홈네트워크에서의 기기 위치 정보와 OTP 알고리즘을 활용한 인증 보안 메커니즘*

김종진°, 조은영, 손진현
한양대학교 컴퓨터공학과
{jjkim, eycho}@database.hanyang.ac.kr, jhson@hanyang.ac.kr

Secure Authentication Mechanism using a Location Information of Device and an OTP Algorithm for Home Network Environment

Jongjin Kim°, Eunyoung Cho, Jinhyun Son
Department of Computer Science and Engineering, Hanyang University in Ansan

요 약

홈네트워크를 이루는 대부분의 기기는 그 위치가 자주 변동되지 않는다. 때문에 기기의 실제적인 위치 값은 기기를 구분할 수 있는 유일한 ID로 활용이 가능하다. 위치 측정 센서를 통해 홈네트워크를 구성하는 제품의 위치정보를 측정하여 그 값을 인증 보안 메커니즘에 활용한다. 홈네트워크를 구성하는 각각의 기기마다 요구하는 보안 수준의 정도가 다르다. 때문에 각 기기마다 차등 보안 레벨 적용이 가능하다. 즉, 낮은 자원을 이용하는 기기에 대해서는 높은 보안 적용을 위해 기기에게 필요한 추가 자원의 만큼을 절약할 수 있게 된다. 보안 인증 통신을 위해 홈네트워크를 구성하는 저성능의 기기에게 효과적으로 적용이 가능한 One-Time Password(OTP) 알고리즘을 이용한다. 본 논문에서는 홈네트워크를 구성하는 기기의 위치정보와 OTP의 두 가지 기술을 활용하여 홈네트워크 상의 보안 인증 문제를 해결하고자 한다.

1. 서론

최근 활발한 연구가 진행 중인 홈네트워크 구성 기술은 보안이라는 문제를 간과 할 수 없다. 홈네트워크는 인증 절차의 신뢰성을 통해 악의적인 공격으로부터 내부 네트워크를 안전하게 보호하는 방법을 요구한다. 그 결과 공개키 방식의 보안 인증 방법이 거론되었지만 공개키 인증 방식은 소형기기에 적용하기에는 너무 무거운 알고리즘이다. 가전기기를 구성하는 소형장치의 경우 기기를 구성하는 적은 자원으로 인해 보안 인증을 위한 계산 처리 용량의 한계를 지니게 있게 된다. 때문에 좀 더 가벼우면서 RSA 방식과 비슷한 수준의 보안 인증을 제공할 수 있는 다른 메커니즘이 요구 되었다. 홈네트워크는 그 특성상 밀집된 네트워크를 구성하게 되는데 밀집된 무선 네트워크 환경에서 정확하게 갖가지 기기들을 관리하고 유지할 수 있는 방법이 요구된다.

본 논문에서 제안하고자 하는 보안 인증 메커니즘은 위 문제를 해결하기 위해 홈네트워크를 구성하는 기기의 위치정보와 One-Time Password (OTP) 알고리즘을 활용한다. 논문의 구성은 다음과 같다.

2 절에서는 제안하는 보안 인증 메커니즘에 사용되는 기술에 대한 이해를 돕는다. 3절에서는 홈네트워크 보안을 충족시키기 위해 고려되어야 할 사항에 대해서 살펴본다. 4절에서는 제안하는 인증 보안 메커니즘에 대해서 서술한다. 5절에서는 제안하는 인증 보안 방법이 안전한지 검증해 보며 마지막으로 6절에서는 결론을 맺고 향후 연구 방향에 대해 기술 한다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원 사업(IITA-2006-C1090-0603-0031)의 연구결과로 수행되었음.

2. 관련 연구

2.1. 가전 기기의 위치 측정

홈네트워크를 구성하는 가전 기기의 위치 정보를 측정할 수 있다면 그 정보를 이용하여 다양한 응용 서비스를 사용자에게 제공할 수 있다. 사물의 위치를 파악하는 것을 위치 측정 기술이라고 하는데 센서 네트워크를 활용한 위치 측정 기술은 응용분야가 매우 다양하여 IT 산업 분야를 비롯하여 물류, 환경, 교통, 유통 등 산업 전반에서 필요한 중요한 핵심기술이다[1]. 관련된 많은 연구가 진행 중이며 가장 대표적인 시스템으로 GPS (Global Positioning System)을 들 수 있다. 하지만 GPS 기술은 실내에서 사용하기에는 그 오차범위가 크므로 적합하지 않다.

센서 네트워크 위치 측정 기술은 위치 측정 규모에 따라 Macro Positioning과 Micro Positioning으로 구분할 수 있다. 그림 1에서 자세하게 분류하며 관련 내용은 [2]를 참고한다. 간단하게 살펴보자면 Macro Positioning은 먼 거리에서 위치를 측정하는 기술들의 집합이다. 때문에 일반적인 오차 허용 범위도 크다. GPS 기술이 이 범주에 속한다. 그와 반대로 Micro Positioning은 가까운 거리에서 위치를 측정하게 되며 오차범위도 매우 작다.

