디바이스 융합 보안을 위한 향상된 RF4CE 키 교환 기법에 관한 연구

정회원 손 태 식*, 구 본 현*, 한 규 석**°

A Study on Advanced RF4CE Key Agreement for Device Convergence Security

Taeshik Shon*, Bonhyun Koo*, Kyusuk Han**° *Regular Members*

요 약

방송과 통신의 융합으로 시작된 미디어 플랫폼간의 융합은 이제 다양한 컨버전스 서비스를 창출하기 위한 S/W 생태계 구축을 시작으로 IT 및 비IT를 망라하여 전 업종으로 융·복합화를 앞당기고 있다. 이러한 컨버전스 환경의 대두와 함께 가정 및 산업용, 그리고 다양한 환경에서의 기기간 자동화 및 연결을 통한 새로운 부가 서비스를 창출하려는 RF4CE (Radio Frequency for Consumer Electronics) 기술이 대두되고 있으며, 본 논문에서는 기기간 효율적인 연결 및 제어를 위해 활용될 수 있는 ZigBee 표준화 기구의 RF4CE 기술에서의 향상된 키 교환 스킴에 대한 방안을 제시하였다. 제시된 방안은 기기간 상호 인증 및 두 단계의 Key Seed 분배 기법 등으로 구성되어 있으며, 본 논문에서는 제안 방안의 분석 및 실제 구현 및 실험을 통해 그 유용성을 검증하였다.

Key Words : RF4CE, ZigBee, Device Convergence, Key distribution, WPAN

ABSTRACT

Platform convergence originated from the convergence of broadcast and telecommunication is making rapid progress including IT and not-IT fields in order to provide a variety of converged services, S/W eco-system construction, and so on. With the advent of convergence environment, IEEE 802.15.4-based RF4CE technology is rising because of creating momentum for the market using converged connectivity between home and office devices as well as all around located devices. In this paper, we present enhanced RF4CE key seed distribution approach in order to provide efficient connection and control between devices. The proposed approach consists of device mutual authentication, initial vector assignment, and two-phase key seed distribution. Moreover, we make a development real RF4CE test board and its key agreement simulator to verify the proposed approach.

Ⅰ. 서 론

다양한 스마트폰과 태블릿 PC와 같은 IT 기기의 폭발적 증가와 그리고 댁내 CE(Consumer Electronics) 기기들의 연동 및 제어를 기반으로 하는 스마트 그리드 환경의 대두 등 최근 유무선 통신 기술을 기반으로 하는 모바일 기기의 증대는 다양하고 새로운 컨버전스 서비스를 출현 시키고 그 발전을 촉진시키는 중요한 요인이 되고 있다. 이러한 최근의 흐름은 개인화된 욕구를 만족시키는 다양한 서비스에 대한 새로운 패러다임을 요구하며 이에 따른 새로운 융합형 서비스 및 개방형 미디어 플랫폼들이 출현하고 있다. 기기간

* 삼성전자 Digital Media & Communication R&D Center, Convergence S/W Lab (ts.shon@samsung.com)
** 한국과학기술원 정보통신학과 (hankyusuk@kaist.ac.kr) (° : 교신저자)
논문번호 : KICS2010-03-138, 접수일자 : 2010년 3월 31일, 최종논문접수일자 : 2010년 5월 26일

개방화 된 플랫폼 기반 컨버전스 서비스들은 기존의 기기간 (D2D : Device-to-Device) 컨버전스에서 기기 대 솔루션 (D2S : Device-to-Solution) 컨버전스 그리고 단순한 기기와 기기 및 솔루션의 융합이 아닌 기기간 상호 작용을 바탕으로 하는 모든 사물 대 사물 (M2M : Machine-to-Machine) 컨버전스로 진화하고 있다. 여기서 일반적인 D2D는 앞서 언급과 같이 기존에 널리 사용되는 전통적인 성격의 기기간 연결과 이에 따른 융합 서비스를 의미하며, D2S는 기기와 솔루션간 융합 서비스를 위한 결합된 컨버전스 서비스로서 새로운 사용자 경험 창출을 위한 Content 기반의 컨버전스라고 말 할 수 있다. 또한 포괄적 개념의 M2M 컨버전스는 물리적으로는 D2D와 유사하나, 기기간 네트워크 상호 작용이 있는 D2S, B2B 성격의 컨버전스로서 향후 기존 이동 통신 및 무선 초고속 인터넷이나 Wi-Fi, Zigbee 그리고 Bluetooth 등 WPAN 솔루션과 연계하여 더욱 다양한 용도로 활용되어 더 이상 B2B, B2C 시장에 국한하지 않고 컨버전스 된 시장으로 영역을 확대할 것이다[1-3].

