정 보 보 호 학 회 지
제24권 제5호, 2014. 10

산업제어시스템의 보안 적용을 위한 구간 암호화 모듈의 가용성 성능 분석

이 재 훈*, 최 현 덕**, 이 옥 연***

요 약

산업제어시스템(Industrial Control System, ICS)은 전력, 가스, 수도, 교통 등과 같은 국가기반시설 및 산업분야에서 원거리에 산재된 시스템을 효율적으로 관리하기 위한 시스템이다. 초창기 제어시스템은 특정 용도에 맞게 독립적으로 운영하였다. 하지만 최근 시스템의 효율적인 유지관리 및 경쟁력 강화 등의 이유로 인터넷과 같은 다양한 통신 인터페이스를 활용한 시스템 운영의 연구가 진행되면서 외부적인 보안 위협에 대한 보안관리가 요구되고 있다.

본 논문은 산업제어시스템에 적용 가능한 구간 암호화 기술을 이더넷 통신 환경에서 분석하였다. 구간 암호화 기술 적용 전후의 통신 속도를 측정 및 비교하여, 실제 암호화 적용 시의 통신 성능을 예측 하고자 한다.

Ⅰ. 서 론

산업제어시스템(Industrial Control System, ICS)은 전력, 가스, 수도, 교통 등과 같은 국가 주요 기반 시설을 감시 또는 제어하는 시스템으로, 산업설비가 복잡하고 대형화됨에 따라 효과적으로 운영할 수 있도록 설계된 시스템이다. 이는 또한 원방감시 및 제어 데이터수집 시스템(Supervisory Control and Data Acquisition), 분산제어시스템(Distributed Control Systems), PLC(Programmable Logic Controllers)와 같은 여러 종류의 제어시스템을 통칭하는 용어로서 광범위하게 사용된다[1].

초기의 제어시스템은 모두 독립적인 시스템으로 설계되어 내부에서만 운영되었지만, 최근에는 시스템의 효율적인 유지관리 및 경쟁력 강화 등의 이유로 공용망을 통해 외부 시스템과의 연동이 이루어지고 있다. 기존의 RS232 또는 RS485와 같은 시리얼 케이블 제어 방식에서 벗어나 이제는 이더넷, 광케이블, 전력선 통신(Power Line Communication) 등의 유선통신 인터페이스뿐만 아니라 Wi-Fi, LTE, TVWS 등의 무선통신 인터페이스를 이용한 원격제어 방식으로 변하고 있다. 이렇게 다양한 통신 인터페이스가 제공되면서 편리성과 효율성이 증가한 반면 사이버 공격에 의한 위협 역시 빠르게 증가하고 있다.

2010년에는 미국이 'Olympics Games'라는 코드명으로 최초의 국가기반시설 제어시스템 사이버공격 무기인 스턱스넷(stuxnet)을 개발하여 이란 원전을 공격하는데 성공했다[2]. 실제로 스턱스넷은 부셰르 원자력핵발전소의 원심분리기 가운데 20%의 가동을 중단시켜 수개월간 이란의 핵무기 개발을 지연시켰으며[1], 2010년 스턱스넷을 시작으로 플레임(Flame), 가우스(Gauss), 스카이와이퍼(sKyWiper) 등의 국가기반시설을 대상으로 하는 공격이 지속적으로 출현하고 있다[2].

이러한 국가기반시설을 목표로 하는 공격에 대응하기 위해 세계 각국은 안전성이 검증된 암호모듈 사용으로 보안을 강화하고 있다[3]. 국내에서는 KCMVP (Korea Cryptographic Module Validation Program) 암호모듈 검증 제도를 통해 암호모듈의 안전성뿐만 아니라 구현 적합성 등을 검증함으로서 안전한 암호모듈 사용을 위해 많은 투자와 노력을 기울이고 있다. 실제로 전자정부법 시행령 제69조에 의거, 국가기관 및 공공기

본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [10039140, 스마트 디바이스용 칩(ARM7/9/11, UICC 등)에 최적화된 암호(ARIA, SEED, KCDSA 등)의 국가 인증 모듈 및 배포 체계 개발].
* 국민대학교 금융정보보안학과 (guderian88@kookmin.ac.kr)
** 국민대학교 금융정보보안학과 (jakehdc@kookmin.ac.kr)
*** 국민대학교 금융정보보안학과 (oyyi@kookmin.ac.kr)

관에 도입되는 암호모듈의 검증을 의무화 하고 있으며 [4], 산업제어시스템도 검증된 암호모듈의 탑재가 불가피하다.