제안하는 매커니즘은 기기의 정확한 위치를 측정할 수 있어야 하며 그 오차범위도 최소로 하는 위치 측정 시스템을 필요로 한다. 또한 센서의 관리 비용이 저렴하여 다수의 수신 센서를 활용해도 구축에 큰 비용이 들지 않아야 한다. 위의 조건을 만족하는 위치 측정 시스템으로 AT&T 캠브리지 연구소에서 개발된 액티브 배트(Active Bat) 시스템이 있다[3].

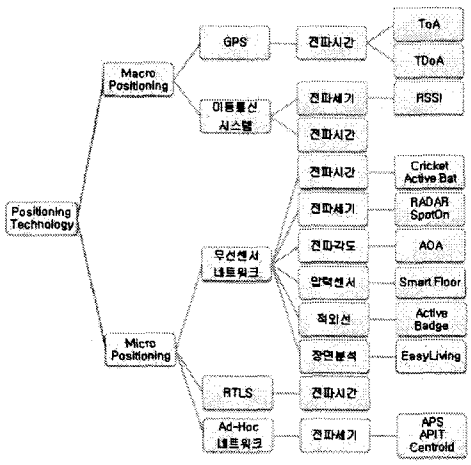

그림 1. 위치 측정 방법 분류

액티브 배트는 전형적인 ToA(Time of Arrival) 위치 측정 방법을 이용하며, 일반적으로 천정에 수신기를 위치시키고 주기적으로 배트(Bat unit)가 보내는 초음파 신호를 감지하도록 한다. 수신기가 초음파 신호를 판단하여 배트의 고유 아이디와 도착시간을 유선 네트워크를 통해서 서버로 전송하면 배트 신호의 도착 시간을 통해 각각의 거리를 측정할 수 있다. 3개 혹은 그 이상의 거리 정보를 통해 정확한 위치를 측정할 수 있다. 제안하고자 하는 매커니즘은 액티브 배트 시스템을 통해 홈네트워크를 구성하는 기기의 위치 정보를 홈서버가 알아 낼 수 있다고 가정한다.

2.2. One-Time Password (OTP)

보안 시스템에서 가장 많이 사용하는 기술은 공개키 암호방식의 RSA 인증 시스템이다. 기술의 발전을 통해 많은 개선이 있었지만 RSA의 가장 큰 단점은 계산양이 많다는 것이다. 비트 수에 따라 다르나 RSA 방식으로 암호화를 하기 위해서는 상당한 시간이 소요된다. RSA의 이 단점은 자원이 한정되어 있는 시스템에서 사용하고자 할 때 문제가 된다. 또한 계속적으로 RSA 방식으로 보안을 유지한다고 할 때 많은 시간이 암호와, 복호와에 소요되게 된다. 이 문제의 해결을 위해서 대칭키 방식으로 알려진 비공개키 암호화 방식을 생각해 볼 수 있다. 비공개키 암호화 방식은 공개키 암호화 방식에 비해서 암호화, 복호화에 소요되는 시간이 적다는 이점이 있다. 즉, 암호화 모듈의 간소화가 가능하기 때문에 센서네트워크 또는 임베디드 시스템에서는 아주 유용할 수 있다. 하지만 키 분배를 소홀히 해서 자칫 암호키가 노출될 경우 무방비 상태가 된다. 이러한 키 관리의 문제점을 해결하기 위해서 등장한 암호화 방식이 바로 OTP이다[4]. OTP는 Lamport에 의해 처음으로 소개되었으며, OTP의 목적은 컴퓨터 계정과 같은 제한된 자원에 비인증 접속을 더 어렵게 만드는데 있다. OTP를 사용하면 공개키 암호화 방식에 필요한 계산 비용을 줄일 수가 있다. 인터넷 환경과는 달리 홈네트워크 안에서 OTP는 안전한 동시에 매우 유용하고 효율적으로 사용될 수 있다. 예를 들면 OTP 값을 기기를 인증하거나 기기 간에 주고받는 정보를 안전하게 암호화 하는 키를 유도하는 값으로 사용될 수 있다.

