https://doi.org/10.33778/kcsa.2024.24.1.051

이중 해시체인 기반의 명령어 메시지 인증 메커니즘 설계★

박 왕 석*, 박 창 섭**

요 약

최근 산업제어시스템은 정보기술과 운영기술을 융합하는 Industrial IoT의 도입과 함께 진화를 계속하고 있지만, 과거에는 경험하지 못한 다양한 사이버 공격 역시 증가하고 있다. 제어센터에서 전송되는 다양한 명령어 메시지를 통해 시스템을 구성하는 필드 디바이스들에 대한 모니터링 및 운영 제어가 행해지기에 명령어 메시지에 대한 무결성과 더불어 제어센터에 대한 인증은 필수 요구사항이 되고 있다. 기존의 대칭키 기반의 메시지인증코드 방식 또는 공개키 기반의 서명 방식은 제어센터 그리고 자원 제약적 필드 디바이스의 비대칭성에 따른 적용상의 제약들이 존재한다. 특히, 대칭키 방식에서는 필드 디바이스에 설치된 대칭키가 공격자에게 노출되면 시스템 전반적인 보안 문제점이 발생한다. 본 논문에서는 명령어 메시지를 구성하는 구성 필드들이 취할 수 있는 데이터 값들이 제한적(낮은 엔트로피)이라는 점에 착안하여 암호해시함수로 구축된 이중 해시체인을 통한 메시지 인증기법을 제안한다. 한 쌍의 이중 해시체인은 오직 한 개의 명령어 메시지에 적용되기에 다중 사용을 위한 Merkle 트리에 기반을 둔 확장 기법 역시 제안한다. 메시지 인증을 위해 암호해시함수 이외의 암호 프리미티브는 사용이 안 되기에 계산 복잡도는 매우 낮게 유지될 수 있음을 성능평가를 통해 확인한다.

Design of Authentication Mechinism for Command Message based on Double Hash Chains

Park Wang Seok*, Park Chang Seop**

ABSTRACT

Although industrial control systems (ICSs) recently keep evolving with the introduction of Industrial IoT converging information technology (IT) and operational technology (OT), it also leads to a variety of threats and vulnerabilities, which was not experienced in the past ICS with no connection to the external network. Since various control command messages are sent to field devices of the ICS for the purpose of monitoring and controlling the operational processes, it is required to guarantee the message integrity as well as control center authentication. In case of the conventional message integrity codes and signature schemes based on symmetric keys and public keys, respectively, they are not suitable considering the asymmetry between the control center and field devices. Especially, compromised node attacks can be mounted against the symmetric-key-based schemes. In this paper, we propose message authentication scheme based on double hash chains constructed from cryptographic hash function without introducing other primitives, and then propose extension scheme using Merkle tree for multiple uses of the double hash chains. It is shown that the proposed scheme is much more efficient in computational complexity than other conventional schemes.

Key words : Industrial Control System, integrity, cryptographic hash function, Merkle tree, double hash chain, command message, source authentication

접수일(2024년 02월 14일), 게재확정일(2024년 03월 04일)

★ 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00240037)

* 단국대학교/컴퓨터학과 (주저자)
** 단국대학교/산학협력단 (교신저자)

1. 서 론

산업제어시스템(ICS: Industrial Control System)은 원자력발전소, 정유시설, 상하수시스템, 스마트그리드 등의 다양한 제조산업 및 국가중요시설의 자동화 시스템에 대한 감시와 제어를 위한 필수 시스템이다. ICS는 최근 정보기술과 운영기술 융합에 따른 지속적 진화를 계속하고 있지만 사이버 위협 역시 계속 증가하고 있다 [1]. ICS에 대한 사이버 공격은 ICS의 정상적인 운영을 제약할 뿐만 아니라 인간에 대한 위해요소가 될 수도 있다. 따라서, 제어센터(control center)로부터 ICS를 구성하는 필드 디바이스(field device)들에 유니캐스트 또는 멀티캐스트 방식으로 전송되는 제어 명령어(control command)에는 무결성 및 인증(source authentication) 기능의 내재화가 요구된다.

