Asia-pacific Journal of Convergent Research Interchange
Vol.9, No.7, July 31 (2023), pp.41-55
http://dx.doi.org/10.47116/apjcri.2023.07.04

A Study on the Performance Measurement and Analysis of Cryptographic Algorithms for Gas AMI

가스 AMI를 위한 암호 알고리즘 성능 측정 및 분석 연구

Hyo-jin Song[1], Min-woo Kim[2], Jae-seong Park[3], Im-yeong Lee[4]

송효진[1], 김민우[2], 박재성[3], 이임영[4]

[1] Student, Department of Software Convergence, Soonchunhyang University, Republic of Korea, hjsong@sch.ac.kr

[2] Researcher, G-guru, Republic of Korea, minwoo@g-guru.co.kr

[3] CEO, G-guru, Republic of Korea, jspark@g-guru.ac.kr

[4] Professor, Department of Computer Software Engineering, Soonchunhyang University, Republic of Korea, imylee@sch.ac.kr

Corresponding author: Im-yeong Lee

Abstract: The advancement of private gas Advanced Metering Infrastructure (AMI) necessitates the establishment of robust security operation techniques and guidelines to address the existing gaps. In order to enhance market competitiveness, it is imperative to conduct thorough research on the security aspects of gas AMI. One crucial consideration is the fact that gas AMI operates on battery power, making the implementation of security measures a potentially risky endeavor from an operational standpoint. This paper aims to address these challenges by presenting comprehensive simulation results that explore a range of security techniques specifically tailored for gas AMI. These simulation results serve a dual purpose: not only do they provide valuable insights into the effectiveness of different security approaches, but they also lay the groundwork for a management and operation standard guideline for ensuring public energy security. By analyzing and evaluating the simulation outcomes, this study seeks to offer practical recommendations and best practices that can be adopted to safeguard the security of gas AMI systems. This, in turn, is expected to have a positive impact on market competitiveness. By bolstering the security of gas AMI, energy providers and stakeholders can instill confidence in consumers, thereby fostering a favorable business environment and strengthening their position in the market. In conclusion, this research endeavors to bridge the gap in security operation techniques and guidelines for private gas AMI. By addressing the unique challenges posed by battery-operated gas AMI devices and offering valuable insights through simulation-based analysis, this study aims to enhance market competitiveness and ensure the robustness of gas AMI systems in terms of security.

Keywords: Smart Metering, Advanced Metering Infrastructure(AMI), Cryptographic Algorithm, Security Protocol

요약: 현재 민간 도시가스 AMI(Advanced Metering Infrastructure)의 보안 운영 기술 및 보안

Received: March 16, 2023; 1st Review Result: April 29, 2023; 2nd Review Result: May 27, 2023
Accepted: June 30, 2023

운영 가이드에 대한 정립은 미비한 실정으로, 시장 경쟁력 제고를 위하여 가스 AMI 보안성에 대한 연구가 필요하다. 그러나 가스 AMI는 배터리로 동작하는 기기로 보안 적용 시 운영상의 리스크가 발생할 수 있다는 점이 고려되어야 한다. 본 논문에서는 가스 AMI에 적용 가능한 다양한 보안 기술에 대한 시뮬레이션 결과를 제공하고 이를 분석하여 공공재 에너지 보안에 대한 관리 및 운영 표준 가이드라인으로서 활용될 수 있도록 한다. 이러한 시뮬레이션 결과는 다양한 보안 접근 방식의 효과에 대한 통찰력을 제공할 뿐만 아니라 공공 에너지 보안을 보장하기 위한 관리 및 운영 표준 지침의 기초를 마련한다는 이중적인 목적을 제공한다. 시뮬레이션 결과를 분석하고 평가함으로써 가스 AMI 시스템의 보안을 보호하기 위해 채택할 수 있는 실질적인 권장사항을 제공하는 동시에 시장 경쟁력에 긍정적인 영향을 미칠 수 있으며 가스 AMI의 보안을 강화함으로써 에너지 공급자와 이해관계자는 소비자에게 신뢰를 심어줌으로써 유리한 사업 환경을 조성하고 시장에서의 입지를 강화할 수 있다. 따라서, 본 연구는 가스 AMI 시스템의 보안성을 보장하여 시장 경쟁력을 강화하는데 기여할 것으로 기대된다.

핵심어: 스마트 미터링, 지능형 계량 인프라, 암호 알고리즘, 보안 프로토콜

1. 서론

가스 계량 선진화를 위한 정부의 가스 AMI(Advanced Metering Infrastructure) 보급사업 추진 정책 하에, 물리적으로 분산된 가스미터(Gas Meter)의 계량 데이터를 수집, 관리 및 분석하는 지능형 계량 인프라가 보급되었다. 가스 AMI는 ICT(Information Communication Technology) 기술을 활용하여 무선검침, 정밀계량, 가스누출 실시간 감지 등의 서비스가 가능한 지능형 계량·검침 인프라이다. 가스 AMI를 이용하여 가스 수요 및 공급 정보를 실시간으로 모니터링하고 분석함으로써 가스 공급 업체가 수요를 예측하고 관리할 수 있도록 도우며, 이를 통해 시스템의 안정성을 높이고 에너지 효율성을 개선할 수 있다[1].

가스 AMI 시스템은 고객의 에너지 사용량 정보를 수집하고 처리하는 과정에서 민감한 정보를 다룬다. 따라서, AMI 시스템의 보안성 보장은 필수적으로 요구된다. 또한 스마트 가스미터는 검침 자료를 원격에서 취득하는 기능 외에 누출 알림, 누출 자동차단과 같은 화재/폭발 위험을 원격에서 감지하고 차단하는 기능을 기본 기능으로 운영된다. 이러한 기능들이 일반 통신망을 통해 운영되는 경우 침입자에 의해 가스 공공에너지 전체의 위험성이 증가할 가능성이 있다. 이에 실증 연구가 진행되고 있는 제품에도 보안성을 높이기 위한 장치들을 도입하고 있으나, 적용되고 있는 보안에 대한 강도는 일반 기업에서 운영되고 있는 수준으로 진행 중이다.“도시 가스사”에서 정의된 시장 경쟁력은 ‘보안성, 운영성, 경제성’이다. 그러나 현재 민간 도시가스 AMI의 보안 운영 기술 및 보안 운영 가이드에 대한 정립은 미비한 실정으로, 시장 경쟁력 제고를 위하여 보안성에 대한 연구가 필요하다. 본 연구에서는 사설 표준을 기반으로 가스 AMI의 보안성을 보증하여 안전성을 확보하고자 한다. 추가적으로 배터리로 운용되는 가스미터의 실 사용 환경을 고려하여 배터리 수명과 효율을 저해하지 않는 선에서 보안성과 효율성의 균형을 확보하는 것을 목표로 한다. 따라서 각 알고리즘의 특성 및 성능 분석을 통해 가스 AMI에서의 키 관리, 기기인증, 기밀성 및 무결성, 부인방지, 접근제어 등의 보안 이슈에 적절한 알고리즘을 선택하여야 한다[2].

