http://dx.doi.org/10.14400/JDC.2015.13.10.343

M2M 환경의 디바이스 키 보호를 위한 암호 알고리즘 응용 기법

최도현*, 박중오**
숭실대학교 컴퓨터학과*, 동양미래대학 정보통신공학과**

Encryption Algorithm Technique for Device's key Protect in M2M environment

Do-Hyeon Choi*, Jung-Oh Park**
Computer Science, Soongsil University*
Information & Communication Engineering, DongYang Mirae University**

요 약 현재 M2M 환경은 다양한 서비스가 기관 및 기업이나 일상생활로 확대되면서 관련 기술의 보안 취약성 발생 가능성이 이슈화되고 있다. 본 논문은 이러한 보안 취약성 문제를 해결하기 위해 M2M 환경의 디바이스 키 보호를 위한 암호 알고리즘 응용 기법을 제안한다. 제안 기법은 타원곡선 암호 기반으로 초기 키 교환과 서명 교환을 통해 보안 세션을 생성하였고, 화이트박스 암호는 보안 세션 키를 이용하여 화이트박스 테이블을 생성하는 암호화에 응용하였다. 암호 알고리즘 적용 결과, 타원곡선 암호는 통신 세션에 대한 경량 화된 상호인증, 세션 키 보호를 제공하고, 화이트 박스 암호는 기존 암호 알고리즘과는 다른 방식으로 암호화에 사용되는 세션 키 보호를 보장하였다. 제안하는 프로토콜은 데이터변조 및 노출, 중간자 공격, 데이터 위조 및 변조 공격에 대해 안전한 장점이 있다.

주제어 : 사물지능통신, 화이트박스 암호화, 디바이스 인증, 타원곡선 암호, 상호 인증

Abstract With the diverse services of the current M2M environment being expanded to the organizations, the corporations, and the daily lives, the possibility of the occurrence of the vulnerabilities of the security of the related technologies have become an issue. In order to solve such a problem of the vulnerability of the security, this thesis proposes the technique for applying the cryptography algorithm for the protection of the device key of the M2M environment. The proposed technique was based on the elliptic curve cryptography Through the key exchange and the signature exchange in the beginning, the security session was created. And the white box cipher was applied to the encryption that creates the white box table using the security session key. Application results cipher algorithm, Elliptic Curve Cryptography provides a lightweight mutual authentication, a session key for protecting the communication session and a conventional white-box cipher algorithm and was guaranteed the session key used to encrypt protected in different ways. The proposed protocol has secure advantages against Data modulation and exposure, MITM(Man-in-the-middle attack), Data forgery and Manipulation attack.

Key Words : M2M, White Box Encryption, Device Authentication, Elliptic Curve Cryptography, Mutual Authentication

Received 8 August 2015, Revised 18 September 2015
Accepted 20 October 2015
Corresponding Author: Jung-Oh Park
(DongYang Mirae University)
Email: jopark13@dongyang.ac.kr

ISSN: 1738-1916

1. 서론

사물지능통신(M2M, IoT)은 인간 대 사물, 사물 대 사물 간 영역에 걸쳐 다양한 네트워크 인프라를 연계하여 공유하고 상호 전달하는 서비스로 최근 전 산업 분야에서부터 일상생활까지 광범위하게 확대되고 있다[1].

M2M 연결된 디바이스는 현재 전 세계 1.5조개 단말기 중 99.4%는 미연결 상태에서 2020년까지 세계 500억개의 단말기가 인터넷으로 연결될 것으로 전망하였으며, 2018년 고정형 및 모바일 연결을 포함한 전 세계 IP 트래픽이 연간 1.6 제타바이트에 달해 1조 5천억 기가바이트를 넘어설 것으로 예상하고 있다[2].

현재 M2M 시장 활성화와 수요 증가 등 세계 글로벌 선도업체들의 기술을 선두로 플랫폼, SW, 하드웨어, 보안 등 M2M 관련 표준화를 진행 중으로, 이중 M2M 서비스 활성화를 위한 위협 요건 중 핵심요인으로 핵킹, 개인정보 유출 등 보안 분야의 기술적, 정책적 대응방안에 대한 문제를 논의 중에 있다[3].

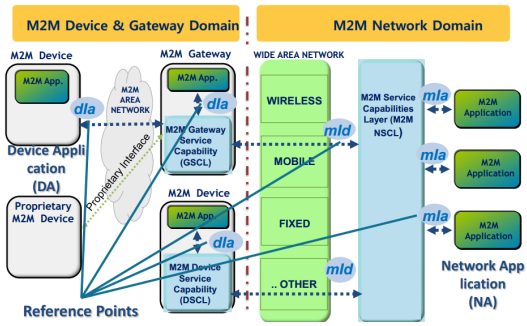
M2M 환경의 보안 프로토콜 기술은 데이터 보호를 위한 보안 프로토콜과 반드시 디바이스의 낮은 연산 능력과 적은 메모리 공간의 특성을 고려하는 것을 요구사항으로 정의하고 있다[4,5]. 최근 서비스 요구사항에 적절한 보안 기술 적용을 위해 국제전기통신연합(ITU-T SG17)은 M2M 환경에 적용될 보안 기술로 부분 암호화 방안, IP 기반 네트워크에서 보안 문제 해결 메커니즘, 역추적 기법 등 보안 기술에 대한 신규 아이템을 제안 중에 있다[6,7,8].

