情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

디바이스별 패스워드에 기반한 사물지능통신상의 인증 패러다임

이 재 성*, 최 필 주**, 김 동 규***

요 약

사물지능통신은 주변의 정보를 다양한 방식의 통신 장비를 이용해 장비 스스로 수집하여 제어하는 기술로서 미래의 새로운 통신 사업으로 주목받고 있다. 사물지능통신의 성장은 신뢰성 있는 네트워크 구축이 선결되어야 한다. 기존의 보안 시스템은 소유기반 인증 방식과 사용자가 패스워드를 입력하는 지식기반 인증 방식이 결합된 이중 인증 방식을 사용하였다. 그러나 사물지능통신 환경과 같이 사용자가 직접 개입할 수 없는 환경에서는 디바이스별 패스워드 기반의 지식기반 인증 방식은 구현이 어렵다. 본 논문에서는 디바이스별로 고유의 값이 생성되는 PUF(Physical Unclonable Function)에 기반하여 사물지능통신 상의 디바이스별로 패스워드 인증의 효과를 구현하는 새로운 지식기반 인증 패러다임을 제시하고자 한다.

Ⅰ. 서 론

사물지능통신(M2M : Machine-To-Machine)은 주변 정보를 수집할 수 있는 센서 및 정보를 전달할 수 있는 통신 장비를 탑재한 임베디드 시스템 또는 컴퓨터가 스스로 필요한 정보를 수집, 가공하여 시스템에 필요한 의사를 결정하고 스스로를 제어하는 기술이다. 필요에 따라 관리자 또는 사용자에게 가공된 정보를 보고할 뿐 사람의 간섭을 최소화하며, 사람이 직접 하기 위험한 일이나 시간이 많이 소요되는 일, 또는 보안이 필요한 일을 기계가 대신함으로써 정보의 효율적인 이용이 가능하다. 과거의 정보 수집 체계는 센서가 발달함에 따라 점차 자동화되었으나, 수집된 정보의 처리 및 이를 이용한 의사 결정은 오랜 기간 사람에 의존하였다. 그러나, 실생활 속 정보는 시간 및 장소에 구애 받지 않으며 그 양이 매우 방대할 뿐만 아니라 끊임없이 변화하는 성질을 가지고 있어 이러한 방대한 양의 변화하는 정보를 사람이 직접 처리하기에는 많은 제약이 따른다. 따라서, 이러한 실생활 속 범람하는 데이터를 더욱 가치 있고 효율적으로 활용하기 위하여 사물지능통신이라는 개념이 등장하게 되었다.

1990년에 등장한 사물지능통신은 초기에는 단순한 원격 조정, 차량 무선통신 서비스 등 적용 범위가 한정되어 있었으며, 관련 시장 및 산업이 제한적이었다. 그러나, 최근 유무선 통신기술이 급속도로 발전하고 있으며, 이와 함께 인터넷 생태계가 크게 확대되었다. 특히 최근의 RFID, NFC, ZigBee, Bluetooth 등의 새롭고 저렴한 통신 기술의 등장으로 인해 막대한 인프라 구축이 필요한 사물지능통신 산업의 걸림돌이었던 통신 장비 및 임베디드 시스템 장비의 비용이 하락하고 있으며, 기존 통신 시장의 중심인 이동전화 서비스는 현재 가입자의 포화로 인해 시장 성장의 한계에 다다르고 있어 사물지능통신 산업은 새로운 미래 시장으로 떠오르고 있다.

사물지능통신 산업의 안정적인 성장은 안전한 네트워크 환경을 기반으로 하며 이를 위해 통신 경로를 설정하기 전 서로가 정당한 개체인지 확인하는 인증 절차가 필수적으로 수행된다. 인증 시스템에는 패스워드 또는 PIN(Personal Identity Number) 등을 알고 있다는

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 받아 수행된 기초연구사업임 (No. 2010-0013441).
* 한양대학교 공과대학 융합전자공학부 (jslee@esslab.hanyang.ac.kr)
** 한양대학교 공과대학 융합전자공학부 (pjchoi@esslab.hanyang.ac.kr)
*** 한양대학교 공과대학 융합전자공학부 (dqkim@hanyang.ac.kr), 교신저자

사실에 기반한 지식기반 인증과 주민등록증과 같이 자신을 증명할 유무형의 것을 소유함에 기반하는 소유기반 인증이 있으며, 필요에 따라 소유기반 인증은 생략될 수 있으나 대부분의 경우 지식기반 인증은 필수적으로 수행된다.

