JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 1, pp. 87-92, January 2020
https://doi.org/10.9708/jksci.2020.25.01.087

Blockchain-based Lightweight Mutual Authentication Protocol for IoT Systems

Wonseok Choi*, Sungsoo Kim**, Kijun Han*

*Ph.D candidate, School of Computer Science and Engineering, Kyungpook National University, Daegu, Korea
**Professor, Department of Aeronautical Software Engineering, Kyungwoon University, Gumi, Korea
*Professor, School of Computer Science and Engineering, Kyungpook National University, Daegu, Korea

[Abstract]

Various devices, which are powerful computer and low-performance sensors, is connected to IoT network. Accordingly, applying mutual authentication for devices and data encryption method are essential since illegal attacks are existing on the network. But cryptographic methods such as symmetric key and public key algorithms, hash function are not appropriate to low-performance devices. Therefore, this paper proposes blockchain-based lightweight IoT mutual authentication protocol for the low-performance devices.

▸ **Key words**: IoT, Lightweight Authentication Protocol, Blockchain, Security, Cryptography

[요 약]

IoT 네트워크 환경에서는 서버 등의 고성능 장치부터 각종 센서, 수동형 RFID 등 저사양 장치까지 다수의 여러 장치들이 연결되어 있다. 그렇기에 불법적인 공격에 노출되어 있으며 데이터를 암호화하여 통신을 수행하여야 한다. 암호화 알고리즘으로 대칭키, 공개키 암호화 및 해시 기법 등을 사용할 수 있으나 저성능 IoT 디바이스는 암호화 프로세스를 처리하기에는 적합하지 않는 하드웨어 성능을 가지고 있어 이러한 방법을 채택할 수 없는 경우가 발생한다. 본 논문에서는 블록체인 시스템과 연동한 경량 상호 인증 프로토콜을 적용하여 IoT 환경에서 저성능 단말장치의 안전한 통신을 보장하는 인증 기법을 제안한다.

▸ **주제어** : 사물인터넷, 경량 인증 프로토콜, 블록체인, 보안, 암호

• First Author: Wonseok Choi, Co-Author: Sungsoo Kim, Corresponding Author: Kijun Han
*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
*Kijun Han (kjhan@knu.ac.kr), School of Computer Science and Engineering, Kyungpook National University
• Received: 2019. 11. 18, Revised: 2020. 01. 13, Accepted: 2020. 01. 14.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

5G 무선 통신 서비스가 시작되었으며 현재는 서비스 영역이 한정적이지만 점차 그 서비스 가능 영역이 확산되고 있다. 이와 같은 대용량의 빠른 무선 통신이 가능한 네트워크가 구축됨으로써 해당 네트워크에서 운용될 서비스들도 함께 발전할 것인데 민간 및 산업 분야에서 활용되고 있는 IoT 기술과 서비스는 더욱 다양한 분야에 적용되고 발전할 것으로 예상된다. IoT 네트워크에서는 수동형 RFID 태그, 온도나 진동 등을 모니터링할 수 있는 센서류 등 수 많은 다양한 저성능 단말 장치들이 연결되는데 장치의 하드웨어 성능 제한에 의하여 데이터의 암호 처리 프로세스 처리에 부적합하여 불법적인 외부 공격에 노출되어 있다.

저성능 장치들에 대한 불법적인 공격을 해소하기 위한 기존 연구들로써, ECC(Elliptic Curver Cryptography) 암호화 프로세서의 경량화 방법[9]과 IoT 환경을 구성하는 초경량 센서 대상의 인증 및 키 공유 방법[8]이 제안되었다. 또한 블록체인을 이용하여 통신 대상을 인증하여 통신을 수행하는 IoT 인증 기법이 제안되었다[5][10][15].