제한적인 M2M 환경에서 보안 프로토콜은 표준 요구사항의 통신의 효율성을 준수해야 하는 것이 선행되어야 한다. 본 논문은 M2M 환경을 고려한 통신의 효율성과 보안성을 제공하는 디바이스 키 보호를 위한 암호 알고리즘 응용 기법을 제안한다. 본 논문의 2장은 관련연구 3장은 제안하는 응용 기법, 4장은 안전성 및 성능분석, 5장 결론으로 마친다.

2. 관련연구

2.1 M2M Architecture & Security Requirement

M2M 표준은 M2M 시장 확대 및 활성화, 단일 플랫폼 확보, 서비스 활성화 등을 위해 oneM2M, ETSI TC M2M, 3GPP, IEEE 등 광범위하게 표준화가 논의되고 있으며 ETSI TC M2M에서는 타 기술/표준의 호환성과 실제 구현할 때 참조 가능한 서비스 인터페이스 규격 표준화를 담당하고 있다[9,10,11]. [Fig. 1]은 ETSI TC M2M의 High level architecture를 나타낸다[12].



[Fig. 1] ETSI TC M2M - Architecture(Service Layer)

제어와 데이터 전송을 위한 mla(M2M application interface), mld(M2M to device interface), dla (Device application interface) 각 인터페이스 간 연결을 담당하는 보안 파트 영역인 xSEC(NSEC, GSEC, DSEC)은 SCL(Service capabilities layer)의 서비스 요구사항 항목으로 정의된다[13].

<Table 1>은 ETSI TS의 M2M 서비스 보안 요구사항을 나타낸다.

〈Table 1〉 ETSI TS Security Requirement (Service Layer)

	Category
1	Authentication
2	Authentication of M2M service layer capabilities or M2M applications
3	Data integrity
4	Prevention of abuse of network connection
5	Privacy
6	Multiple actors
7	Device/Gateway Integrity Validation
8	Trusted Environment
9	Security credential and software upgrade at the Application level
10	System protection

보안 요구사항은 디바이스, 게이트웨이 등 각 M2M 환경 구성요소의 상호인증과 무결성, 데이터 보호 등 다수의 디바이스와 서비스 제공자 간의 신뢰된 end-to-end

서비스를 요구사항 등으로 정의한다. 기타 M2M에 관련된 기본 통신 프로토콜은 M2M 환경에 상호연동을 위한 IETF RFC CoAP 프로토콜이 진행단계에 있다[14].

2.2 ECC and Whitebox Cipher

2.2.1 ECC(Elliptic Curve Cryptography)

ECC는 유한체(Finite field)상의 타원곡선 점들 간의 연산에서 정의되는 이산대수 문제(Discrete logarithm problem)의 어려움을 이용하여 기존 대표적으로 사용되는 RSA 암호와 더불어, ANSI와 IEEE 표준 공개키 암호 방식으로 WAP(Wireless Application Protocaol) 표준으로 채택되어, 스마트폰 등에 의한 이동통신 환경에서 암호화 기능을 처리하는 수단으로 각광받고 있다. ECC는 RSA 비해 암호화 과정에 소요되는 연산 처리량이 적고, 키 관리가 용이하다[15,16]. <Table 2>은 ECC와 RSA/DSA의 키 크기 별 보안강도 비교를 나타낸다.

〈Table 2〉 ECC vs RSA(Key sizes for Security levels)

MIPS	ECC (bit)	RSA/DSA (bit)
104	106	512
108	132	768
1011	160	1024
1020	210	2048
1078	600	21000

ECC의 국제 표준 IOS/IEC 표준은 알고리즘의 추상적인 기능위주의 기술만을 담고 있어 실제 구현을 위해서는 IETF의 응용 표준(IPSec, TLS, WTLS, S/MIME 등)을 참조하도록 하고 있다[17].

최근에 채택된 WIPO 특허들(Nokia, Thomson Licensing, Amtel, IBM 등)의 핵심 사항들은 양정수 k에 대해 모듈러 감소 등의 기법을 적용하여, 2배화 및 점들의 덧셈들의 반복 횟수를 감축하는 기법들과 2배화 및 덧셈 자체를 효율적으로 처리하는 기법들이다[18,19].

ECC의 덧셈 연산은 최근까지 안전하다고 알려진 RSA의 모듈러 곱셈연산과 대등한 것으로 알려졌기 때문에 연산의 효율성에 있어서 자원이 제한적인 환경에 적절한 암호로 활용될 수 있다[20,21].

