센서 네트워크 환경에서 유일한 이동 노드를 사용한 트리 구조의 효율적인 그룹 키 관리

성순화
충남대학교 전기정보통신공학부
shsung@cnu.ac.kr

Tree-based Optimized Group Key Management using Unique Mobile Node in Sensor Networks

Soonhwa Sung
Division of Electrical and Computer Engineering College of Engineering,
Chungnam National University

요 약

센서 네트워크에서의 그룹 키 관리가 안전한 그룹 통신을 위해 관심이 증가되고 있다. 본 논문에서는 [1]에서 제안한 그룹 통신을 위한 그룹 키 관리의 단점을 개선한다. 본 논문은 [1]에서의 그룹 리더 대신 알맞은 센서 네트워크 특성을 가진 유일한 이동 노드를 사용하여 효율적인 그룹 키 관리를 한다. 그 결과, 제안한 방안은 [1]에서 제안한 것보다 비용면에서 개선이 있었다.

1. 서 론

센서 네트워크는 센서 노드들이 좁은 영역에 조밀하게 분포되고, 대량의 노드들이 산재하며 이 노드들의 동작이 항상 성공적이지 못하다는 특징으로 네트워크 토폴로지는 매우 빈번하게 변경된다. 이러한 센서 네트워크는 일반적으로 특정 지역에 수없이 많은 센서들이 무작위로 뿌려져서 대상에 대해 감지하고 감지된 데이터를 중앙 베이스스테이션으로 전송하는 구조를 갖는다. 각 센서 노드가 다른 노드의 데이터를 중계하는 기능을 하는 점에서 기존의 모비일 애드 혹 네트워크의 특수한 형태로 간주되기도 하지만, 센서 노드는 일회성을 갖는 경우가 많아 가격도 매우 저렴하고 크기도 작아야 하며 작은 기억 공간, 제한된 계산 능력 등 애드 혹 네트워크보다 훨씬 제약사항이 많다[2].

또한 센서 네트워크는 구조에 따라 크게 분산된 센서 네트워크(Distributed Sensor Network:DSN)와 계층적 센서 네트워크(Hierarchical sensor Network:HSN)로 나눌 수 있다.

분산된 센서 네트워크는 고정된 인프라 구조가 없으며 네트워크 토폴로지가 사전에 알려져 있지 않은 구조이다. 센서 노드들은 목표 지역에 랜덤하게 뿌려지며, 뿌려진 노드들은 자신의 라디오 주파수 범위 내에서 이웃 노드들을 검색하고 데이터를 전송한다.

반면에 계층적 센서 네트워크에서는 센서들의 능력에 따라 베이스 스테이션(base station), 클러스터 헤드(cluster head), 센서 노드로 구분된다. 베이스 스테이션은 다른 네트워크로 연결되는 게이트웨이 역할을 하며, 데이터를 처리하고 저장하기 위해 상대적으로 강력한 능력을 가진 노드이다. 따라서 각 센서들로부터 전송되는 메시지를 수집하고 센서 노드들을 대신해서 연산을 수행하고 네트워크를 관리하는 역할을 수행한다.

클러스터 헤더는 특정 지역의 데이터를 수집하여 베이스 스테이션으로 전송하는 역할을 수행하는 노드를 말한다. 일반적으로 베이스 스테이션은 모든 노드들에게 데이터를 전송할 수 있는 능력을 가지지만, 센서 노드들은 베이스 스테이션까지 데이터를 전송하기 위해 애드 혹 통신에 의존한다. 즉 노드들 간에 유니캐스트 메시지를 전송하기도 하고, 자신이 포함된 클러스터에 멀티캐스트 메시지를 전송하거나 베이스 스테이션부터 센서 노드들까지 전체 네트워크에 브로드캐스트 메시지를 전송하기도 한다.