기존의 명령어 인증방식은 제어센터가 명령어에 전자서명 또는 MIC(message integrity code)을 첨부하여 전송하고 각각의 디바이스는 이를 검증하게 된다. 따라서, 디바이스들에는 제어센터의 (서명 검증용) '공개키' 또는 (MIC 검증용) '대칭키'가 사전 설치되어 있어야 한다. 특히, 전자서명 방식의 경우 암호해시함수(cryptographic hash function) 및 다양한 전자서명 알고리즘들이 적용되며 MIC 방식의 경우는 AES-CBC-MAC 또는 HMAC 알고리즘 등이 적용된다. 전자서명에 사용되는 서명 알고리즘은 계산 복잡도가 매우 높으며, 반면에 MIC 방식의 경우 디바이스에 대칭키의 안전한 설치가 요구된다. 특히, 후자의 경우 디바이스에 탑재된 대칭키가 노출되면 (i.e. compromised device attack) 안전한 명령어 실행은 실패하게 된다.

본 논문에서는 전자서명의 단점인 "높은 계산 복잡도" 및 MIC 방식의 단점인 "대칭키 노출 가능성"을 회피하기 위해 디바이스에는 기밀성이 요구되지 않는 검증용 공개 정보만이 설치되며 암호해시함수만으로 동작하는 명령어 인증 메커니즘을 제안한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 ICS 환경에서의 기존 명령어 인증기법들을 소개하고, 3장에서는 제안 메커니즘에 관해 설명한다. 4장에서는 본 제안 메커니즘에 대해 실시한 성능평가를 통해 실현이 가능한 인증 메커니즘임을 입증한다.

2. 관련 연구

산업제어시스템에 적용이 가능한 다양한 제어 명령어 메시지 인증기법들이 제안되었다.

첫째, ICS Modbus 환경에서 Modbus master와 Modbus slaves 사이에 교환되는 명령어 유형의 개수가 n이고 그리고 명령어 전송회수가 최대 m번인 경우, 길이가 n인 m개의 해시체인 사용을 제안하였다 [2]. 하지만, 설계상의 결함으로 보안상의 문제점[3]을 내포하고 있다. 또한, chameleon 해시함수[4]를 이용한 경량 서명 기법[5]의 경우 이산대수 문제에 기반을 두고 있고 ICS 필드 디바이스 측에 과도한 계산 부담이 전가되는 명령어 인증 방식이다.

둘째, TESLA[6] 기반의 명령어 인증기법 [6, 7]들도 제안되었다. [7]의 경우 TESLA의 기본적인 체계가 지연인증(delayed authentication)의 특성을 가지기에 즉각적인 인증(instant verification)은 불가능하며, [8]에서는 즉각적인 인증을 위한 방안을 제시했으나 키 관리상의 문제점을 내포하고 있다.

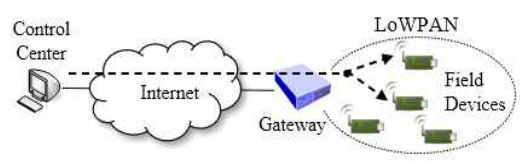
셋째, TESLA 지연인증의 문제점을 극복하기 위한 condensed RSA[9] 기반의 online/offline 신속 인증(rapid authentication) 기법[10]의 경우 RSA 연산에 따른 과도한 부담이 ICS 필드 디바이스 측에 가해진다.

마지막으로 Lamport-Diffie[11], Winternitz[12], HORS[13] 등의 일회용 서명(OTS: one time signature)을 활용한 명령어 인증기법들[14, 15] 역시 제안되었다. 하지만 이들 방식의 공통된 제약조건은 일회성이라는 제약사항을 극복하기 위해 제어센터와 디바이스 간에 별도의 대칭키 사전 공유가 요구되며 서명 및 공개키의 크기가 매우 크다는 단점을 가지고 있다.

