계층적 센서 네트워크에서 상호 인증을 통한 그룹키 관리 메커니즘

고혜영, 도인실, 채기준
이화여자대학교 컴퓨터공학과
e-mail : nyanglove@naver.com, isdoh@ewhain.net, kjchae@ewha.ac.kr

A Group Key Management Mechanism using Mutual Authentication for Hierarchical Sensor Networks

Hye Young Ko, In Shil Doh, Ki Joon Chae
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

센서 네트워크의 효율적인 구성을 위해서는 이종(異種)의 센서들을 두고 그룹으로 나누어 관리하여야 하며 그룹 내의 안전하고 효율적인 통신을 위해 그룹키가 필요하고 이 키는 주기적으로 갱신되어야 한다.

본 논문에서는 그룹키를 갱신할 때에 필요한 정보들을 이용하여 그룹키 정보를 교환하는 엔티티간의 상호 인증을 함으로써 안전하게 그룹키를 관리할 수 있는 메커니즘을 제안하였다.

1. 서론

센서 네트워크는 유비쿼터스 환경 구축에 있어서 없어서는 안될 필수적인 분야로서 이에 대한 관심이 증가되고 있고 그에 따라 센서 네트워크 기술 연구의 중요성이 강조되고 있다. 센서 네트워크는 군사, 의료, 위치 인식 등 다양한 분야에서 활용되고 있으며 일반적인 네트워크와는 달리 개방형 네트워크이기 때문에 보안이 크게 중요시된다.

본 논문에서는 센서 네트워크의 보안 중에서도 중요한 분야인 키 관리 메커니즘에 초점을 맞추어 polynomial 을 이용하여 클러스터헤드(CH)와 노드간에 그룹키 정보를 교환할 때 상호간 인증을 수행함으로써 그룹키를 안전하게 분배하는 기법을 제안하였다.

2. 시스템 모델 및 가정 사항

먼저 네트워크는 베이스스테이션(BS)과 CH, 그리고 노드로 구성된다. 노드들은 CH 주변에 배치되어 1 홉(one hop)으로 통신이 가능하며 CH 는 보통 노드보다 메모리나 전송범위가 크다. 노드들이 네트워크에 배치된 후 일정 시간 안에는 공격받지 않으며 주기적인 그룹키 갱신을 위해 동기화가 되어 있다.

3. 효율적인 그룹키 분배 기법 제안

본 논문에서는 기존에 제안된 PCGR[1] 기법을 바탕으로 먼저 계층적 센서 네트워크를 구성하기 위해 CH 를 추가하고 이 CH 를 통해 그룹키를 관리하되 [1]에서 일방의 인증만을 수행했던 보안상 취약점을 보완하기 위해 CH 가 보낸 그룹키를 노드가 재인증함으로써 상호 인증을 수행하도록 하였다. 본 논문에서 사용될 표기법은 아래 <표 1>과 같다.

<표 1> 표기법

표기	설명
u, v	노드 아이디
g(x)	CH 와 노드간의 g-polynomial
h(x)	CH 간의 그룹키 g-polynomial
$e_u(x)$	CH u 에서 만들어진 e-polynomial
$E_{g(x)}\{M\}$	M 을 g(x)로 암호화한 메시지
K_{uv}	u 와 v 사이의 pairwise key

3.1 PCGR

PCGR scheme 은 group key polynomial (g-polynomial)인 g(x)를 만들어서 그룹키를 생성하고 이것을 숨기기 위해서 encryption polynomial (e-polynomial)인 e(x,y) 를 생성하며 g-polynomial 을 암호화하여 다음과 같은 g'-polynomial 을 만든다.

$$g'(x) = g(x) + e_u(x,u)$$

e(x,y)는 $e_u(x,v_i)$형태로 주변 노드들에게 보내고 그룹키를 갱신할 때 t+1 개의 $e_u(c,v_i)$ share 들을 노드로부터 돌려받아 다음과 같은 식으로 그룹키를 갱신한다.

$$g(c) = g'(c) - e_u(c,u)$$

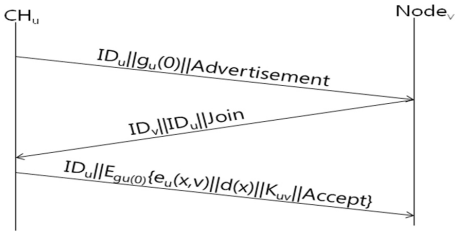
여기서 c 는 count 값으로 그룹키의 버전을 가리킨다.

3.2 그룹키 초기화

먼저 CH 와 노드는 네트워크에 배치되기 전에 BS 로부터 키 정보를 받는다. CH 일 경우, BS 와의 pairwise key, g(x), h(x)를 받고, 노드일 경우, BS 와의 pairwise key 를 받는다. 그리고 BS 는 CH 에게 준 g(x)

를 g(x)=a(x)d(x)+q(x)의 형태로 변환하여 q(x)를 보관한다.

각 CH 는 주변 노드들에게 advertisement 메시지를 보내고 노드는 신호 세기를 비교하여 하나의 CH 만을 선택하고 Join 메시지를 보낸다. CH 는 e(x,y)를 만들어서 g(x)을 암호화하여 g'(x)를 만들고 각 멤버들에게 $e(x,v_i)$를 포함한 Accept 메시지를 보낸다. 그리고 CH 는 자신이 가지고 있던 g(x), e(x,y)를 만들 때 사용했던 $a_e(x)$, h(x)의 $a_e(x)$를 삭제한다.



