Journal of The Korea Society of Computer and Information
Vol. 24 No. 7, pp. 87-91, July 2019

www.ksci.re.kr
https://doi.org/10.9708/jksci.2019.24.07.087

Blockchain-based IoT Authentication techniques for DDoS Attacks

Wonseok Choi*, Sungsoo Kim**

Abstract

In the IoT(Internet of Things) environment, various devices are utilized and applied for different sites. But attackers can access easy to IoT systems, and try to operate DDoS(Distributed Denial-of-Service) attacks. In this paper, Sensor nodes, Cluster heads, and Gateways operates lightweight mutual authentication each others. Since authenticated sensor nodes and cluster heads only send transactions to Gateways, proposed techniques prevent DDoS attacks. In addition, the blockchain system contains secure keys to decrypt data from sensor nodes. Therefore, attackers can not decrypt the data even if the data is eavesdropped.

▸Keyword: Authentication Protocol, Blockchain, IoT, DDoS

I. Introduction

IoT(Internet of Things) 기술의 발전으로 일상 가정에서도 IoT 제품이 사용되는 것을 볼 수 있으며 산업계에서도 센서류에 적용하여 모니터링 기술에 적용하는 등 적용 사례를 늘어나고 있다. 5G 무선 기술이 더해진다면 더 많은 IoT 단말들이 해당 서비스에 연동될 수 있을 것이며 다양한 서비스들이 상용화될 것으로 예상된다. IoT 단말들은 센서 등과 같은 저성능 장치부터 멀티 코어 마이크로 프로세서를 장착한 고성능 장치까지 다양할 것인데, 기존 연구들에서도 저성능 장치를 대상으로 한 경량 인증 방법과 관련한 연구들[7][9][11][13]과 인증을 통한 DoS(Denial-of-Service) 공격 차단 관련 연구[10]가 수행되었다. 본 논문에서는 저성능 하드웨어 시스템에 적용되며 DDoS(Distributed Denial-of-Service) 공격을 차단할 수 있는 블록체인 기반 IoT 인증 프로토콜을 제안한다.

블록체인은 P2P(Peer to Peer) 통신 방식으로 연결된 블록체인 노드 간에 트랜잭션 데이터들을 블록 단위로 구성하고, 블록 간 연결하여 데이터 무결성을 확보할 수 있는 분산 컴퓨팅 기반 기술이다. 기존에 연구된 블록체인 기반 IoT 인증 연구[2]에서, 각 단말은 할당받은 공개키와 관련 데이터를 해시 연산한 뒤 최상위 Aggregator인 블록체인 시스템까지 전송한다. 단말들이 발생시킨 인증 트랜잭션들의 Root Hash 값과 블록체인 시스템에 저장된 App Hash 간의 동일 여부로 해당 단말들을 인증하는 방법을 제안하였다. 그러나 [2]에서는, 단말에서 Aggregator에 인증 트랜잭션 전송 시 상호 인증없이 데이터를 노출시킴으로써 중간자 공격, 재전송 공격 등에 취약하다.

본 논문에서 제안하는 IoT 인증 프로토콜은 Sensor node, Cluster head 및 Gateway 간 상호 인증을 수행하여 인증된 대상만이 Gateway에 블록체인 트랜잭션을 발생시킬 수 있게 함으로써 DDoS 공격을 차단한다. 그리고 저성능 단말 장치 상에서의 적용 가능하도록 암호화 알고리즘 연산을 최소화하며, 블록체인 시스템에 비밀키를 저장하고 이를 이용하여 복호화하는 방법을 적용하였기에 암호화한 데이터가 전송 시 노출되더라도 공격자로부터 원문을 보호할 수 있다.

2장에서는 블록체인 기술과 기존 블록체인 기반 IoT 인증 프로토콜의 전반적인 설명을 기술한다. 3장에서 제안 프로토콜의 상세 내용을 제시하며 4장에서는 제안 프로토콜의 보안성 분석을 기술한다. 그리고 5장에서 본 제안 기법을 요약하며 결론을 맺는다.

• First Author: Wonseok Choi, Corresponding Author: Sungsoo Kim
*Wonseok Choi (theenemys@knu.ac.kr), School of Computer Science and Engineering, Kyungpook National University
**Sungsoo Kim (ninny@ikw.ac.kr), Department of Aeronautical Software Engineering, Kyungwoon University
• Received: 2019. 07. 02, Revised: 2019. 07. 26, Accepted: 2019. 07. 26.