OTP는 역방향으로 계산하는 것이 거의 불가능한 공개된 단방향 해쉬 함수f를 기초로 한다. 처음 비밀키로 사용할 임의의 값 x가 있다고 가정하고 x로부터 길이가 n인 해쉬 체인 $f^1(x), \cdots, f^i(x), \cdots, f^n(x)$ 를 만들기 위해서는 다음과 같은 과정을 거치게 된다. i를 해쉬 함수가 적용된 횟수라고 하고 $i=1,...,n$ 일 때, $f^0(x)=x$, $f^1(x)=f(f^0(x))$이고 $f^i(x)=f(f^{i-1}(x))$이다. 처음 공유한 비밀키와 해쉬 함수가 몇 번이 적용되었는지 최종 i 값을 알면 처음 비밀키에서 현재의 OTP 값을 유도할 수 있게 된다. 매 통신 때마다 해쉬 함수 적용 카운트를 증가시켜 OTP 알고리즘은 계속적으로 패스워드를 변경하게 되고 공격자의 위험으로부터 시스템을 보호하게 된다. OTP 시스템은 암호를 생성하는 제너레이터가 필요하게 되는데 이는 OTP 알고리즘을 통해 구현이 가능하다[5].

2.3. 홈서버 (Home Server)

홈네트워크 환경에서는 네트워크를 구성하는 모든 장치들의 중앙 집중적 관리를 맡아 줄 서버가 필요하다. 서비스의 처리 장소가 분산되지 않으므로 해서 발생될 수 있는 위험적인 요소는 방화벽 등의 여타 보안 방법으로 충분히 미연에 방지할 수 있을 것이다. 홈서버는 홈네트워크 보안을 위해 인증 서버(Authentication Server)의 역할을 수행하여 네트워크 영역 내의 모든 유무선 통신을 감시한다. 홈서버는 홈네트워크 영역 내에서 발생하는 모든 통신에 관여한다. 즉, 모든 통신은 홈서버를 통해서 이뤄지는 것이다.

기존의 유선 연결은 중앙 통제하기가 비교적 무선 통신의 방법 보다 수월하다. 하지만 홈네트워크에서는 무선 통신 환경도 고려되어져야 한다. 무선 통신의 경우 두 가지 방식이 있다. 하나는 Infrastructured network로서, 고정되고 유선으로 연결된 게이트웨이(Gateway) 내에서 사용되는 형태이다. 이러한 네트워크를 위한 중계기(Bridge)들을 기지국(Base-station)이라 한다. 이 네트워크 내의 무선기기들은 통신 반경 내의 가장 가까운 기지국에 연결되어 통신하게 된다. 무선기기가 이전의 기지국의 영역을 벗어나 다른 기지국의 영역으로 들어가게 되면, 이전의 기지국으로부터 새 기지국으로의 'Handoff'가 일어나게 된다. 그리고 이 과정에서 기기는 네트워크로의 접속을 유지한 채 계속 통신을 할 수 있다. 대표적으로 무선랜(WLAN)이 있다. 무선 통신의 두 번째 형태로는 일반적으로 Ad-Hoc라 불리는 Infrastructureless network가 있다. 이 형태의 경우 고정된 라우터가 없다. 모든 노드들은 이동을 할 수 있어서 임의의 방법으로 동적으로 서로 접속할 수 있다. 이러한 네트워크의 노드

들은 라우터로서 네트워크 내의 다른 노드로의 라우팅 경로를 찾아내고 유지하는 기능을 한다. 하지만 각 노드에 라우팅 정보를 담은 테이블을 유지하고 갱신해야 하는 부담이 있고 각 노드들이 중앙통제 되지 않기 때문에 보안이 상대적으로 취약하다고 할 수 있다. 본 논문에서는 홈네트워크 내의 기기들의 중앙 통제를 위해 무선 통신 기기들의 통신 및 제어 방법에 위의 방법 중 첫 번째 방법을 사용한다.

홈서버는 홈네트워킹을 위해 많은 작업을 수행하지만 가전기기의 모든 요청에 즉각 응답 할 수 있는 수준의 기기이며, 복잡한 암호 연산 및 여러 장치의 동시 제어에 알맞은 시스템이 되어야 한다. 또한 외부에서의 접근을 적절히 통제하여 홈네트워크의 보안을 유지해야 한다[6]. 방화벽, 가상사설네트워크, 무선 랜 보안 등 홈네트워크를 위한 많은 보안메커니즘, 제품이 있다[8]. 이러한 프레임워크는 홈네트워크와 인터넷 그리고 상태 기반 방화벽 트래픽 사이에 보안 채널을 구현함으로 서비스거부(Denial of Service) 공격으로부터 홈서버를 지킨다[7]. 홈네트워킹을 위한 대표적인 프레임워크로는 OSGi Alliance에서 주도하는 OSGi 프레임워크가 있으며, 자체의 보안 서비스를 가지고 있다. 하지만 그것은 제한적이며 충분하지 않기 때문에 추가적인 보안 방법을 적용하여 보완되어야 한다.