사물지능통신에서는 사람이 아닌 디바이스 스스로가 지식기반 인증을 수행해야 하나 PIN을 인위적으로 생성 후 기기에 주입하는 현재의 방법으로는 인터페이스를 통해 키 노출의 위험성이 존재한다. 또한 디바이스의 특성상 소형이며 휴대가 용이하고 외부에 노출되어 있어 물리적으로 탈취가 용이하기 때문에 탈취된 디바이스는 레이아웃 분석, 버스 프루빙, 메모리 공격 등의 물리적인 공격에 노출되어 메모리에 저장된 PIN, 키 값 등의 주요 인증 파라미터들이 유출될 수 있다. 따라서, 안전한 PIN을 기기가 자체적으로 생성할 수 있고 물리적 공격에 강인한 새로운 기술의 도입이 필요하다.

본 연구에서는 공정변이로 발생하는 특성 편차를 이용하여 동일 설계 도면으로 제작하더라도 서로 다른 함수 값을 발생하는 회로인 PUF를 사용하여 이에 기반한 지식기반인증 패러다임을 제시하였으며, 이를 위한 사물지능통신의 구성요소를 정의하고 각 구성요소의 특징을 설명하였다. 그리고 공장 출하에서부터 디바이스가 네트워크에 삽입되어 통신을 위한 인증을 수행하기까지의 프로토콜 과정에 대해 설명하고, 제시한 PUF 기반의 PIN을 적용한 지식기반인증 패러다임이 일반적인 지식기반인증의 요구사항을 충족하는 지 그 부합성에 대해 분석하였다.

본 논문은 2장에서 배경지식으로써 PUF의 정의 및 특징, 인증 시스템에 대해 기술한다. 3장에서는 제안하는 PUF 기반의 사물지능통신의 프로토콜에 대해 설명하고 4장에서 결론과 향후 연구로 본 논문을 맺는다.

Ⅱ. 배경지식

1. PUF(Physical unclonable Functions)

PUF에 대해서 개요 및 정의를 간단히 설명하고, 이전에 연구된 PUF들의 현황과 문제점을 기술한다. 이를 통해 실제 PUF회로가 인증 등의 보안 회로에서 실제로 활용될 수 있도록 실효성을 바탕으로 요구 사항을 정리한다. 그리고 이러한 문제점을 보완하고 요구 사항에 부합하는 PUF 회로를 한 가지 예를 들어 설명하고 PUF의 활용 가능성에 대해 설명한다.

1.1 개요 및 정의

PUF(Physical unclonable Functions) 또는 PRF(Physical Random Function) [2]라고도 불리는 전기 또는 광학 소자의 무작위적인 부정합을 이용 물리적인 구조로 이식된 복제 불가능한 함수를 말한다. 하드웨어 칩 생산 과정에서 발생하는 공정 변이로 발생하는 특성 편차를 활용했기 때문에, 동일한 설계 도면으로 제작하더라도 서로 다른 함수 값을 발생하여 원천적으로 복제 방지가 가능하다.

1.2 PUF의 이전 연구와 문제점

PUF에 대한 연구는 1998년 최초로 개발된 IC의 top layer에 random하게 doping된 입자를 이용한 Coating PUF를 시작으로, latch와 같은 하드웨어 칩에 일반적으로 쓰이는 CMOS 소자 내부의 공정 변이를 이용하여 FPGA에서도 구현 가능한 최근의 butterfly PUF까지 다양한 방식의 PUF가 연구되어 왔다.

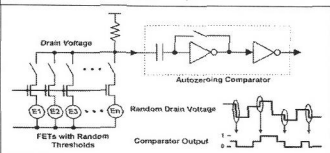
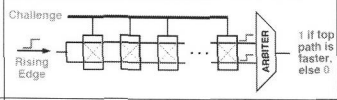
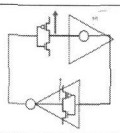
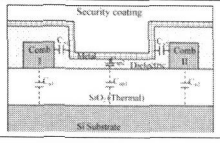
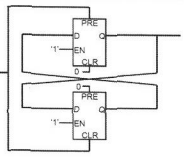
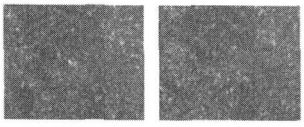
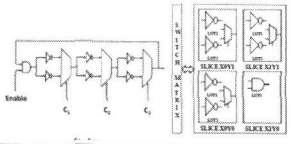
[표 1]은 기존의 연구된 PUF의 특징 및 장·단점과 상용화 여부를 나타낸다. 대부분의 PUF 회로들이 상용화 여부가 결정되지 않았거나 결국에는 실패했다. 이는 PUF 또는 PRF로서 충족시켜야 하는 랜덤성과 값의 안정성 등을 제대로 만족시키지 못했기 때문이다. 대부분의 회로들이 값의 쏠림 현상이나 온도나 시간에 따라 값이 변하는 현상 등의 발생하였다. 그렇지 않은 회로들은 PUF를 구현하는데 기존의 칩을 제작하는 반도체 회로 공정 이외에 새로운 도핑이나 투명 물질 등과 같은 별도의 제조 공정이 필요하다. 값의 측정도 CMOS 카메라나 Capacitance 측정기기 등의 별도의 장비들을 이용해야 하는 등의 실제 제품을 구현하는데 있어서 다양한 추가 비용 발생 요소들이 존재한다.