특히, 산업제어시스템은 국기기반시설을 총괄하는 시스템으로서 침해사고 발생 시 국가적으로 그 영향이 매우 크고 국민의 안정에 영향을 미칠 수 있으므로, 철저한 사전예방 및 보안관리가 요구된다. 따라서 본 논문은 산업제어시스템을 살펴보고 비화기 방식의 구간 암호화 모듈을 활용하는 보안 솔루션을 제공한다. 또한 실험을 통해 구간 암호화 기술의 성능을 분석하고, 산업제어시스템에 보안을 적용할 때 실제로 발생하는 통신 지연 시간을 예측할 수 있는 기준을 제시하고자 한다.

Ⅱ. 본 론

2.1. 산업제어시스템의 문제점

국가기반시설은 대부분 보안상의 이유로 외부에 공개되는 것을 원천적으로 차단하고 있는데, 시설들의 규모가 커지고 다양해지면서, 중앙에서 제어 및 관리할 수 있는 운영환경에 대한 요구가 증가하고 있다. 하지만 국가기반시설은 대부분 거대한 규모의 시설들이기 때문에 시스템의 일부분을 바꾸는 것조차 쉽지 않다. 따라서 산업제어시스템을 포함한 대부분의 국가기반시설들은 운영 된지 20년에서 30년 이상이며, 아직까지도 기존의 아날로그 방식의 제어시스템을 고수하는 경우가 많다. 그럼에도 불구하고 IT 기술의 발전과 산업기반시스템 수출 사업을 통해 디지털 제어시스템에 관한 많은 연구가 이루어졌고 시스템 설계에 관한 상당한 기술들을 이미 확보한 상태이다. 이에 따라 과거 아날로그 방식의 제어시스템이 점차적으로 디지털화되고 있지만, 많은 인프라의 변화가 발생함과 동시에 기존의 네트워크에서 제기되었던 다양한 공격들이 이제는 국가기반시설 및 산업제어시스템도 위협하게 되었다.

산업제어시스템이 아날로그에서 디지털로 변함에 따라, 기존의 시리얼 통신 기반에서 이더넷, 광케이블, WiFi, LTE 등의 다양한 유무선 통신 인터페이스를 가지게 되었다. 디지털화의 단점 중 하나는 기존에 존재하지 않았던 보안상의 취약점들이 발생하는 것인데, 보안적 관점에서는 기존의 네트워크 환경에서 수없이 연구되었던 보안 기술들을 이제는 산업제어시스템에 접목시킬 수 있게 된 것이다. 다만, 산업제어시스템은 초기 아날로그 방식의 설계 특수성 때문에 현존하는 보안 기술들을 바로 적용하기는 어렵지만, 시스템의 특성에 맞게 가공된다면 기존의 연구된 기술들의 활용도와 효용가치는 매우 높을 것이다. 또한 현재 산업제어시스템이 직면하고 있는 많은 보안상의 문제를 해결하는 방안이 될 것이다.