3. 보안 문제

홈네트워크에는 유무선 통신 환경이 모두 고려되어야 한다. 즉 유선 환경의 보안 문제들과 무선 환경의 보안 문제들이 함께 고려되어야 한다는 것이다. 또한 다세대 주택의 홈네트워크 환경과 같은 경우에는 밀집된 주거 환경으로 인해 중복되는 여러 무선 홈네트워크 환경이 구축될 수 있기 때문에 무선 환경에서 네트워크 중복 영역을 컨트롤 할 수 있는 방법이 모색되어야 한다.

모든 공격 또는 침입에 완벽하게 대응하기에는 가전기기들의 성능이 상대적으로 떨어진다. 그러므로 최대한 방어할 수 있는 전략과 보안을 위해 필요한 비용을 최소화 할 수 있는 보안 매커니즘이 요구된다.

또한 홈네트워크 내에서 유무선으로 전달 받는 메시지의 변조, 위조 등의 공격을 막아 홈네트워크를 안전하게 보호할 수 있도록 반드시 몇 가지 보안과 기능적 요구 사항을 만족해야 한다. 간단하게 요약하자면 홈네트워크 서비스는 기밀성, 보전성, 최신성, 인증과 키 관리, 유효성, 부인방지에 대한 부분이 반드시 제공되어져야 한다[9]. 하지만 보안성을 높일수록 시스템에 가해지는 오버헤드가 커지기 때문에 가장 효율적이며 시스템에 가장 적합한 보안 방법으로 보안 인증 시스템을 구축해야 한다.

4. 제안하는 인증 보안 메커니즘

4.1. 구성 요소 및 요구 사항

홈네트워크를 구성하는 각각의 기기들은 자신의 위치 정보를 측정하기 위한 센서를 가지고 있고 MAC 주소와 같은 유일한 ID로 네트워크 영역 내에서 자신을 구분한다. 기기의 ID와 위치 정보는 기기를 구분하기 위한 정보로 사용 된다. 그림 2를 통해 제안하고자 하는 시스템의 개괄적인 모습을 살펴 볼 수 있다. 각 가전기기의 특징에 따라 유무선으로 네트워크 연결이 되고 중앙제어 방식으로 연결된다. 그림 2에서는 무선 통신의 경우를 부각시켜 나타내었다. 유선 통신을 하는 경우는 홈서버와 직접 연결이 된다. 그림 2에 의하면 두 개의 무선 네트워크 영역이 존재하고 각 네트워크 영역은 기지국을 중심으로 형성되어 있다. 무선 가전기기는 기지국을 통해 중앙 처리 및 제어된다. 중앙 처리 장치인 홈서버는 가정에서 사용되는 모든 기기의 위치정보와 ID를 관리하게 되며 별도의 다른 여러 가지 방법으로 외부의 공격으로부터 보호 받는다. 타 기기의 동작을 제어하기 위해서는 홈서버에게 동작제어를 요청하고 홈서버는 요청 작업을 수행하여 다른 기기를 동작시킨다.

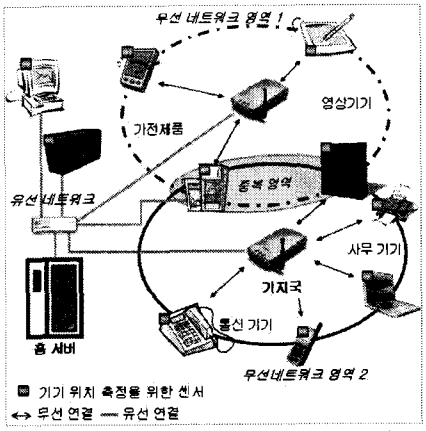

그림 2. 제안하는 시스템에서 기기 간 통신방법의 전반적인 모습

여러 기지국이 존재하게 되면 네트워크 영역이 중복되는 곳에 위치하는 가전기기가 있을 수 있다. 이 때 중복영역에 위치하는 기기들에 대해서는 각 기지국으로부터 홈서버로 전달된 정보가 중복됨이 판단되면 홈서버는 한쪽의 정보만 취하여 홈네트워크를 유지시킨다. 그림 2에서 중복영역에 있는 냉장고는 네트워크 영역1에 위치하고 TV는 네트워크 영역2에 위치하는 것을 확인할 수 있다. 기지국은 필요에 따라 홈네트워크 영역을 모두 덮을 수 있을 만큼 존재하며 홈서버에 의해 각 기지국은 관리되어 진다.

4.2. 홈서버에 새로운 기기 등록

홈네트워크 영역에 처음 접근하는 기기는 인증과정을 거쳐 홈네트워크의 구성 요소로 홈서버에 등록이 된다. 제안하는 보안 인증 매커니즘은 2절에서 살펴본 OTP와 기기의 위치정보를 활용하기 위한 준비과정이 필요하다.