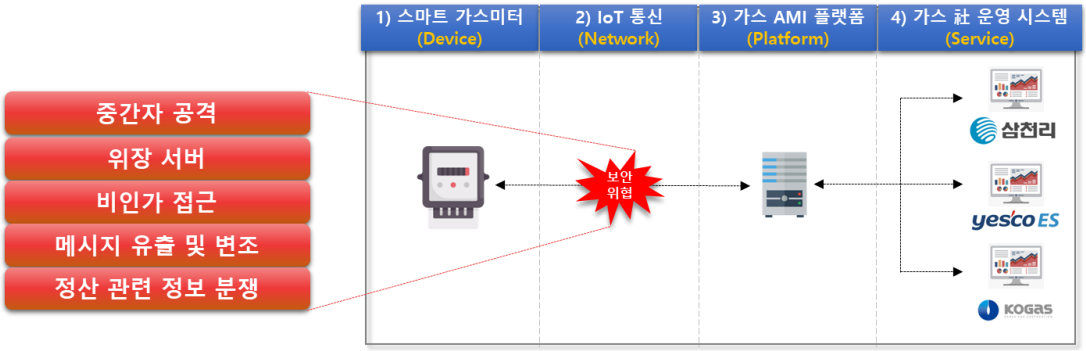
본 연구에서는 도시가스를 운영하는 주체(민간도시가스사) 중심 보안이 아닌

도시가스라는 공공재(국가에너지) 중심 보안으로 전자정부법 시행령 제69조와 [암호모듈시험 및 검증시험]에 의거, 국가.공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않는 중요정보의 보호를 위해 사용되는 암호모듈의 안정성과 구현 적합성을 검증하는 제도인 KCMVP(Korea Cryptographic Module Validation Program) 인증 보안 모듈을 적용하여 가스 AMI의 보안성을 확보한다. 또한 본 논문에서는 가스 AMI의 보안 이슈를 분석하고, 이를 해결하기 위한 보안 구성 요소별 기술 및 알고리즘에 대하여 분석한다. 그리고 각 보안 구성 요소에 대한 실행 시간을 측정하여 비교 및 분석한 결과를 제시한다. 이로써 가스 AMI의 시장 경쟁력을 강화하기 위한 보안성 향상 연구에 기여한다.

2. 배경 지식

2.1 가스 AMI 구성 및 보안 위협

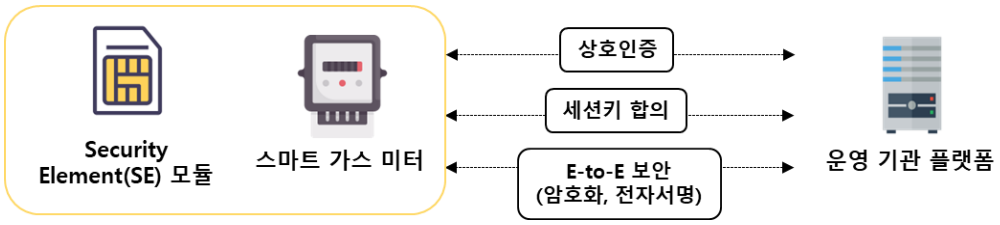
가스 AMI 전체 시스템은 [그림 1]과 같이 1) 스마트 가스미터, 2) IoT 통신, 3) 가스 AMI 플랫폼, 4) 가스사 운영시스템으로 구성된다. 본 논문에서의 연구 범위는 스마트 가스미터와 가스 AMI 플랫폼 간의 IoT 통신에 해당된다[1]. 해당 구간에서 발생할 수 있는 보안 위협과 취약점을 분석하고, 이를 방지하기 위한 해결 방안을 가스 AMI에 최적화된 형태로 제공하고자 한다. 에너지 공급자가 스마트 가스미터를 통해 사용량을 원격으로 검침하고, 가스 AMI 플랫폼을 통해 해당 정보를 수집하거나, 소비자에게 알려주는 서비스를 제공하는 과정에서의 통신을 가스 AMI 통신으로 정의한다. [그림 1]에서와 같이 가스 AMI 통신에서는 중간자 공격(Man In The Middle Attack), 위장 서버, 비인가 접근, 메시지 유출 및 변조, 정산 관련 정보에 대한 분쟁이 발생 가능하다[3].



[그림 1] 가스 AMI 구성 및 보안 위협
[Fig. 1] Gas AMI Configuration and Security Threats

중간자 공격은 공격자가 통신을 연결하는 두 대상 즉, 소비자와 공급자 사이에 자리잡고 대화를 엿듣거나 데이터 전송을 가로채는 공격 기법이다. 소비자와 공급자는 서로가 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달한다. 위장 서버 공격은 공격자가 가스사 서버를 위장하여 사용자가 위장 서버 측으로 계량정보를 보내하는 공격 기법이다. 비인가 접근은 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령어의 발행을 포함한다. 또한 메시지 유출 및 변조 공격을 통해 공격자는 고객의 인터넷 연결 장치에서 패킷 스니핑 공격 혹은 악성 코드 실행으로

PII(Personal Identifiable Information)를 가로챌 수 있으며, 유틸리티 시스템에서 고객에게 전달하는 실시간 가격을 위조하여 고객을 속일 수 있다. 스마트 가스미터 이용 고객은 사용량 혹은 과금 정보에 대하여 부인할 수 있기 때문에 정산 관련 정보에 대한 분쟁이 발생할 수 있다. 따라서 이러한 보안 위협을 방지하기 위해 가스 AMI 통신에서 보안성이 확보되어야 하며, 이는 표준에서 [그림 2]와 같은 흐름으로 구성된다[4][5].



[그림 2] 가스 AMI 통신
[Fig. 2] Gas AMI Communications

상호인증 단계에서는 클라이언트와 서버 즉, 스마트 가스미터와 가스사 서버가 상호인증을 수행한다. 가스 AMI 통신 과정에서 스마트 가스미터와 서버 간 상호인증 결여 시 중간자 공격, 인가되지 않은 접근 등이 발생할 수 있다. 따라서 상호인증과 함께 인증 후 발행되는 세션키의 주기적인 갱신이 요구된다. 또한 디바이스에 키 저장 시 안전한 방식으로 관리되어야 하며, 공유키 설정, 폐기, 갱신 과정의 안전성을 필요로 하고 KCMVP 인증 모듈을 이용할 것이 권고된다.

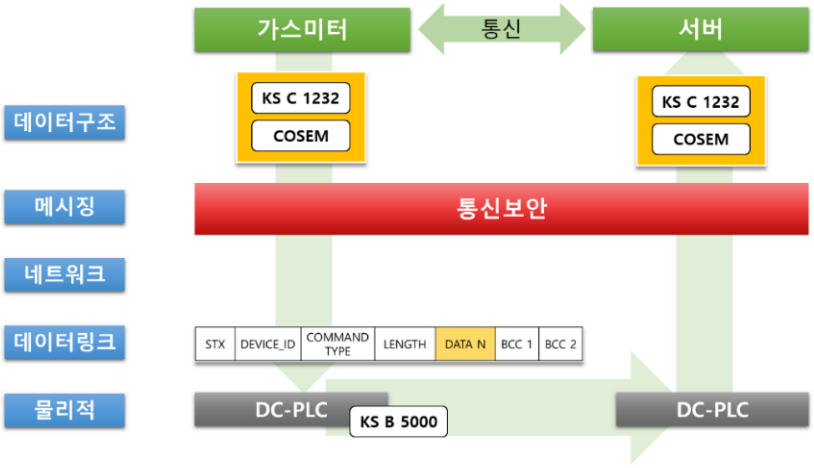
세션키 생성 단계에서는 스마트 가스미터와 서버 간 암호화 통신 시 이용할 대칭키를 확립한다. 이때 장기적인 키 사용에 대한 키 노출의 위험성을 고려하여 일정 주기마다 세션키의 변경이 고려되어야 한다. 또한, 디바이스에 세션키를 저장할 경우 안전한 방식으로 관리되어야 한다. 즉, 공유키 설정, 폐기, 갱신에 이르는 키 라이프 사이클에서의 안전성 제공이 필요하다.