1.3 PUF의 요구사항

실제 제품 등에 적용할 수 있는 PUF 또는 PRF로서 가치 있는 구현 회로는 다음과 같은 특성을 만족시켜야 한다는 것을 알 수 있다.

- 같은 회로도에 의해서 제작 되지만 기기별 다른 값

〔표 1〕 기존의 PUF

이름(발표연도)	PUF 회로	특 징	장·단점	구현 기관	상용화여부
(2000) [3]		CMOS의 랜덤한 drain 전압을 이용	- 랜덤성 좋음 - Drift bit error로 인한 출력 값 변동	SiidTech, Portland State University	Hitachi ULSI 칩에 시도
Arbiter PUF (2005) [4]		두 경로간의 랜덤한 delay 차이를 이용	- 구현이 간단함 - Delay model을 이용해 출력값 예측 가능	MIT	Verayo 시제품 출시 (2008)
SRAM PUF (2007) [5]		SRAM의 unstable state를 이용	- SRAM을 이용하여 FPGA에서도 구현 가능 - 온도와 시간에 따라 값이 변동	Philips	Philips 생산칩에 시도
Coating PUF (2009) [6]		코팅 layer에 의한 랜덤한 capacitance값을 이용	- 안정성 및 랜덤성 좋음 - 두 가지 이상의 불투명한 물질에 의한 도핑 필요	NXP semiconductors	-
Butterfly PUF (2009) [7]		Latch의 불확실성을 이용한 SRAM PUF와 유사한 방식	- SRAM이 없는 FPGA에서도 구현 가능 - 0과 1중 하나로 쏠리는 현상 발생	Philips	Philips 생산칩에 시도
Optical PUF (2009) [8]		빛을 산란하는 도핑 물질의 랜덤한 반점 패턴을 이용	- 랜덤성 및 안정성 좋음 - 별도의 코팅을 위한 코팅 물질 및 측정 장비 필요	Philips	-
Ring oscillator PUF (2009) [9]		Ring Oscillator의 랜덤한 주파수를 이용	- 구현이 간단하고 FPGA에서도 구현 가능 - 환경에 따라 Oscillation 횟수 변경으로 값 변경	Virginia Tech.	-

을 가지는 회로

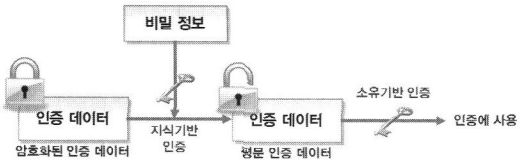
- 한번 제조 후에는 영구적으로 그 값을 유지하는 회로
- 인위적으로 추측이 불가능하며 진성 난수(True Random Number) 생성
- 저비용으로 높은 반도체 수율을 보장하는 회로

이전 연구를 살펴보면 많은 경우 안정성 및 랜덤성을 보장하지만 추가 설비를 필요로 하거나 회로는 간단하지만 환경 변화에 따른 안정성을 보장하지 못하는 것을 확인할 수 있었다. 그러므로 기존의 PUF는 위의 모든 요구사항들을 동시에 만족하기가 매우 어려움을 알 수 있다.

기존의 PUF 회로들은 반도체 소자들의 전기적 특성의 차이에 기반을 두고 랜덤값을 추출한다. 이러한 소자들의 전기적 특성은 시간이나 온도에 따라 변할 가능성이 높다. 따라서, 안정성을 강화하기 위해 공정 자체의 특성에 해당하는 소자를 생성하거나 단락 여부 등에 의한 무작위성을 이용하여 랜덤값을 만들어 내는 연구결과[10]가 발표되고 있는 상황이다.