3. 제안 메커니즘

3.1 시스템 모델 및 보안요구사항

(그림 1)에서처럼 제어센터는 사전에 지정된 다수의 ICS 필드 디바이스들에 제어 명령어 메시지를 전송한다. ICS 디바이스는 자원 제약적 디바이스로 가정하고 IEEE 802.15.4와 같은 LoWPAN (Low-power Wireless Personal Area Network) 네트워크 환경에서 동작한다. LoWPAN과 Internet 사이의 인터페이스 역할을 하는 Gateway는 명령어 메시지를 탑재한 패킷의 크기가 너무 크면 압축(compression) 및 단편화(fragmentation) 작업을 수행한다.



(그림 1) 시스템 모델

공격자는 제어센터를 가장해서 위조된 명령어 메시지를 보낼 수도 있고, 제어센터가 전송한 메시지를 변조 및 재생할 수 있다. 또한, 필드 디바이스에 저장된 비밀정보는 공격자에 의해 노출될 수도 있다. 따라서 언급된 공격모델에 대응하기 위해서는 무결성을 포함한 메시지 인증기능이 요구되며 개별 디바이스에는 공개가 가능한 검증용 키 정보만이 설치되어야 한다.

3.2 제어 명령어 인코딩

ICS 디바이스에 적용되는 제어 명령어 메시지는 address, command, data 필드로 구성된다. 특히, 메시지의 개별 필드들은 사전에 정의된 작은 데이터 세트에 속하는 값으로 채워진다. 예를 들면 특정 디바이스 가동 시작/중지, 전원차단기 작동, 또는 모터 속도 10% 가속/감속과 같이 command 및 연계된 data 값 유형은 제한적이다.

$\boldsymbol{cmd} = \{cmd_i \mid i \in [1, S]\}$를 command 집합, $d_i = \{d_{ij} \mid j \in [1, q_i]\}$ for $i \in [1, S]$는 각각의 command에 적용되는 data 값들의 집합으로 정의되며 적어도 1개 이상의 data 값들이 command와 함께 사용된다. (즉, $1 \le |d_i| = q_i$). 이때 각각의 command와 data 값 쌍은 다음과 같이 인코딩된다.

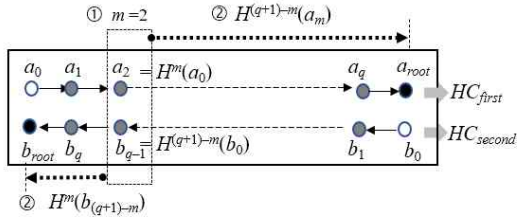
$$\begin{aligned} &m = 1 \text{ for } (cmd_1, d_{11}),\\ &m = 2 \text{ for } (cmd_1, d_{12}),\\ &\cdots\\ &m = q \text{ for } (cmd_S, d_{Sq_S}),\\ &\quad \text{where } q = q_1 + q_2 + \ldots + q_S \end{aligned} \tag{1}$$

명령어 메시지 {*header*, *payload*}는 사전에 지정된 디바이스들에 전달되기에 *header* 필드는 고정된 값으로 가정하고, 앞으로 명령어 메시지는 {*header*, *m*}로 표현한다.