블록체인이란, 분산된 노드들 간의 합의에 의해 데이터를 블록화하여 생성하고 동일한 블록체인 데이터를 동기화하는 분산 원장 기술이다. 합의 알고리즘에 의한 데이터 무결성에 강한 특성 때문에 IoT 인증 기술에 이용하는 사례가 늘어가고 있다. 블록체인에 특정 데이터를 기록하기 위해서, 단말 장치는 트랜잭션 발생시켜야 하는데, 이 때 전자 서명 알고리즘을 이용하여 서명 작업을 수행하여야 하고 데이터 암호화도 필요할 수 있다. 저성능 센서의 경우, 전자 서명 및 데이터 암복호화 작업을 수행하기에 적합하지 않다.

본 논문에서는, 저성능 단말 장치에서 동작 가능한 블록체인 기반의 경량 상호 인증 프로토콜을 제안한다. Sensor Node에서는 난수를 이용하여 상호 인증을 수행하고 Cluster Head에서 Sensor Node들의 ID를 그룹화시켜 Gateway 상의 블록체인에 저장되어 있는 Sensor Node ID와 비교하여 인증함으로써, 저성능 단말 장치 대상으로 블록체인 기반 상호 인증을 가능케 하였다.

2장에서는 기존에 제안되었던 IoT 인증 방법과 블록체인을 이용한 연구를 설명하고 3장에서는 본 논문에서 제안하는 경량 IoT 상호 인증 기법을 기술한다. 4장에서 본 제안 기법의 안전성 및 성능 분석을 제시하고 5장에서 연구 결과와 향후 계획을 기술하며 결론을 맺는다.

II. Related Works

본 장에서는 블록체인 기술 및 기존에 연구되었던 블록체인 기반 인증과 경량 IoT 인증 기법을 소개한다.

블록체인은 트랜잭션에 의하여 발생된 데이터를 합의 알고리즘으로 확정하고 블록 단위로 그룹화 시켜, 블록 간에 블록의 해시 값으로 연결시킴으로써 데이터 무결성을 확보하는 분산 원장 기술이다. 블록체인 기술을 화폐 시스템으로 적용한 사례로써, 비트코인 및 이더리움 등이 있으며 프라이빗 블록체인으로 하이퍼레저 등의 시스템이 있다[2][16][17].

Omar 등은 블록체인 기반의 헬스케어 데이터 관리 시스템을 제안하였다[10]. 사용자의 ID에 대응되는 데이터를 블록체인에 기록하는 프로토콜, 그리고 트랜잭션 ID를 이용하여 사용자의 데이터 획득하는 프로토콜 2가지로 구분된다. 해당 프로토콜의 취약점으로써 사용자 ID와 데이터, 트랜잭션 ID가 노출된다.

Lee는 블록체인 기술을 신원 인증 도구로 이용한 연구로써 모바일 사용자에 대한 인증 시스템을 제안하였다[15]. BIDaaS(Blockchain Based ID As a Service) provider가 모바일 사용자의 가상 ID 및 공개키를 블록체인 시스템에 저장하면, 모바일 사용자가 파트너 사로 인증(로그인) 요청 시 블록체인 시스템에서 해당 모바일 사용자의 가상 ID를 조회하여 인증 여부를 결정할 수 있다. 프라이빗 블록체인을 적용한 사례이기 때문에 프로토콜 상에서 통신 대상 간 상호 인증에 대한 부분은 적용되어 있지 않다.

Park 등은 LWIG 워킹 그룹에서 정의한 Class 0에 해당하는 초경량 센서에 적용될 수 있는 인증 및 키 공유 방법을 제시하였다[8]. 통신 대상 간 상호 인증 후 대칭키를 생성하여 공유하고 해당 키를 이용하여 데이터를 암호화한 뒤 송수신한다. 그러나 상호 인증 전에 인증 개시자의 ID 및 난수, 응답자의 ID가 공개되어 암호화된 데이터의 패턴 분석 공격에 노출되어 있다.