2.2. 산업제어시스템의 보안

산업제어시스템의 다양한 취약점이 제기되면서 그에 따른 각종 보안 솔루션들이 제안 되고 있지만, 많은 시스템 관리자들은 보안이 적용되면 시스템에 부하가 발생하고 성능저하가 따른다고 생각하는 경우가 많다. 하지만 감시 및 정보 수집을 목적으로 하는 시스템의 중요 데이터가 유무선 통신 인터페이스를 통해 그대로 노출되는 상황에서는, 정보 유출의 가능성이 항상 존재하기 때문에 데이터의 기밀성 보장에 관한 보안 솔루션은 선택이 아닌 필수다. 또한 산업제어시스템은 원격지에 위치한 기기를 유무선 통신 인터페이스를 통해 제어하는데, 이때 송수신되는 제어 데이터가 평문형태라면 공격자에 의해 위변조 될 가능성이 존재한다. 악의적인 목적을 가진 누군가가 시스템의 오류나 오작동을 일으킬 가능성이 있는 것이다.

암호학적으로 보안은 데이터의 무결성, 기밀성, 가용성을 중요시 하는데, 산업제어시스템의 경우 데이터의 무결성이 특히 중요시 된다. 원자력 발전소나 수력발전소와 같이 대규모 시설을 안전하게 제어하고 통제하기 위해서는 통신 인터페이스로 송수신되는 데이터의 무결성 확인은 반드시 거쳐야하는 작업이다.

또한 보안이 적용됨으로 인해 시스템에 부하가 발생하거나 데이터 송수신 시에 지연시간이 발생한다면, 실시간 모니터링과 제어가 요구되는 산업제어시스템 운영에는 치명적인 문제가 될 수 있다. 따라서 산업제어시스템에 보안을 적용하기 위해서는 가용성 측면 역시 세심하게 고려되어야 한다.

현재 산업제어시스템은 대부분이 MCU(Micro Controller Unit)라는 특정 역할에 최적화된 칩을 활용해 구현되어 있다. 이 칩들은 정해진 역할만을 수행하도록 설계되었으며, 범용 OS를 탑재하지 않은 Firmware 형태이다. 이러한 제한된 칩 환경에서 보안을 추가하는

것은 매우 까다로운 작업이며 막대한 비용이 요구된다. 그러나 가장 큰 문제는 이미 특정 기능만을 수행하기 위해 최적화된 칩에 추가적인 기능을 넣을 경우 상당한 성능저하가 발생할 수 있다는 것이다. 따라서 기존에 운영하던 칩에 보안을 추가함으로서 성능저하를 발생시키기보다, 비화기 형식으로 디자인된 별도의 보안장비를 통해 보안기능을 제공한다면, 불필요한 성능저하를 막을 수 있다. 즉, 기존 시스템의 역할 수행과 보안 역할을 분리함으로서, 프로세서에 부담을 주지 않고 성능저하를 최소화할 수 있다.

또한 공용망에 가상 사설망을 구축해서 운영하는 VPN(Virtual Private Network) 기술이 제안되기도 하는데, 가상 사설망은 산업제어시스템 보안에 해결책으로 제시하기는 어렵다. 가상 사설망 장비는 높은 보안강도를 제공하며 다양한 보안기능을 탑재한 장비로서, 대부분 PC나 서버 환경에 적합하도록 설계되어 있다. 따라서 가상 사설망 장비와 통신하는 기기들은 그에 상응하는 기능 수행 능력 및 성능이 받쳐줘야 하는데, 산업제어시스템을 구성하는 대부분의 장비들은 단순한 기능만을 수행하는 저가의 기기들이다. 이러한 환경에서 가상 사설망 장비와 호환이 되는 별도의 장비를 추가적으로 구성한다면 심한 비용 낭비가 발생할 수 있기 때문에, 가상 사설망 장비를 활용하는 방안은 분명 우려스러운 부분이 존재한다.

따라서 보안이 적용될 산업제어시스템은 세부적인 분석을 통해 각 시스템과 장비들의 역할에 맞는 보안레벨을 정해야하며, 보안레벨에 적합한 보안강도를 제공해야 할 것이다.