2.2.2 Whitebox Cipher

화이트박스 암호는 콘텐츠의 저작권 보호를 위한 방안으로 소프트웨어로 구현되어 신뢰할 수 없는 디바이스에서 암호 알고리즘이 실행되어도 외부의 공격에 대해서 키를 안전하게 보관할 수 있고, 비 인증 단말에서 암호키가 드러나지 않는 특징을 가진다. 기존의 암호 키를 유추하기 위한 방법으로 알려진 블랙박스 공격, 그레이박스 공격, 화이트 박스 공격에 대한 저항성을 가졌으며, 기존 암호 동작 과정과 달리 암호 키가 암호 메커니즘 속에 섞여(Obfuscation)있기 때문에 공격자 입장에서 암호 키의 중간 계산과정과 메모리 정보에서 키를 유추하기 어려운 가정 하에 동작한다[22,23]. [Fig. 2]은 화이트박스 암호의 기본 원리를 나타낸다.

$$\underbrace{F^{-1}\circ M_1^{-1}}_{\text{table}}\circ\underbrace{M_1\circ X_1\circ M_2}_{\text{table}}\circ\underbrace{M_2^{-1}\circ M_3^{-1}}_{\text{table}}\circ\cdots\underbrace{M_{2i-1}\circ X_i\circ M_{2i}}_{\text{table}}\circ\underbrace{M_{2i}^{-1}\circ G}_{\text{table}}$$

$$\Leftrightarrow F^{-1}\circ X_1\circ X_2\circ\cdots\circ X_i\circ G$$

[Fig. 2] Whitebox cipher basics

화이트박스 암호는 암호 동작과정에 룩업 테이블을 생성하고 그 내부에 암호 키를 숨기는 것이 특징이지만 암호화 데이터와 함께 테이블 전체를 하나의 키로 볼 수 있기 때문에 통신 데이터양과 저장소, 메모리 부족 등 해결할 문제가 존재한다.

대표적으로 알려진 화이트박스 암호로는 S.Chow가 제안한 화이트박스 AES(WB-AES), 화이트박스 DES(WB-DES), Y Xiao의 화이트박스 AES, P Jong-Yeon의 화이트 박스 AES 등 동일한 개념의 화이트박스 암호를 룩업테이블 생성과정 및 동작과정을 변형하고 경량화한 연구들이 있다[24, 25, 26].

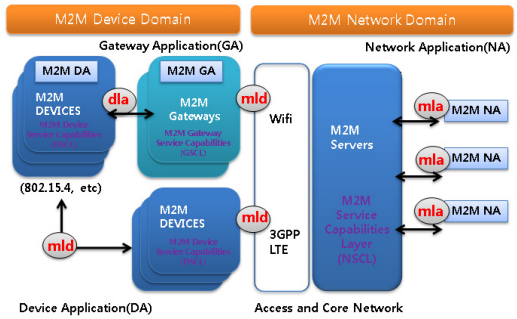
화이트박스 암호는 현재 콘텐츠 등 보안 분야 이외에 다른 분야 응용에 대한 연구가 부족한 실정이다. 테이블 증가로 인한 통신량 증가, 비교적 많은 메모리 사용량 등 문제를 해결할 수 있다면 디바이스 내부 키 보호에 특화되어 활용될 수 있을 것으로 판단된다.

3. 제안하는 암호 알고리즘 응용 기법

3.1 M2M 환경 및 통신 프로토콜 정의

본 논문의 통신 프로토콜 정의를 위한 M2M 환경은

[Fig. 3]와 같다. 본 논문에서 암호 알고리즘을 적용하는 프로토콜은 가장 통신구간의 자원이 제한적인 M2M 디바이스 to M2M 디바이스(mld) 구간을 대상으로 정의한다.



[Fig. 3] M2M Environment

ETSI 표준 통신 프로토콜 시나리오를 기반으로 DA가 제외된 M2M 디바이스가 데이터 전달을 위해 근접한 M2M 디바이스와 통신하고 M2M GA로 데이터를 교환한다. DA가 제외된 M2M 디바이스는 Wifi, 3GPP, LTE 등 M2M GA로 직접 통신할 수 없는 센서 모듈들이 사용된다. <Table 3>은 전체 프로토콜 시나리오와 통신 모듈의 종류를 설명한다.

〈Table 3〉 Communication scenarios and M2M module type

CASE	Connection Scenario	Feature
1	M2M DA - M2M GA - M2M Sersers	Wifi, 3GPP, LTE, etc.
2	M2M DA - M2M Servers	
3	M2M Devices(non- DA) - M2M DA - M2M GA - M2M Servers	Not provide(M2M GA, M2M Servers)

CASE 1,2의 M2M 디바이스는 Wifi, 3GPP, LTE 등 IP 기반 통신이 가능한 M2M 모듈로 정의한다. CASE 3의 M2M Devices(non-DA)는 저사양의 RF 통신 또는 IR 통신 인터페이스로 디바이스 간 통신을 하고 데이터를 수집하여 M2M DA로 전송한다. 이 통신 구간은 저수준 하드웨어 스펙의 제한된 통신 성능을 제공하기 때문에 암호 알고리즘 적용은 CASE3를 기준으로 통신 성능 최적화를 진행한다.