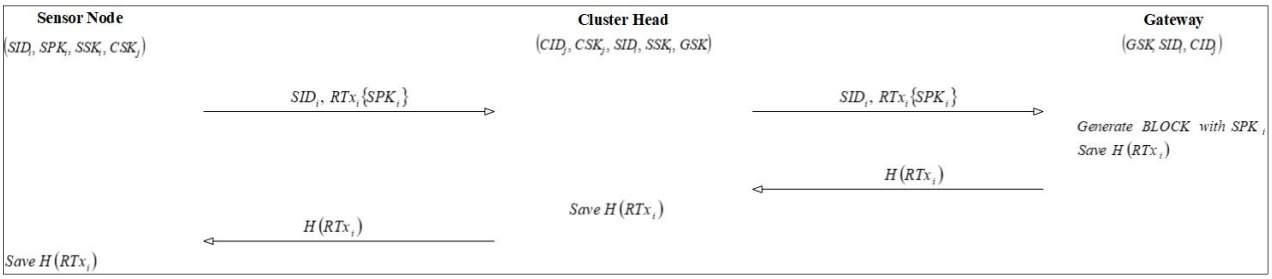

Fig. 1. Registration Protocol

II. Related Works

1. Blockchain

블록체인은 클라이언트로부터 발생되는 트랙잭션 데이터가 P2P 통신으로 연결된 노드 간에 블록 형태로 구성되고, 각 블록은 체인 형태로 연결됨으로써 블록으로 확정된 데이터는 수정 불가하여 데이터 무결성을 보장할 수 있는 분산 컴퓨팅 기반의 데이터 위변조 방지 기술이다. 블록체인 기술을 이용한 대표적인 암호화폐 시스템은 비트코인[1]으로써 퍼블릭 블록체인 방식으로 활용되고 있다.

블록체인의 생성 및 구성 방식을 살펴보자. 블록 생성 권한을 가진 블록체인 노드들은 P2P 통신으로 연결되어 있고, 발생된 트랜잭션을 처리하여 블록으로 확정시켜 체인화하기 위하여 블록체인 노드 간에 합의(Consensus) 프로세스를 수행한다.

블록 간에 체인 형태의 결합 방식을 위하여, 블록 생성 시 직전 블록을 해시 처리한 값을 포함한다. 블록에는 처리한 트랜잭션들을 포함하고 있으며 트랜잭션들의 최상위 해시값인 App Hash는 직후에 생성되는 블록에 포함되므로, 특정 블록체인 노드에서 임의의 블록 내 트랜잭션 데이터를 변경시킨다면 다음에 생성된 블록의 App Hash 값과 달라질 뿐 아니라 다른 블록체인 노드의 블록과도 데이터가 일치하지 않게 되므로 불법적인 변경을 완료하는 것이 어렵다[1][4][5].

2. Review of Existing Research

[3]의 연구에서는 IoT 환경 상에서 통신 개체 간에 사용되는 인증 프로토콜을 제안하였다. 각 개체는 CA(Certificate Authority)를 통하여 Certificate 및 MAC(Message Authentication Code)를 발급받아 인증 프로토콜에 이용하는데, 해당 Certificate와 MAC은 노출된다. [8]에서는 IoT 상에서의 경량화 장치 간에 사용될 수 있는 상호 인증 프로토콜을 제안하였으나 각 통신 개체의 ID(Identification)와 난수가 노출된다.

[2]에서 IoT 디바이스는 할당된 공개키와 관련 데이터를 해시한 값을 인증 값으로 사용하며 이를 상위 Aggregator에게 전송한다. Aggregator들은 수신받은 인증 값을 해시 처리하며 이 값을 자신의 상위 Aggreator에게 전송하게 되고 최상위 Aggregator인 블록체인 시스템에게 전송될 때 까지 해당 과정은 반복된다. 블록체인 시스템은 IoT 디바이스들의 인증 값의 Root Hash 값(App Hash)을 알고 있으므로, IoT 디바이스들로부터의 Root Hash 값과 비교하고 AppHash와 일치하는지 확인함으로써 인증 여부를 결정하는 기법이다.