2.3. 가용성 성능 분석 실험 방법 설명

2.3.1 실험 목적

본 실험의 목적은 산업제어시스템의 보안 솔루션으로써 구간 암호화 기술을 적용함에 있어 가용성 성능분석을 통해 각 환경에 따라 적절한 보안이 적용될 수 있도록 참고자료를 제시하고자 한다. 따라서 기존의 시스템 환경을 최대한 유지하면서 적합한 보안 기능을 수행할 수 있는 장비를 활용 혹은 설계해야 하는데, 이번 실험을 통해 산업제어시스템을 가정한 테스트베드를 구축하고 비화기 형식의 장비를 활용한 구간 암호화 기술의 가용성 성능 평가를 수행하고자 한다.

2.3.2 실험 환경 및 과정

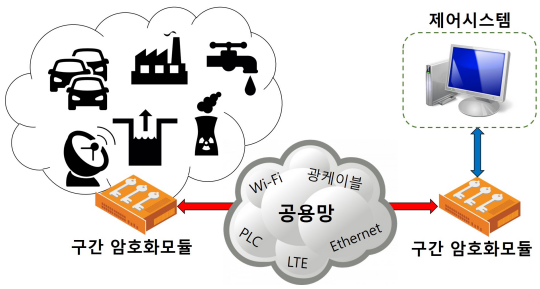
산업제어시스템의 장비들은 원격 제어시스템과 다양한 통신 인터페이스를 통해 데이터를 송수신 한다. [그림 1]과 같이 구간 암호화 모듈을 적용함으로써 산업제어시스템의 장비들과 원격 제어시스템 간의 송수신 되는 데이터를 보호할 수 있다.

이번 실험에서는 암·복호화 및 무결성 보안기능을 제공하는 블록 암호 알고리즘 기반의 메시지인증코드인 CCM과 GCM이 사용되었다. 메시지인증코드는 선택적으로 무결성 기능을 사용할 수 있기 때문에 산업제어시스템 보안으로서 적합하다. 또한 미국뿐만 아니라 국내 CMVP의 보호함수 목록에 있으며 암·복호화 및 무결성 검사를 제공한다[5-7]. 블록 암호 알고리즘으로는 국제 표준 암호 알고리즘인 AES와 KCMVP 검증 대상인 국산 알고리즘 ARIA, 그리고 최근 국내에서 개발한 LEA가 사용되었다[8-10].

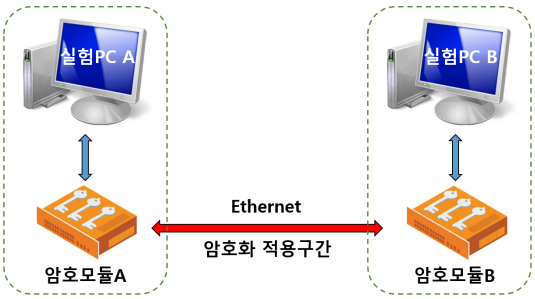
본 논문에서는 산업제어시스템을 가정한 가용성 성능을 실험하기 위해 이더넷 통신 인터페이스를 기반으로 진행하였다. PC A와 PC B 사이에 Server- Client모델을 구현하여 Client는 송신한 데이터의 에코메시지 도달 시간을 측정한다. 즉, [그림 2]와 같이 왕복 시간을 기준으로 실험이 진행되었다.

PC A와 PC B 사이에 송수신된 메시지는 총 4번 구간 암호화 모듈을 통과하게 된다. (단, TCP상 전송완료를 알리는 ACK 메시지는 생략)

PC A와 PC B는 Windows 7운영체제를 사용하여 전송시간을 계산하였으며, 4계층(전송계층)에서 전송데이터 크기를 16, 32, 128, 256, 512, 1024바이트로 측정하



〔그림 1〕 보안 적용을 위한 산업제어시스템 모델 구성도



〔그림 2〕 실험 환경 구성도

였고, TAG(MAC)길이는 128비트 고정으로 측정하였다. 구간 암호화 모듈로 사용한 장비는 ARM926EJ 코어를 사용하며 임베디드 OS를 탑재한 비화기 형식의 하드웨어 모듈이다. 블록 암호 알고리즘으로는 AES, ARIA, LEA를 사용하였고, 메시지 인증코드 CCM과 GCM은 별도의 최적화를 구현하여 차별화를 두지 않았으며, C언어 기반으로 구현하였다.