CASE 1,2는 CASE 3의 통신 프로토콜의 성능 분석 결과에 따라 암호화 강도를 다르게 적용하여 통신 프로토콜의 안전성과 통신 효율성을 최적화한다. 전체 통신 프로토콜의 흐름은 사전키 교환, 암호화, 데이터 재전송, 세션종료 및 키 갱신 과정에 적용한다.

3.2 암호 알고리즘 정의

암호 알고리즘은 다음과 같이 구분된다. 디바이스 상호인증을 위한 타원곡선 암호(ECDSA:Elliptic Curve Digital Signature Algorithm)는 WTLS 권고 곡선 3, Field size 163, y^2 = x^3 + ax^2 + b; over GF(2^163)를 사용한다.

키 교환에는 ECDH(Elliptic Curve Diffie-Hellman) 기반 화이트박스 암호(AES-WB)를 사전키 공유에 적용한다. <Table 4><Table 5>은 각각 타원곡선과 화이트박스 암호 알고리즘 파라미터와 연산과정, 파라미터 설명을 나타낸다.

〈Table 4〉 Parameter calculation process

Parameter	Description	
Eq(a, b)	Public ecc parameter p, n, q	
DPriKey	Select Private Key	
DPuKey	Eq(a, b) X DPriKey	
SPriKey	Select Private Key	
SPukey	Eq(a, b) X SPriKey	
GPriKey	Select Private Key	
GPukey	Eq(a, b) X GPriKey	
R	Generate Random Number	
Dsig(r, s)	Sign : (x1, y1) = R X G(x,y) mod q r = x1 mod n s = (R-1 (H(m) + d * r) mod n	Verification : e = SHA1(m) w = s-1 mod n u1 = ew mod n and u2 = rw mod n X = u1p + u2q v = x1 mod n v compare r
Ssig(r, s)		
H(m)	SHA1(message)	
EPriKey	Selected Eq(a, b) X R	
WCKC	White box(Ciphertext, Dsig)	

공개된 파라미터와 비밀키를 이용하여 공개키를 생성하고, n을 타원곡선의 위수라고 할 때 메시지 m에 대한 서명과 메시지 다이제스트 연산은 <Table 5>와 같다.

ECDH 키 교환을 위해 사전에 공개된 파라미터와 각각의 개인키를 이용하여 공개키를 생성한다. 사전키 교환단계에서 올바른 디바이스임을 인증하기 위해 서명을 사용한다.

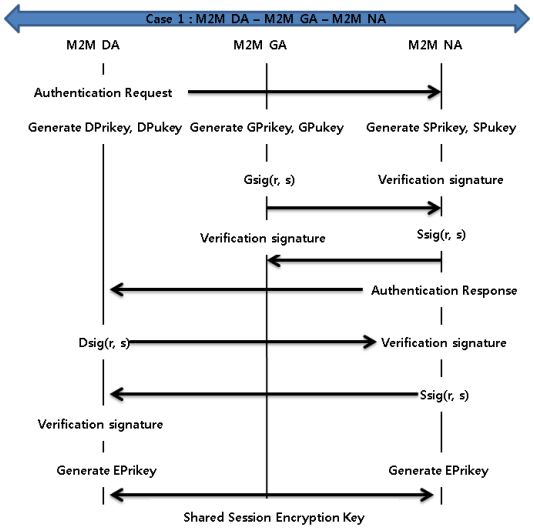
〈Table 5〉 Encryption algorithm parameters

Parameter	Description
Eq(a, b)	elliptic curve with parameters
DPriKey	M2M Device's Private Key
DPuKey	M2M Device's Public Key
SPriKey	Server's Private Key
SPukey	Server's Public Key
R	Random Number
Dsig(r, s)	Device's Signature
Ssig(r, s)	Server's Signature
H(m)	Message Digest
WCKC	White Box Table(AES)
SPriKey	Session Key(Encryption)

3.3 프로토콜 과정과 암호 알고리즘 적용

3.3.1 사전키 교환

ECDH는 중간자 개입 공격의 가능성이 있기 때문에 개인키와 공개키 생성 이후 서명을 교환을 진행한다. 이후 서로 암호화를 위한 세션키를 공유한다. [Fig. 4]은 CASE 1의 사전키 교환과정을 나타낸다.