2. 인증 시스템

인증 시스템은 크게 지식기반 인증과 소유기반 인증으로 나뉠 수 있으며 각각의 장단점이 존재한다. 자기



〔그림 1〕 이중 인증 시스템의 인증 과정

카드, 접속 카드, 보안 카드 등을 이용하여 시설이나 설비 등에 대한 접근 권한을 식별하거나 정당한 소유자임을 인증하는 것을 의미하는 소유기반 인증은 그 자체만으로는 도난이나 분실 등으로 인해 제 3자가 이를 소유할 경우 잘못된 인증이 될 가능성이 매우 높다. 알고 있다는 사실이 인증의 조건이 되는 지식 기반 인증은 PIN, 패스워드 등의 비밀 정보가 유출되지 않아야 되며, 그 값이 쉽게 추측될 수 없어야 한다.

일반적으로 지식기반 인증과 소유기반 인증의 장단점으로 인해 두 가지 인증 방식이 결합된 이중 인증이 사용된다. [그림 1]은 두 가지 인증 방식이 서로의 취약점을 보완한 이중 인증 과정의 한 가지 사용 방법을 나타낸다.

이중 인증 시스템의 대표적 예로는 공개키 암호화 알고리즘 기반의 공인 인증서를 이용한 전자 서명 기법이 있다. 현재 국내외에서 인터넷 뱅킹 등에서 주요 인증 방식으로 사용되고 있으며, 공인 인증 기관(CA:Certificate Authority)이 발행하는 공인 인증서를 이용하여, 신원 인증, 위조 및 변조 방지, 부인 방지를 수행할 수 있다. 정당한 사용자만 공인인증서를 사용할 수 있도록 발급 시 사용자가 알고 있는 패스워드를 필요로 하며 발급 받은 공인인증서도 패스워드를 이용하여 암호화되어 저장된다. 따라서 인증을 위해서는 공인인증서를 보유하고 있어야하며(소유 기반 인증) 이를 복호화하여 사용하기 위해 사용자가 알고 있는 패스워드가 필요하다(지식 기반 인증).

Ⅲ. PUF 기반의 인증 패러다임

디바이스 스스로 지식기반 인증을 수행하기 위해서는 디바이스만이 알고 있는 비밀 정보를 가지고 있어야 한다. 이러한 비밀 정보는 공인인증서 기반의 전자서명 기법을 수행 시 지식 기반 인증을 수행하기 위해서도 필수적이나 기존의 방법을 사물지능통신에 그대로 적용되기 어려움이 따른다. 이를 위해 PUF를 기반으로 한 지식기반 인증 패러다임을 제안하였다.

본 장에서는 제시한 인증 패러다임을 위한 사물지능통신의 구성 요소 및 인증 프로토콜에 대해 설명한다.

1. 구성요소

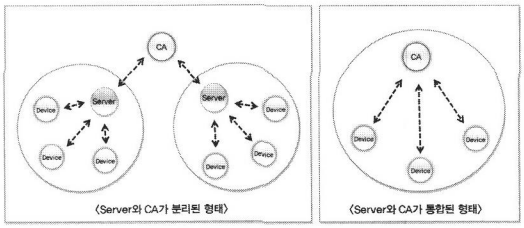
[그림 2]는 사물지능통신의 네트워크 모델을 나타낸다.

[그림 1]에서 볼 수 있듯이 사물지능통신의 구성 요소는 디바이스, 서버, CA로 이루어지며, 경우에 따라 CA와 서버는 통합될 수 있다.

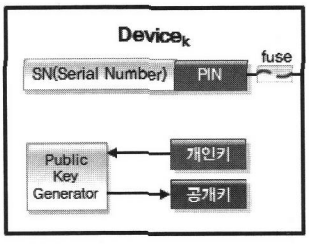
1.1 사물지능통신 디바이스

사물지능통신 네트워크의 터미널로 센서를 이용하여 정보를 수집하는 등 주로 데이터를 생산하여 서버로 전송하는 역할을 한다. 때때로 주변의 동일한 형태의 장치와 데이터를 주고받기도 한다. [그림 3]은 각 디바이스가 가지고 있는 고유 정보를 나타낸다.

각 디바이스는 자신의 고유 ID인 SN(Serial Number)와 함께 PUF 기반의 PIN을 가지고 있으며, PIN의 추출을 1회로 한정 짓기 위하여 퓨즈를 포함한 추출회로를 가지고 있다. 이와 함께 PUF를 개인키로 가지고 있으며 public key generator를 사용하여 공개키를 생성한다.