먼저, 새로운 기기와 홈서버 사이에 신뢰성 있는 연결이 형성될 수 있도록 하는 과정이 필요하다. 바로 새로운 기기 인증 단계가 된다. 이 단계에서 가장 주의해야 할 사항은 서로 공유하게 될 OTP 알고리즘을 위한 초기 암호 키 값의 분배이다. 초기 암호키가 제3자에게 노출될 경우 보안 인증을 계속적으로 적용할 수 없기 때문이다. 기기의 성능에 따라 2가지 방법으로 암호키를

공유할 수 있다. 첫 번째 방법은 간단하게 수동으로 기기의 초기 암호키를 홈서버와 기기에 수동 입력해 주는 방법이다. 홈네트워크를 구성하는 각 기기를 구별할 수 있는 유일한 ID를 직접 홈서버와 기기에 수동 입력하여 초기 OTP알고리즘 암호키를 분배한다. 두 번째 방법은 초기 키 분배를 위해 공개키 암호화 알고리즘을 사용하여 홈서버와 기기의 통신에 의해 암호키를 분배하는 방법이다. 두 번째 방법은 사용자에게 편의성을 제공할 수는 있겠지만 기기의 암호화 모듈의 경량화에는 이바지하지 못하는 방법이 되겠다. 하지만 처음 키 분배 시에만 공개키 암호화 알고리즘을 사용하고 그 후에는 OTP 알고리즘을 활용하는 방법으로 시스템을 구성하면 초기에 기기 등록 단계를 지나면 실제 홈네트워크 상에서는 모든 통신이 OTP 알고리즘을 활용해서 보안 통신이 이뤄진다고 볼 수 있다. 일단 암호키를 공유하게 된 홈서버와 기기는 해당 암호키로 보안 통신이 가능하게 된다.

암호키 분배 이후의 작업으로 홈서버는 기기의 ID를 얻어오고 기기에 입력된 배트 유닛의 ID를 통해 위치를 측정해야 한다. 기기 등록 전체 과정을 그림 3에서 정리한다.

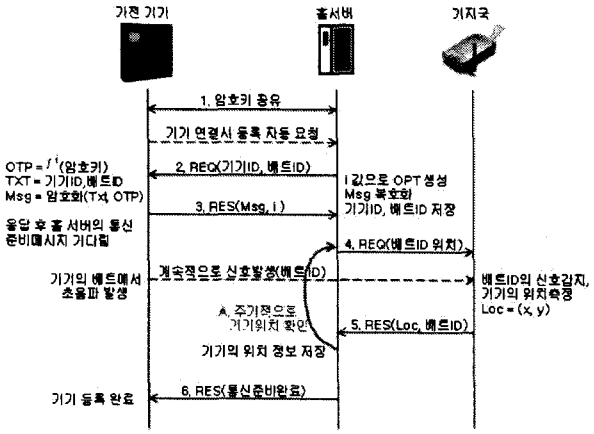

그림 3. 홈네트워크에 새 기기 등록 과정

기기의 인증을 위해서 홈서버는 새로운 기기의 등록 과정을 통해서 얻은 기기의 ID, 기기에 부착된 위치측정 센서인 배트 유닛의 ID 그리고 기지국을 이용해 측정된 기기의 위치 정보를 저장하고 있어야 한다.

4.3. 기기와 홈서버의 보안 통신

홈네트워크 내에 어떤 서비스가 존재하는지 사용자는 알고 있다. 해당 서비스의 작업을 사용자는 홈서버를 통해서 직접 원하는 기기에 요청할 수 있고 경우에 따라 다른 기기를 통해 요청이 가능하다. 단, 모든 통신은 홈서버가 중계한다. 홈네트워크를 통해 메시지를 주고받을 때는 항상 저장된 초기 암호값과 OTP Count 값을 통해 새로운 OTP를 생성하고 생성된 OTP를 사용하여 전달하고자 하는 메시지를 암호화 한다. 홈서버에는 홈네트워크 상의 모든 기기에 대한 OTP 암호 초기값과 OTP Count 값, 기기의 위치 정보값이 저장되어 있다. 작업 요청을 받으면 작업을 수행할 기기의 저장된 정보를 확인하여 기기의 위치 정보를 확인함과 동시에 상태를 체크하고 해당 기기가 현재 작업 수행이 가능한지를 검사한다. 작업 수행이 가능함이 판단되면 작업 요청을 암호화하여 해당 기기에 요청한다. 작업을 수행할 기기는 요청 정보를 복호화하여 작업을 수행하고 수행결과를 다시 암호화 하여 홈서버에 보고한다. 홈서버는 여러 방법으로 사용자에게 요청 작업을 처리되었음을 알리고 경우에 따라서는 요청했던 기기에도 처리되었음을 통보한다. 전체 과정을 그림 4를 통해서 살펴 볼 수 있다. 3,4,5번 메시지 전달 과정에도 그림 상에는 표현하지 않았지만 1번 과정 전에 수행되었던 OTP 생성 과정과 암호화 과정이 포함된다. OTP 카운트의 경우 매 작업을 수행할 때마다 증가시키며 홈서버의 값과 동기화 한다. 그리하여 매 작업 수행할 때마다 다른 암호키로 암호화 하여 보안성을 더욱 높일 수 있다.