암호 통신 단계에서는 스마트 가스미터가 서버 측으로 세션키를 이용하여 암호화한 계량정보를 송신한다. 계량정보를 송/수신 시 암호화와 메시지 인증이 결여되면 비인가된 모니터링으로 사용자의 개인정보에 대한 침해가 발생 가능하며, 메시지 유출 및 변조, 네트워크 계층에서의 데이터 변조 등의 보안 위협이 발생할 수 있다. 따라서 계량정보에 암호화 및 복호화를 적용하여 통신할 수 있어야 하며, 교환 메시지에 AEAD(Authenticated Encryption with Associated Data) 및 전자서명 적용하여 무결성을 제공하여야 한다. 또한 암호화, 전자서명 알고리즘 및 키 길이는 KISA 암호 이용 가이드라인을 참고하여 구성하는 것이 권고된다.

2.2 스마트 미터링 국제 표준 프로토콜

DLMS(Data Language Message Specification)는 전기, 수도, 가스 등 스마트 미터링 통신에 적용되고있는 에너지 관리 시스템 통신의 국제 표준 프로토콜로, COSEM(Companion Specifications for Energy Metering)이라는 계량장치 통신 인터페이스 모델을 통해 객체 기반 정보표현이 가능하도록 하여 제조사가 상이한 계기에서도 상호호환성을 제공한다. [그림 3]은 가스미터와 서버의 통신 및 APDU(Application Protocol Data Unit)를 시각화한 것이다. 이처럼 DLMS는 에너지 공급자와 에너지 소비자 간의 효율적인 데이터 교환을 위해

개발되어 현재 전세계적으로 활용되고 있다.



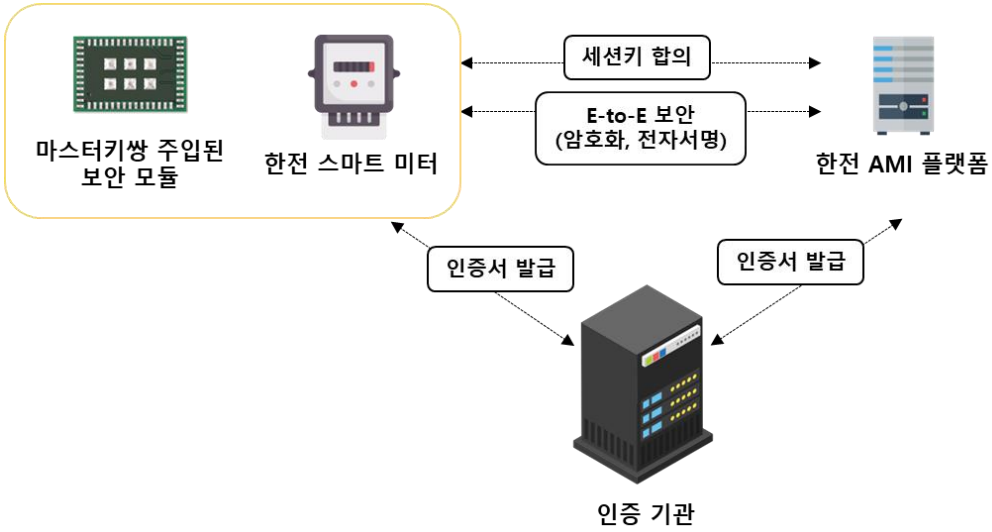
[그림 3] DLMS 프로토콜
[Fig. 3] DLMS Protocol

DLMS는 표준화된 메시지 형식과 프로토콜 스택을 제공하여 에너지 공급자와 소비자 간의 표준화된 데이터 교환을 가능하게 하며, 에너지 사용량, 미터 상태, 요금 정보, 타임스탬프 등 다양한 데이터를 교환할 수 있다. 또한, 다양한 에너지 종류에 대해 적용될 수 있으며, 전기, 가스, 수도, 열 등 다양한 에너지 형태의 미터와 통신할 수 있다. 데이터 통신에 있어서는 데이터 압축, 암호화, 인증, 오류 검출 및 복구 등의 기능을 포함하고 있어 신뢰성 있는 통신을 지원한다. 그리고 다양한 통신 매체를 지원하며, 유/무선 통신, 로컬 네트워크 등을 활용할 수 있다[6-9].

2.3 한국전력공사 AMI 보안 모델

한국전력공사(이하 한전)에서는 2010년 정부의 스마트 그리드 국가로드맵 수립에 따라 AMI 보급 사업을 시행 중에 있다. 2022년 기준으로 1086만호를 보급 완료하였으며, AMI를 통해 고객의 전기 사용량을 원격으로 측정하고 관리함으로써 전력 사용 정보를 효율적으로 수집, 처리 및 분석하고, 전기 요금 산정, 고객 서비스, 에너지 관리 등에 활용하고 있다[6]. 한전은 DLMS 표준 기반의 인증 시스템 구축을 통해 국내 스마트 미터링 시장 확장을 선도하며 스마트 그리드의 초창기 사업화 안착에 기여하였다.

한전에서는 PKI(Public Key Infrastructure) 기반의 인증서를 통해 인증되지 않은 기기가 전력망에 접속할 수 있는 가능성을 차단하고 있으며, 전력량계와 모뎀 간 데이터 교환 규격인 DLMS 원격 검침 프로토콜의 HLS(High Level Security)를 채택하여 고수준 보안을 제공하고 있다. 한전의 AMI 보안 요소 구성은 [표 1]과 같으며, 이를 적용한 한전의 보안 시나리오는 [그림 4]와 같다. 제조사에서 보안 모듈에 주입한 인증서와 마스터키쌍을 이용하여 세션키를 유도하여 암호화 통신에 사용한다. 암호화 통신 시 사용하는 대칭키 알고리즘으로는 KCMVP 검증 대상 알고리즘인 ARIA(Academy, Research Institute, Agency)의 GCM(Galois/Counter Mode) 운용 모드를 128 비트의 키 길이와 함께 사용한다. 또한 ECDSA(Elliptic Curve Digital Signature Algorithm)를 통해 무결성 및 부인방지를 제공한다.