이러한 다양한 개념의 컨버전스 환경의 기기간의 통신에 있어 적용될 수 있는 대표적인 기술로서 현재 다양한 WPAN 환경에 널리 적용되고 있는 IEEE 802.15.4 기술이 있으며, 지난 2009년 3월에 기존 IEEE 802.15.4를 바탕으로 한 ZigBee Alliance에서 주요 가전 4사(파나소닉, 필립스, 삼성전자, 소니)로 구성된 RF4CE (Radio Frequency for Consumer Electronics) 컨소시엄에서 무선 주파수 기반 원격 제어를 위한 표준 규격을 제공하기로 합의 하였다. 이러한 RF4CE는 IEEE 802.15.4 PHY/MAC을 기반으로 하며, CE의 리모트 컨트롤러 외에도 홈 엔터테인먼트 시스템, 홈 및 빌딩 오토메이션 시스템 등 다양한 제품에 적용 가능하다[4-6]. RF4CE 표준 규격에서는 RF4CE 지원 기기간 신뢰성 있는 통신을 위한 키 교환 및 이를 통한 링크 키 생성 기법을 지원하지만, Key Seed를 교환할 때 평문 상태로 교환하기 때문에 이 Key Seed 값이 제 3자에게 그대로 노출될 수 있는 MITM(Man-in-the-Middle) 공격에 취약하여 제3자가 Key Seed 값을 습득하여 Secret Key 생성 가능하다. 이뿐만 아니라 최대 255개의 seed를 순차적으로 조합해야 노드간 암호화 통신을 위한 링크키를 생성할 수 있으므로 DoS와 같은 공격에 의해 하나의 Key Seed라도 유실되는 경우에는 부가적인 Key Seed 재전송이 필요하며 또한 원천적으로 Key Seed 가 노출되어 제 3자에 의해 암호화키가 생성될 가능성을 가지고 있다.

따라서 본 논문에서는 기기간 인증을 통해 위조된 기기의 RF4CE 네트워크 참여를 봉쇄하는 인증서 기반 상호 인증과 노드간 기밀 정보를 활용하여 효율적이고 안전하게 Key Seed를 분배할 수 있는 RF4CE 기반 향상된 키 교환 기법을 제안한다. 제안 기법의 주된 기여 효과는 앞서의 설명과 같이 상호 인증을 통한 기기간 식별 및 위조 방지 기능을 제공하는 것과, Key Seed 분배시 제3자에게 노출 가능성이 있는 모든 정보를 활용하지 않고 일부 정보만을 활용하여 링크 암호화 키를 생성 할 수 있다는 것, 그리고 Key Seed 암호화를 통하여 Key Seed 정보 노출을 근원적으로 해결하는 것이다. 본 논문의 구성은 다음과 같다. 2장에서는 RF4CE 보안 기능 및 이슈에 대해서 다루며, 3장에서는 본 논문에서 제안하는 기법을 인증, 초기 벡터 할당 및 두 단계의 seed 분배 기법으로 나누어 설명한다. 4장에서는 제안 기법을 분석하고, 5장에서 실제 실험 및 구현 결과를 설명한다. 6장에서는 본 논문의 결론을 도출한다.

