사물인터넷(IoT) 환경을 위한 안전한 그룹 키 관리 기법

* 이 수 연

요 약

최근 스마트 기기의 보급화로 Wi-Fi, LTE 등을 이용한 무선인터넷 사용률이 대폭 증가한 반면 유선인터넷의 비율은 감소하고 있는 추세이다. 이렇듯 장소에 구애받지 않고 무선인터넷에 접속하여 사람과 사람뿐만이 아니라 사람과 사물간의 통신, 사물과 사물간의 통신인 사물인터넷의 범위가 점점 다양해지고 있는 추세이다. 사물인터넷(Internet Of Thing)의 빠른 확산과 함께 사물인터넷 보안 위협에 대한 우려도 크게 늘고 있다. 본 논문에서는 사물인터넷 환경에서 그룹 통신을 위한 키 분배와 관리에 대한 새로운 기법을 제안한다. 제안 기법은 키를 분배하지 않고 그룹에 속한 사물이 자신의 비밀 정보와 공개 값을 가지고 계산한 그룹 키를 사용하여 그룹 멤버 사이에 안전한 그룹 통신이 가능하게 된다.

Secure Group Key Agreement for IoT Environment

ABSTRACT

Recently, the popularity of smart devices such as Wi-Fi and LTE has increased the use ratio of wireless dramatically. On the other hand, the use ratio of wired internet is decreasing. The IoT(Internet of Things) is not only for people but also for communication between people and things, and communication between things and things by connecting to a wireless without choosing a place. Along with the rapid spread of the IoT there is a growing concern about the threat of IoT security. In this paper, the proposed scheme is a efficiency group key agreement in IoT environment that guarantees secure communication among light-weight devices. The proposed scheme securely be able to communication with the group devices who share a group key, generated by own secret value and the public value. Such property is suitable to the environment which are required a local area and a group

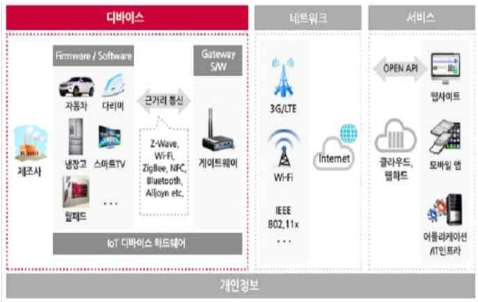
Key words : IoT(Internet Of Things), Group Key Management, Group Communication, Forward Secrecy, Backward Secrecy

접수일(2016년 12월 02일), 수정일(1차: 2016년 12월 22일), 게재확정일(2016년 12월 27일)

* 백석문화대학교 컴퓨터공학부

1. 서 론

사물인터넷(IoT)은 이동통신망을 이용해 사람과 사물의 통신뿐만이 아니라 사물과 사물의 통신으로 모든 사물이 연결되어 센싱, 네트워킹, 정보 처리 등 복합적인 요소가 상호 협력하여 서비스와 가치를 창출하는 기술이다. 그러나 사물 인터넷 환경에서는 플랫폼의 개방화로 인해 기술적이고 관리적인 보안위협이 발생할 수 있다. 특히, 사물 인터넷 환경에서 사용되는 디바이스는 낮은 저전력 및 계산량, 적은 메모리 등과 같은 제한적인 하드웨어 사양을 가진다.



[그림 1] 사물인터넷(IoT) 구조도

그러므로 기존에 제시된 네트워크 요소 보안 방법과 ID기반, 인증서 기반, 스마트카드 기반 디바이스 인증 방법, 경량 암호 방법들은 높은 안전성을 보장하기 위해 전제되는 높은 연산량을 가지므로 사물인터넷 환경에서 사용하기에는 문제점이 존재한다.

따라서 본 논문에서는 사물인터넷에서 디바이스와 디바이스간의 통신 시 안전한 그룹 키 분배와 관리를 위한 기법을 제안한다. 제안 된 기법은 그룹에 속한 디바이스의 비밀 정보와 공개 값을 가지고 계산한 그룹 키를 통해 그룹 멤버 사이에 안전한 그룹 통신이 가능하게 한다.