Kim 등은 Porambage 등이 제안한 IoT 환경 상에서의 센서 네트워크 인증 프로토콜을 개선하였다[6]. 인증 프로토콜은 등록 및 인증 단계로 구성되어 있는데, 인증 단계에서 클라이언트 센서 노드는 서버 센서 노드와 인증 기관으로 대체 식별자 및 메시지 인증 코드를 전송하기에 공격자들에게 노출되어 중간자 공격 및 패턴 분석 공격 등에 취약할 수 있다.

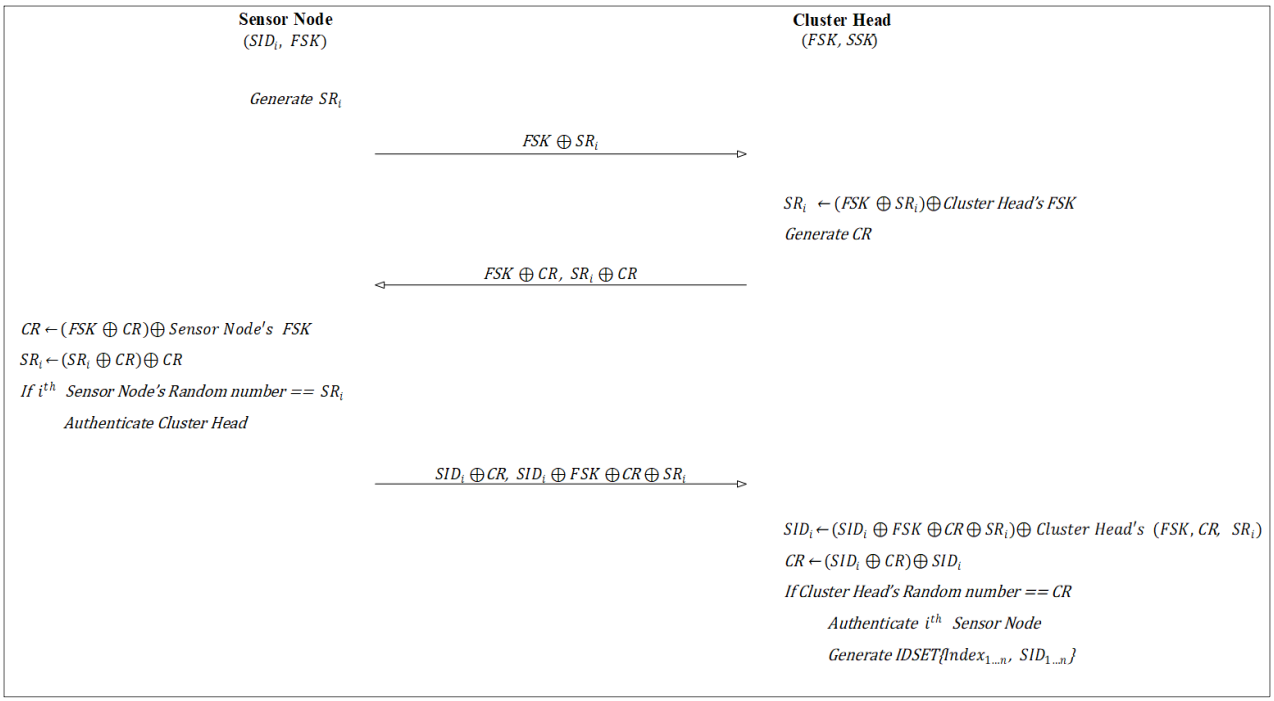


Fig. 1. "Sensor Node-Cluster Head" Authentication Process

III. Proposed Protocol

본 논문에서 제안하는 프로토콜은 Registration phase와 Authentication phase로 구분된다. Registration phase에서는 Sensor node들의 각 ID가 Gateway 상의 블록체인에 등록되고 Authentication phase에서는 Sensor node, Cluster head, Gateway 간의 인증 프로세스가 진행된다. 블록체인 트랜잭션 발생 시 디지털 서명에 사용되는 개인키, 공개키 쌍은 본 제안 프로토콜에서는 별도로 기술하지 않는다.