II. 관련 연구

RF4CE는 그림 1과 같이 IEEE 802.15.4를 기반으로 하기 때문에 MAC 계층에서 MAC 프레임에 대한 암호화 및 데이터 인증과 같은 기본적인 보안 기능을 제공한다. 또한 RF4CE의 네트워크 계층에서는 128bit 암호화 키를 생성하여 Pairing 테이블에 저장하고 Pairing을 맺은 두 노드간의 암호화 통신에 활용한다. Pairing과정 후 Key Seed 값을 교환하여 Pairing된 두 노드간에 보안 채널을 형성하는 과정은 그림 2와 같이 알 수 있다. 그림 2에서 Controller와

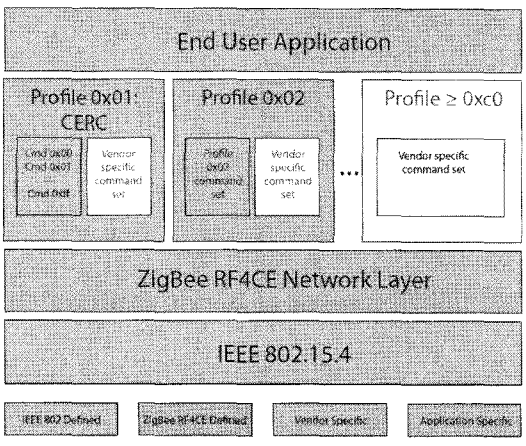


그림 1. RF4CE 프로토콜 구조[5]

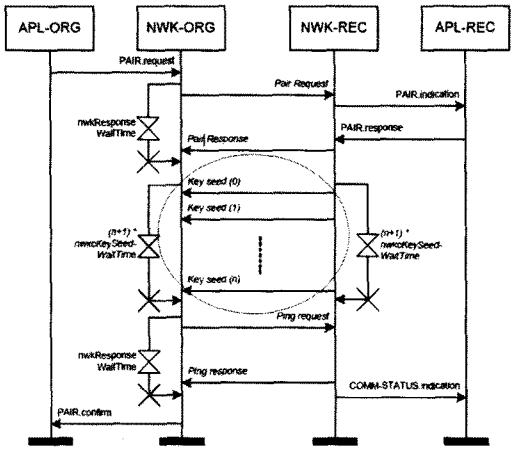


그림 2. RF4CE Pairing에서 Key Seed 교환 과정

Target은 먼저 RF4CE에 정의된 Pairing 과정을 수행한다. 이때 Target은 Pairing을 요청한 대상 노드의 보안 지원 여부를 검사하고, 상대가 보안 기능을 지원하는 경우 상대와 Key Seed 교환 과정에 들어가게 된다. 이 때 n개의 Key Seed 값을 controller에게 제공하여 양단간 동일한 Secret Key를 생성한다. 이때 전송하는 Key Seed 값의 최대 n의 개수는 255개이며, 이 Key Seed 값을 XOR 연산을 통하여 재조합하여 양단의 노드들이 링크 암호화키를 생성하게 된다. 하지만, 이러한 두 노드간 Key Seed 값을 교환 과정에서 Key Seed 값들은 암호화나 어떠한 보안 기능의 제공 없이 plaintext 상태로 전송되기 때문에 중간에서 제 3자에 의한 절취, 위조된 값 삽입, 정상적 노드에게 전송 방해 등 다양한 공격이 가능하다[5-8]. 따라서 악의의 사용자에 의한 Key Seed 습득을 원천적으로 방지해야하며 Key Seed frame의 sequence 나 seed value 자체를 위조하여 Secret Key 생성 방해 할 수 있는 Denial of Service 공격에도 내성을 제공해야 한다. 이러한 문제를 해결하기 위한 방안으로 두 노드간 사전 공유된 Master key를 사용하여 암호화를 통해 Key Seed 값을 보호하는 방법이 있을 수 있지만, 이 또한 master key를 안전하게 분배하는 방법이 여전히 문제로 남을 수 있다.

III. 제안 기법

본 논문의 제안 기법에서는 기존 RF4CE Pairing과정 후 최대 255개의 Seed를 일괄적으로 분배하는 과정과 달리 기기간 인증과 초기 벡터 분배 두 가지 모드의 Key Seed 분배 기법을 사용하였다. 제안기법을 활용하여, RF4CE의 Pairing 과정 이후 양단간 암호화키를 생성하기 위해 교환되는 Key Seed 값에 대한 Confidentiality, Integrity, Availability를 제공 할 수 있는 방안을 제공한다. 이러한 제안 기법은 기기간 인증과정과 초기 벡터 할당 그리고 Quick과 Main 두 가지 모드를 통해서 Key Seed를 분배하는 방법으로 구성되어 있다. 이후 분배된 Key Seed 값을 사용하여 안전한 통신 채널을 확립한다.