[그림 4] 한전 보안 시나리오
[Fig. 4] Korea Electric Power Corporation Security Scenario

[표 1] 한전 보안 요소 구성
[Table 1] Korea Electric Power Corporation Security Suite

이름	ECDH-ECDSA-ARIA-GCM-128-SHA-256
보안 알고리즘	ARIA-GCM-128
전자서명	ECDSA with P256
키 합의	ECDH with P256
해시 알고리즘	SHA-256

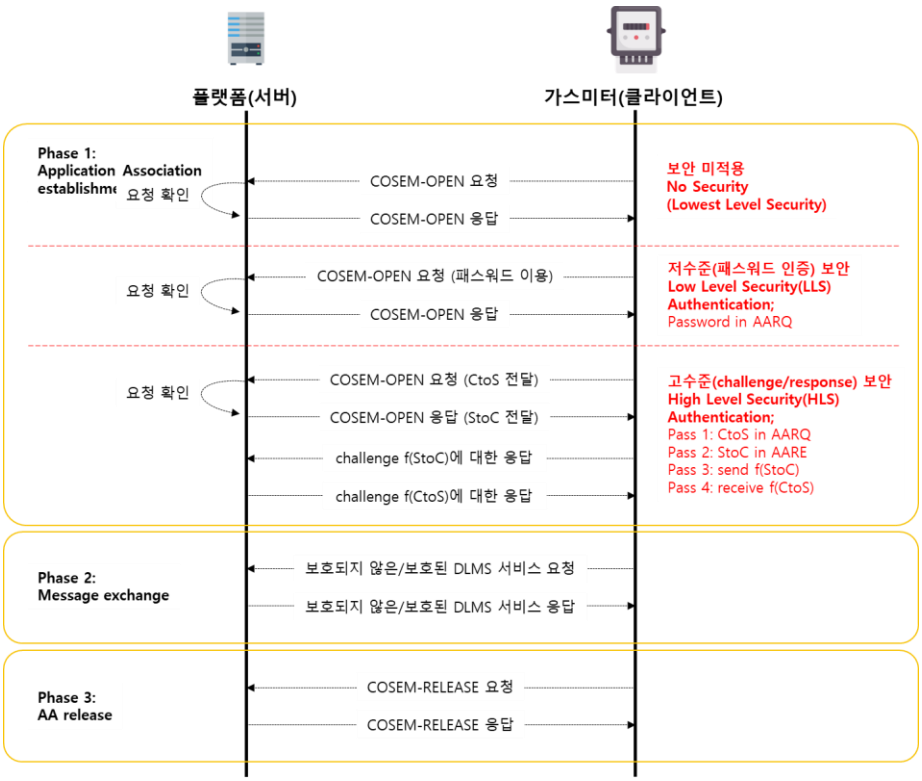
3. 가스 AMI 보안

3.1 가스 AMI 보안 아키텍처

본 절에서는 2.1에 언급된 보안 위협을 방지하기 위한 가스 AMI 보안 아키텍처에 대하여 설명한다. 2.2에서 언급된 스마트 미터링 국제 표준 프로토콜 DLMS에 따라 가스 AMI 보안 아키텍처는 상호인증, 세션키 생성, 암호화 통신으로 구성 가능하며, 각 단계에서 표준에 정의된 알고리즘들을 채택하여 세부 프로토콜을 구성할 수 있다. 이때 가스미터와 가스 AMI 플랫폼은 각각 클라이언트와 서버로 정의한다.

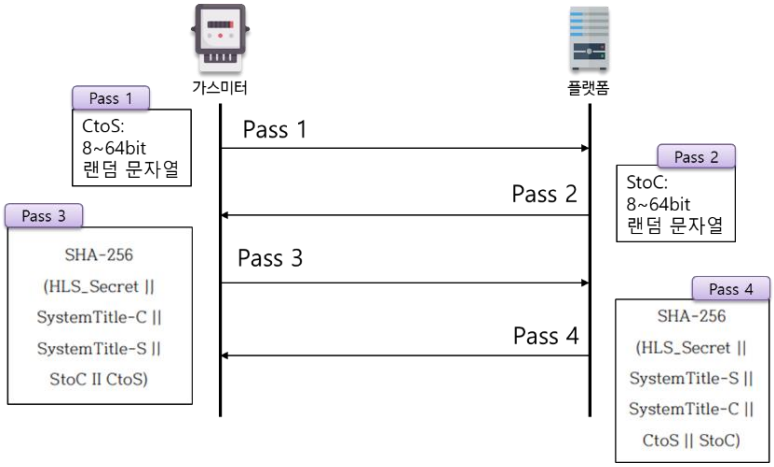
3.1.1 상호인증

클라이언트와 서버가 세션키 발급을 통한 암호 통신 전 Application Association Establishment 과정을 통해 상호인증을 수행한다. 상호인증 시 적용할 수 있는 알고리즘은 DLMS Greenbook에 [그림 5]와 같이 보안을 적용하지 않는 경우, 저수준 보안을 제공하는 경우, 고수준 보안을 제공하는 경우로 나누어져 정의되어 있다.



[그림 5] 상호인증 수행 단계

[Fig. 5] Steps to Perform Mutual Authentication



[그림 6] HLS 상호인증 프로토콜(SHA-256 이용 시)

[Fig. 6] HLS Mutual Authentication Protocol(when using SHA-256)

보안이 없는(최저 수준 보안) 인증의 목적은 클라이언트가 서버에서 일부 기본 정보를 검색할 수 있도록 하는 것이며, 이 인증 메커니즘에는 인증이 필요하지 않다. 저수준 보안 즉 LLS를 위한 인증 메커니즘은 비밀번호(Password)를 기반으로 한다. 서버는 클라이언트에게 서버가 알고 있는 암호를 제공하도록 요청하여 자신을 인증하도록 요구한다. 고수준 보안 즉 HLS를 위한 인증 메커니즘은 [그림 6]과 같이 Pass 1에서 Pass 4에 해당하는 4개 단계로 분류되는 Challenge/Response 모델을 기반으로 한다. Pass 1에서는 클라이언트는 인증 메커니즘에 따라 난수에 서명하여 서버로 보낸다. Pass 2에서는 서버가

난수 인증 메커니즘에 따라 난수에 서명하여 클라이언트 측으로 보낸다. 이후 Pass 3과 Pass 4에서 클라이언트와 서버가 상호 간 인증을 수행한다. 이때 Pass 3과 Pass 4에서 MD5, SHA1, GMAC, SHA2, ECDSA를 사용하도록 명시하고 있다.

3.1.2 세션키 생성

세션키 생성은 임시 통합 모델, 원패스 디피-헬만, 정적 통합 모델의 세 가지로 구분된다.

첫 번째는 Ephemeral Unified Model C(2e, 0s, ECC CDH)로, 임시 통합 모델이다. 해당 모델에서는 클라이언트, 서버 모두 임시 키쌍을 가진다. 2e는 임시(Ephemeral) 키쌍의 개수를 말한다.

임시 통합 모델의 수행 단계는 다음과 같다.

Step 1. 클라이언트는 임시 키쌍을 생성하고, 서버에게 자신의 공개키와 전자서명을 전달한다.

Step 2. 서버는 클라이언트의 전자서명을 검증하고, 임시 키쌍을 생성한다.

Step 3. 서버는 자신의 개인키와 클라이언트의 공개키로 공유 비밀값을 생성한다.