2.3.3 수식 및 용어 정리

$$T_{total} = T_{AB} + 4T_{CA} + \alpha \quad (1)$$

T_{AB} : 실험PC A와 B 사이의 왕복 통신 시간
T_{CA} : 암호모듈의 암호기능 수행 시간
α : 암호화로 인해 추가로 발생한 지연 시간

$$\alpha = \beta + \varepsilon \quad (2)$$

$$\beta = (bits) / (bps) \quad (3)$$

$bits$: 암호화로 인해 발생하는 추가 데이터의 길이
bps : 네트워크의 통신 대역폭
ε : 통신 환경에 따른 시간 변수

2.3.4 성능 분석 방법 및 설명

앞서 제시한 수식을 활용해 측정된 데이터를 분석하는 방법을 제시하고자 한다. 먼저, 수식(2)를 살펴보면 α값을 계산하는데, 실제로 β값은 매우 작은 값이며, 이더넷 환경에서는 시간 변수(ε)가 β값에 비해 매우 크므로, $\alpha = O(\varepsilon)$로 표현할 수 있다. 따라서 수식(1)을 다음과 같이 다시 정의하게 된다.

$$T_{total} \approx T_{AB} + 4T_{CA} + \varepsilon \quad (4)$$

장거리 통신의 경우, 모듈의 연산 소요 시간을 제외한 모든 변수가 변하게 된다. 통신 거리의 증가로 통신 시간(T_{AB})이 증가하고 네트워크 환경에 따른 시간 변수(ε)가 변하게 된다. 따라서 다음과 같은 수식을 얻을 수 있다.

$$T^l_{total} \approx T^l_{AB} + 4T_{CA} + \varepsilon^l,\ l: long\ distance \quad (5)$$

구간 암호화 모듈을 적용했을 경우, 단거리 통신 모델과 장거리 통신 모델의 차이는 통신 거리와 네트워크 환경의 영향을 받을 뿐 암호모듈의 영향은 동일하다는 것을 다음 계산을 통해 확인할 수 있다.

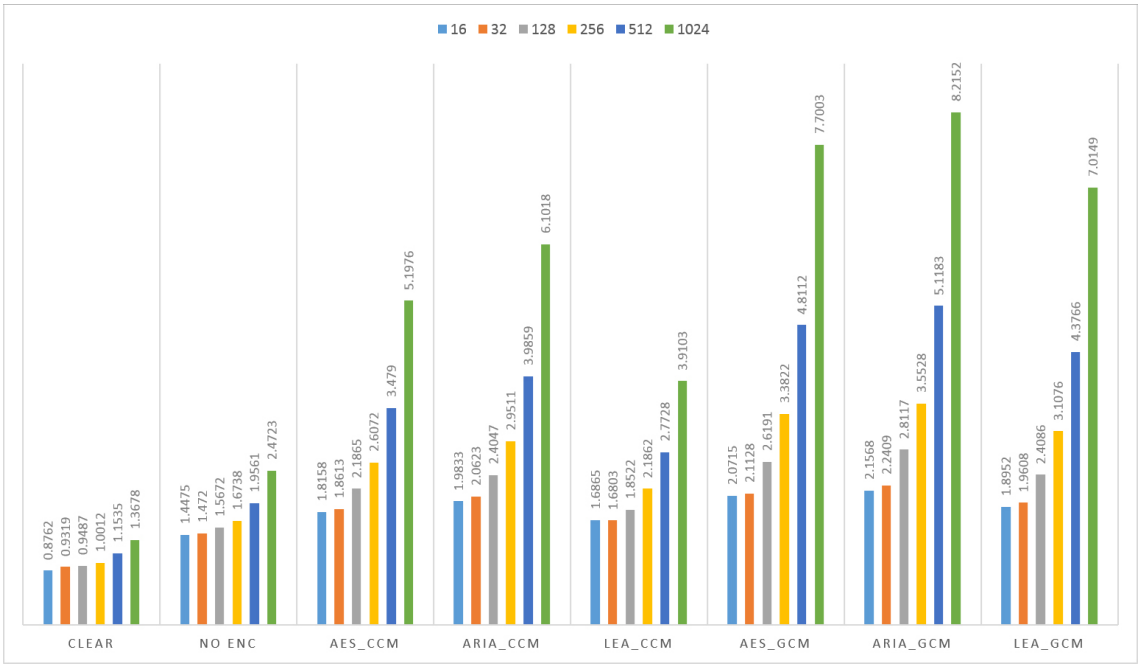
$$\begin{aligned} & T^l_{total} - T^s_{total} \\ & \approx T^l_{AB} + 4T_{CA} + \varepsilon^l - (T^s_{AB} + 4T_{CA} + \varepsilon^s) \\ & \approx T^l_{AB} + 4T_{CA} + \varepsilon^l - T^s_{AB} - 4T_{CA} - \varepsilon^s \\ & \approx T^l_{AB} + \varepsilon^l - T^s_{AB} - \varepsilon^s \\ & \approx (T^l_{AB} - T^s_{AB}) + (\varepsilon^l - \varepsilon^s),\ s: short\ distance \end{aligned}$$