유비쿼터스 컴퓨팅 환경을 구현하기 위해서 센서 네트워크 활용 방안 및 센서 기술 개발과 함께 감지된 정보를 안전하게 처리하고 관리할 수 있는 센서 네트워크 상에서의 보안 메커니즘 개발이 반드시 필요하며, 노드들 사이에 안전한 데이터 전송을 위한 키 분배 방식의 개발이 필수적으로 요구된다.

한편, 센서 네트워크 상에서 노드들이 배치된 물리적 환경이 공격에 그대로 노출되어 전송되는 정보가 쉽게 변경되거나 정당하지 않은 노드가 데이터를 전송함으로써 전체 정보의 무결성을 쉽게 무너뜨릴 수도 있다. 뿐만 아니라 악의적인 노드가 센서 노드로 가장하여 불필요한 정보를 계속 발생시켜 중간 노드의 자원을 소모시

킴으로써 네트워크의 수명을 단축시킬 수 있다. 따라서 이러한 공격자 환경에 대해 안전성을 보장할 수 있는 보안 프로토콜의 개발이 필요하며, 그 중 키 관리 방식은 안전한 통신과 인증을 위해 가장 필수적으로 요구된다[3].

그룹을 기반으로 한 여러 가지 응용 보안은 모든 참가자에게 알려진 공유 비밀키 계산을 요구한다. 그 신뢰 관계의 본질은 중앙 인증 기관이 없다는 것이다. 따라서 그룹 키 관리는 서로 도움이 되는 기본에서 진행되어야 한다. CGKA(Contributory Group Key Agreement) 프로토콜[4]은 이러한 신뢰 관계를 위해 정의되었다. 그리고 [5]프로토콜은 저전력 이동 장치를 위한 그룹키 어그리먼트와 효율적인 상호 인증을 제공한다. 그러나 이는 대량의 통신을 형성하는 강력한 신뢰 서버(base station)를 가진 무선 기반을 요구한다.

따라서 센서 네트워크에서 서로 협력하는 그룹 셋팅은 분산 키 어그리먼트 기술을 요구한다. 또한 네트워크 장애는 랜덤이고 예측할 수 없으므로 cascaded membership events를 고려한다[6]. 본 논문에서는 [6]의 동적인 협력 그룹을 위한 간단한 결함 허용 키 어그리먼트를 이용한 트리를 기반으로 한 유일한 이동 노드를 가진 분산 그룹 키 어그리먼트를 제안한다.

[6]은 트리의 멤버쉽 이벤트에서 join, leave, merge, partition의 오퍼레이션에서 sponsor, new intermediate node가 필요하다. 이러한 멤버쉽 이벤트 오퍼레이션을 간단하게 하기 위하여 유일한 이동 노드가 필요하다.

2. 관련 연구

그룹 키 관리 프로토콜은 작은 그룹의 중앙 집중을 위한 contributory key agreement 프로토콜과 큰 그룹을 위한 서버 기반 키 분산 프로토콜의 두 종류가 있다[6]. CGKA(Contributory Group Key Agreement) 프로토콜은 그룹 통신 시스템의 기초 사용을 가능하게 한다. 즉 모든 메시지가 보내진 후 그 목적지에 도달해야만 하고(public broadcast channel), 보내진 메시지의 주문은 보호되어야 한다(reliability). 그리고 CGKA 프로토콜은 모방과 중간 공격 통신 채널을 피하기 위해 인증되어야 한다. 이러한 인증 절차는 실제의 CGKA 프로토콜과는 독립적이기 때문에 인가된 공개키를 가진 디지털 서명으로 이루어진다. 그룹의 모든 참가자는 계산 과정 동안 동등한 권리를 가진다. 이것은 [4]에서 CGKA 프로토콜을 위한 VTR(Verifiable Trust Relationship)의 정의에서 강조된다. 즉 모든 프로토콜 메시지는 적어도 하나 다른 참가자에 의해 검증되어야만 한다.