〔그림 2〕 사물지능통신 네트워크 모델



〔그림 3〕 Device 내 고유 정보

1.2 사물지능통신 서버

서버는 사물지능통신 서비스 플랫폼이 기반이 되어 네트워크에서 디바이스들이 생산한 데이터를 수집 및 가공하여 사용자에게 제공한다. 서비스 플랫폼에는 개방형 API(Application Platform Interface)를 활용하여 다양한 응용들이 실행된다. 서로 다른 목적을 위해 동작하는 각각의 응용은 디바이스와 데이터를 주고받고, 이를 유용한 정보로 가공하여 PC, 스마트폰과 같은 단말을 통해 사용자에게 제공한다. CA와 결합된 경우 각 디바이스들에 대한 인증 역할도 수행한다.

1.3 CA

각 디바이스가 정당한 사용자인지를 판단하기 위한 인증과정을 수행하며 디바이스와 디바이스가 통신을 할 경우 서로의 공개키를 자신의 개인키로 암호화하여 전송함으로써 각 디바이스가 통신을 원하는 다른 디바이스의 공개키의 정당성을 믿고 사용할 수 있도록 도와주는 역할을 수행한다.

2. 프로토콜

프로토콜은 인증을 위하여 사물지능통신 디바이스들의 정보(PIN, 공개키)를 수집하는 단계가 필수적으로 선행되어야 되며, 이 과정에서 수집한 정보는 사물지능통신 네트워크에서 각 디바이스의 정당성을 판단하는 기준 정보가 된다.

전체 과정은 다음의 4가지로 나뉘어 진행된다.

2.1 PIN 리스트 추출 단계

생산 공장에서 생산된 디바이스의 고유 ID에 해당하는 SN(Serial Number)를 디바이스에 삽입하고 각 디바이스에서 PIN를 추출하여 PIN 리스트를 생성하는 단계로 PIN 추출 회로를 차단하는 과정도 함께 일어난다. [그림 4]는 PIN 추출 및 추출회로 차단 과정을 나타낸다.

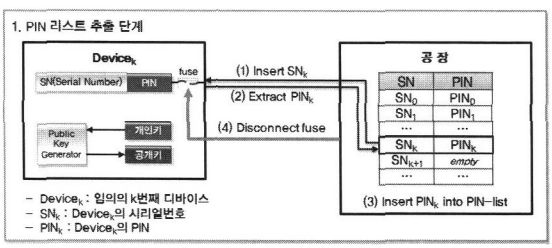
[그림 4]의 과정을 각각 설명하면 다음과 같다.

(1) Device 내부로 SN을 삽입한다.

(2) Device의 추출회로를 통해 PIN을 추출한다.

(3) 추출한 PIN을 해당 Device의 SN에 맞춰 PIN-list에 삽입한다.

(4) 추출회로에 과전류를 흘려보내 퓨즈를 절단시킨다.



〔그림 4〕 PIN 리스트 추출 과정

2.2 PIN 리스트 등록 단계

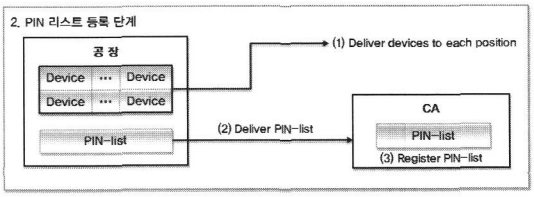
제품 구매 시 제품 인도와 함께 2.1에서 생성한 PIN 리스트를 안전한 오프라인 경로를 통해 전달하고 리스트 정보를 CA에 등록하게 된다. [그림 5]는 리스트 등록 단계를 나타낸다.

그림 5의 과정을 각각 설명하면 다음과 같다.

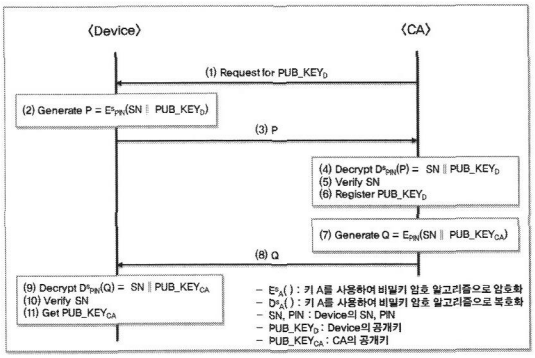
(1) 각 디바이스를 각자 사용될 위치로 배달한다.

(2) CA는 PIN-list를 안전한 오프라인 경로를 통해 전달받는다.