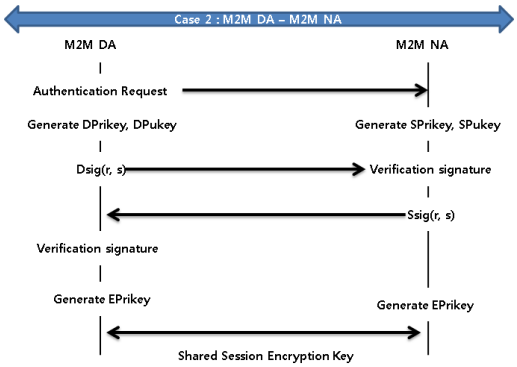


[Fig. 4] Key exchange(CASE 1)

CASE 1 통신은 중간 지점인 게이트웨이 디바이스의 인증을 선행한 후 M2M 디바이스 인증을 수행한다. [Fig. 5]은 CASE 2의 사전키 교환과정을 나타낸다.

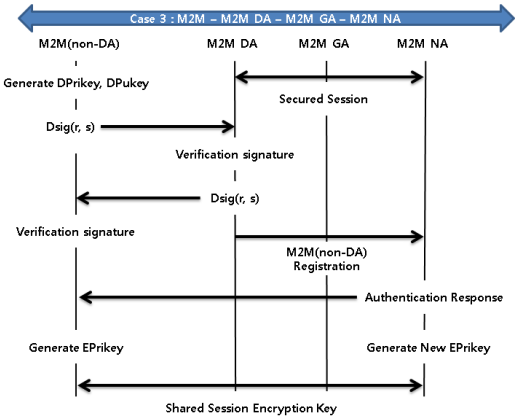
CASE 2 통신은 게이트웨이를 거치지 않기 때문에 서버와 M2M 디바이스 인증을 수행한다. CASE 1과 동일하게 세션키를 공유한다.

CASE 3 통신은 기존에 설립되어 있는 CASE 1,2 보안세션에서 생성한 파라미터를 이용하여 M2M (non-DA)를 인증한다. 연산에 필요한 하드웨어 성능을 충족하지 못하는 저수준 모듈들은 자체적으로 연산 수행이 불가능하기 때문이다.



[Fig. 5] Key exchange(CASE 2)

[Fig. 6]은 CASE 3의 사전키 교환과정을 나타낸다. 중간과정에서 M2M 서버에서 각 장비에 대한 제어를 수행하기 때문에 M2M 디바이스에 대한 등록을 진행하고 M2M(non-da) 대신 새로운 세션키를 공유한다.



[Fig. 6] Key exchange(CASE 3)

M2M 디바이스(non-DA)의 인증을 위해서는 CASE 1,2의 구간에 보안 세션이 설립되어 있어야 한다. 세션이 미리 설립되지 않은 경우 이전 통신과정에서 등록된 서버의 M2M 디바이스 정보를 활용하여 CASE 1,2의 과정

으로 인한 통신 효율성 감소를 최소화한다. 이는 세션이 설립되어 있는 경우 화이트박스 테이블을 교환하여 키 교환 과정을 생략할 수 있는 장점을 활용한 것이다.

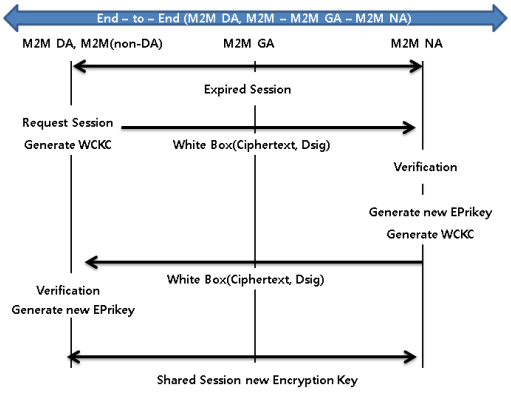
3.3.2 데이터 암호화

CASE 1,2,3에서 생성된 세션키는 암호화 용도로 생성된 키이다. 세션키를 이용하여 화이트 박스 테이블을 생성하고 교환한다. 기존 보안 프로토콜과 달리 테이블 자체에 암호문과 검증용 서명을 포함하는 특징이 있다.

검증용 서명은 암호화 용도인 세션키를 생성하는 파라미터 R을 이용하여 생성하였기 때문에 암호문의 변조 확인 용도로 사용할 수 있다. 이는 화이트 박스 암호 연산 이외에 추가 연산의 오버헤드를 최소화하기 위해서이다.

3.3.3 세션 키 갱신 및 키 폐지

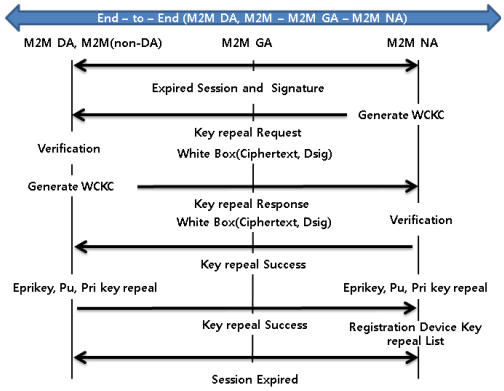
슬립 모드 혹은 연결 종료 및 데이터 전송의 문제로 키 갱신을 필요로 할 때에는 키 생성에 필요한 파라미터를 화이트 박스 암호 테이블 내에 암호화된 키 갱신 또는 종료 메시지, 갱신된 키와 서명을 포함하여 전송한다. [Fig. 7]은 키 갱신 과정을 나타낸다.