해당 기법에서, 각 IoT 디바이스는 Aggregator 간 상호 인증 여부를 확인하지 않으며, Data를 공개키 해시 처리에 이용하여 인증 값을 변화시키지만 Data에 대한 노출 방지 방법은 제시하지 않았다. 따라서 중간자 공격, 재전송 공격 등에 취약할 수 있으며, 공격자들이 반복적인 트랜잭션을 전송시키는 DDoS 공격도 발생 가능하다.

III. Proposed Protocol

본 제안 프로토콜은 Sensor node의 비밀키를 블록체인 시스템 내 블록에 저장하기 위한 Registration protocol, 그리고 Sensor node를 인증하고 전송된 데이터를 복호화하는 Authentication protocol로 구성되어 있다.

1. Assumptions

Table 1. Notations

Notation	Description
SID_i	Identification of sensor node *i*
SPK_i	Private key of sensor node *i*
SSK_i	Session key of sensor node *i*
SR_i	Sensor node's random number
CID_j	Identification of cluster head *j*
CSK_j	Session key of cluster head *j*
CR_j	Cluster head's random number
GSK	Session key of gateway
GR	Gateway's random number
$RTx_i\{Data\}$	Register transaction with data
$H(RTx_i)$	Hash function for register transaction
$DTx_i\{Data\}$	Data transaction with data
$E_{key}(Data)$	Encrypt data by key

제안 프로토콜은 Sensor node, Cluster head, Gateway 간의 insecure area에서 적용된다. Sensor node에는 SID_i, SPK_i, SSK_i, CSK_j가 저장되어 있으며 Cluster head는