3.3 이중 해시체인 생성

제어센터는 초기화 과정에서 무작위로 생성한 $\boldsymbol{a}_0$, $\boldsymbol{b}_0 \in \{0, 1\}^n$를 기반으로 $a_0 = (\boldsymbol{a}_0 \oplus \boldsymbol{header})$ 및 $b_0 = (\boldsymbol{b}_0 \oplus \boldsymbol{header})$를 구성하여 (그림 2)에서와 같이 이중 해시체인 HC_{first}와 HC_{second}을 생성한다. 여기서 $H(.)$는 암호해시함수, $H^c(.)$는 암호해시함수를 c번 연속해서 적용하는 것을 의미한다.

$$\begin{aligned} HC_{first} &= \{a_j \mid a_{j+1} = H(a_j) \text{ for } j \in [0, q]\},\\ HC_{second} &= \{b_j \mid b_{j+1} = H(b_j) \text{ for } j \in [0, q]\}. \end{aligned} \tag{2}$$



(그림 2) 이중 해시체인

$H^{q+1}(a_0) = a_{q+1} = a_{root}$와 $H^{q+1}(b_0) = b_{q+1} = b_{root}$는 각각 HC_{first}와 HC_{second}의 루트 값이며 (a_{root}, b_{root})는 시스템 부트스래핑 과정에서 ICS 필드 디바이스에 설치된다.

3.4 명령어 메시지 전송 및 검증

생성된 이중 해시체인 $HC_{first} = \{a_0, a_1, \cdots, a_q, a_{q+1}\}$의 각각의 a_j for $j \in [1, q]$에 인코딩된 command {m=1, m=2, ⋯, m=q}을 매핑시킨다. (즉, m=j가 a_j에 매핑된다)

예를 들어 제어센터가 명령어 메시지 {*header*, *m*

= 2}를 필드 디바이스에 전송하는 경우, (그림 2)-①에서처럼 메시지 인증을 위해 σ_m을 다음과 같이 생성하여 함께 전송한다.

$$\{header,\ m=2,\ \sigma_m\},\ \text{where}$$
$$\sigma_m = (a_m = H^m(a_0),\ b_{(q+1)-m} = H^{(q+1)-m}(b_0)) \quad (3)$$

해당 명령어 메시지를 수신한 디바이스는 (그림 2)-②에서처럼 a_m과 $b_{(q+1)-m}$으로부터 다음을 도출하여 설치된 $(a_{root},\ b_{root})$과 일치하는지를 확인하여 명령어 메시지의 무결성(메시지 인증)을 검증하게 된다.

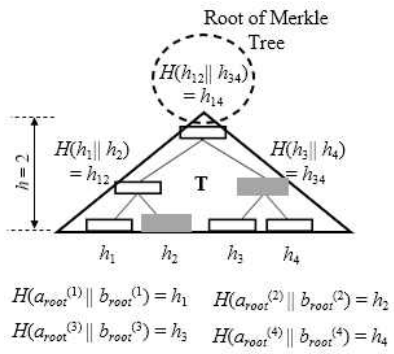
$$\text{check if } (\ H^{(q+1)-m}(a_m) = a_{root} \text{ and}$$
$$H^m(b_{(q+1)-m}) = b_{root}\ ) \quad (4)$$

3.5 다중 사용을 위한 확장 기법

3.4절에서 제안된 인증기법은 생성된 이중 해시체인의 루트 값 $(a_{root},\ b_{root})$에 대해 오직 한 번 사용이 가능하다. 따라서 다중 사용을 위해서는 높이가 h인 Merkle 트리를 구성하고 2^h 개의 리프노드에 [Algorithm 1]을 통해 도출한 2^h 개의 이중 해시체인 루트 값들을 대응시켜 2^h 개의 명령어 메시지에 대한 무결성 보장을 위해 사용할 수 있다.