2. 보안요구사항

본 절에서는 사물인터넷(IoT) 디바이스에서의 보안인증 기술을 살펴보고자한다. 사물인터넷 환경에서 디바이스와 디바이스, 디바이스와 센서 등의 통신이 이루어질 때 보안 위협 공격자로부터의 안전성 확보를 위하여 전송된 데이터가 정당한 기기에서 전송된 것인지 식별 및 인증할 수 있어야 한다. 이러한 보안 위협을 최소화하기 위한 가장 기본적인 인증 방식으로 ID/PW 인증이 있으며, 이를 위해서는 별도의 애플리케이션 및 프로토콜이 요구된다. 또 다른 방식인 인증서 방식에서는 PKI(Public Key Infrastructure) 기술이 주로 이용되고 있으며, 단말에 탑재된 USIM 또는 UICC 등을 활용한 인증 방식인 SIM(Subscriber Identification Module) 방식도 활용되고 있다. 특히, SIM 인증 방식에 대한 연구가 최근 활발히 진행되고 있으며 ETSI, 3GPP 등에서 표준화 작업을 진행 중이다[1].

3. 그룹 키 관리 기법

본 절에서는 기존의 그룹 키 관리기법에 대한 내용을 다루고자 한다. 사물인터넷 환경에서는 다양한 사물이 그룹으로 관리되어야 하며 다양한 키 관리기법이 고려되어야한다. 즉, 안전성과 경량화를 고려하여 시스템을 구축해야하고 또한 그룹 키를 생성할 때 보안 요구사항인 데이터 비밀성, 그룹 키 안전성, 역방향 안전성, 순방향 안정성을 만족해야한다. 다음은 기존의 그룹 키 관리 기법을 살펴본다.

(1) 중앙형 키 관리 기법

이 기법은 중앙 집중화 그룹 키 관리 방식으로 하나의 키 분배 서버가 전체 그룹 멤버에 대한 그룹 키를 관리하고 키 상태 정보를 관리한다. Group Key Management Protocol (GKMP)[5]에서는 하나의

Group Controller(GC)가 전체 멤버의 정보를 관리하며 키 생성과 분배를 담당한다. 이 방식은 중앙 노드에서 단방향으로 메시지를 보내 그룹 관리를 수행하지만 반대로 그룹 안에 있는 노드가 갱신 및 운영 데이터를 중앙노드에게 다시 보낸다면 사물인터넷 보안 요구사항에서와 같이 하나의 노드에서 발생하는 오버헤드 및 고비용 문제를 해결해야하며 보안을 고려했을 경우에 취약한 부분을 발견할 수 있다[2][3].

(2) 중앙 분산형 키 관리 기법

이 기법은 여러 개의 작은 부분 그룹을 생성하여 각 그룹에는 그룹을 관리하는 노드가 있고 노드는 중앙 노드와 통신하는 계층적 구조를 가지는 특징이 있다. 이 구조는 안전성을 추구할 수 있지만 사물인터넷 환경에서 인증서를 사용하게 되어 수많은 디바이스들에 대해서 인증서 기반 구조 시스템이 필요하므로 하드웨어 자원의 제약사항이 생기고 인증서를 관리해야하는 인증기관의 비용이 기하급수적으로 증가하게 되는 문제점을 발생하게 된다.[4]

(3) 분산형 키 관리기법

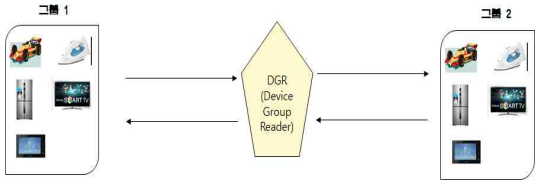
이 기법은 각 노드가 상호 통신을 통해서 키를 생성하고 갱신하는 방법으로 두 기법들보다 속도면에서 빠르지만 보안 취약점이 발생될 가능성이 크다. 사물인터넷 환경에 대입할 경우 악의적인 사용자의 위장 공격이 가능하기 때문에 한정된 보안을 구축할 수 밖에 없는 디바이스에서는 저비용 및 낮은 오버헤드를 추구할 수 있지만 보안측면에서는 취약하다.[5]