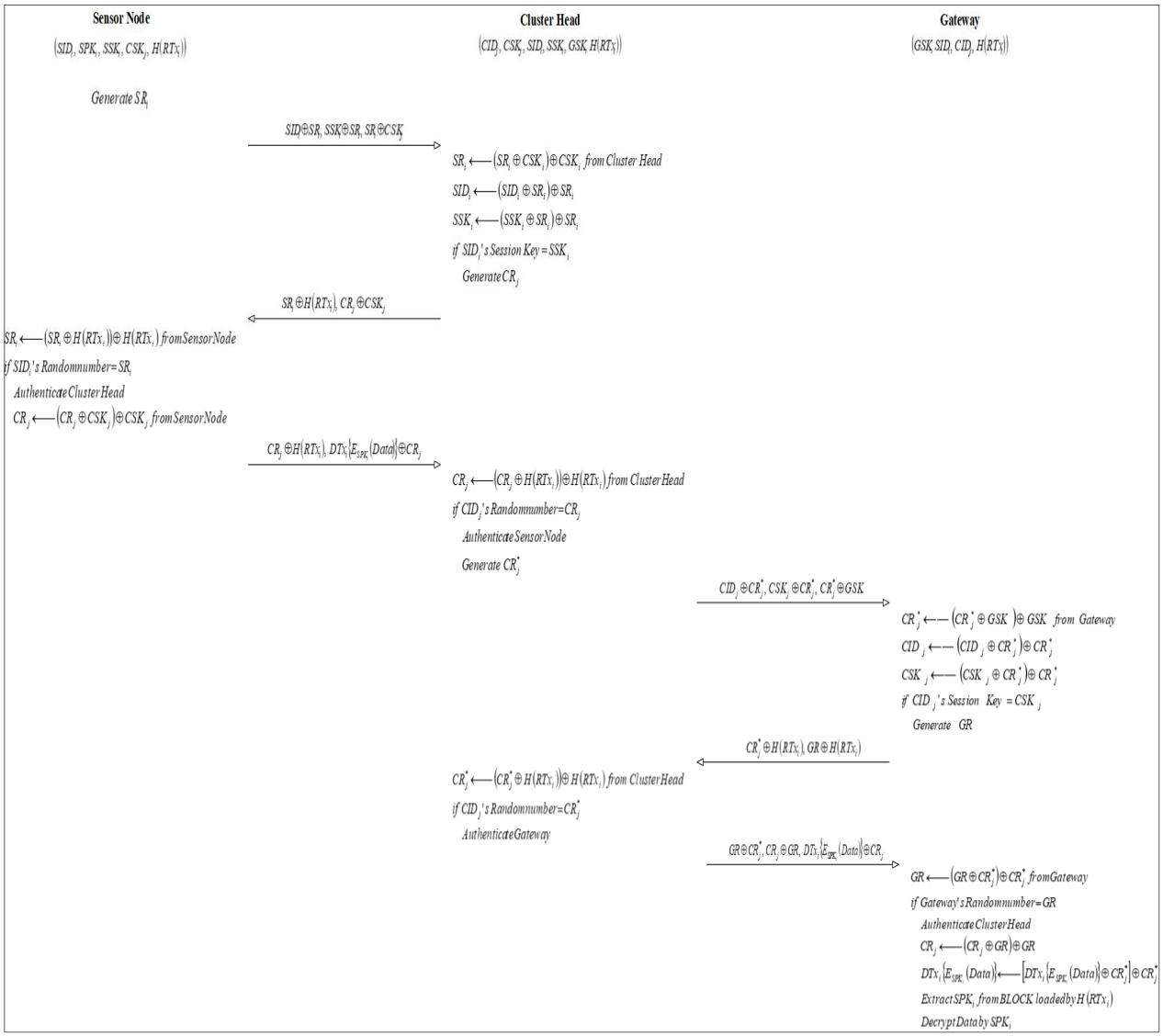

Fig. 2. Authentication Protocol

CID_j, CSK_j, SID_i, SSK_i, GSK를, Gateway는 GSK, CID_j, CSK_j, SID_i를 저장하고 있다. 또한, Sensor node는 블록체인 트랜잭션 발생을 위한 별도의 개인키를 이용하며 본 논문에는 관련 내용은 언급하지 않는다.

2. Registration Protocol

Sensor node는 자신의 비밀키를 포함한 트랜잭션 $RTx_i\{SPK_i\}$를 Gateway로 전송한다. Gateway는 해당 트랜잭션을 수신하여 블록체인 시스템에 SPK_i를 포함한 블록을 생성하고 트랜잭션 해시값인 $H(RTx_i)$를 Sensor node로 전송한다. Sensor node, Cluster head, Gateway는 $H(RTx_i)$를 저장한다.

3. Authentication Protocol

Sensor node는 난수 SR_i를 생성하여 $SID_i \oplus SR_i$, $SSK_i \oplus SR_i$, $SR_i \oplus CSK_j$를 Cluster head로 전송한다. Cluster head는 자신의 CSK_j를 이용하여 XOR 연산 후 SR_i를 추출한다. SR_i를 이용하여 SID_i, SSK_i를 계산하고 같은 ID, Key 세트가 맞다면 난수 CR_j를 생성한다.

Cluster head는 Sensor node로 $SR_i \oplus H(RTx_i)$, $CR_j \oplus CSK_j$를 전송한다. Sensor node는 $H(RTx_i)$를 이용하여 SR_i를 추출하고 자신이 전송한 난수가 맞다면 Cluster head를 인증한다. 그리고 CSK_j를 이용하여 CR_j를 계산한다.

Sensor node는 비밀키로 Data를 암호화하여 트랜잭션 생성 후, $DTx_i\{E_{SPK_i}(Data)\} \oplus CR_j$, $CR_j \oplus H(RTx_i)$를 Cluster head로 전송한다. Cluster head는 $H(RTx_i)$를 이용한 XOR 연산으로 CR_j를 계산하고 이 값이 자신이 전송한 난수와 동일하다면 Sensor node를 인증한다.

Cluster head는 난수 CR_j^*를 생성하고 Gateway로

$CID_j \oplus CR_j^*$, $CSK_j \oplus CR_j^*$, $CR_j^* \oplus GSK$ 를 전송한다. Gateway는 GSK로 CR_j^*를 추출한 뒤, CID_j, CSK_j를 계산하고 해당 두 값이 같은 ID, Key 세트가 맞다면 난수 GR를 생성한다.

Gateway가 $CR_j^* \oplus H(RTx_i)$, $GR \oplus H(RTx_i)$를 전송하고, 이를 수신한 Cluster head는 $H(RTx_i)$에 의해 추출한 CR_j^*가 자신의 난수가 맞다면 Gateway를 인증한다. Cluster head는 $GR \oplus CR_j^*$, $CR_j \oplus GR$, $DTx_i\{E_{SPK_i}(Data)\} \oplus CR_j$를 Gateway로 전송한다.