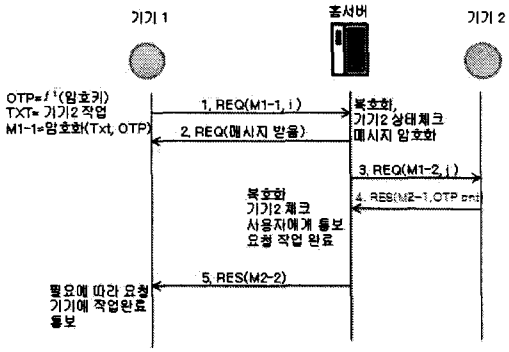

그림 4. 기기와 홈서버의 보안 통신 과정

작업 요청 시 실제 기기의 물리적 위치를 측정함으로 홈네트워크 영역 내에 있는 기기의 요청임을 확인하고 응답할 수 있다. 다른 기기에게 명령 시에도 마찬가지로 위치 정보 확인과 동시에 명령한다. 항상 기기의 위치를 측정하는 과정을 통해 기기를 인증한다. 기존의 전달되어진 패킷 정보 분석을 통한 인증에 비해 물리적인 직접 기기 인증이 가능하기 때문에 홈네트워크 환경 구성에 더욱 효과적이라고 할 수 있다.

4.4 기기 위치 정보와 암호키 값의 주기적 갱신

위치 측정에는 경우에 따라 오차가 발생할 수 있기 때문에 오차범위를 설정하여 위치 판단의 기준을 홈서버에 입력해 주어야 한다. 그 때문에 두 가전기기가 근접해 있을 경우 위치 측정 오차에 의해서 홈서버에서 두 가전기기가 같은 기기로 인식될 수 있는 문제가 있다. 이 경우에는 기기의 위치정보와 함께 저장된 기기 고유의 ID 쌍으로 기기의 판단을 해야 한다. 4.3 절에서 홈서버와 기기간의 통신 시간을 단축하기 위해서 홈서버는 기기의 요청이 있을 경우 작업 요청 기기의 위치를 측정하여 검증하는 것이 아니라 자체적으로 등록된 모든 기기의 위치를 주기적으로 측정하여 갱신한다. 그러면 홈서버는 기기의 동작요청이 있을 때에 대상 기기의 저장되어져 있는 위치정보를 확인해서 동작요청 검증을 할 수가 있게 된다. 이 과정을 통해서 홈서버는 현재 홈네트워크에 참여중인 기기를 체크할 수 있고 무선 네트워크 구성으로 인해 이웃의 홈네트워크와 중복되는

영역에 대한 감지를 할 수 있게 된다. 또한 외부 접근을 통제하기 위해 이 기능은 필수적이라고 할 수 있다. 기기의 위치 정보를 측정하여 이전에 저장된 값과 오차범위 이상의 큰 차이가 있을 경우 홈서버는 관련 상태정보 또한 갱신하여 홈네트워크를 구성하는 기기의 위치정보를 최신으로 항상 유지한다. 기기의 위치가 측정시마다 바뀐다거나 동시에 서로 다른 두 곳에서 같은 배트ID가 보고 될 경우 홈서버는 사용자에게 경고 메시지를 보낼 수 있다. 위와 같은 경우 기기가 이동 중이거나 기기에 이상이 있을 수도 있다. 또한 공격자의 침입 등의 경우를 고려하여 홈네트워크 내의 보안을 점검할 수 있을 것이다.

위에서 논의한 것과는 반대로 기기가 홈서버에게 자신의 위치 측정을 요청할 수도 있다. 하지만 이 방식의 경우 홈서버에 아직 인식되지 않은 임의의 기기가 자신을 홈네트워크 내의 구성기기로 인식되도록 하는 악의적인 침입방법으로 사용될 수 있기 때문에 고려하지 않는다.

기기 ID	배트 ID	위치정보	초기 암호키	OTP 카운트	상태정보

그림 5. 홈서버에 저장되는 기기정보 스키마

OTP 알고리즘에 의해서 네트워크 내의 모든 메시지는 암호화되지만 초기 암호키가 변경되지 않은 상태이기 때문에 위험성은 여전히 존재 한다. 또한 OTP 카운트 값이 증가 할수록 해수 함수 적용 계산양이 많아지게 되어 시스템에 부담이 생기게 된다. 홈서버는 이 문제를 해결하기 위해 주기적으로 초기 암호키를 다시 정해주는 작업을 할 수 있다. 이때 초기암호키를 다른 암호키로 리셋하며 동시에 OTP 카운트 또한 리셋 한다. 변경된 암호키는 홈서버와 기기가 서로 공유한다. 이와 같은 고려는 시스템 가동 시간이 경과해도 계속적으로 견고하게 시스템을 유지할 수 있도록 해 준다.