3.1 디바이스 인증

제안 기법에서는 디바이스 인증서를 기반으로 하여 RF4CE 키 교환을 위한 사전 준비 단계에서 기기간의 상호 인증과정을 수행한다. 이러한 인증 과정은 IEEE 802.16 표준(모바일 와이맥스)의 기기간 인증과 같이 제품 제조시 적용된 인증서를 사용하여 기기 복제(Cloned SS)와 같은 위조 공격을 방지하는 데 사용된다[9-10]. 즉, 디바이스 자체의 인증에 초점을 맞추지만 RF4CE Pairing 과정에 참여한 기기의 정상적 제조 및 유통을 검증 할 수 있으며 모바일 와이맥스와 같이 위조된 기기(Controller/Target)로부터의 공격을 방지할 수 있다. 그림 3과 같이 Pairing 과정이 시작하기전 Controller와 Target 두 노드는 서로의 인증서를 제공하여 상호 인증 과정을 수행한다. 처음 Target의 인증서를 받은 Controller는 먼저 Target 인증서에서 CA의 서명 검증을 통해 적합한 Target으로부터의 인증서 제공여부를 확인하고 이후 Controller는 자신의 인증서와 Key Seed 분배 과정에서 사용될 unique ID 값을 전달한다. Target은 먼저 UID값을 복호화하여 자신의 인증서를 수신여부를 확인하며, 다시 Controller의 인증서를 검증하여 상호 인증 과정을 마친다. 이 과정에서의 UID 값은 각 노드에게 유일하게 할당되는 IEEE 802.15.4 MAC 주소와 같은 값으로 생성 될 수 있다. 본 논문에서는 MAC 주소 값에 시간값 등의 난수를 활용하여 4바이트의 유일한 값을 전송한다. 제안 방안은 실제 CA와 연동된 인증을 수행하지 않고 기 발급된 CA의 인증서를 활용한다. 따라서 향후에는 온라인으로 CA를 통한 검증 등의 PKI 연동 방안을

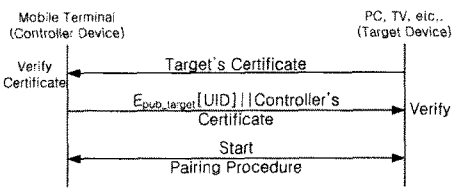


그림 3. 기기간 상호 인증 및 UID 전달

고려하는 것이 필요하다.

3.2 초기 벡터 할당

일반적으로 RF4CE Pairing 과정은 Pairing에 참여한 두 노드 간에 적절한 인증 절차가 진행된 이후에 수행된다. 만약 Pairing이 성공적으로 수행된다면, 이 과정 속에서 Pairing을 요청한 노드는 Target 노드(coordinator)로부터 2바이트의 네트워크 주소 값을 할당 받는다. 이때 제안 기법에서는 주소 값의 할당과 함께 추후 replay 공격 등을 방지하기 위한 시간 정보 값을 함께 전송한다. 또한 이렇게 전송된 값은 향후 key seed 분배 과정에서의 매스킹 함수의 랜덤값 생성을 위한 인자로서 사용된다. 그림 4에서 본 과정을 설명하고 있으며 이때 Pairing과정이 수행되며 상호간 key seed 분배를 결정하기 위한 보안 설정을 확인하는 부분이 있는데 이것은 RF4CE 표준에서 네트워크 계층의 node capability 상수값 설정을 통해서 알 수 있다.