Gateway는 CR_j^*를 이용하여 자신이 전송한 난수 GR을 추출하여 Cluster head를 인증하고 XOR 연산을 통하여 $DTx_i\{E_{SPK_i}(Data)\}$, CR_j를 도출한다. 그리고 블록체인 시스템에서 $H(RTx_i)$에 이용하여 블록을 로드하고, 해당 블록에서 SPK_i를 추출한 뒤 $E_{SPK_i}(Data)$를 복호화하여 Data를 추출한다.

IV. Security Analysis

1. Mutual Authentication

Sensor node와 Cluster head, Gateway와 Cluster head 간의 Insecure area에서는 상호 전송한 자신의 난수를 수신하여 확인함으로써 정당한 통신 대상임을 확인한다. 각 난수는 세션키에 의한 XOR 연산 처리되므로 공격자들에게 노출되지 않는다.

Sensor node는 SR_i을 해시 처리한 뒤 Cluster head로 전송한다. Cluster head는 생성한 CR_j 및 SR_i을 Sensor node로 전송한 뒤 CR_j을 재수신하면 상호 간 인증을 완료한다.

그리고 Cluster head는 CR_j^*를 생성하여 Gateway에 전송한다. Gateway는 생성한 GR과 CR_j^*을 해시 처리하여 Cluster head로 전송한 뒤 자신의 난수를 재수신하면 상호 간 인증이 완료된다.

또한, 본 상호 인증 방법에서는 대칭키 및 공개키 알고리즘 등의 암호화 방법을 배제하고 XOR 연산을 이용한 경량 기법을 적용함으로써 저성능 장치에서도 저비용으로 상호 인증 기능을 적용한다.

2. Non-Repudiation

각 Sensor node는 개인키를 이용하여 트랜잭션 데이터를 Signing하고 해당 서명 값과 데이터를 포함하여 블록체인 트랜잭션 $DTx_i\{E_{SPK_i}(Data)\}$을 발생시킨다. 각 Sensor node만이 자신의 개인키로 트랜잭션 발생시키기 때문에 부인 방지 기능을 확보할 수 있다.

3. Man-in-the-middle Attack

Sensor node, Cluster head 및 Gateway는 모든 트랜잭션 및 데이터를 암호화하여 전송한다. 각 통신 대상자들의 비밀키, 세션키 등은 난수와의 XOR 연산에 의하여 노출되지 않고 각 연산 값은 매회 변경되기 때문에 공격자는 송신 데이터의 내용을 확인 불가하여 공격을 수행할 수 없다.

4. Reply Attack

Sensor node, Cluster head 및 Gateway는 데이터 전송 시 일회성 난수를 각자 생성하여 전송할 데이터와 XOR 연산 처리하여 전송한다. 따라서 공격자는 도청한 데이터를 재사용하여 공격을 시도하더라도 매 세션마다 통신 데이터는 변경되기 때문에 해당 공격은 차단된다.

5. DDoS Attack

Gateway는 Cluster head에 의하여 상호 인증된 Sensor node들의 트랜잭션만 수신할 수 있으므로 공격자의 무작위 트랜잭션 공격을 원천 차단한다. 그리고 Cluster head 간에도 상호 인증을 수행하기 때문에, 공격자가 트랜잭션을 반복적으로 발생시켜 Gateway가 공개키 및 대칭키 알고리즘 기반의 복호화 연산을 반복하여 시스템이 무력화되는 DDoS 공격을 효과적으로 차단한다.

6. Location Tracking Attack

Sensor node, Cluster head 및 Gateway는 데이터 전송 시 각자의 일회성 난수 SR_i, CR_j, GR를 이용하여 전송할 데이터를 XOR 연산 처리한 뒤 전달하기 때문에 통신 데이터는 매 세션마다 변경된다. 따라서 동일 또는 유사 패턴의 데이터 송신 및 수신을 추적하는 위치 추적 공격을 차단할 수 있다.