4.5. 요구 보안 수준에 따른 차등 레벨 적용

기기 인증 절차를 기기가 요구하는 보안 수준에 따라 다르게 구현함으로 제한된 자원에 더욱 효과적이고 유연한 보안 인증 시스템을 구현할 수 있다. 낮은 보안 수준을 필요로 하는 서비스의 경우는 제안하는 보안 인증을 적용하지 않고 기기의 ID 인증만으로 해당 서비스를 이용할 수 있도록 해 주는 것이 시스템을 구현 및 유지하는데 더욱 간단하고 효과적일 것이기 때문이다. 기기가 중요한 역할을 수행한다면 ID 인증만으로는 보안에 취약할 수가 있다. 이때는 본 논문에서 제안하는 기기의 물리적 위치 측정과 OTP알고리즘을 통한 방법을 활용한다. 표 1에 간단히 정리하였다.

표 1. 요구 보안 수준에 따른 보안 수준

	Level 1	Level 2
기기등록 과정	OTP 초기 암호값 수동으로 홈서버에 등록	공개키 암호화 방식을 활용한 자동 등록
기기간 통신과정	기기 ID만으로 인증, MAC ACL 사용	제안 알고리즘 사용

Level 1은 Level 2보다 낮은 보안 수준을 요구하는 경우이다. 기기 간 통신 수행 시 Level 1에서 기기의 ID를 별도로 부여할 수 있겠지만 대부분의 시스템에서는 기기의 MAC Address를 활용한다. 각 기기의 MAC Address를 홈서버에서 관리하게 되는데 이 관리 테이블을 MAC Access Control List(ACL)이라고 한다. 기기 등록 과정의 경우 4.2절에서 논의된 부분이다.

5. 안전성 및 성능 분석

5.1. 암호 메커니즘 분석

기존에 많이 활용되어지던 공개키 방식으로도 충분히 그 안정성이 확인된다. 하지만 공개키 방식의 암호화 기법의 경우 기기의 성능에 많은 영향을 받으므로 OTP 방식으로 암호화에 드는 비용을 감소시켰다. 제안하는 기법의 경우 대칭키 알고리즘을 사용함으로 공격자가 네트워크 내의 메시지를 모니터링 했을 때 암호키 없이 복호화를 하기 위해서는 많은 시간이 소요됨으로 안정성을 보장 받는다고 할 수 있다. 단, 초기에 기기를 네트워크에 등록할 때에 초기 OTP 암호키 분배를 유의한다면 네트워크 내에서는 계속적으로 보안이 유지된 통신을 할 수 있다. 또한 4.4절에서와 같이 주기적으로 초기 암호와 OTP Count를 변경함으로 시스템을 더욱 견고히 한다. 하지만 홈서버를 통해서 모든 기기의 암호키와 위치정보를 관리하기 때문에 홈서버가 보안에 취약하다면 홈네트워크 전체 시스템에 문제가 생길 수 있다. 때문에 홈서버는 별도의 보안 방법으로 시스템을 보호해야함을 2.3절에서 언급하였다.

유사 위치의 기기의 경우 허용하는 위치 범위 내에서 위치 측정값이 같은 위치로 보고될 수가 있다. 이 문제를 해결하기 위해서는 항상 기기ID와 위치 정보값을 쌍으로 체크하여 검증해야 한다. 그리하면 홈서버를 통해서 해당 위치에 두 개의 기기가 동작하고 있음을 알 수 있다.

5.2 기존 홈네트워크 프레임워크에 활용

홈네트워크 상의 통신이 보다 안전하고 신뢰성이 보장되도록 구성하기 위해 많은 연구가 진행되어 왔다. 썬마이크로 시스템즈가 개발한 프로토콜에 관계없이 네트워크에서 주변 장치들의 식별을 가능하게 하는 네트워크 분산 기술로 '지니(JINI)' 프레임워크[11], 마이크로소프트사의 기존 PC인터페이스를 그대로 적용하여 가전제품 제어를 할 수 있는 표준기술로 UPnP(Universal Plug and Play)[12]가 대표적이다. 이 기술들 모두가 가지고 있는 문제점 중에 하나가 홈네트워크 보안에 관한 문제이다. 보안을 강력하게 유지하기 위해서는 그만큼 효율성이 떨어지는 반비례 관계가 유지되기 때문이다. 때문에 보다 강력하면서 적은 자원을 활용하며 효율적으로 구동이 가능한 보안 메커니즘이 요구된다. 대부분의 홈네트워크 미들웨어 프레임워크는 공개키 방식의 암호화 알고리즘을 활용하여 네트워크 보안을 꾀하고 있다. 만약 우리가 제안하는 알고리즘을 인증 보안 메커니즘으로 활용한다면 공개키 방식의 인증 보안 메커니즘에 비해 네트워크 트래픽양이 감소하게 될 것이다. 또

한 향후 홈네트워크 기기 구성을 위해 필수적인 각 기기의 위치정보를 활용하여 이중 보안을 적용함으로 더욱 견고한 홈네트워크 미들웨어 프레임워크를 구성할 수 있다.