[Algorithm 1: 이중 해시체인 루트 값 도출]
for k = 1 to 2^h {
  generate $\boldsymbol{a}_0^{(k)}$, $\boldsymbol{b}_0^{(k)} \in \{0,\ 1\}^n$;
  $a_0^{(k)} \leftarrow (\boldsymbol{a}_0^{(k)} \oplus header)$; $b_0^{(k)} \leftarrow (\boldsymbol{b}_0^{(k)} \oplus header)$;
  generate $HC_{first}^{(k)}$ and $HC_{second}^{(k)}$;
  derive $(a_{root}^{(k)},\ b_{root}^{(k)})$;
}

(그림 3)은 h=2인 경우의 Merkle 트리 구성을 보여주고 있다. 4개의 이중 해시체인을 통해 4개의 해시체인 루트 값들을 생성하여 리프노드 h_1, h_2, h_3, h_4에 대응시키고 내부 노드들은 자식 노드들의 해시값으로 구성된다. 최종적으로 Merkle 트리의 루트 값 (h_{14}) 그리고 $(stored\_k$=0)가 시스템 부트스래핑 과정에서 디바이스에 설치된다. 첫 번째 command m_1을 포함하는 명령어 메시지는, (식 5)와 같이 구성되어 디바이스에 전송된다.



(그림 3) 다중 사용 Merkle 트리 구성

$$\{header,\ m_1,\ k=1,\ (\sigma_{m_1},\ h_2,\ h_{34})\},\ \text{where}$$
$$\sigma_{m_1} = (a_{m_1},\ b_{(q+1)-m_1}) \quad (5)$$

해당 명령어 메시지를 수신한 디바이스는 (식 6)과같이 첫째 순번(sequence number) 역할을 하는 k=1이 저장된 $stored\_k$=0보다 큰지를 확인, 둘째 σ_{m_1}을 검증하고, 셋째 $(\sigma_{m_1},\ h_2,\ h_{34})$로부터 설치된 Merkle 트리의 루트 값 h_{14}와 일치하는지를 확인하여 명령어 메시지의 무결성을 검증하게 된다. 검증이 성공적으로 종료되면 저장된 k는 갱신된다.

check if $(k=1) > (stored\_k=0)$;
check if ($H^{(q+1)-m_1}(a_{m_1}) = a_{root}^{(1)}$ and
$H^{m_1}(b_{(q+1)-m_1}) = b_{root}^{(1)}$);
derive $h_1 \leftarrow H(a_{m_1}||b_{(q+1)-m_1})$;
check if $H(H(h_1||h_2)||h_{34}) = h_{14}$: (6)

command m_2, m_3, m_4에 대해서도 같은 방식으로 명령어 메시지를 구성하고 검증할 수 있다.

4. 분석 및 평가

4.1 제안 메커니즘 안전성

3.3절에서 소개된 이중 해시체인에 기반을 둔 인증기법의 안전성은 암호해시함수의 역상 저항성(pre-image resistance)에 의해 보장된다. (그림 2)의 예에서 (m=2)를 (m=1) 또는 (m=4)로 변조시키기 위해서는 공격자는 $(a_1,\ b_{(q+1)-1})$ 또는 $(a_4,\ b_{(q+1)-4})$를 도출할 수 있어야 가능하지만, 이는 암호해시함수의 역상 저항성에 의해 불가능

하게 된다.

다중 사용을 위한 확장 기법에서는 Merkle 트리의 리프노드에 할당된 command m_1, m_2, m_3, m_4가 순차적으로 사용되며 명령어 메시지에는 순번 k가 포함되기에 공격자에 의한 재생 공격(replay attack) 역시 불가능하다.

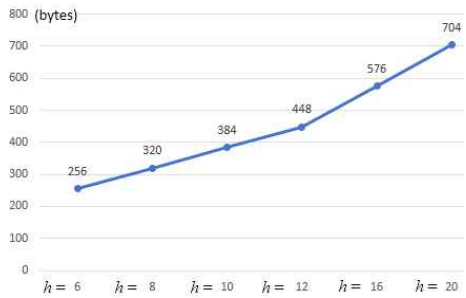
4.2 성능분석

(식 5)를 일반화시키면 즉, Merkle 트리의 높이가 h인 경우에는 (식 7)과 같다.

$$\{header,\ m_k,\ k,\ (\sigma_{m_k},\ auth\_path)\}, \qquad (7)$$

where *auth_path* is a set of sibling nodes of th e nodes on the way from the leaf node to the Merkle root.