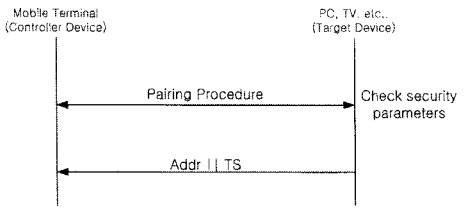


그림 4. 초기 벡터값 할당

3.3 Key Seed 분배

기존의 방법에서는 보통 255개 seed 값을 분배한 후에 이 값들 XOR 연산하여 128bit의 링크 암호화를 위한키를 생성하였다. 하지만, 분배되는 key seed 값들이 평문 상태로 전송되며 매번 255개의 key seed 값들이 모두 전송되어야 하는 등의 문제가 있었다. 따라서 제안 방안에서는 Quick Mode와 Main Mode의 두 가지 Key Seed 기법을 활용하여 적은 키를 활용하여 보안성을 향상 시키거나 또는 Key Seed 값을 원천적으로 암호화하여 전송한다. 먼저 Quick Mode 기법은 그림 5와 같이 수행되며, Target노드는 N개(N <= 255)의 Random Seed를 Controller에게 전달하며 이때 Controller 노드는 이 중 X개(X <= N)를 선택하여 링크 암호화 키 생성에 활용한다. 이때 X개 Key Seed의 선택과정은 앞서의 인증과정과 IV 할당과정에서 공유된 주소값과 UID (Address || UID)를 Random Selection Mask 함수의 인자로서 생성한 값(255bits)으로 수행한다. 예를 들어 생성된 255bits의 비트열중

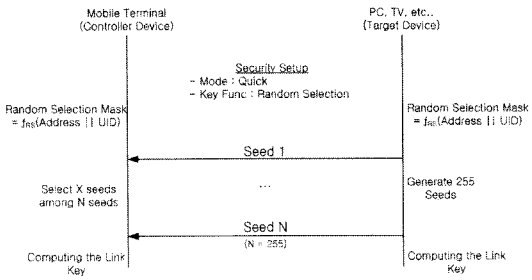


그림 5. Key Seed 분배 - Quick Mode

1의 값을 가지는 sequence number의 key seed 값을 선택하는 방법 등을 취할 수 있다. 따라서 Quick Mode 기법에서는 255개 보다 적은 수의 Key Seed 값을 가지고 Link 키를 생성할 수 있음으로 연산 시간을 줄임과 함께 제3자에게 255개의 키가 모두 노출되어도 제 3자는 링크키를 유추하기가 어렵다는 장점이 있다.

Main mode의 경우 기존 표준안과 같이 최대 255개의 key seed 값 모두를 전송하지만, 기존 방법이 Key Seed를 평문 상태로 전송하여 발생했던 문제점을 해결하기 위하여 N개(N <= 255)의 Random Seed를 생성한 후 Seed 암호화 키를 사용하여 Seed 값을 암호화하여 전송한다. 이때 Key Seed를 암호화하기 위한 최초의 Seed 암호화 키는 수식 1)과 같이 인증과정에서의 UID 및 IV을 사용하여 생성한 랜덤값을 활용한다. 이후 연속하여 전송되는 Key Seed 값들에 대한 암호화 키는 이전 생성된 Seed 암호화 키와 UID, IV를 함께 활용하여 재생성 한다. 따라서 전송되는 모든 Key Seed 값은 서로 상이한 암호화 키로 암호화 된다.

$$SEK_1 = F_{SEK}(Addr \parallel UID)$$
$$SEKn = F_{SEK}(Addr \parallel UID \parallel Seed_{n-1}) \quad (1)$$
$$E_{SEKn}[Seed_n] : Seed\ 암호화$$

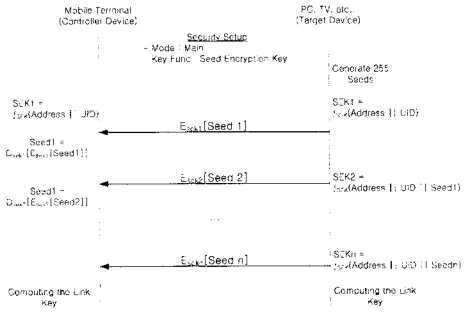


그림 6. Key Seed 분배 - Main Mode

Ⅳ. 제안 기법 분석

본 장에서는 제안 기법의 안전성과 효용성에 대하여 인증, 무결성, 기밀성 그리고 알려진 공격에 대한 보안성의 관점에서 분석하였다.