따라서 실험실 환경에서 T_{CA}값을 계산함으로써 실제 산업제어시스템에 보안을 적용하는데 발생하는 비용을 예상하고자 한다.

2.4. 실험 결과

실험 결과는 [그림 3]과 [표 1]을 통해 확인 할 수 있다. [그림 3]에서, *CLEAR*는 구간 암호화 모듈이 없는 경우, 즉 기존 네트워크 환경에서 평문 통신을 측정한 결과이다. *NO ENC*의 값은 구간 암호화 모듈이 설치된 환경에서 암호화 연산을 하지 않은 경우를 나타내고 있으며, 암호화 연산 시간(비교군)을 측정하기 위한 대조군으로 활용했다.

*CLEAR*와 *NO ENC*만을 비교했을 때 차이를 확인 할 수 있는데, 이 결과를 통해 기존의 네트워크 환경에 별도의 통신장비가 도입됨으로서 발생할 지연시간을 예상할 수 있고 구간 암호화 모듈의 성능에 따라 오차범위가 다를 수 있다. 장비의 순수 암호연산 기능에 따른 가용성 성능 분석을 위해 구간 암호 모듈의 설치에 따른 지연시간은 고려하지 않는다.



〔그림 3〕 PC A와 PC B 사이의 왕복 시간(ms) 측정

다음 [표 1]은 AES, ARIA, LEA 블록 암호 알고리즘별 CCM과 GCM 암호 연산 소요시간(각 비교군과 대조군의 차이)이다.

CCM과 GCM을 객관적으로 비교해 봤을 때 암호기능 수행시간은 CCM이 GCM보다 적게 소요됨을 확인할 수 있다. 하지만 본 실험에서 사용된 CCM과 GCM은 객관적인 성능분석을 위해 최적화 기법을 적용하지 않고 표준의 내용대로 구현하였으며, 구간 암호 모듈의 메모리 가용 범위에 따라 GCM의 성능을 개선할 수 있으며 이는 장비에 종속적인 문제이기 때문에 본 논문에서는 자세히 다루지 않는다.