Step 4. 서버는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다. 이후 클라이언트에게 자신의 공개키와 전자서명을 전달한다.

Step 5. 클라이언트는 자신의 개인키와 서버의 공개키로 공유 비밀값을 생성한다.

Step 6. 클라이언트는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다.

이로써 클라이언트와 서버는 동일한 세션키를 합의하게 되며, 이를 이용하여 데이터를 대칭키로 암호화하여 통신 가능하다.

두 번째는 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH)로, 원패스 디피-헬만 모델이다. 해당 모델에서는 임시키쌍 1개, 정적키쌍 1개로, 클라이언트는 임시 키쌍, 서버는 정적 키쌍을 가진다. 1e는 임시 키쌍의 개수, 1s는 정적(Static) 키쌍의 개수를 말한다.

원패스 디피-헬만 모델의 수행 단계는 다음과 같다.

Step 1. 클라이언트는 임시 키쌍을 생성한다.

Step 2. 클라이언트는 자신의 개인키와 서버의 공개키로 공유 비밀값을 생성한다.

Step 3. 클라이언트는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다. 그리고 이 세션키로 암호화한 암호문을 서버에 전달한다.

Step 4. 서버는 자신의 개인키와 클라이언트의 공개키로 공유 비밀값을 생성한다.

Step 5. 서버는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다. 그리고 이 세션키를 이용하여 클라이언트로부터 받은 암호문을 복호화한다.

이로써 클라이언트와 서버는 동일한 세션키를 합의하게 되며, 이를 이용하여 데이터를 대칭키로 암호화하여 통신 가능하다.

세 번째는 Static Unified Model C(0e, 2s, ECC CDH)로, 정적 통합 모델이다. 해당 모델에서는 클라이언트, 서버 모두 정적 키쌍을 가진다. 2s는 정적 키쌍의 개수를 말한다.

정적 통합 모델의 수행 단계는 다음과 같다.

Step 1. 클라이언트는 정적 키쌍과 논스를 이용하여 세션키를 생성한다.

Step 2. 클라이언트는 자신의 개인키와 서버의 공개키로 공유 비밀값을 생성한다.

Step 3. 클라이언트는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다. 그리고

이 세션키로 암호화한 암호문을 서버에 전달한다.

Step 4. 서버는 자신의 개인키와 클라이언트의 공개키로 공유 비밀값을 생성한다.

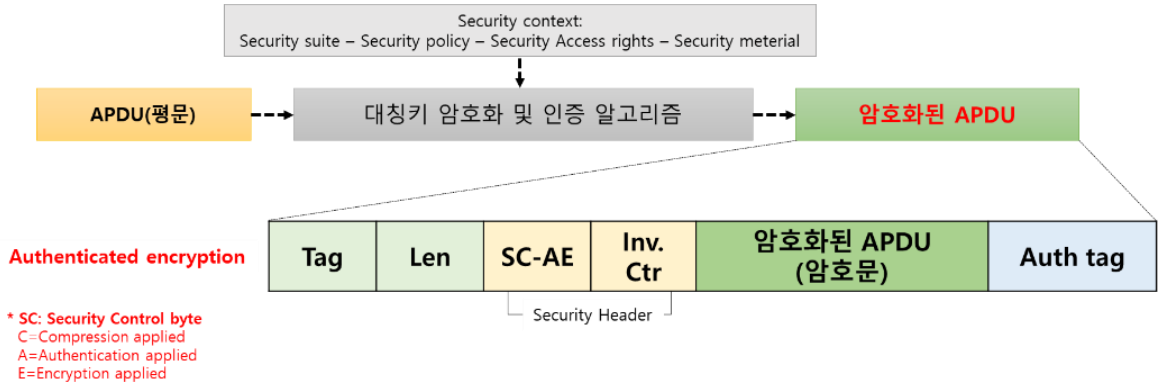
Step 5. 서버는 공유 비밀값과 키 생성 요소를 통해 세션키를 생성한다. 그리고 이 세션키를 이용하여 클라이언트로부터 받은 암호문을 복호화한다.

본 모델에서는 세션키 생성 시 세션키의 신선도를 위해 논스가 추가된다. 논스처럼 변화하는 값 없이, 고정된 정적 키쌍만을 이용하면 매번 동일한 값의 세션키만 만들어지기 때문에 이를 방지하기 위함이다. 이로써 클라이언트와 서버는 동일한 세션키를 합의하게 되며, 이를 이용하여 데이터를 대칭키로 암호화하여 통신 가능하다.

3.1.3 암호화 통신

클라이언트와 서버가 세션키 합의 과정을 통해 ECDH 모델로 대칭키를 생성한 이후 데이터를 암호화하여 통신하는 과정을 수행한다. 암호화 통신 시 데이터 스트럭처는 [그림 7]과 같은 형태이다. 스마트 가스미터의 계량정보를 서버에 저장하는 것을 LP(Load Profile)이라고 하며, 이는 시간 당 28 바이트로 기록된다.

DLMS Greenbook의 메시지 암호화 유형을 Authentication Only, Encryption Only, Authenticated Encryption의 세 가지로 구분한다. 이들 중, 서버와 클라이언트 간에만 적용할 수 있고, 패킷오버헤드가 상대적으로 적은 방식인 Service-Specific Global/dedicated Ciphering(SSGC)을 사용한다. 이 방식에서 평문에 더해지는 오버헤드는 인증(Authentification)을 적용 시 23 바이트이다. DLMS 보안 표준에서는 인증을 통한 무결성 제공을 위하여 AEAD 혹은 전자서명을 이용할 것을 권고한다. 평문 APDU가 암호화되어 Authenticated Encryption 형태로 저장되는 경우 시큐리티 헤더와 함께 인증 태그인 Auth tag가 추가된다.



[그림 7] 암호화 통신 데이터 스트럭처

[Fig. 7] Encryption Communication Data String

4. 가스 AMI 보안 알고리즘 성능 평가

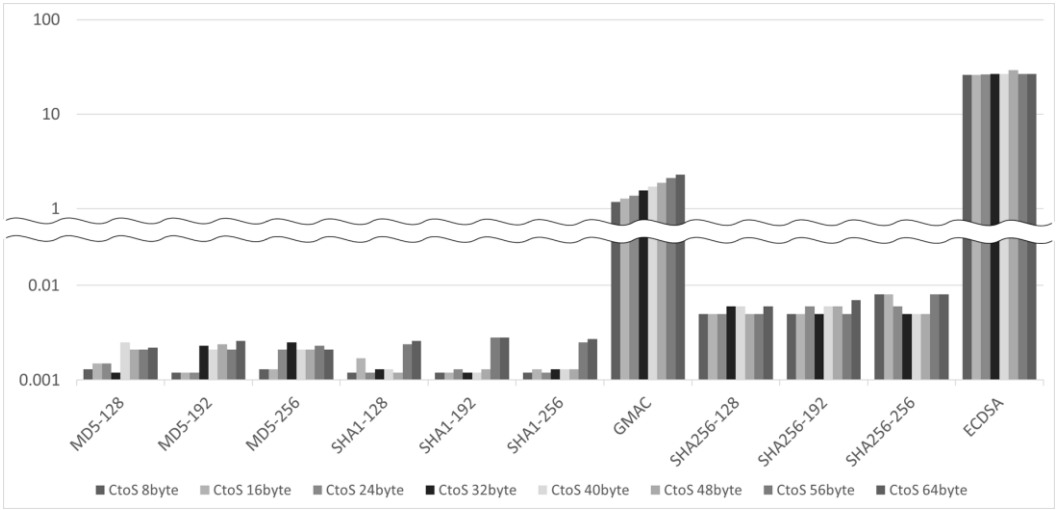
i5-4460, RAM 16GB의 H/W 환경에서 시뮬레이션을 진행하였다. C언어를 통해 Visual Studio 2022에서 프로그램을 구현하였으며, main 함수 내 for문 루프를 통해 100회 실행 결과 소요시간(ms) 측정 평균값을 연산하였다.