Authentication : 인증 기능에 있어서 기존 RF4CE 표준안에서는 Pairing 과정을 수행하고 Key Seed를 분배하기 위한 두 노드간의 어떠한 기능도 제공하지 않고 있다. 하지만, 제안 기법에서는 IEEE 802.16과 같은 이동 단말의 고속 무선 네트워크 환경을 위한 표준에서의 인증과 유사한 방법을 활용하였다. 즉, RF4CE 통신에 참여하는 각 노드는 인증기관의 인증서를 탑재하고 있고, 초기 Pairing 과정에서 기기간의 상호 인증 기능을 수행함으로써 근본적으로 비정상적인 방법을 통해 제조된 기기의 참여를 원천 배제하고, 또한 공개키 인증을 통해 불법적인 제3자로부터의 노드 가장이나 위조 기법을 방지 할 수 있다.

Integrity : RF4CE 네트워크에 참여하는 노드들 사이에 공유되는 Key Seed 값들은 기본적으로 RF4CE MAC FCS(Frame Check Sum) 및 네트워크 계층의 MIC (Message Integrity Code)의 지원을 받는다. 또한 제안 기법의 Quick Mode에서는 최대 255개의 Key Seed 값 중 무작위하게 선택된 n개를 활용함으로써 최대 255개의 Key Seed가 평문으로 노출되어 위조 될 수 있는 기존 기법에 비해서 상대적으로 높은 수준의 integrity를 제공할 수 있다.

Confidentiality : Key Seed 분배 과정에서 Main mode가 적용되는 경우, 본 논문의 제안 기법에서는 최대 255개의 모든 Seed Key에 대해서 서로 다른 키로 기밀성을 유지하기 위한 암호화를 지원하여 평문 상태로 모든 Key Seed 값을 전송하는 기존 기법에 비해 높은 수준의 기밀성을 제공 할 수 있다.

Security about Known Attacks : 기본 기법은 일반적으로 평문 상태의 Key Seed를 전송하므로써 Key Seed가 노출되어 제3자가 링크 암호화 키를 생성 할 수 있는 문제점은 물론이거니와 제3자에 의해서 악의적으로 Key Seed 가 위조되는 Man-in-the-Middle 공격등에 취약하였다. 하지만, 제안 기법에서는 제3자가 Key Seed를 습득하여 Secret Key 생성 하지 못하거나 생성 가능성을 매우 낮게 하기 위한 선택적 Key Seed 조합을 통한 링크 암호화 키 생성이나 Key Seed의 암호화 전송등의 기법이 적용 되었다. 또한, 제3자가 DoS(Denail of Service)등의 공격을 통해 Key Seed를 공유하는 두 노드간의 정상적인 통신을 방해하는등의 문제가 발생할 수 있었지만, 제안 기법에서는 앞서 Key Seed 노출을 줄이기 위해 선택적 Key Seed 조합을 통한 링크키 생성과 같은 방법을 적용하여 반드시 두 노드간 최대 N개의 Key Seed를 환하지 않아도 링크키를 생성 할 수 있는 방안을 제시하였다.

Ⅴ. 실험 및 구현

본 절에서는 제안기법의 검증을 위해 구현 내용과 실험 결과물을 제시한다. 그림 7은 실험에 사용된 Radiopulse사의 LM2455칩[11]기반으로 제작된 RF4CE 테스트 보드이다. 테스트보드는 USB 인터페이스를 통해 PC와 연결되어 C#기반의 시뮬레이터와 통신을 수행하게 된다. 이를 통해, RF4CE 기반의 제안된 내용의 데이터 내용들의 확인 및 검증을 수행하였다.