[1]은 분산된 그룹 키 분산 프로토콜을 제안한다. 이는 네트워크 파티션과 다른 네트워크 이벤트를 잘 견디나, 특별한 그룹 멤버(leader)가 그룹 키를 선택하여 그 키를 모든 다른 멤버에게 분산시키므로 contributory key agreement를 제공하지 못한다. 게다가 리더가 새로운 키를 안전하게 분산시키기 위해 리더와 다른 그룹 멤버 사이의 안전한 N-1 two-party 채널을 확립하기를 요구한다. 동적 그룹에서 그러한 채널을 유지하는 것은 각 채널을 셋업하는 것이 각각의 two-party key agreement를 포함하기 때문에 비용이 많이 든다(그룹 리더가 떠나면 $O(N)$의 새로운 채널이 셋업된다).

한편, 센서 네트워크에서 키 관리는 인증과 암호와 같은 보안 서비스의 기초가 된다. 낮은 가격의 키 관리 기술에 관한 연구로 새로운 key pre-distribution 계획안들[7,8,9]이 발표되었다. 그러나 센서 노드들의 제약된 소스와 타협하려는 노드들의 위협 때문에 이러한 계획안들은 노드들 사이의 통신을 위한 안전한 키들을 보장할 수가 없다. 따라서 이들 key pre-distribution 계획안들은 어떤 노드들이 각 센서 노드의 이웃인지를 알아야만 한다. 해결책으로 센서 노드들의 배치 지식을 활용한 key pre-distribution 프로토콜이 제안되었다[10,11,12]. 그러나 이러한 계획안들은 센서 노드들의 위치가 미리 어떤 규모로 결정되어야 하는 가정이 있어야 한다. 실제로 예정된 위치의 센서들 지식을 보장하기란 매우 어렵고 때로는 불가능하다.

그러므로 센서 노드들의 예정된 위치 정보없는 key pre-distribution 기술을 연구할 필요가 있다. 이러한 연구를 위해서는 센서 네트워크 특성상 저가격 저전력으로 키 관리가 이루어져야 한다. 또한 작은 기억 공간, 제한된 계산 능력, 항상 동적으로 변하는 센서 네트워크 노드들의 특성을 고려한 효율적인 키 관리가 필요하다.

3. 제안 모델

3.1 유일한 이동 노드가 있는 트리 구조의 그룹 키 관리

본 논문의 목적은 유일한 이동 노드가 모든 키들을 관리하는 중앙 서버 없이 효율적으로 그룹 키 관리를 하는데 있다. 효율적인 그룹 통신을 위한 키 관리는 트리를 기반으로 한 키 트리를 구성한다. 하나의 그룹 키 트리에 유일한 이동 노드는 각각의 ID를 가진다. 그림 1에서 유일한 이동 노드를 $U(ID)_{node}$라고 할 때, 8명을 구성한 그룹을 위한 키 그래프가 그림1과 같이, 각 멤버가 가지고 있는 키 k_1, k_2,……,k_8 의 상호 역할을 하는 키 k_{12}, k_{34}, k_{56}, k_{78}, k_{14}, k_{58}, k_{18} 는 유일한 이동 노드가 작업을 할 때만 그 역할을 수행하고 유일한 이동 노드가 작업을 중지할 때는 그룹 각 멤버의 공유 키만을 유지한다. 이러한 유일한 이동 노드는 상호 역할을 하는 키 k_{12}, k_{34}, k_{56}, k_{78}, k_{14}, k_{58}, k_{18} 를 필요에 따라 관리하는 이동 관리 노드이다. 상호 역할을 하는 키 k_{12}, k_{34}, k_{56}, k_{78}, k_{14}, k_{58}, k_{18} 는 필요에 따라 생성

되나 유일한 이동 노드의 ID가 없으면 그 암호화 및 복호화를 할 수가 없다.