상호인증 단계에서의 각 알고리즘별 성능 측정 결과는 부록의 [표 2]와 같다. DLMS Greenbook의 HLS에 정의된 알고리즘인 MD5, SHA1, GMAC, SHA2, ECDSA에 대한 성능

측정을 진행하였다. 세션키 생성 단계에서의 각 알고리즘별 성능 측정 결과는 부록의 [표 3, 4]와 같다. DLMS Greenbook에 정의된 세 가지 ECDH 모델인 임시 통합 모델, 원패스 디피-헬만 모델, 정적 통합 모델에 대하여 세션키 생성 성능 측정을 진행하였다. 이때 임시 통합 모델의 경우, 인증서를 주입하고 불러오는 사전 단계를 생략하였다. 암호화 통신 단계에서의 ARIA-GCM 및 AES-GCM 알고리즘 성능 측정 결과는 부록의 [표 5]와 같다. DLMS Greenbook에 정의된 세 가지 암호화 유형인 Authentication Only, Encryption Only, Authenticated Encryption에 대한 암호화 성능 측정을 진행하였다.

상호인증 단계에서의 시간 측정 결과를 그래프로 나타내면 [그림 8]와 같다. MD5, SHA-1, SHA-256, ECDSA는 입력 크기에 큰 영향을 받지 않는다. 또한 해시 알고리즘인 MD5 및 SHA 계열 알고리즘의 경우 일반적으로 빠른 계산 속도를 가지기 때문에 함께 비교된 알고리즘인 GMAC과 ECDSA에 비해 현저히 낮은 소요시간을 보인다. GMAC의 경우 입력 데이터의 길이에 따라 실행 시간이 선형적으로 증가하는 것을 확인할 수 있다. GMAC은 대칭키 암호화를 기반으로 한다. 출력값의 길이를 96~128 비트 범위 중 8의 배수로 설정해야 하며, 짧은 출력 길이로 인해 경량성을 가진다. 그러나 대칭키 암호화의 특성 상 키 배송에 대한 문제를 가진다. ECDSA의 경우 동일 크기 입력 데이터에 대한 알고리즘 실행 소요시간에 대하여 다른 알고리즘보다 높은 실행 시간을 요구하는 것으로 확인된다. ECDSA는 동일한 보안 강도를 제공하는 경우 대칭키 알고리즘에서보다 긴 키 길이와 더 많은 연산량을 요구한다. 또한 키 길이의 2배에 달하는 output 길이를 가진다. 이러한 이유 때문에 배터리 오퍼레이팅 기기인 스마트 가스미터에서의 적용에 대한 적합성이 떨어질 수 있다. 따라서 가스 AMI 하드웨어 적용 시험 후, 운영성에서의 리스크가 존재할 경우 GMAC의 사용에 대한 고려가 가능하다.

세션키 생성 단계 중 임시 통합 모델에서의 세션키 생성이 가장 오래 걸리며, 정적 통합 모델에서의 세션키 생성이 가장 빠르게 진행됨을 확인할 수 있다. 또한 각 모델의 성능 차이가 5ms 정도임을 확인 가능하다. 암호화 통신 단계에서의 시간 측정 결과를 입력 데이터의 크기에 따라 암호화에 걸리는 시간이 큰 증가폭을 보이지 않음을 확인 가능하며, ARIA가 AES에 비해 동일 크기 데이터에 대한 빠른 처리 속도를 보임을 알 수 있다.



[그림 8] HLS 상호인증 알고리즘 성능 비교
[Fig. 8] HLS Mutual Authentication Algorithm Performance Comparison

5. 결론

본 연구에서는 가스 AMI 보안성 강화를 위해 가스 AMI의 보안 위협을 파악하고 이에 대한 보안 구성 요소들을 분석하여 PC 환경에서 각 알고리즘별 시뮬레이션을 수행하였다. 그 결과로 보안 표준 모델인 상호인증, 세션키 생성, 암호화 통신에 정의된 알고리즘들의 소요시간 데이터를 확보하였다. 상호인증 단계에서는 ECDSA의 높은 실행 시간으로 운영성에 문제가 예상될 경우 GMAC의 사용을 고려할 수 있다. 세션키 생성 단계에서는 세 개의 모델이 근소한 성능 차이를 보이며, 암호화 통신 단계에서는 AES의 경우 Encryption Only의 소요시간이 ARIA 보다 길게 나타난다. 따라서 한전과 같이 가스 AMI에도 KCMVP 인증 알고리즘인 ARIA의 적용을 고려할 수 있다.

본 연구 결과는 가스 AMI 사업의 경쟁 요소로 활용 가능하며, 민간 관리 공공재 에너지 보안에 대한 관리 및 운영 표준 직접 적용 및 활용될 수 있다. 이로써 가스 AMI 보안성 강화를 통한 시장 경쟁력을 확보할 수 있도록 한다. 최종적으로 민간 공공재 에너지 보안에 대한 국가기관 수준의 보안성을 확보할 수 있는 계기를 통해 민간 부분 보안에 있어서 사회적인 해법을 제시한다. 이로써 안전한 가스 스마트 미터링 환경을 조성하는 데 기여할 수 있다. 후속 연구로는 본 연구 결과를 PC 환경이 아닌 스마트 가스미터 하드웨어에 적용하여 보안 모듈 적용 시의 리스크에 대한 조사가 수행되어야 한다. 스마트 가스미터는 배터리 오퍼레이팅 기기로서 배터리 전력 소모가 발생하기 때문에 후속 연구에서는 실증 데이터를 기반으로 한 보안 모듈 적용 최적화의 필요성이 요구된다.

6. 감사의 글

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구이며(No. 2022R1A2B5B01002490), 중소벤처기업부 중소기업기술정보진흥원의 2021년 창업성장기술개발사업(전략형)의 주식회사 지구루 주관 "(S3149214)시장 경쟁력 강화 하드웨어 보안칩 적용 스마트 가스계량기 (가스 AMI) 개발" 과제 (개발기간 '21.11.01~'23. 10.31) 및 2023년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음 (2021-0-01399).