4. 안전한 그룹 키 관리 기법

본 장에서는 사물인터넷 환경에서 디바이스 그룹간의 인증요구사항을 해결하기 위해 그룹 키 관리기법을 제안하고자한다. 기본 환경은 스마트 기기와 센서에 내장된 네트워크 인터페이스를 이용해서 두 디바이스의 직접 통신을 가능하게 하는 디바이스 간 직접융합 방식이다. 그룹 키 관리기법은 중앙 분산형 관리 기법을 기반을 사용한다.

[표 1] 제안 프로토콜의 약어

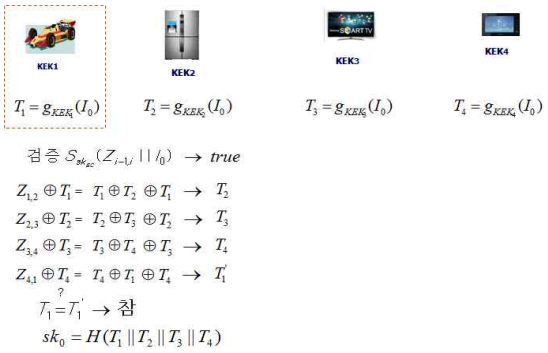
구 분	내 용
KEK	키 암호화 키(Key Encryption Key)로써 디바이스에서 디바이스에 데이터 전송을 보호하기 위해 사용된다.
GCK	그룹 암호화 키(Group Cipher Key)는 그룹 디바이스 사이에 공유되는 공통된 세션 키이다.
TEK	데이터 암호화 키(Traffic Encryption Key)는 디바이스 사이에 데이터 전송 시 사용되는 암호화 키이다.



[그림 2] 제안 기법 구성도

[그림 2]에서 볼 수 있듯이 사물인터넷에서는 두 가지 형태의 통신을 제공한다. 첫째, 일-대-일 통신으로 디바이스가 서로 통신하고자 할 때 두 디바이스는 자기들이 있는 그룹에서 디바이스 그룹 리더(*DGR*)에 의해서 일대일 통신을 실행할 수 있다. 예를 들어, 디바이스(D_1)과 디바이스(D_4)가 통신하고자 할 때, 디바이스 그룹 리더는 KEK_1과 KEK_4을 사용하여 데이터 암호화 키(*TEK*)를 암호화한 다음 D_1과 D_4에게 전송한다. 둘째, 일-대-다 통신으로서 그룹 내에 있는 디바이스들이 안전하게 통신하고자 할 때 디바이스 그룹 리더(*DGR*)는 각 디바이스의 키 암호화 키(*KEK*)를 사용하여 그룹 암호화 키(*GCK*)를 암호화한 다음에 각 디바이스에게 전송한다.

본 논문에서는 공개된 해쉬 함수$H: 0,1^{*} \rightarrow 0,1^{k}$ 와 충돌회피 의사 난수 함수집합인 G 가 사용된다. 색인은 법 n에 대해 계산된다. 즉, 만약 $i = j \bmod n$이라면 $D_i = D_j$이다. 그리고 키 생성 서명알고리즘(g)를 사용한다.

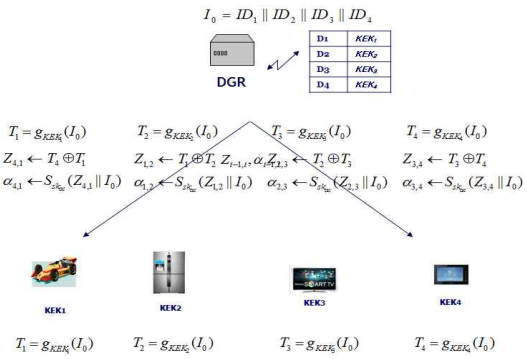


[그림 3] 그룹 키 생성 과정

하나의 그룹 키를 공유하기 위해 정당한 D들은 다음 단계를 실행한다.