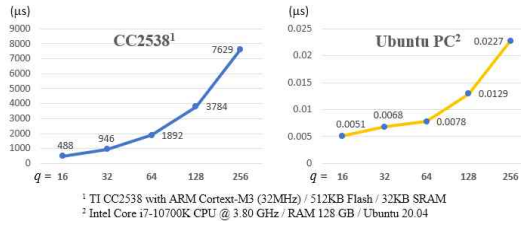
SHA-256의 경우, $|\sigma_{m_k}|$ = 64 bytes, $|auth\_path|$ = h*32 bytes이다. (그림 4)는 Merkle 트리의 높이 변화에 따라 $(\sigma_{m_k},\ auth_path)$이 차지하는 바이트 길이를 보여주고 있다.



(그림 4) Merkle 트리 height에 따른 바이트 길이

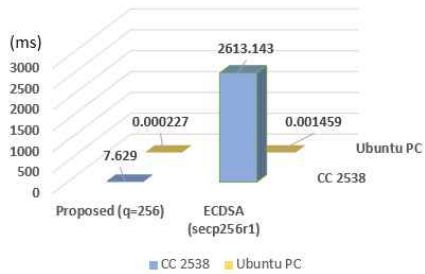
결국 다중 사용 횟수를 증가시키기 위해서는 명령어 메시지의 길이는 늘어날 수밖에 없다.

제안 메커니즘에서는 암호해시함수만이 사용된다. 각각의 command의 경우 $|m|$ = $\lceil \log_2 q \rceil$ 이기에 σ_{m_k} 생성과 검증에는 q번의 암호해시함수가 반복적으로 적용되어야 한다. (그림 5)는 q의 변화에 따른 암호해시함수 회수를 Ubuntu PC 및 mote(TI CC2538)에서의 실행시간(micro-second)을 보여주고 있다.



(그림 5) 암호해시함수(SHA-256) 처리시간

3.1절에서의 보안요구사항 중의 하나는 "개별 디바이스에는 공개가 가능한 검증용 키 정보만이 설치"이다. 물론 공개키 서명이 사용되면 (서명 확인용) 공개키가 설치되기에 보안요구사항을 충족시키지만 (그림 6)에 나타나 있는 것처럼, ECDSA는 서명 생성 및 검증에 암호해시함수보다 매우 높은 계산량(milli-second)을 요구하고 있다.



(그림 6) ECDSA 및 SHA-256 처리시간 비교

5. 결 론

정보기술 및 운영기술 융합에 따른 산업제어시스템의 진화가 계속됨에 따라서 사이버 공격의 가능성 역시 증대되고 있다. 본 논문에서는 제어센터로부터 ICS 필드 디바이스들에 전송되는 명령어 메시지의 무결성을 보장하는 인증 메커니즘을 제안하였다.

제안의 핵심은 무결성 보장을 위해 오직 암호해시함수만이 사용되기에 자원 제약적인 필드 디바이스들에도 적용할 수 있다. 특히, 필드 디바이스에 설치되는 초기 정보는 무결성 검증을 위한 공개된 정보이기에 공격자의 디바이스 탈취에 따른

비밀정보 획득은 무의미하게 된다. 제안 방식은 ICS 환경에서뿐만 아니라 전송 메시지를 구성하는 개별 필드들의 엔트로피가 낮게 유지되는 모든 응용환경에 적용할 수 있다.

본 논문과 연계된 후속 연구에서는 다중 사용을 위한 확장 기법이 가지는 단점인 사용횟수 증가에 따른 메시지 길이 증대를 완화하는 방안을 마련하고자 한다.

참고문헌

[1] G. M. Makrakis, C. Kolias, G. Kambourakis, C, Rieger, and J. Benjamin, “Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents,” IEEE Access Vol. 9, pp. 165295-165325, Dec. 2021.