Table 2. Security Comparision

	Proposed	[2]
Mutual Authentication	SAFE	UNSAFE
Man-in-the-middle Attack	SAFE	UNSAFE
Reply Attack	SAFE	UNSAFE
DDoS Attack	SAFE	UNSAFE
Location Tracking Attack	SAFE	SAFE
Non-Repudiation	SAFE	SAFE

V. Conclusions

본 논문에서 제안하는 블록체인 기반 IoT 인증 기법은 저성능 IoT 장치에서 원활히 인증 기능을 수행할 수 있도록 공개키

및 대칭키 암호화 알고리즘 연산을 최소화하고 경량 암호 방식을 적용하여 저성능 장치를 활용하기에 용이하다. 그리고 IoT 시스템에 대한 DDoS 공격을 차단하기 위하여 Sensor node, Cluster head 및 Gateway 간 상호 인증 후에 Gateway로 트랜잭션을 발생시킴으로써 공격자의 무작위 서버 공격을 원천 차단한다. 또한, Sensor 노드는 자신의 비밀키를 이용하여 데이터를 암호화하여 전송하고 Gateway는 해당 트랜잭션에 대응하는 비밀키를 블록에서 추출하여 암호화된 데이터를 복호화한다. 그러므로 공격자는 암호화된 데이터를 획득하더라도 이를 복호화하여 원문을 획득할 수 없다.

본 논문에서 제안한 블록체인 기반 IoT 인증 기법을 활용함으로써, 저성능 장치가 연동되는 IoT 환경에서 시스템의 가용성, 데이터 기밀성 및 무결성을 확보할 수 있으며 CA를 제거하여 시스템 구조를 단순화 시킬 수 있는 이점이 있다. 향후 연구로써 본 제안 방법을 적용하여 실제 애플리케이션에서의 보안성 및 성능을 분석할 예정이다.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, 2008.

[2] B. Park, T. Lee, and J. Kwak, "Blockchain-Based IoT Device Authentication Scheme," Journal of The Korea Institute of Information of Information Security & Cryptology, Vol. 27, No. 2, Apr. 2017.

[3] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications," International Journal of Distributed Sensor Networks, Vol. 14, 2014.

[4] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," M.Sc. Thesis, University of Guelph, Canada, June 2016.

[5] V. Buterin, "A next-generation smart contract and decentralized application platform," White paper, 2014.

[6] D. Kim, and J. Kwak, "Design of Improved Authentication Protocol for Sensor Networks in IoT Environment," Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 2, Apr. 2015.

[7] W. Choi, S. Kim, Y. Kim, Y. Park, and K. Ahn, "PUF-based encryption processor for the RFID systems," 2010 IEEE 10th International Conference on Computer and Information Technology, pp. 2323-2328, United Kingdom, Jun.-Jul. 2010.

[8] J. Park, S. Shin, and N. Kang, "Mutual Authentication and Key Agreement Scheme between Lightweight Devices in Internet of Things," The Journal of Korean of Communications and Information Sciences, Vol. 38B, No. 09, 2013.

[9] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, "Low-Cost Elliptic Curve Cryptography for Wireless Sensor Networks," Proceedings of Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks, 2006.

[10] D. Duc, and K. Kim, "Defending RFID authentication protocols and against DoS attacks," Computer Communications, Journal of Computer Communications, 2011.

[11] W. Choi, S. Kim, Y. Kim, T. Yun, K. Ahn, and K. Han, "Design of PUF-based Encryption Processor and Mutual Authentication Protocol for Low-Cost RFID Authentication," The Journal of Korean Institute of Communications and Information Sciences, Vol. 39B, No. 12, Dec. 2014.

[12] M. Stamp, Information Security Textbook(Principles and Practice) 1st Ed., NY: John Willey & Sons Inc., 2005.

[13] P. Gope, J. Lee, and T. Quek, "Lightweight and Practical Anonymous Authentication Protocol for RFID Systems Using Physically Unclonable Functions," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 13, No. 11, Nov. 2018.

Authors

Wonseok Choi received the B.S. degree in Computer Engineering from Andong National University, Korea in 2007. And M.S. degree in School of Electrical Engineering and Computer Science from Kyungpook National University, Korea, in 2011, respectively He is interested in Security, Blockchain systems, IoT, and Embedded systems.

Sungsoo Kim received the B.S. degree in Computer Engineering from Kumoh National Institute of Technology, Korea in 2002. M.S. and Ph.D. degrees in School of Computer Science and Engineering from Kyungpook National University, Korea, in 2005, and 2012, respectively He is currently a Professor in the Department of Aeronautical Software Engineering, Kyungwoon University. He is interested in Embedded systems, RFID, and Security.