6. 결론 및 향후 연구

본질적으로 홈네트워크 응용은 사용에게 지능적으로 더 향상된 환경에 대한 정보를 제공해 줘야 할 것이다 [10]. 그러한 시스템 구현을 위해서는 홈네트워크 구성 기기의 위치 파악이 중요한데 그 위치 정보를 활용하여 홈네트워크 통신의 보안 인증 매커니즘을 제안했다. 기기의 위치 정보를 활용하면 ID인증만으로 부족한 부분을 보완하여 더욱 견고한 상호 인증을 할 수 있음을 확인했다. 또한 기기들 간의 메시지 전달 과정 중 발생할 수 있는 침입자의 공격으로부터 메시지를 보호하기 위해서 사용하는 암호화 매커니즘을 경량화 하고 실제 수행시간 단축을 위해 OTP를 보안 인증 방법에 적용했다. 그 결과 5절에서와 같은 안정성이 분석되었다. 그리고 요구되는 보안 정도에 따라 차등보안레벨을 적용함으로 낭비될 수 있는 가전기기의 자원을 효율적으로 관리하여 절약할 수 있다. 제안하는 매커니즘으로 시스템을 구축했을 때의 다음의 추가적인 기능 제공이 가능하다.

a. 위치정보를 통해 홈네트워크에 참여중인 기기들을 알 수 있다. 반대로 외부의 침입자를 감지할 수도 있다.
b. 위치 검증, OTP 검증의 두 번의 인증 과정을 거치므로 더욱 안정한 홈네트워크를 구성할 수 있다.
c. 홈네트워크 기기의 위치정보를 통해 정확한 네트워크 영역의 구분이 가능하게 되므로 무선 네트워크에서도 다른 네트워크 영역과 구별이 가능하며 홈서버의 영역의 설정이 가능하다. 때문에 홈네트워크 중복 영역에 대해서 보안문제를 해결할 수 있다.

앞으로 홈서버의 역할을 분산시켜서 위험성을 감소하기 위해 중앙 집중 방식의 홈네트워크 방식에서 Ad-Hoc 네트워크에의 적용 점을 찾아 볼 수 있을 것이며 더욱 정확한 기기 위치 측정을 위해 저비용, 저소비전력으로 통신이 가능한 초광대역(UWB) 기술을 활용하는 것도 모색해 볼 수 있겠다.

7. 참고문헌

[1] Asis Nasipuri and Kai Li. "A Directionality based Location Discovery Scheme for Wireless Sensor Networks", WSNA September, 2002.

[2] 박종태, 이위혁, 조영훈, 나재욱. "유비쿼터스 센서 네트워크에서 위치 측정 기술". 대한전자공학회, 전자공학회지 제32권 제7호, pp, 81~94, 2005.

[3] A. Harter, A. Hopper, P. Steggles, A. Ward, and Paul Webster, "The Anatomy of a Context-Aware Application," in Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, USA, August 1999, pp. 59-68.

[4] L. Lamport, "Construction digital signatures form one-way function." Technical Report SRI-CSL-98, SRI international, October, 1979.

[5] J. Archer Harris. "OPA: A One-time Password System", Proceedings of the International Conference on Parallel Processing Workshops (ICPPW), 2002.

[6] Takeshi Saito, Ichiro Tomoda, Yoshiaki Takabatake, Junko Ami and Keiichi Teramoto. "Home Gateway Architecture and Its Implementaion", Toshiba Corp. IEEE. 2000.

[7] Zhefan Jiang, Sangok Kim, Kanghee Lee, Hyunchul Bae and Sangwook Kim. "Security Service Framework for Home Network", Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05), IEEE, 2005.

[8] MC. M. Ellison, "Home Network Security," Intel Technology Journal, 2002.

[9] Jianwei Zhuge and Richard Yao. "Security Mechanisms for Wireless Home Network", GLOBECOM, IEEE, 2003

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. "Wireless sensor networks: a survey". Computer Networks, Volume 38, Issue 4, Pages 393-422. 15 March 2002.

[11] http://www.jini.org/

[12] http://www.upnp.org/