■ 초기화 단계

$G_0 = \{D_1, ..., D_n\}$은 그룹 키를 공유하기 원하는 디바이스 n개로 구성된 초기 그룹이라고 하자. $ID_i = D_i$를 나타낸다. $I_0 = ID_1 \| ... \| ID_n$이라고 하자.

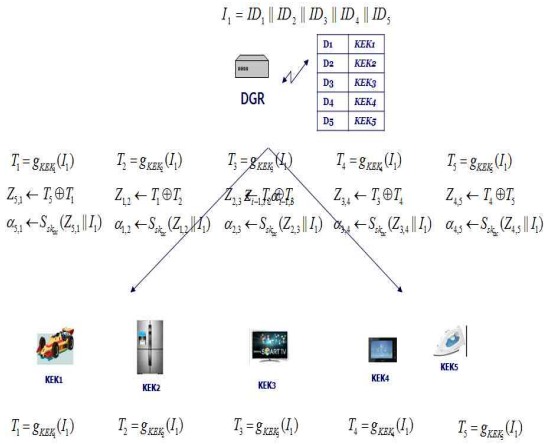


[그림 4] 초기화 과정

[그림 4]에서 보듯이 KEK_i는 D_i와 DGR 사이에 공유된다. DGR은 $T_i = G_{KEK_i}(I_0)$를 계산한 다음 키 생성 서명알고리즘(g)을 통해 생성된 서명 값을 D_i에게 방송한다.

■ 가입 절차

크기가 n 인 그룹 $\{D_1, ..., D_n\}$ 에 새로운 D_{n+1}가 참여하고자 한다고 가정하자. i은 현재 세션이고 $I_i = ID_1 \| ... \| ID_{n+1}$라고 하자.



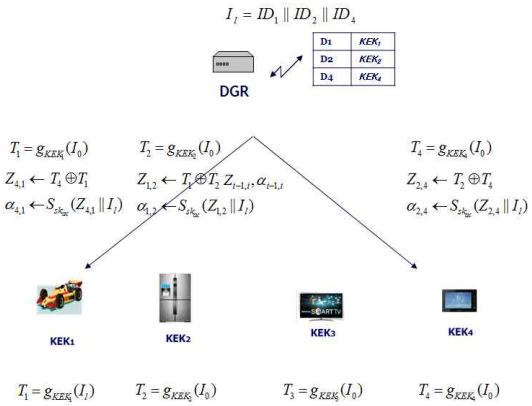
[그림 5] 새로운 디바이스 가입

[그림 5]에서처럼 새로운 D_{n+1}가 그룹에 참여하기 전에 KEK_{n+1}가 D_{n+1}에 내장되어 있고 D_{n+1}와 DGR 사이에 공유되고 있다. DGR은 새로운 KEK_{n+1}를 사용하여 $T_{n+1} = G_{KEK_{n+1}}(I_i)$을 계산하고 이전의 KEK_i와 새 I_i을 이용하여 $T_i = G_{KEK_i}(I_i)$을 다시 계산한다. 그리고 키 생성 서명알고리즘(g)을 통해 생성된 서명 값을 D_i에게 방송한다. D_{n+1}는 새 KEK_{n+1}를 사용하여 $T_{n+1} = G_{KEK_{n+1}}(I_i)$을 생성하고 각 D_i는 자신의 KEK_i와 새 I_i를 사용하여 $T_i = G_{KEK_i}(I_i)$를 재계산한다. 모든 디바이스는 세션

마다 새로운 세션 I_i를 사용하여 새로운 T_i를 계산하므로 전방향 안전성(Forward Secrecy)을 제공한다.

■ 탈퇴 절차

크기가 n 인 그룹 $\{D_1,.....,D_n\}$ 에서 $D_l(1 \le l \le n)$가 그룹에서 탈퇴하고자 한다고 가정하자. k는 현재 세션이고 $I_k = ID_1 \| ID_{l-1} \| ID_{l+1} \| ... \| ID_n$이라고 하자.