(3) 전달받은 PIN-list를 등록한다.



〔그림 5〕 PIN 리스트 등록 과정



〔그림 6〕 공개키 리스트 등록 과정

2.3 공개키 리스트 등록 단계

각 사물지능통신 디바이스의 공개키를 등록하는 단계이다. 디바이스가 네트워크에 추가된 후 [그림 6]의 과정을 거쳐 CA에 각 디바이스의 공개키가 등록된다.

[그림 6]의 등록과정을 자세히 설명하면 다음과 같다.

(1) CA가 Device로 공개키 요청 메시지를 전송한다.

(2) Device는 자신의 SN와 공개키를 자신의 PIN으로 암호화하여 메시지 P를 생성한다.

(3) P을 CA로 전송한다.

(4) CA는 이를 받아 해당 Device의 PIN으로 복호화한다.

(5) 복호화된 SN이 인증을 수행 중인 Device의 SN과 맞는지 동일성을 비교한다.

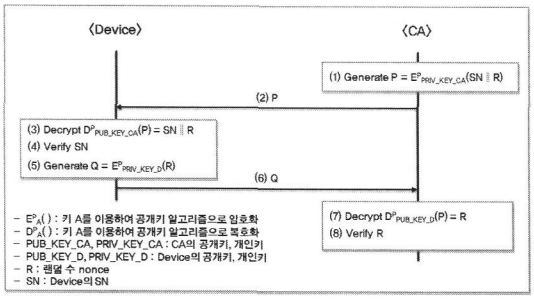
(6) SN의 동일성이 확인되면 Device의 정당성이 확인되었으므로 Device의 공개키를 등록한다.

(7-11) 동일한 방법으로 CA의 공개키를 Device에게 전달한다.

서로의 정당성은 복호화하여 나온 SN의 동일성을 비교함으로써 확인할 수 있다. 정당성이 확인되면 CA는 PIN 리스트에 Device의 공개키를 추가하고 Device는 CA의 공개키를 Device 내부의 비휘발성 메모리에 저장한다.

2.4 PIN 인증 단계

통신 개시 전 서로의 정당성을 확인하는 단계이다. 인증 과정은 서버와 CA가 같고 CA가 디바이스의 통신하는 경우와 서버와 CA가 다르거나 디바이스와 디바이스가 서로 통신하는 경우로 나뉜다.



〔그림 7〕 디바이스의 정당성 확인 과정

2.4.1 PIN 인증 - 서버와 CA가 같고 CA와 디바이스 간의 통신 시

CA와 디바이스는 서로 간의 공개키를 알고 있기 때문에 이를 이용하여 인증을 수행한다. 그 과정은 [그림 7]과 같다.

[그림 7]의 인증과정을 자세히 설명하면 다음과 같다.

(1) CA가 자신의 개인키로 Device의 SN과 인증용 랜덤 수인 nonce R를 암호화하여 메시지 P를 생성한다.

(2) 암호화한 메시지 P를 디바이스로 전송한다.

(3) 전송받은 메시지 P를 CA의 공개키로 복호화한다.

(4) 복호화하여 나온 SN을 자신의 SN과 동일성을 비교한다.

(5) 동일성이 확인되면 Device는 복호화하여 나온 R을 자신의 개인키로 암호화하여 메시지 Q를 생성한다.

(6) 암호화한 메시지 Q를 CA로 전송한다.

(7) 전송받은 메시지 Q을 해당 디바이스의 공개키으로 복호화한다.

(8) 복호화하여 나온 nonce R값이 자신이 보낸 nonce R과 동일한지 확인한다.

Device는 SN을 확인함으로써 P가 정당한 서버로부터 온 메시지임을 확인할 수 있으며 CA는 R을 확인함으로써 Device의 정당성을 확인할 수 있다.

2.4.2 PIN 인증 - 서버와 CA가 다르거나 디바이스와 디바이스간의 통신 시

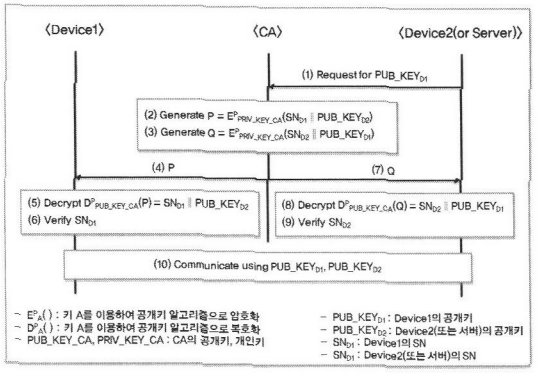
디바이스와 디바이스 간의 통신 시 서로의 공개키를 가지고 있지 않기 때문에 CA로부터 공개키를 안전하게 전달받아야 된다. 서버와 CA가 다른 경우 서버는 CA 입장에서 디바이스와 동일한 개체이기 때문에 이 경우 서버와 디바이스 간의 통신은 디바이스와 디바이스 간의 통신과 동일하다. 인증 과정은 [그림 8]과 같다.