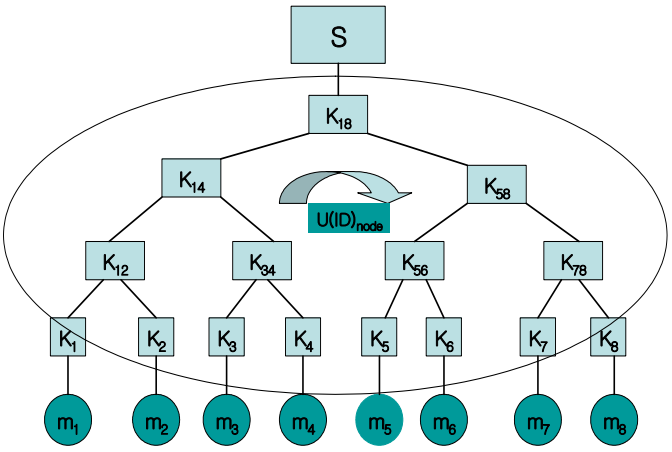

그림 1 A keygraph for a group of 8 members

[1]에서 제안한 그룹 리더는 새로운 키를 선택하고 그룹 모든 멤버에게 그 키를 안전하게 보내기 위해 안전한 채널을 사용하는 반면, 제안한 모델에서는 유일한 이동 노드가 새로운 키를 선택하고 그룹 모든 멤버에게 그 키를 안전하게 보내기 위해 안전한 채널을 사용한다고 가정한다.

그림1에서 멤버 1은 키 k_{12}, k_{14} , k_{18} 를 선택하고 멤버 3은 k_{34} 를 선택하고 멤버 5는 k_{56}, k_{58} 를 선택하고 멤버 7은 k_{78} 를 선택한다. 유일한 이동 노드는 안전한 채널을 통해 다음과 같이 선택된 키를 보낸다.

$m_1 \rightarrow m_2$: k_{12}, k_{14}, k_{18}
$m_1 \rightarrow m_3$: k_{14}, k_{18}
$m_1 \rightarrow m_5$: k_{18}
$m_3 \rightarrow m_4$:k_{34}
$m_5 \rightarrow m_6$:k_{56}, k_{58}
$m_5 \rightarrow m_7$:k_{58}
$m_7 \rightarrow m_8$:k_{78}

모든 멤버는 유일한 이동 노드의 ID로 암호화 및 복호화를 할 수 있다.

3.2 유일한 이동 노드가 있는 트리 구조의 그룹 키 통신 방법

그룹에 새로운 멤버가 join할 경우, 새로운 노드가 더해진다. 멤버 m_9가 조인한다면 그림2에서와 같이 키 k_{19}가 더해진다. 키 k_{19}는 새로운 그룹 키가 된다. 멤버 m_1와 m_9는 유일한 이동 노드 $U(ID)_{node}$에 동의하고, 멤버 m_1은 유일한 이동 노드 $U(ID)_{node}$로 키 k_{19}를 암호화하여 모든 멤버 m_1, m_2,……,m_8에게 보낸다.

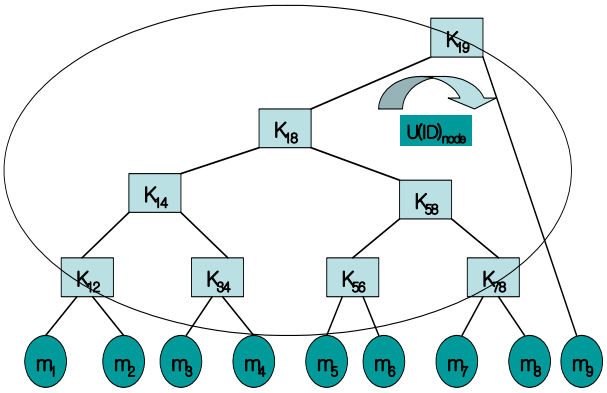

그림 2 Single member join case

그룹의 어떤 멤버가 실패할 경우, 트리의 어떤 노드가 교체된다. 만약 멤버 m_1이 실패된다면 키 k_{14}와 k_{18}가 교체되어야 한다. 그리고 유일한 이동 노드는 안전한 채널을 통해 다음과 같이 선택된 키를 보낸다.