다음의 그림 8은 두 대의 PC에 각각 연결된 검증 테스트베드 환경으로서 두 대의 PC에는 RF4CE 시뮬레이터가 설치되어 있으며 또한 USB로 연결된 RF4CE 보드가 장착되어 있다. 다음의 그림 9에서는

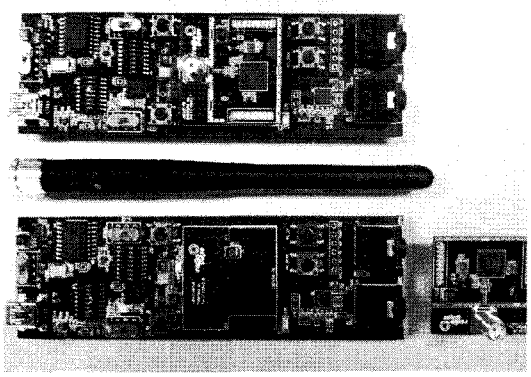


그림 7. 제안 기법 검증용 RF4CE 테스트 보드

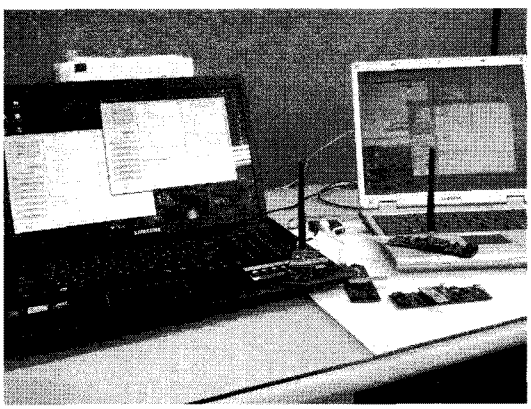


그림 8. RF4CE 키분배 기능 실험 환경

제안 기법이 적용된 Controller/Target 시뮬레이터에서의 수행 결과이다. 그림의 시뮬레이터를 동작시킴으로써 Controller와 Target 노드 상에서의 Device간 상호 인증과정, 초기 벡터 수행과정 그리고 Key Seed 분배 과정이 성공적으로 수행되었으며 특히 그림 9에서는 Quick 모드를 통한 Seed 값 분배가 성공적으로 이루어진 것을 확인 할 수 있다.

제안 기법의 경우 Quick 모드에서는 평균 120~150여개의 Key Seed가 선택되어 Link Secrete Key 계산에 활용되었으며, Main 모드의 경우 Key Seed의 암복화에 있어서 오버헤드가 발생 할 수 있지만, 일반적인 센서 노드와 같은 기기와 달리 CE기기는 배터리가 상전으로 공급되면 보다 높은 프로세싱 파워를 가지므로 고려하지 않을 정도로 작다고 볼 수 있다.

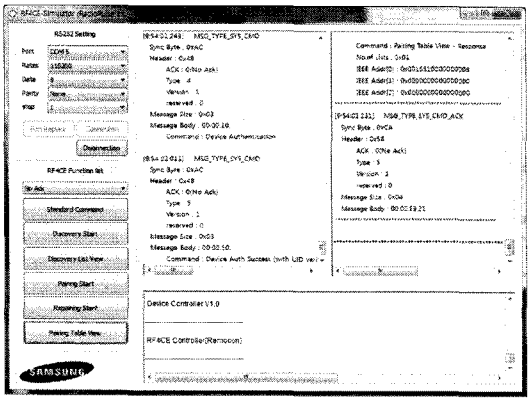


그림 9. RF4CE Key Seed 시뮬레이터

VI. 결 론

다양한 기기와 유·무선 기술이 융합되는 컨버전스 환경에서 저전력 소모와 단순한 Pairing등으로 강점을 가지고 있는 ZigBee의 RF4CE가 가정내 기기의 연결 및 IT기기에 활용되고 있다. 본 논문에서는 이러한 흐름에 맞추어 현재 RF4CE에 적용 되고 있는 키 교환 기법을 좀 더 향상시킬 수 있는 방안을 제시하였다. 본 논문의 향상된 Key Seed 분배 기법은 RF4CE 기기간 인증서를 활용하여 상호 인증을 제공하며 이러한 인증수단을 바탕으로 기기 위조 등의 문제를 효과적으로 해결할 수 있는 방안을 제시하였다. 또한 초기 인증과정에서의 UID 값 및 Pairing 과정에서의 주소 값을 교환하여 이후 Key Seed 분배 과정에서 선택적 Seed 값 재조합 및 암호화된 Seed 전송에 활용한다. 제안된 Key Seed 분배 기법은 최대 255개의 Seed 값에서 일부만을 선택 할 수 있는 방안을 제시하여 제3자에게 노출시에도 안전한 링크 암호화키 생성을 보장한다. Main Mode에서는 분배되는 Seed 값을 암호화하여 기존 방안에서 평문 전송시 발생 할 수 있었던 문제점을 해결해 주었다.