1. Registration Phase

Table 1. Notations

Notation	Description
SID_i	Identifier of sensor node i
SR_i	Sensor node's random number
FSK	Secret key between sensor node and cluster head
CR	Cluster head's random number
SSK	Secret key between cluster head and gateway
GR	Gateway's random number
$IDSET$	Set of all sensor node's IDs
$Tx\{Data\}$	Blockchain transaction with data
$E_{key}(Data)$	Encrypted data by key

Gateway 상에 구축된 블록체인에 Sensor node들의 ID를 저장하기 위하여, Cluster head는 Sensor node들로부터 ID를 수신한다. Cluster head는 ID들을 그룹화하여 $IDSET$을 생성하고, 트랜잭션에 첨부하여 Gateway로 전송한다. Gateway는 수신 받은 $IDSET$을 블록체인 시스템에 저장한다. 제안하는 IoT 시스템에서 다수의 Gateway 상에 구성된 블록체인 네트워크는 합의 알고리즘을 이용하여 인증 데이터의 무결성을 확보한다.

2. "Sensor Node-Cluster Head" Authentication Phase

Sensor node는 난수 SR_i을 생성하여 Cluster head에게 $FSK \oplus SR_i$을 전송한다. Cluster head는 자신의 FSK를 이용하여 XOR 연산을 취하여 SR_i를 획득한다. 그리고 난수 CR을 생성하여 Sensor node에게 $FSK \oplus CR, SR_i \oplus CR$을 전송한다. Sensor node는 자신의 FSK를 이용하여 XOR 연산을 수행 후 CR를 계산하고 이를 이용하여 SR를 도출한다. 계산한 SR이 Sensor node가 전송하였던 난수와 동일하다면 Cluster head를 인증하고 $SID_i \oplus CR, SID_i \oplus FSK \oplus CR \oplus SR_i$를 Cluster head로 전송한다.

Cluster head는 자신의 FSK, CR, SR_i로 XOR 연산을 수행하여 SID_i를 도출한 뒤 $(SID_i \oplus CR) \oplus SID_i$ 연산으