[Fig. 7] Session Key Update(Data Encryption)

보안 세션이 유지되는 경우 키 갱신은 세션키(암호화키)를 화이트박스를 연산에 적용되는 세션키를 갱신하고, 새로운 디바이스 등록이나 통신 문제로 인한 보안 세션의 종료 이후 새로운 키 발급 과정에만 재발급(CASE 1,2,3) 과정을 수행한다.

기존키 갱신 과정과는 달리 화이트박스 테이블 자체에 키가 섞여 있는 특징을 이용하기 때문에 추가적인 키 교환 과정을 생략할 수 있다. [Fig. 8]은 키 폐지 과정을 나타낸다.



[Fig. 8] Key revocation process

전체키 폐지 과정에서는 타원곡선 및 화이트 박스 암호에서 사용된 세션키와 서명에서 사용한 개인키와 공개키 쌍 또한 폐기하고, M2M 디바이스에 대한 등록을 제거하여 키 폐지 리스트에 등록하여 이후 키 관리 용도로 활용한다.

4. 성능 평가

제안 프로토콜의 안전성과 성능을 분석 비교분석 한다. 본 논문에서 응용된 타원곡선과 화이트박스 암호는 공개 검증된 자체 알고리즘의 순수 암·복호화에 대한 성능이 안전하다고 가정한다.

4.1 안전성 분석

• 데이터 유출 및 노출 방지 : RSA 1024 비트에 준하는 163 비트 타원곡선군을 선택하였고 상호인증을 위해 사전키 교환에 필요한 보안 세션 설립 후, 화이트박스 암호화를 통해 통신을 수행하기 때문에 강력한 데이터의 안전성을 보장한다.

ECC 기반 서명용 개인키의 보안성은 오프라인 수준에서 무차별 공격에 대해 RSA와 동일한 수준인 1024 비트키에 대하여 $(1/2)^{1024} \times 100\%$ 수준의 공격 성공률을,

2048 비트 키에 대하여 $(1/2)^{2048} \times 100\%$ 수준의 공격 성공률로 공격이 어렵다.

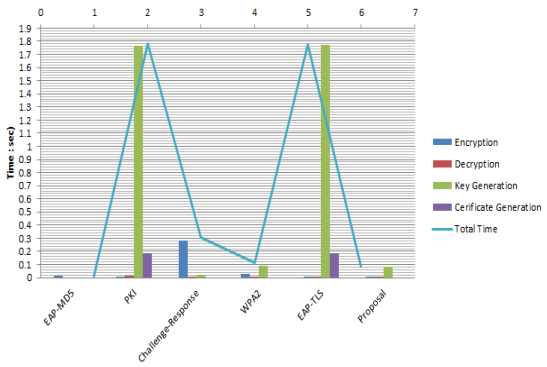
• MITM : 각 노드는 자기 자신을 인증 할 수 있는 상호인증 과정, 각 서명에 타임스탬프를 포함하여 중간자 공격(디바이스의 인증정보를 재사용)에 안전성을 보장한다. 공격자가 중간 세션을 가로채더라도 1차적으로 화이트박스 테이블 내부에 키가 섞여 있기 때문에 암호키를 유추할 수 없다.

• 위조 및 변조 방지 : 위조나 변조 시도가 있을 시 보안 세션에서 생성하는 임의키(r)를 이용하여 안전한 서명을 생성하고 보안 세션 이후 화이트박스 내 세션키를 섞고 서명을 포함하는 암호화를 진행하기 때문에 위조 및 변조에 대한 무결성을 제공하며, 공격자가 화이트박스 내 세션키를 알게 되더라도 타원곡선에서 생성한 임시 비밀키를 계산하기 어려운 수학적 문제이기 때문에 공격에 안전성을 보장한다.

• 인증정보 생성값 유출 방지 : 모든 통신 수행 과정은 사전키 교환을 위한 서명과 타원곡선 암호화를 초기 통신과정에서 수행하기 때문에 생성값 유출에 대한 안전성을 보장한다. 또한 이전 사용된 세션키는 보안 세션의 종료시 재발급하는 과정과 전체 키 폐지과정에서 재발급되거나 폐지되기 때문에 긴 세션키에 대한 문제점을 키 갱신 과정으로 해결하였다.

4.2 성능분석

[Fig. 9]와 <Table 6>은 기존 알고리즘과 제안 알고리즘의 성능분석 결과를 나타낸다.