[그림 8]의 인증과정을 자세히 설명하면 다음과 같다.

(1) 디바이스 중 하나(Device2 or Server)가 CA에 다른 디바이스의 공개키를 요청한다.

(2) CA는 자신의 개인키로 Device1의 SN과 Device2의 공개키를 암호화하여 메시지 P를 생성한다.

(3) CA는 자신의 개인키로 Device2의 SN과 De-



〔그림 8〕 TC 발급 과정

vice1의 공개키를 암호화하여 메시지 Q를 생성한다.

(4) 메시지 P를 Device1에게 전송한다.

(5) Device1은 P를 CA의 공개키로 복호화한다.

(6) 복호화하여 나온 SND1과 자신의 SN의 동일성을 비교한다.

(7-9) Device2는 4-6과 마찬가지 방법으로 진행하고 SND2과 자신의 SN의 동일성을 비교한다.

(10) 동일성이 확인되면 함께 복호화하여 나온 공개키의 정당성이 확인된 것이므로 이를 이용하여 서로 통신 한다.

각 디바이스는 CA에 인증 받은 서로의 공개키 값을 알게 되므로 이 공개키를 이용하여 안전하게 통신할 수 있다.

Ⅳ. 결론

본 논문에서는 사물지능통신에서 기존의 소유기반 인증과 양립이 가능한 PUF에 기반을 둔 새로운 지식기반 인증의 패러다임을 제시하였다. 제안한 인증 패러다임에서는 2개의 PUF가 사용되어 하나는 PIN을, 나머지 하나는 개인키로써 이에 대응되는 공개키 생성에 사용된다. 공장 생산 출하 과정에서 1회에 한해 출력된 PIN은 디바이스와 CA만이, 개인키는 디바이스만이 알고 있기 때문에 이를 기반으로 지식기반 인증이 일어나게 된다.

PUF로 구현된 두 가지 인증 요소인 PIN과 개인키는 복제가 불가능하고 값을 예측하기 어렵다는 PUF의 특징을 가지고 있어 유출이 거의 불가능할 뿐만 아니라 공격자가 매우 큰 비용을 소모하여 값 유출에 성공하거나 설계 도면을 획득하게 되더라도 디바이스마다 그 값이 다르므로 획득한 비밀값을 다른 디바이스에 적용하는 것이 불가능하다. 그리고 PUF의 높은 랜덤성으로 인해 값이 추측될 가능성도 거의 불가능에 가깝다. 또한 PUF를 사용함으로써 중요 정보를 비휘발성 메모리에 직접 저장할 필요성이 없어지기 때문에 메모리 공격으로부터 자유로우며 PUF회로는 비트 단위로 구현되어 내부에 흩어져 있기 때문에 *PUF 자체가 나타내는* 정보를 물리적 공격으로 파악하기란 불가능에 가깝다.

제안하는 새로운 지식인증 패러다임은 각 디바이스의 PIN 리스트 추출 및 등록 단계, 공개키 등록 단계의 사전 정보 수집 단계를 거쳐 디바이스와 CA간, CA를 통한 디바이스와 디바이스간의 인증을 수행하는 프로토콜을 가지고 있으며 이는 RFID 센서 네트워크, 스마트 그리드, 클라우드 컴퓨팅 네트워크 등 통신 및 데이터 처리 방식 등에 따라 매우 다양하게 구현되는 사물지능통신에 보편적으로 적용이 가능할 것으로 기대된다. 또한, 새로운 인증 패러다임은 PUF에 기반을 두어 안정적인 지식기반 인증을 수행할 수 있고 물리적 공격에 강인할 뿐만 아니라 기존의 소유기반 인증과 양립이 가능하기 때문에 기존의 공인인증서에 기반한 인증 기법의 지식 기반 인증 영역에 적용될 수 있을 뿐만 아니라 내부에 공개키 쌍 중 개인키를 보유하고 있으므로 공인인증서 발급 없이 그 자체적으로도 안정적인 인증을 수행할 수 있을 것으로 기대된다.