References

[1] S. Lee, S. Lee, M. Song, Y. Kwon, An Empirical Research on the IoT Basis Gas AMI Platform and Smart Metering Services, Journal of the Korean Institute of Gas, (2020), Vol.24, No.3, pp.1-10.
DOI: https://doi.org/10.7842/KIGAS.2020.24.3.1

[2] G. Lee, Security Guidelines for Smart Metering Services in Smart Grids(TTAE.IT-X.1332), TTA, (2020)
Available form: https://committee.tta.or.kr/data/standard_view.jsp?nowPage=2&pk_num=TTAE.IT-X.1332& commit_code=PG504

[3] S. Kim, Smart Energy Cybersecurity Guide, KISA, (2019)
Available form: https://www.kisa.or.kr/2060205/form?postSeq=8&lang_type=KO&page=

[4] DLMS User Association, DLMS/COSEM architecture and protocols, Green Book Ed. 9, (2019)

[5] N. Lurin, D. Szameitat, S. Hoffmann, G. Bumiller, Analysis of security features in DLMS/COSEM: vulnerabilities and countermeasures, In 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference

(ISGT), IEEE, (2018)
DOI: https://doi.org/10.1109/ISGT.2018.8403340

[6] I. Choi, B. Park, H. Choi, N. Myung, S. Lee, Case Study on Auto Meter Reading Protocol Certificate System for Smart Grid and Standardization, The Journal of Korean Institute of Communications and Information Sciences, (2012), Vol.37, No.1, pp.75-85.
DOI: https://doi.org/10.7840/kics.2012.37b.1.75

[7] C. A. Wülfing, F. G. Reck, F. G. Carloto, C. H. Barriquello, P. R. Marin, E. Nascimento, Evaluation of DLMS/COSEM Data Processing Setups Applied to Smart Metering, In 2022 14th Seminar on Power Electronics and Control (SEPOC), IEEE, (2022)
DOI: https://doi.org/10.1109/SEPOC54972.2022.9976442

[8] S. Biswas, S. Ghosh, P. Das, K. Saha, S. De, Efficient Data Transfer Mechanism for DLMS/COSEM Enabled Smart Energy Metering Platform, ACM SIGMETRICS Performance Evaluation Review, (2023), Vol.50, No.4, pp.14-16.
DOI: https://doi.org/10.1145/3595244.3595250

[9] T. Lieskovan, J. Hajny, Security of Smart Grid Networks in the Cyber Ranges, In Proceedings of the 17th International Conference on Availability, Reliability and Security, pp.1-8, (2023)
DOI: https://doi.org/10.1145/3538969.3543801

부록

[표 2] 상호인증 소요시간 측정 결과
[Table 2] The Results of Inter Authentication Time Measurement

구분	소요시간(ms)										
	MD5			SHA-1			GMAC	SHA-2			ECDSA
	128	192	256	128	192	256		128	192	256	
StoC 8byte	0.0012	0.0012	0.0013	0.0012	0.0012	0.0012	1.2000	0.0050	0.0050	0.0050	25.9900
CtoS 8byte	0.0013	0.0012	0.0013	0.0012	0.0012	0.0012	1.1800	0.0050	0.0050	0.0080	26.1200
StoC 16byte	0.0015	0.0012	0.0016	0.0013	0.0012	0.0013	1.4600	0.0060	0.0050	0.0050	25.9100
CtoS 16byte	0.0015	0.0012	0.0013	0.0017	0.0012	0.0013	1.2800	0.0050	0.0050	0.0080	26.2300
StoC 24byte	0.0015	0.0012	0.0021	0.0012	0.0013	0.0013	1.3900	0.0060	0.0050	0.0060	26.2300
CtoS 24byte	0.0015	0.0012	0.0021	0.0012	0.0013	0.0012	1.3700	0.0050	0.0060	0.0060	26.0800
StoC 32byte	0.0012	0.0027	0.0021	0.0012	0.0013	0.0013	1.5000	0.0050	0.0050	0.0050	26.4900
CtoS 32byte	0.0012	0.0023	0.0025	0.0013	0.0012	0.0013	1.5500	0.0060	0.0050	0.0050	26.1300
StoC 40byte	0.0023	0.0021	0.0021	0.0012	0.0013	0.0013	1.7200	0.0050	0.0050	0.0050	26.4700
CtoS 40byte	0.0025	0.0021	0.0021	0.0013	0.0012	0.0013	1.7200	0.0060	0.0060	0.0050	28.6000
StoC 48byte	0.0026	0.0024	0.0021	0.0013	0.0014	0.0014	1.8500	0.0050	0.0050	0.0050	29.1700
CtoS 48byte	0.0021	0.0024	0.0021	0.0012	0.0013	0.0013	1.8700	0.0050	0.0060	0.0050	26.1700
StoC 56byte	0.0021	0.0021	0.0026	0.0025	0.0026	0.0026	2.0800	0.0050	0.0050	0.0070	26.6700
CtoS 56byte	0.0021	0.0021	0.0023	0.0024	0.0028	0.0025	2.1000	0.0050	0.0050	0.0080	26.0300
StoC 64byte	0.0022	0.0023	0.0021	0.0028	0.0033	0.0027	2.4200	0.0050	0.0080	0.0090	26.5200
CtoS 64byte	0.0022	0.0026	0.0021	0.0026	0.0028	0.0027	2.2900	0.0060	0.00700	0.0080	26.5200

[표 2]에 대한 그래프는 [그림 8]의 형태로 본문에 제시되었음.

[표 3] 세션키 생성 중 임시 통합 모델 소요시간 측정 결과
[Table 3] Time Measurement Results of The Temporary Integrated Model During Session Key Generation

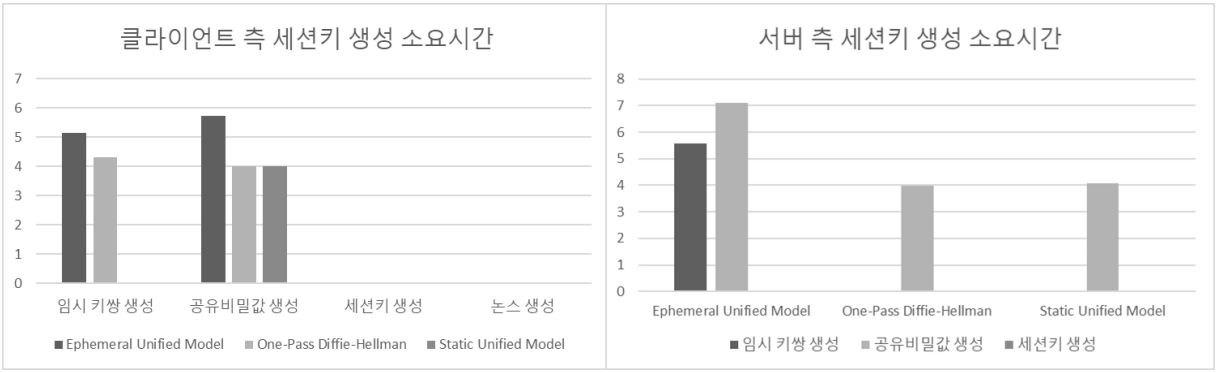
구분	소요시간(ms)									
	Party U(클라이언트)					Party V(서버)				
	인증서 공개키 검색	임시 키쌍 생성	서명검증	공유 비밀값 생성	세션키 생성	인증서 공개키 검색	서명검증	임시 키쌍 생성	공유 비밀값 생성	세션키 생성
Ephemeral Unified Model	-	5.15	-	5.73	0.01	-	-	5.58	7.11	0.01