[Fig. 9] Performance Chart

〈Table 6〉 Protocol Performance Analysis

Protocol	EAP-MD5	PKI	Challenge-Response	WPA2	EAP-TLS	Proposal
Properties	One-way authentication	Mutual authentication	One-way authentication	One-way, Mutual authentication	Mutual authentication	Mutual authentication
Algorithm	MD5	RSA2048bit SHA2	Triple DES	AES-CCMP	RSA1024bit SHA1	ECC160bit SHA1
feature	Symmetric Key	Public Key	Symmetric Key	Symmetric Key	Dynamic key generation	Public Key, White Box
Encryption	0.014094700	0.002331281	0.285572238	0.027160418	0.001907062	0.001383524
Decryption	-	0.014008471	0.001219149	0.000111251	0.003996590	0.001885504
Key Generation	-	1.764595332	0.019076773	0.087751385	1.770333840	0.085066332
Certification Generate	-	0.186428914	-	-	0.185458446	-
Total Time	0.014094700	1.780935084	0.305868160	0.115023054	1.776237492	0.088335360

• 성능분석 환경 : Intel(R) Core(TM)2 Quad CPU Q9400 2.66GHz, 6.00GB Memory, Windows7 64bit, EClipse(JAVA) Security API - Cryptography API

• 알고리즘 비교대상 : 현재 M2M 표준은 암호화 이외에 상호인증 프로토콜 등 보안 관련된 표준화와 다양한 연구가 진행 중에 있다. 본 성능 분석의 비교대상인 기존 알고리즘은 범용 적이고 일반적인 단방향 및 상호 알고리즘들을 대상으로 비교분석 한다.

각 알고리즘 대상은 통신 노드의 지연을 제외한 순수 알고리즘의 연산 능력을 비교하였다. 각 연산 능력의 비교 분석을 통해 본 논문에서 제안한 알고리즘의 성능의 효율성을 비교할 수 있다. 키 생성이나 복호화 자체가 필요 없는 단순 해쉬 함수 연산으로 인해 MD5가 가장 빠른 것으로 나타났으며, 이외 Triple DES가 AES-CCMP에 비해 약 0.19(sec) 차이로 50% 이상 효율적인 것으로 나타났다.

Triple DES(알고리즘 구조상 키 생성 연산 2회)는 AES-CCMP와 비교하여 키 생성 속도가 빠르고, 암호화 부분에서 성능의 차이 약 0.258(sec)로 90% 이상 효율적인 것으로 나타났다. 순수 AES가 아닌 CBC 모드 MAC

생성 과정에서 성능의 차이가 발생하는 것으로 분석된다.

제안 알고리즘인 ECC의 경우 암호화 부분에서 Triple DES, 키 생성에서 AES-CCMP와 성능이 비슷한 성능으로 나타났다. MD5의 경우 키 생성 부분의 연산에서 제외되었고, 나머지 두 단방향 알고리즘과 비교했을 때 ECC의 경우 상호인증을 위한 개인키와, 공개키를 생성하는 ECC(화이트박스로 암호화 구간 포함)가 비교적 효율적인 것을 알 수 있다.

비대칭키(상호인증) 유형에서는 RSA 기반 암호 알고리즘은 암·복호화 성능은 효율적인 것으로 나타났지만, 키생성과 인증서 생성에서 연산의 오버헤드가 큰 것으로 나타났다. 때문에 M2M 환경에서 기존 RSA 기반 알고리즘을 활용하는 것은 비효율적인 것으로 분석된다.

기존 단방향 알고리즘이나 ECC같은 경량화된 상호인증 알고리즘이 적용되어야 한다는 것을 알 수 있다. 화이트박스의 경우 기존 AES와 구조적으로 알고리즘이 비슷한 연산을 수행하기 때문에 ECC와 함께 사용해도 전체 연산속도에 큰 영향을 끼치지 않는 것으로 분석되었다. 또한 제안 논문 프로토콜 상 연산 파라미터로 임의 키(R)를 재사용하기 때문에 키 생성 연산부분의 암·복호화 연산 속도가 크게 증가 하지 않았음을 확인 하였다.

5. 결론

본 논문은 현재 표준화 중인 M2M 표준 프로토콜에서 정의하는 통신 시나리오를 기반으로 보안 요구사항을 준수하는 암호 알고리즘 응용기법을 제안하였다. ECC의 경우 현재 다양한 무선 환경에서 적용되고 있는 경량화된 알고리즘으로써 암호키에 비해 암호 알고리즘의 강도가 매우 높고 신뢰성이 있는 것으로 알려져 있다.

본 논문은 M2M 통신 프로토콜의 연산 성능을 준수하기 위해 1차적으로 ECC를 사용하였고, 화이트박스 암호의 응용은 추가적인 연산의 오버헤드 없이 통신 세션의 보안강도를 높일 수 있는 방안으로 적용되었다. 또한 키 갱신이나 키 폐지에 따른 추가적인 키 교환 과정(보안 세션의 재설립)에서 암호문 유출에 대한 확률을 크게 감소시킬 수 있는 화이트박스 암호의 특징(키 자체가 테이블에 섞여 있음)을 활용하였다.