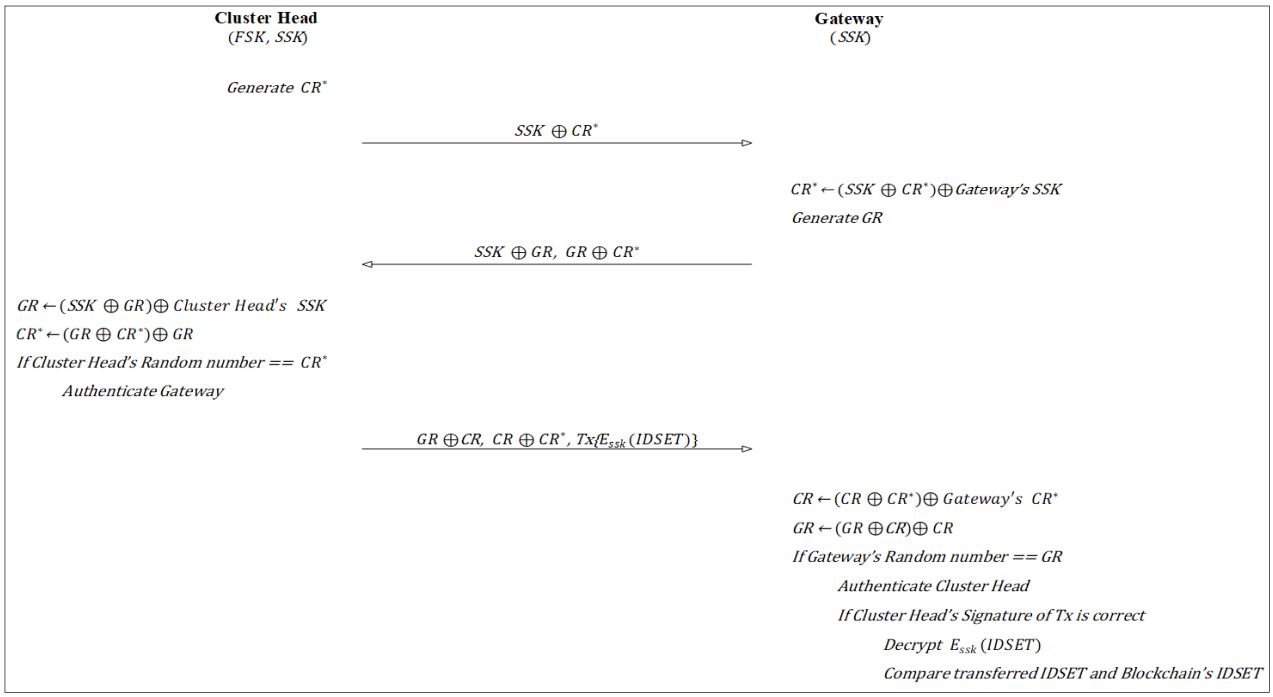


Fig. 2. "Cluster Head-Gateway" Authentication Process

로 CR를 획득한다. 해당 값이 자신이 생성했던 난수와 동일하다면 Sensor node를 인증한다. Cluster head는 인증된 Sensor node들의 SID들을 그룹화 시켜 $IDSET$을 생성한 뒤 Gateway와의 인증 단계로 진입한다.

3. "Cluster Head-Gateway" Authentication Phase

Cluster head가 난수 CR^*을 생성한 뒤$SSK \oplus CR^*$을 전송하면 이를 수신한 Gateway는 자신의 SSK를 이용하여 CR^*을 계산한다. 그리고 난수 GR을 생성한 뒤 Cluster head로 $SSK \oplus GR, GR \oplus CR^*$을 전송한다.

Cluster head는 자신의 SSK로 XOR 연산을 취하여 GR을 도출하고 $(GR \oplus CR^*) \oplus GR$을 수행하여 CR^*을 획득한다. 해당 값이 자신의 생성한 난수와 동일하다면 Gateway를 인증하고 $GR \oplus CR, CR \oplus CR^*, Tx\{E_{ssk}(IDSET)\}$을 전송한다.

Gateway는 자신의 CR^*을 이용하여 CR을 획득하고 $(GR \oplus CR) \oplus CR$ 연산을 수행하여 GR을 도출한다. 이 값이 자신이 생성한 난수와 동일하다면 Cluster head를 인증하고 트랜잭션의 서명을 확인한 뒤 암호화된 $IDSET$를 복호화한다. Gateway는 복호화한 $IDSET$을 블록체인에 저장되어 있는 $IDSET$과 비교하여 Sensor node들의 ID가 동일한지 검증하여 인증을 완료한다.

IV. Security Analysis

본 논문에서 제안한 프로토콜의 안전성과 성능을 기존 연구와 비교 분석한다. Table 2에서는 도청공격, 중간자 공격, 재전송 공격, 위치 추적, 상호인증, 부인 방지에 대하여 제안 기법과 기존 연구들을 비교한 결과이며 제안 프로토콜은 기술된 6가지 공격에 대하여 안전함을 확인할 수 있다.

Table 3은 제안 프로토콜과 IoT 인증 프로토콜인 [6]과의 연산량을 비교 분석한 결과이다. [6]에서는 MAC(Message Authentication Code) 생성, Hash 등 고비용의 연산이 포함되어 있으며 클라이언트인 Sensor node에서도 해당 연산이 수행된다. 제안 프로토콜은 주로 저비용의 XOR 연산으로 구성되어 있고, Sensor node에 대하여 OTP(One-Time Pad) 기법[18]으로써 일회성 난수 생성 및 XOR 연산을 수행하여 보안성을 확보한다. 암호화 및 전자 서명 연산은 Sensor node가 아닌 Cluster head에서 수행된다.