[그림 6] 디바이스 탈퇴

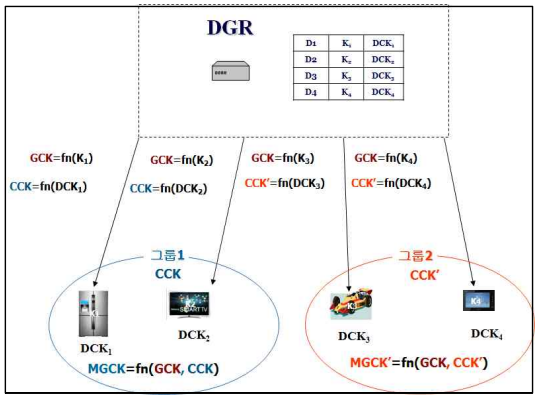
[그림 6]에서 DGR은 이전의 KEK_i와 새 I_k을 이용하여 $T_i = G_{KEK_i}(I_k)$을 다시 계산한다. 그리고 키 생성 서명알고리즘(g)을 통해 생성된 서명 값을 D_i에게 방송한다. 각 D_i는 자신의 KEK_i와 새로운 I_k를 사용하여 $T_i = G_{KEK_i}(I_k)$를 갱신한다. 여기서 탈퇴한 D_l은 새롭게 계산된 T_i를 모르므로 후방향 안전성(Backward Secrecy)를 제공한다.

제안 기법에서 보듯이 그룹에 속한 디바이스가 자신의 비밀 정보와 공개 값을 가지고 계산한 그룹 키를 사용하여 그룹 간 안전한 그룹 통신이 가능하게 된다.

[그림 7]에서 [그림 9]까지는 디바이스들이 자체적으로 생성한 그룹 키를 가지고 그룹 간 통신을 하는 대한 예시이다. 두 그룹이므로 $DCK(Drived\ Cipher\ Key)$와 $CCK(Common\ Cipher\ Key)$가 사용된다.

■ 그룹 키 공유

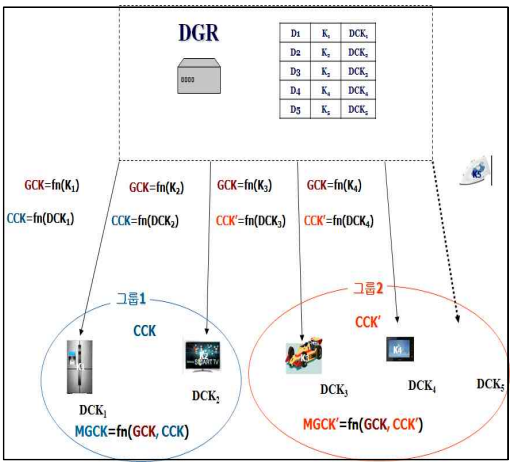
[그림 7]은 그룹 1과 그룹2에 속해있는 디바이스들이 그룹 키를 공유하는 과정이다. 그룹 1에서 냉장고와 스마트 TV는 그룹 키 $MGCK$를 $GCK = f_n(K_i)$와 $CCK = f_n(DCK_i)$를 사용하여 계산한 후 함께 공유한다. 마찬가지로 자동차와 월패드가 속해있는 그룹2도 $GCK = f_n(K_j)$와 $CCK' = f_n(DCK_j)$를 사용하여 $MGCK'$를 함께 공유한다. 두 그룹 내에 있는 냉장고와 자동차간의 통신은 디바이스그룹리더(DGR)에 의해 그룹 1에 있는 디바이스와 그룹 2에 있는 디바이스가 상대방의 그룹의 키를 생성할 수 있도록 하여 안전하게 통신이 이루어진다.