[표 4] 세션키 생성 중 원패스 디피-헬만 모델 및 정적 통합 모델 소요시간 측정 결과
[Table 4] Measurement Results of Time Required for One-Pass DP-Hellman Model and Static Integration Model During Session Key Generation

구분	소요시간(ms)						
	Party U(클라이언트)				Party V(서버)		
	Nonce 생성	임시 키쌍 생성	공유 비밀값 생성	세션키 생성	임시 키쌍 생성	공유 비밀값 생성	세션키 생성
One-Pass Diffie-Hellman		4.31	4.01	0.01		3.98	0.02
Static Unified Model	0.001		3.99	0.02		4.08	0.02

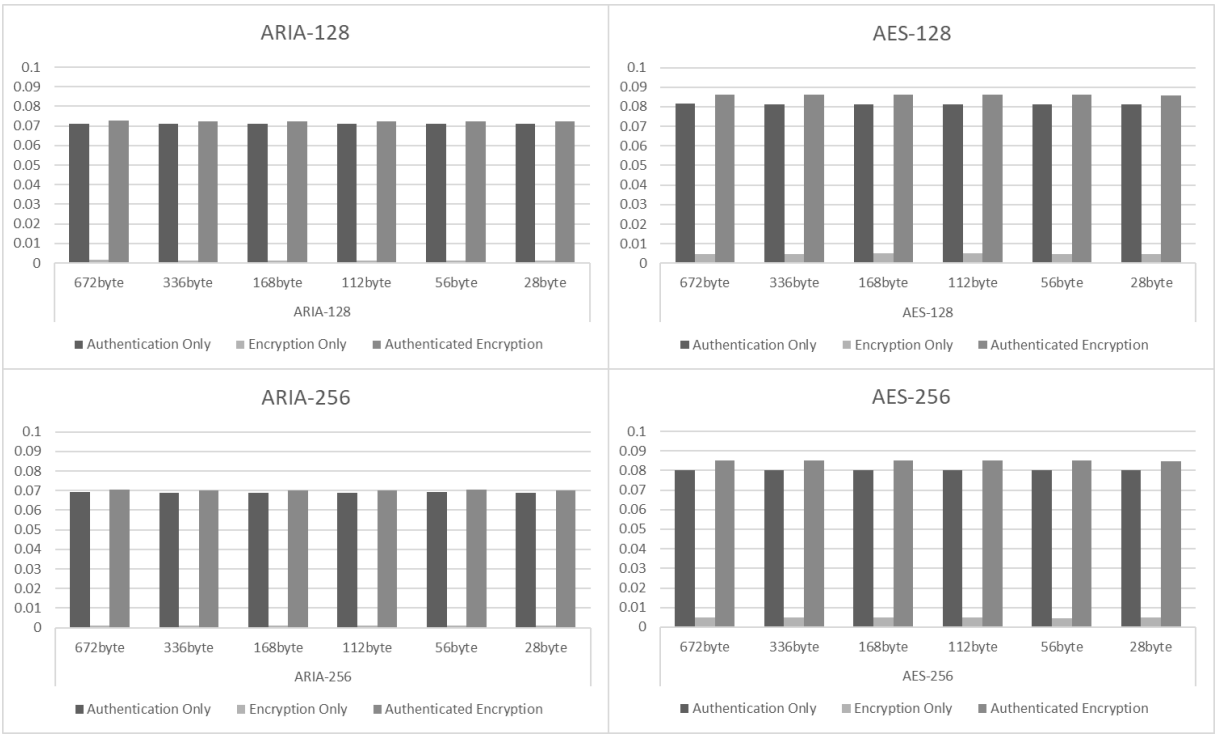
[표 5] 암호화 소요시간 측정 결과
[Table 5] Measurement Results of Encryption Time

구분	암호 알고리즘	전자서명 없이 진행			전자서명	전자서명 후 진행		
		소요시간 (ms)						
		Authenti-cation Only	Encryption Only	Authenti-cated Encryption	Digital Signature Only	Authenti-cation Only	Encryption Only	Authenti-cated Encryption
LP 1일 1회 전송 (672byte)	ARIA 128	0.07108	0.00154	0.07262	26.15740	0.07312	0.00141	0.07453
	AES 128	0.08147	0.00489	0.08636	26.47100	0.08350	0.00476	0.08826
	ARIA 256	0.06936	0.00124	0.07060	25.93778	0.07244	0.00124	0.07368
	AES 256	0.08014	0.00489	0.08503	25.99778	0.08305	0.00476	0.08781
LP 1일 2회 전송 (336byte)	ARIA 128	0.07104	0.00137	0.07241	26.11720	0.07034	0.00141	0.07175
	AES 128	0.08133	0.00491	0.08624	26.29680	0.08062	0.00496	0.08558
	ARIA 256	0.06906	0.00117	0.07022	25.96444	0.06925	0.00116	0.07041
	AES 256	0.08020	0.00486	0.08506	25.95300	0.08068	0.00485	0.08553
LP 1일 4회 전송 (168byte)	ARIA 128	0.07099	0.00140	0.07239	26.14660	0.07029	0.00144	0.07173
	AES 128	0.08106	0.00505	0.08611	26.34600	0.08053	0.00468	0.08521
	ARIA 256	0.06902	0.00119	0.07021	25.87000	0.06913	0.00117	0.07030
	AES 256	0.08021	0.00488	0.08509	25.91330	0.08037	0.00484	0.08521
LP 1일 6회 전송 (112byte)	ARIA 128	0.07097	0.00142	0.07239	26.14380	0.07026	0.00147	0.07171
	AES 128	0.08104	0.00506	0.08610	26.26800	0.08061	0.00460	0.08521
	ARIA 256	0.06901	0.00119	0.07020	26.00667	0.06902	0.00116	0.07018
	AES 256	0.08022	0.00480	0.08502	25.96600	0.08051	0.00468	0.08519
LP 1일 12회 전송 (56byte)	ARIA 128	0.07099	0.00136	0.07235	26.27380	0.07022	0.00137	0.07168
	AES 128	0.08120	0.00482	0.08602	26.36040	0.08042	0.00469	0.08511
	ARIA 256	0.06931	0.00121	0.07052	25.97222	0.06893	0.00119	0.07012
	AES 256	0.08020	0.00470	0.08490	26.03100	0.08012	0.00494	0.08506
LP 1일 24회 전송 (28byte)	ARIA 128	0.07094	0.00138	0.07232	26.28960	0.07077	0.00151	0.07228
	AES 128	0.08106	0.00487	0.08593	26.30020	0.08031	0.00460	0.08491
	ARIA 256	0.06894	0.00122	0.07017	25.83222	0.06888	0.00115	0.07003
	AES 256	0.07996	0.00476	0.08472	25.97000	0.07999	0.00505	0.08504



[그림 9] 세션키 생성 알고리즘 성능 비교

[Fig. 9] Session Key Generation Algorithm Performance Comparison Performance



[그림 10] 암호 통신 알고리즘 성능 비교

[Fig. 10] Crypto Communication Algorithm Performance Comparison