[2] G. Y. Liao, Y. J. Chen, W. C. Lu, and T. C. Cheng, “Toward Authenticating the Master in the Modbus Protocol,” IEEE Trans. Power Delivery, Vol. 23, No. 4, pp. 2628-2629, Oct. 2008.

[3] R. Phan, “Authenticated Modbus Protocol for Critical Infrastructure Protection,” IEEE Trans. Power Delivery, Vol. 27, No. 3, pp. 1687-1689, Jul. 2012.

[4] H. Krawczyk and T. Rabin, “Chameleon Hashing and Signatures,” in Proc. Network and Distributed System Security 2000, pp: 143-154, San Diego, Feb. 3-4, 2000.

[5] Z. Yang, C. Jin, Y. Tian, J. Lai, and J. Zhou, “LIS: Lightweight Signature Schemes for Continuous Message Authentication in Cyber-Physical Systems”, in Proc. ACM ASIA Conf. Computer Communication Security, pp. 719-731, Taipei, Taiwan, Oct. 5-9, 2020.

[6] A. Perrig, D. Song, R. Canetti, J. D. Tygar, and B. Briscoe, “Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction”, IETF RFC 4082, Jun 2005.

[7] S. Aghapour, M. Kaveh, D. Martin, and M. R. Mosavi, “An Ultra-Lightweight and Provably Secure Broadcast Authentication Protocol for Smart Grid Communications,” IEEE Access, Vol. 8, pp. 125477-125487, Jul. 2020.

[8] U. Tefek, E. Esiner, D. Mashima, B. Chen, and Y. C. Hu, “Caching-based Multicast Message Authentication in Time-critical Industrial Control Systems,” in Proc. IEEE conf. Computer Comm., pp. 1039-1048, London, May 2-5, 2022.

[9] E. Mykletun, M. Narasimha, and G. Tsudik, “Authentication and Integrity in Outsourced Databases,” ACM Trans. Storage, Vol. 2, No. 2, pp. 107 - 138, 2006.

[10] A. A. Yavuz, “An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages,” IEEE Trans. Info. Forensics and Security, Vol. 9, No. 10, pp. 1733-1742, Oct. 2014.

[11] L. Lamport, “Constructing Digital Signatures from a One-way Function, Technical Report CSL 98, SRI International, 1979.

[12] R.C. Merkle, A certified digital signature based on a conventional function,” Advances in Cryptology - Crypto 87, LNCS, Vol. 293, pp. 369 - 378, Springer, 1987.

[13] L. Reyzin and N. Reyzin, “Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying,” Information Security and Privacy, LNCS, Vol. 2384. pp. 144 - 153, Springer, 2002.

[14] Q. Li and G. Cao, “Multicast Authentication in the Smart Grid with One-Time Signature,” IEEE Trans. Smart Grid, Vol. 2, No. 4, pp. 686-696, Dec. 2011.

[15] N. Saxena and S. Grijalva, “Efficient Signature Scheme for Delivering Authentic Control Commands in the Smart Grid,” IEEE Trans. Smart Grid, Vol. 9, No. 5, pp. 4323-4334, Sep. 2018.

〔저자소개〕

박 왕 석 (Wang-seok Park)
1998년 2월 단국대학교 이학학사
2001년 2월 단국대학교 이학석사
2002년 8월 ~ 안랩 연구원
2024년 2월 단국대학교 공학박사
email :
wangseok.park @ahnlab.com

박 창 섭 (Chang-seop Park)
1983년 8월 연세대학교 경제학사
1987년 1월 Lehigh Univ. 공학석사
1990년 5월 Lehigh Univ. 공학박사
1990년 9월 ~ 2023년 8월 단국대학교 소프트웨어학과 교수
2023년 9월 ~ 단국대학교 산학협력단 연구원
email : csp0@dankook.ac.kr