성능분석 결과 기존 단방향 또는 상호인증을 제공하는 프로토콜 중 M2M 환경에 적절한 수준의 성능을 보여주는 알고리즘은 단방향 알고리즘 수준에서 적용되어야 한다.(M2M 표준 암호알고리즘 진행사항 : 단방향을 이용한 상호인증(기존 EAP 방식 개선), 성능 효율성을 위한 부분 암호화를 고려중)

M2M 환경의 가장 큰 보안 취약성 중 하나는 공격자가 정상적인 디바이스를 가장하는 것이다. 이는 각 노드가 신뢰성 있는 상호인증을 수행해야 하는 보안기능이 필수이다. 본 논문에서는 M2M 환경에 적절한 상호인증 수행과 통신 세션 보안 강화를 위해서 암호 알고리즘을 응용하였고 성능분석 결과 성능의 효율성이 적절한 수준인 것을 확인 하였다.

REFERENCES

[1] KISA(Korea Internet Security Agency), “Internet Security Issue”, 2012.

[2] Cisco, “Cisco Visual Networking Index: Forecast and Methodology, 2013 - 2018”, Cisco, 2014.

[3] KIET(Korea’s Industrial Economy & Trade), “Activating the Internet of Things (IoT)”, 2014.

[4] TTA(Telecommunications Technology Association), “Machine-to-Machine(M2M) Security protocol for communication Standardization”, 2013.

[5] ITU(International Telecommunication Union), “ITU Kaleidoscope Academic Conference”, 2013.

[6] TTA(Telecommunications Technology Association), “ITU-T SG17 International conference”, 2014.

[7] ITU-T SG17, “TD 0721, Koji Nakao, Report of Working Party 1/17, Fundamental security Geneva”, p.15-24, 2014.

[8] ITU-T SG17, “TD 0722, Sacid Sarikaya, Report of Working Party 2/17, Network and information security, Geneva”, p.15-24, 2014.

[9] ETSI, “ETSI TS 102 689 V2.1.1”, ETSI, 2013.

[10] ETSI, “ETSI TS 102 690 V2.2.0”, ETSI, 2014.

[11] Barbara Pareglio, Ericsson, “Overview of ETSI M2M Architecture”, ETSI, 2011.

[12] FI-WARE, “ETSI M2M Architecture Overview”, http://forge.fiware.org/plugins/mediawiki/wiki/fiwa

re/index.php/ETSI_M2M_Architecture_Overview, FI-WARE, (2014).
[13] (TTA)Telecommunications Technology Association, "M2M Device Middleware Platform", 2012.
[14] Wen-Quan JIN, Do-Hyeun Kim, "Implementation and Experiment of CoAP Protocol Based on IoT for Verification of Interoperability", The Journal of The Institute of Internet, Broadcasting and Communication, 2014.
[15] Daniel R. L. Brown, "SEC 1: Elliptic Curve Cryptography", Certicom, 2009.
[16] Daniel R. L. Brown, "SEC 2: SEC 2: Recommended Elliptic Curve Domain Parameters", Certicom, 2010.
[17] Kristin, Lauter, "The advantages of elliptic curve cryptography for wireless security", IEEE Wireless communication, 2004.
[18] Seung-Cheol Go, Gilh-Yeon Nam, "Elliptic Curve Cryptography Implementation WIPO Patents" Korea Institude of Information Security & Cryptology, 2011.
[19] NOKIA Corporation, "Method, apparatus and computer program product for efficient elliptic curve cryptography", PCT, WO 2010/0034886, 2010.
[20] ATMEL Corporation, "Modular reduction using a special form of the modulus", PCT, WO 2009/091748, 2009.
[21] Thomson Licensing, "An Apparatus and a emthod for calculating a multiple of a point on Ecliptic Curve", PCT, WO 2009/095492, 2009.
[22] S Chow, et al, "A white-box DES implementation for DRM applications", In Digital Rights Management (pp. 1-15). Springer Berlin Heidelberg, 2003.
[23] Shin hyo-Kim, Yun kyung-Lee, Byung ho-Chung, "Analysis on Trends for White-Box Cryptography and Its Application Technology", ETRI, 2010.
[24] Chow, Stanley, et al, "White-box cryptography and an AES implementation", Selected Areas in Cryptography. Springer Berlin Heidelberg, 2003.
[25] Joye, Marc, "On white-box cryptography", Proceedings of the 1st International Conference Security of Information and Networks, 2008.
[26] Xiao, Yaying and Xuejia Lai, "A secure implementation of white-box AES" Computer Science and its Applications, 2009. CSA 09. 2nd International Conference on IEEE, 2009.

최 도 현(Choi, Do Hyeon)

- 2008년 2월 : 동서울대학 컴퓨터소프트웨어 공학사
- 2010년 8월 : 숭실대학교 컴퓨터학과 석사
- 2010년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 모바일보안, 가상화, PKI
- E-Mail : cdhgod0@ssu.ac.kr

박 중 오(Park, Jung Oh)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 현재 : 동양미래대학교 조교수
- 관심분야 : PKI, Network security, 암호학
- E-Mail : jopark13@dongyang.ac.kr