[그림 7] 그룹 키 공유 과정

■ 가입 과정

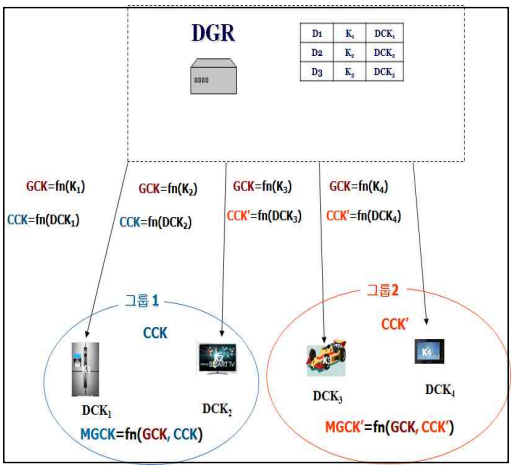
[그림 8]은 새로운 디바이스 다리미가 그룹 2에 가입하고자 할 때의 과정이다. [그림 5]에서처럼 가입 단계를 거쳐 새로운 그룹 키$MGCK'$가 생성이 된다. 설정 과정과 유사하게 디바이스간 그룹 통신은 디바이스 그룹 리더(DGR)에 의해 안전하게 통신이 이루어진다.



[그림 8] 디바이스 가입 과정

■ 탈퇴 과정

그룹 2에 있는 월패드가 그룹2에서 탈퇴 시 새로운 그룹 키 *MGCK'*가 생성이 된다. 따라서 그룹 1에 있는 디바이스가 그룹 2에 있는 탈퇴한 디바이스와 통신을 원할 때 디바이스그룹리더(*DGR*)에 의해 그룹 키가 변경되었음을 인식하고 통신이 불가능함을 알게 되므로 통신이 이루어지지 않는다.



[그림 9] 디바이스 탈퇴 과정

5. 결 론

사물인터넷(IoT)은 이동통신망을 이용해 사람과 사물의 통신뿐만이 아니라 사물과 사물의 통신으로 모든 사물이 연결되어 센싱, 네트워킹, 정보 처리 등 복합적인 요소가 상호 협력하여 서비스와 가치를 창출하는 기술이다. 하지만 사물인터넷 환경에서 디바이스와 디바이스 간 통신이 이루어질 때 보안 위협 공격자로부터의 안전성 확보를 위하여 전송된 데이터가 정당한 기기에서 전송된 것인지 식별 및 인증할 수 있어야 한다. 그러므로 본 논문에서 제안된 그룹 키 관리 기법은 디바이스간에 안전하게 그룹 키를 공유할 수 있고 자체적으로 계산이 되므로 통신비용 측면에서 효과성을 가질 수 있다. 향후에는 프로토콜에 대한 검증기법을 적용하여 안전성을 검증하고자 한다.

참고문헌

[1] Donghee Kim, Seokung Yoon, Yongpil Lee, Security for the IoT Service, The Korean Institute of Communications and Information Sciences. (2013), Vol.30, No.8, pp.53-59.

[2] Carlo Blundolz , Alfred0 De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, Moti Yung, Perfect-Secure Key Distribution for Dynamic Conference, Information and Computation, Volume 146, Issue 1, 10 October 1998, Pages 1 - 23, (2007).

[3] Yong Wang, Group Rekeying Schmees for Secure Group communication in Wireless Sensor Networks, (2007). ICC '07. IEEE International Conference on 24-28 June 2007,pp3419 - 3424, (2007)

[4] J.C.M. Teo, C.H. Tan, J.M. Ng Authentication Group Key Agreement against Dos in Heterogeneous Wireless Networks, WCNC 2007. IEEE pp3563 - 3568, (2007)

[5] Zhen Yu, Yong Guan , A Robust Group-based Key Management Scheme for Wireless Sensor Networks,Wireless Communications and Networking Conference, 2005 IEEE, Volume 4, 13-17 March 2005, pp1915-1920,(2005)
[6] Katz, J. and Yung, M.: Scalable Protocols for Authenticated Group Key Exchange. In Advances in Cryptology Crypto'03, Springer-Verlag, LNCS 2729 (2003) 110-125

[著者紹介]

이수연
1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 컴퓨터공학부 교수