본 논문에서 제안된 내용은 Authentication, Integrity, Confidentiality, Known Attacks 분석 등의 관점에서 그 활용 가능성과 기존 방안 대비 장점을 검증하였다. 또한 실제로 RF4CE 검증용 테스트보드를 제작하고 시뮬레이터를 구현하여 실제 기능이 수행됨을 또한 확인하였다. 향후 연구에서는 실제 가정 내 전력 사용 제어 등에 활용될 스마트 그리드의 홈 네트워크(Home Area Network)등에 적용하여 RF4CE 기반 기기간 안전하고 효율적인 통신 방안 제공을 검증해야 할 것이다.

참 고 문 헌

[1] Z. Jianliang, M. J. Lee, Will IEEE 802.15.4 make ubiquitous networking a reality?: a discussion on a potential low power low bit rate standard, IEEE Communications Magazine. Vol.42, No.6, pp.140-146. June 2004.

[2] Ed Callaway, Paul Gorday and Lance Hester, Home Networking with IEEE 802.15.4: "A Developing Standard for Low-Rate Wireless Personal Area Networks", in IEEE Communications Magazine, August 2002.

[3] E. D., "The emergence of Zigbee in building automation and industrial control", *Computing & Control Engineering Journal*, Vol.16, No.2, pp.14- 19, Apr 2005.

[4] RF4CE Overview, ZigBee Alliance, http://www.zigbee.org/Markets/ZigBeeRF4CE/

[5] RF4CE Standard, Zigbee alliance, RF4CE Specification Version 1.0, Mar 2009.

[6] IEEE STD 802.15.4-2006, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Network, Sept 2006.

[7] P. Baronti, P.t Pillai, V. W.C. Chook, S. Chessa, A. Gotta, Y. Fun Hu, "Wireless

sensor networks: A survey on the state of the art and the 802.15.4 and Zigbee standards", Computer Communications, vol. 30, no. 7, pp 1655-1695, May 2007.

[8] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe '04 Proceeding, pp.32-42, 2004.

[9] IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE Std 802.16-2004. IEEE, 2004.

[10] Airspan, "Mobile WiMAX security", Airspan Networks Inc. 2007. http://www.airspan.com

[11] LM2455 specification, Radiopulse http://www.radiopuse.co.kr

손 태 식 (Taeshik Shon) 정회원

2000년 2월 아주대학교 정보 및 컴퓨터공학부 학사

2002년 2월 아주대학교 정보통신공학 석사

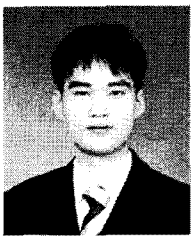
2005년 8월 고려대학교 정보호호학 박사

2004년~2005년 Research Scholar, Univ. of Minnesota

2005년 8월~현재 삼성전자 DMC 연구소 책임연구원

<관심분야> Wireless/Mobile Network Security, Wireless Sensor Network, Anomaly Detection

구 본 현 (Bonhyun Koo) 정회원



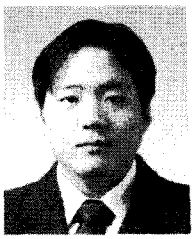
2005년 2월 동서대학교 정보통신공학과 학사

2007년 2월 고려대학교 정보보호대학원 석사

2007년 1월~현재 삼성전자 DMC 연구소 선임연구원

<관심분야> Mobile Security, Wireless Sensor Network, Visualization

한 규 석 (Kyusuk Han) 정회원



2001년 2월 홍익대학교 기계공학과 학사

2004년 8월 한국정보통신대학교 공학부 석사

2010년 8월 한국과학기술원 정보통신학과 박사

<관심분야> Wireless/Mobile Network Security, Wireless Sensor Network, Security Policy