〔표 1〕 암호 모듈의 연산 시간

	16 bytes	32 bytes	128 bytes	256 bytes	512 bytes	1024 bytes
AES_CCM	0.3683	0.3893	0.6193	0.9334	1.5229	2.7253
ARIA_CCM	0.5358	0.5903	0.8375	1.2773	2.0298	3.6295
LEA_CCM	0.239	0.2083	0.285	0.5124	0.8167	1.438
AES_GCM	0.624	0.6408	1.0519	1.7084	2.8551	5.228
ARIA_GCM	0.7093	0.7689	1.2445	1.879	3.1622	5.7429
LEA_GCM	0.4477	0.4888	0.8414	1.4338	2.4205	4.5426

Ⅲ. 결 론

지금까지의 산업제어시스템은 격리된 폐쇄망을 구축하고, 자체적으로 개발한 프로토콜과 OS 등을 사용함으로서 최소한의 보안을 유지하는데 그쳤다. 하지만 최근 다양한 통신 인터페이스와 범용 OS 등을 사용한 개발이 증가하면서 다양한 취약점과 공격들을 고려하지 않을 수 없게 되었다. 이런 보안 위협으로부터 보호하기 위해서는 산업제어시스템의 운영환경, 기기 성능 등을 고려한 적절한 보안정책 수립이 요구된다.

하지만 산업제어시스템의 장비들은 대부분 보안이 적용되기 어려운 환경이고 거대 규모의 산업제어시스템의 경우 전체를 바꾸는 일은 쉽지 않다. 또한 각 환경에 따른 응용서비스 또한 종류가 다양하기 때문에 산업제어시스템 전체를 통합할 수 있는 보안정책 수립은 어려울 수밖에 없다.

따라서 기존의 운영환경을 크게 변경하지 않고 각 기기들의 성능저하를 최소화 할 수 있는 보안 솔루션으로서 구간 암호 모듈을 활용한 방안을 제안한다. 본 논문의 실험 데이터를 통해 구간 암호 모듈이 설치됨으로서 발생하는 지연시간을 측정함으로서, 구간 암호 모듈의 가용성 성능평가 결과를 제공하고 이를 통해 각 운영환

경에 적합한 보안 정책을 수립하기 위한 평가 지표로서 활용되기를 바란다.

참 고 문 헌

[1] 권정옥, 홍유진, “산업제어시스템의 보안 관리방안에 관한 연구”, *Samsung SDS Journal of IT Services Vol.8 / No.2*, 2013.

[2] IT보안인증사무국, 국내·외 상용 암호모듈 검증정책, *정보과학회지 제25권 제5호*, May 2007.

[3] 국가사이버안전센터, 암호모듈검증 - 개요 및 체계, http://service1.nis.go.kr/

[4] 서정택, “북한 사이버전에 대비할 국가기반시설 제어시스템 강화해야”, *과학과 기술*, May 2013.

[5] Morris Dworkin, “Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality ”, *NIST Special Publication 800-38C*, May 2004.

[6] Morris Dworkin, “Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC”, *NIST Special Publication 800-38D*, November 2007.

[7] 지식경제부 기술표준원, “128비트 블록 암호 알고리즘 ARIA－제2부: 운용 모드”, *KS X 1213－2:2009*, December 2009.

[8] Federal Information Processing Standards, “ADVANCED ENCRYPTION STANDARD (AES)”, *FIPS PUB 197*, November 2001.

[9] 지식경제부 기술표준원, “128비트 블록암호 알고리즘 ARIA”, *KS X 1213:2004*, December 2004.

[10] 한국정보통신기술협회 (TTA), “128 비트 블록 암호 LEA”, *TTAK.KO-12.0223,* December 2013.

〈저 자 소 개〉

이 재 훈 (Jaehoon Lee)
정회원

2013년 3월 : 국민대학교 수학과 졸업
2013년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
관심분야 : 네트워크 보안, 정보보호, 산업제어시스템

최 현 덕 (Hyunduk Choi)
정회원

2014년 1월 : Northeastern University 수학과 졸업
2014년 3월~현재 : 국민대학교 금융정보보안학과 석사과정
관심분야 : 네트워크 보안, 정보보호, 산업제어시스템

이 옥 연 (Okyeon Yi)
정회원

1990년 2월 : 고려대학교 대수학 석사 졸업
1996년 8월 : University of Kentucky 대수학 박사 졸업
2001년 9월~현재 : 국민대학교 자연과학대학 금융정보보안학과 교수
관심분야 : 네트워크 보안, 정보보호, 산업제어시스템