$m_2 \rightarrow m_3$: k_{24}, k_{28}
$m_3 \rightarrow m_4$: encryted$\{k_{24}, k_{28}\}$ with $U(ID)_{node}$
$m_2 \rightarrow m_5$: k_{28}
$m_5 \rightarrow m_6$: encryted $\{k_{28}\}$ with $U(ID)_{node}$
$m_5 \rightarrow m_7$: encryted $\{k_{28}\}$ with $U(ID)_{node}$
$m_5 \rightarrow m_8$: encryted $\{k_{28}\}$ with $U(ID)_{node}$

그룹의 멤버가 그룹을 떠날 경우, 프로토콜은 간단해진다. 만약 그룹 멤버 m_1이 그룹을 떠날 경우, 키 k_{24} , k_{28}를 선택하고 분산시키는 문제를 가진다.
즉 m_2는 키 k_{24} , k_{28}를 선택하고 안전한 채널인 $U(ID)_{node}$는

$m_2 \rightarrow m_3$: k_{24}, k_{28}
$m_2 \rightarrow m_5$: k_{28}
$m_3 \rightarrow m_4$: encryted $\{k_{24}, k_{28}\}$ with $U(ID)_{node}$
$m_5 \rightarrow m_{6,7,8}$: encryted $\{k_{28}\}$ with $U(ID)_{node}$

를 전달한다.

4. 기대 효과

본 연구는 [1]에서의 two-party key agreement를 포함하기 때문에 비용이 많이 드는 단점을 개선하기 위한 모델 제안이다. 따라서 그 문제점을 비교 분석하기 위한 표를 사용한다.

pt-2-pt: The number of point-to-point messages sent
multicast: The number of multicast messages sent
bytes: The total number of bytes sent
rounds:The number of rounds the algorithm takes to complete

먼저 2^n 크기의 그룹을 위한 키 트리를 구성하는 경우 [1]과 제안 모델과의 비교이다.

표1의 경우, [1]모델은 보내진 총 바이트수가 $O(n\log_2 n)$인 반면, 제안 모델은 유일한 이동 노드 아이디 때문에 n으로 나눈 값이 된다. 알고리즘을 완성하기 위한 라운드 수는 [1]모델은 키 트리를 생성하고, 조인하고, 떠나는 3라운드이지만, 제안모델은 유일한 이동 노드가 능동적으로 키 트리를 생성, 조인, 떠나는 알고리즘을 1라운드로 처리한다.

표 1

	# pt-2-pt	# multicast	# bytes	# rounds
[1]모델	$O(n)$	1	$O(n\log_2 n)$	3
제안모델	$O(n)$	1	$O(\log_2 n)$	1

표2의 경우, 그룹 멤버가 떠나는 경우 비교 표로서 [1]모델은 보내진 총 바이트수가 $O((\log_2 n)^2)$인 반면, 제안 모델은 유일한 이동 노드의 역할로 $\log_2 n$ 으로 나눈 값이 된다. 알고리즘을 완성하기 위한 라운드 수는 [1]모델은 키 트리를 생성하고, 떠나는 2라운드만 필요하며, 제안모델은 능동적인 유일한 이동 노드의 생성, 떠나는 알고리즘을 1라운드로 처리한다.