이 패러다임에서 보완해야 할 향후 연구로는 디바이스가 다른 사용자에게 탈취되어 사용될 때에 발생될 수 있는 문제에 대한 문제점 분석 및 해결 방안이다. PUF를 이용하여 PIN과 개인키를 구현했기 때문에 디바이스가 복제되어 사용되는 것은 방지할 수 있으나, 공격자가 신용 카드나 스마트 미터기와 같은 디바이스를 탈취한 후 그대로 사용하여 결제 등이 일어나는 경우, 이를 막을 방법이 없다. 따라서, 이러한 취약점이 발생할 수 있는 상황에 대한 use case를 분석하고 이를 해결하기 위한 인증 방안에 대해 필요하다.

참고문헌

[1] 이승훈, 이재성, 김동규, "TPM(Trusted Platform

Module) 칩상의 코어 모듈의 취약성 분석", 대한전자공학회 하계종합학술대회, pp. 70, 2010.

[2] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld. "Physical One-Way functions," Science, 297(5589), pp. 2026-2030, September 2002.

[3] K. Lofstrom, W. Daasch, D. Taylor, "IC Identification Circuit using Device Mismatch," IEEE Intl. Solid-State Circuits Conf. Digest of Technical Papers, 43, 2000.

[4] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas. "Extracting Secret Keys From Integrated Circuits," IEEE Trans. on VLSI Systems, 13(10), pp. 1200-1205, October 2005.

[5] J. Guajardo, S. S. Kumar, G. Schrijen, P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," CHES2007, September 2007.

[6] D. Roy, J. H. Klootwijk, S. Member, N. A. M. Verhaegh, H. H. A. J. Roosen, R. A. M. Wolters, "Comb Capacitor Structures for On-Chip Physical Unclonable Function," IEEE Trans. on Semiconductor Manufacturing, 22(1), February 2009.

[7] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, P. Tuyls, "Extended Abstract: The Butterfly PUF Protecting IP on every FPGA", IEEE Intl. Workshop on Hardware-Oriented Security and Trust, pp. 67-70, June 2008.

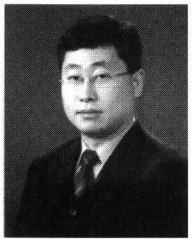
[8] K. Kursawe, A.R. Sadeghi, D. Schellekens, B. Skoric, P. Tuyls, "Reconfigurable Physical Unclonable Functions : Enabling Technology for Tamper-Resistant Storage," IEEE Intl. Workshop on Hardware-Oriented Security and Trust, pp. 22-29, 2009.

[9] A. Maiti, P. Schaumont, "Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators," Intl. conf. on Field Programmable Logic and Applications, pp. 703-707, 2009.

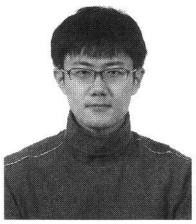
[10] 김동규, 최병덕, 김태욱, "식별키 생성 장치 및 방법", PCT 특허(KR2011/000605), 2011.

[11] 방송통신위원회, "사물통신 기반구축 기본계획", 2009.

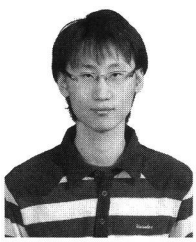
〈著者紹介〉



김 동 규 (Kim, Dong Kyue)
정회원
1992년 2월 : 서울대학교 컴퓨터공학과 졸업
1994년 2월 : 서울대학교 컴퓨터공학과 석사
1999년 2월 : 서울대학교 컴퓨터공학과 박사
1999년 9월~2006년 2월 : 부산대학교 컴퓨터공학과
2006년 3월~현재 : 한양대학교 전자통신컴퓨터공학부 및 융합전자공학부
관심분야 : 암호 알고리즘, 임베디드보안시스템 설계, Security System on Chip(SoC)



이 재 성 (Lee, Jae Seong)
2008년 2월 : 한양대학교 전자전기컴퓨터공학과 졸업
2010년 2월 : 한양대학교 전자컴퓨터통신공학과 석사
2010년 3월~현재 : 한양대학교 전자컴퓨터통신공학과 박사과정
관심분야 : Cryptology, 암호화 모듈 칩 설계, PUF



최 필 주 (Choi, Piljoo)
2010년 2월 : 한양대학교 전자통신컴퓨터공학과 졸업
2010년 3월~현재 : 한양대학교 전자컴퓨터통신공학과 석사과정
관심분야 : Cryptology, 암호화 모듈 칩 설계