 절에서 제시한 슬라이딩 윈도우 개념을 도입하여 적은 통신량과 메모리에 적합한 Self-healing 키 관리 기법을 제시한다.

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) $\{R_i\}_{i=1,\cdots,j}$

|| $\{ w_i(x) = g_i(x)a_i(x) + h_i(x) \}_{i=j-\delta,\cdots,j-2,j-1,j}$

|| $\{ w_i'(x) = r_j(b_i(x) + d_i(x)) \}_{i=j,j+1,\cdots,j+\delta}$

|| $r_j(x) = g_j(x) \% q$

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

3. 각 노드의 개인키 복원 단계

각각의 멤버노드 u는 $g_i(x) \% q$를 계산한다.

$r_i(x)$와 $g_i(x)$를 바탕으로 $a_i(x)$와 $b_i(x)$를 획득한 후에 세션 j의 비밀 키 $f_j(u)$를 얻어낸다. 그리고 아래와 같은 secret-share들을 저장한다.

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

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 복원한다.

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

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.

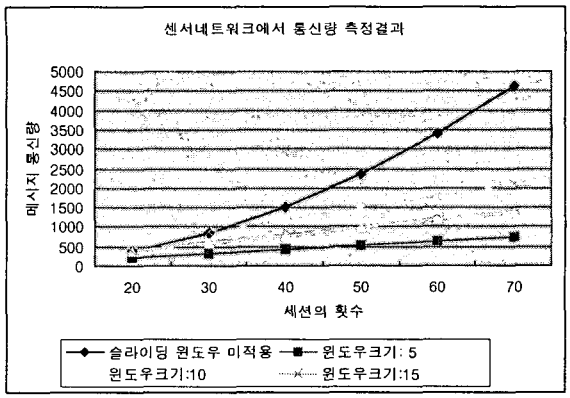
IV. 실험 및 분석

본 절에서는 제안한 메커니즘의 타당성을 확인하기 위하여, 기존의 Self-healing 키 분배 방식과 슬라이딩 윈도우 개념이 적용된 Self-healing 키 분배 방식을 NS-2(Network Simulator 2) 시뮬레이터[6] 상에서 각각 구현하여, 기존의 방법과 제안한 방법을 통신비용과 저장 공간의 효율성 측면에서 비교 및 분석하였다.

본 논문에서 제안한 방법의 우수성을 평가하기 위하여, 센서네트워크 환경에서 키 분배 과정이 이루어질 때의 브로드캐스트 메시지의 크기와 통신량을 평가의 척도로 정하였다.

그림 4에서는 슬라이딩 윈도우 개념을 사용하지 않는 Self-healing 기법과 슬라이딩 윈도우 크기를 다양하게 설정한 Self-healing 기법들을 적용하여 NS-2 시뮬레이터 상에서 실험한 결과이다.

그림 4는 슬라이딩 윈도우 개념을 적용한 Self-healing 키 분배 기법이 그룹 키와 그룹 키 복원 정보를 전달하는데 있어서 훨씬 적은 통신량을 사용하고도 효율적인 키 분배 과정을 완수할 수 있다는 것을 의미한다. 또한 슬라이



※메시지 통신량의 단위 1은 키 복원 정보 혹은 키 하나 단위를 의미함. 메시지 손실률은 3~7%라 가정했음.

그림4: 센서네트워크에서 통신량 측정결과

기법	저장 오버헤드	통신 오버헤드	키 분배 소요시간
[2]의 방식	$m^2 \cdot \log q$	$(3mt+t^2) \cdot \log q$	$t^2 \cdot \log q$
슬라이딩 윈도우 적용 전	$2m \cdot \log q$	$2mt \cdot \log q$	$2t \cdot \log q$
슬라이딩 윈도우 적용 후	$m \cdot \log q$	$\delta \cdot t \cdot \log q$	$t \cdot \log q$

※ m은 세션의 횟수, t는 공모할 수 있는 최대 그룹 멤버의 크기, log q는 다항식계수의 기본 단위임.

그림5: 서로 다른 기법을 적용한 성능분석 결과

딩 윈도우의 크기가 작을수록 메시지 통신량이 줄어들고 있음을 알 수 있다.

그림 5는 위의 실험결과를 바탕으로 각각 저장 오버헤드 측정결과와 통신 오버헤드에 관한 측정결과와 그리고 키 분배 시 소요시간에 대한 성능 분석 결과이다. 즉, 키 분배를 할 때 통신량의 감소되었으며 제시한 Self-healing 키 분배 방식의 간결성으로 인하여 그룹 멤버노드의 저장량 및 키 분배를 수행 시, 소요되는 시간 또한 획기적으로 감소하고 있음을 확인할 수 있다.

그러나 세션의 횟수가 굉장히 커질 때는 슬라이딩 윈도우 크기가 작아질수록 그에 따른 메시지 통신 빈도 또한 높아지기 때문에, 슬라이딩 윈도우 크기가 작다고 하여 통신량 관점에서 반드시 효율적이라고는 볼 수 없다. 그러므로 슬라이딩 윈도우의 크기를 조절하는 문제를 과제로 남기고자 한다.

V. 결론 및 추후과제

본 논문에서는 센서 네트워크 환경을 고려한 Self-healing 키 분배 기법을 효율적으로 구현하기 위하여 슬라이딩 윈도우 개념을 적용하였다. 이를 토대로 향상된 Self-healing 키 분배 기법을 제안하였으며, NS-2에서 시뮬레이션을 통하여 통신비용과 저장 공간상의 효율성을 확인하였다.

추후과제로는 제안된 기법이 Self-healing 키 분배 기법의 기본정의 및 증명모델[2][7]의 모든 조건들을 만족하는지 검증할 예정이며, 이를 통하여 본 논문에서 제시한 기법의 신뢰성 및 안전성을 증명할 것이며 침입 탐지와 관련된 연구 또한 더불어 수행할 예정이다.

[참고문헌]

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", Computer Networks, vol. 38, no. 4, March 2002.

[2] 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.

[3] 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.

[4] S. Miner More, M. Malkin, J. Staddon, and D. Balfanz, "Sliding-window self-healing key distribution" In Proceedings of ACM CCS, 2003.

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

[6] NS-2: http://www.isi.edu/nsnam/ns/

[7] C. Blundo, P. D'Arco, and A. De Santis, " Definitions and Bounds for Self-Healing Key Distribution Schemes" In the Proceedings of ICALP'04, LNCS, 3142 (2004) 234-245.