표 2

	# pt-2-pt	# multicast	# bytes	# rounds
[1] 모델	$\log_2 n$	$\log_2 n$	$O((\log_2 n)^2)$	2
제안모델	$\log_2 n$	$\log_2 n$	$O(\log_2 n)$	1

표3의 경우, 그룹 멤버가 조인할 경우 비교 표로서 [1]모델은 보내진 메시지수,총 바이트수가 제안모델과 같으나, 알고리즘을 완성하기 위한 라운드 수는 [1]모델은 키 트리를 생성하고, 조인하는 2라운드만 필요하며, 제안모델은 역시 1라운드로 능동적인 처리를 한다.

표 3

	# pt-2-pt	# multicast	# bytes	# rounds
[1] 모델	1	2	$O(1)$	2
제안 모델	1	2	$O(1)$	1

4. 결론

본 연구는 안전한 그룹 통신을 위한 효율적인 키 관리 방안으로 유일한 이동 노드를 사용함으로써 비용 측면에서 개선을 얻었다. [1]에서는 제안한 그룹 키 관리 방안에서의 상호 키들을 저장할 서버가 필요한 반면, 제안한 모델은 유일한 ID 이동 노드가 안전한 채널을 통해 이동함으로써 키 저장 서버가 필요가 없다. 또한 트리 구조의 상호 키를 기억할 필요없이 유일한 이동 노드 ID만 알면 인가된 그룹 멤버 누구나 그룹 키 암호화 복호화가 가능하다.

제안한 모델의 알고리즘을 완성하기 위해, 유일한 이동 노드가 트리 구조의 상호 키들을 필요할 때만 실행시키므로 [1]에서 제안한 방법보다 훨씬 간편하다.

참고문헌

[1]O.Rodeh, K.Birman, and D.Dolev, “Opimized Group Rekey for Group Communication Systems”, In NDSS2000, pp.37-48, 2000.

[2]Joao B.D.Cabrera, Lundy Lewis,et.al., “Proactive Intrusion Detection and Distributed of Denial of Service”, Journal of Network and System Management, Vol.10, No.2, June 2002.

[3]Soohyun Oh and Jin Kwak, “Analysis of Security and Efficiency of Key Distribution schemes for Distributed Sensor Network”, Journal of The Korean Data Analysis Society, Vol.8, No.6, 2006.

[4]M. Manulis, “Contributory Group Key Agreement Protocols”, Revisited for Mobile Ad-hoc Groups, In Processings of MASS 2005, WSNS 2005, IEEE Computer Society, 2005.

[5]A.E.E. Bresson, O. Chevassut and D. Pointcheval, “Mutual authentication and group key agreement for low-power mobile devices”, In Proceedings of MWCN 2003, Singapore, pp.59-62, World Scientific Publishing, 2003.

[6]Yongdae Kim, Adrian Perrig, Gene Tsudik, “Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups”, CCS’00, Athens, Greece, pp.235-244, 2000.

[7]H.Chan, A.Perrig, “PIKE:Peer Intermediaries for Key Establishment in Sensor Networks, In

Proceedings of IEEE Infocom, Mar. 2005.
[8]H.Chan, A.Perrig, and D.Song, “Random Key Predistribution Schemes for Sensor Networks”, In IEEE Symposium on Research in Security and Privacy, pp.197-213, 2003.
[9]W.Du, J.Deng, Y.S.Han, S.Chen, and P.Varshney, “A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge, In Proceedings of IEEE INFOCOM’04 , Mar. 2004.
[10]D.Huang, M.Mehta, D. Medhi, and L. Harn, “Location-aware Key Management Scheme for Wireless Sensor Networks”, Inn Proceedings of the 2nd ACM workshop on SASN’04, pp.29-42, Oct.2004.
[11]D.Liu, P.Ning, “Location-based Pairwise Key Establishments for Static Sensor Networks”, In 2003 ACM workshop on SASN’03, pp.72-82, Oct.2003.
[12]Z.Yu, Y.Guan, “A Key Pre-distribution Scheme using Deployment Knowledge for Wireless Sensor Networks”, In Proceedings of ACM/IEEE IPSN, Apr. 2005.