(그림 1) 그룹키 초기화

3.3 그룹키 갱신

그룹키 갱신에는 두 종류가 있는데 CH 와 노드간의 그룹키 갱신과 CH 간의 그룹키 갱신이 있다.

3.3.1 CH 와 노드 사이의 그룹키 갱신

CH 는 그룹키 갱신을 알리는 메시지를 브로드캐스트하여 노드로부터 받은 $e(c,v_i)$들이 제대로 된 값이 왔는지 검사하기 위해서 $e(c,v_i)$와 $q(c,v_i)$ 각각에 $d(c,v_i)$를 이용한 나머지 연산(modulo)을 수행하여 결과를 비교함으로써 인증을 수행한다. 검증에 통과하지 못한 노드는 그룹키를 전송받지 못한다.

메시지를 받은 노드들은 그룹키를 검증하기 위해 BS 에 q(c)값을 요청하여 받은 노드는 g(c)와 q(c)의 나머지 연산을 통해 그룹키가 제대로 된 값인지 검사한다. 그리고 자신의 옆 노드에게 $e(v_1,v_2)$로 키를 만들어 BS 로부터 받은 q(c)값을 암호화해서 보내 준다. 만약 잘못된 그룹키가 들어온 경우 노드는 BS 에게 CH 가 공격받았음을 알린다.

3.3.2 CH 사이의 그룹키 갱신

CH 간의 그룹키 갱신은 CH 와 노드 사이의 그룹키가 갱신된 후에 진행된다.

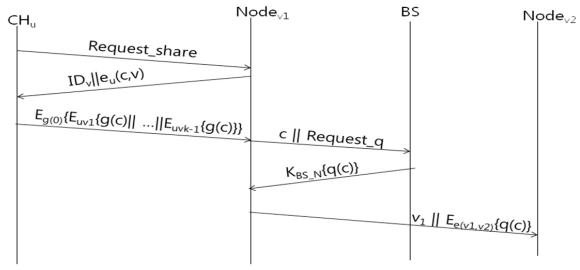
BS 는 공격 당한 CH 들을 제거하기 위해서 아래와 같은 메시지를 보낸다.

$$\text{BS} \Rightarrow \text{CH}: \; a_h(x)(x-w_1)\ldots(x-w_l)\frac{1}{(x-w_1)}\ldots\frac{1}{(x-w_l)}$$

x 에는 CH 의 아이디 값이 들어가고 w 들은 제거되어야 할 CH 의 아이디를 가리킨다.

3.4 새 노드 추가

새로운 노드가 들어오거나 CH 가 없어져서 새로운 그룹을 찾는 노드가 생기는 경우 그룹키 갱신이 필요하다. 갱신이 시작되어 기존 멤버들이 가지고 있던 e(x)의 share 를 받아 e(x)를 복구한 CH 는 새로 들어



(그림 2) CH 와 노드간에 그룹키 갱신

온 노드의 아이디를 받아서 $e(x,v_i)$를 만들어 새로운 그룹키와 함께 BS 에게 보내주고 BS 는 노드와의 pairwise key 로 암호화해서 안전하게 건네주며 d(x)는 그룹 안의 주변에 있는 노드에게 받게 된다. 이렇게 함으로써 새로 들어오는 노드는 이전 그룹키를 알 수 없으며 Backward secrecy 를 만족시킬 수 있다.

3.5 노드 제거

노드가 그룹에서 떠나는 경우 Forward secrecy 를 위하여 그룹키를 갱신할 필요가 있다. 자발적으로 떠나는 경우에는 CH 에게 알리게 되며 CH 는 새롭게 그룹키를 갱신한다. 만약 예상치 못한 이유로 알리지 못하게 되면 CH 는 일정 시간 동안 메시지가 오지 않는 것을 체크하였다가 그룹키를 갱신한다.

4. 결론

본 논문은 기존의 PCGR 의 방법을 이용하여 계층적인 네트워크 안에서 안전하게 키를 분배하는 방법에 대해서 제안하였다. 계층적 네트워크를 위해 CH 를 두어 그룹키를 관리하도록 하였고 노드로부터 받은 부분정보를 인증하는 과정만을 포함하는 기존 방식의 단점을 보완하여 노드의 입장에서도 CH 로부터의 정보를 인증함으로써 상호 인증을 통해 보안성을 강화하였다. 또한 그룹키를 전송할 때 그룹키와 pairwise 키로 중복 암호화하여 보안성을 높이고 노드의 추가 및 삭제 시에 그룹키를 갱신함으로써 Forward/Backward secrecy 를 보장한다.

향후 퀄넷을 이용한 시뮬레이션을 진행하여 기존 PCGR 과 제안된 논문의 성능과 보안성을 비교, 분석할 예정이다.

참고문헌

[1] Wensheng Z, Guohogn C, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboratio-Based Approach", IEEE INFOCOM, 2005

[2] Sencun Z, Sanjeev S, Sushil J, "LEAP+: Efficient Security Mechanisms for Large-Scale Disributed Sensor Networks," ACM Transactions on Sensor Networks, 2006

[3] Jin-Hee C, Ing-Ray C, Mohamed E, "On Optimal Batch Rekeying for Secure Group Communications in Wireless Networks," Wireless Networks, 2007