1. Eavesdropping Attack

Sensor node, Cluster head, Gateway는 ID, 난수, 비밀키, 트랜잭션 및 데이터를 단일 값으로 노출시키지 않으며 난수와의 XOR 연산, 암호화 연산 후 전송하기 때문에 도청 공격에 안전하다.

2. Man-in-the-middle Attack

Sensor node, Cluster head, Gateway는 상호 인증 시에 비밀키와 난수를 XOR 연산 후 전송한다. 또한 Sensor node의 ID를 전송 시에도 난수와의 XOR 연산을 하고, 트랜잭션 값도 $IDSET$의 조합이 매번 변경되어 암호화 되기 때문에 공격자가 통신 데이터를 불법적으로 취득하더라도 단일 값 분석이 불가능하여 공격에 사용할 수 없다.

Table 2. Security Comparision **(O: Safe, X: Unsafe)**

	Our	[6]	[8]	[10]	[15]
Eavesdropping Attack	O	X	X	X	X
Man-in-the-middle Attack	O	O	X	X	X
Reply Attack	O	O	O	X	O
Location Tracking Attack	O	O	X	X	X
Mutual Authentication	O	X	X	X	X
Non-Repudiation	O	X	X	O	O

Table 3. Performance Analysis

		Our	[6]
Sensor Node (Client)	Random Number Generation	1	1
	XOR Operation	9	1
	MAC(Message Authentication Code) Generation	-	2
	Hash	-	3
Cluster Head (Server)	Random Number Generation	2	2
	XOR Operation	19	1
	MAC(Message Authentication Code) Generation	-	2
	Hash	-	2
	Encryption	1	-
	Digital Signature	1	-
Gateway (Certificate Authority)	Random Number Generation	1	2
	XOR Operation	8	4

3. Reply Attack

매 세션마다 갱신되는 난수를 이용하여 전송 데이터를 XOR 연산 후 전송하기 때문에 공격자는 통신 데이터를 가로채어 다음 세션에 재전송 하더라도 난수 값은 이미 변경되었으므로 해당 공격은 차단된다.

4. Location Tracking Attack

매 세션마다 난수를 갱신되어 데이터의 경량 암호에 사용되므로 기존 세션과 다른 출력 값을 가진다. 그리고 Sensor node, Cluster head, Gateway는 자신의 난수, 비밀키, ID, 트랜잭션을 단독으로 전송하지 않고 계산된 값은 매번 변경되기 때문에 위치 추적 공격에 안전하다.

5. Mutual Authentication

Sensor node와 Cluster head, Cluster head와 Gateway는 상호 간 공유된 비밀키를 이용하여 자신의 난수를 상대방이 올바르게 재전송하는 것을 이용하여 상호 인증을 수행한다. XOR 연산을 이용하기 때문에 연산 비용이 적어 저성능 장치 적용에 적합하고 연산 처리 시간이 빠르다.

6. Non-Repudiation

Cluster head는 인증된 Sensor 노드들의 ID로부터 $IDSET$을 생성하고 자신의 개인키로 트랜잭션을 발생시킨다. 또한 Gateway는 인증된 Cluster head로부터 트랜잭션을 수신하여 서명을 검증하고 $IDSET$을 복호화한 후 블록체인에 저장된 값과 비교하여 인증을 수행함으로써 부인 방지를 확보한다.

V. Conclusions

IoT 네트워크 상의 다양한 장치들이 연결되는 특성 상 기기 인증 및 데이터 암호화는 필수적이다. 이에 본 논문에서는 IoT 네트워크 상의 저성능 Sensor node 인증 작업 수행 시 Cluster Head가 경량 상호 인증이 완료된 Sensor node ID들을 그룹화하여 블록체인에 등록 및 검증하는 방법으로써 저성능 IoT 기기의 인증 기법을 제안하였다.

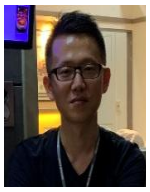
PKI(Public Key Infrastructure) 구성과 다르게 별도의 인증 기관 없이 Gateway 상에 블록체인 플랫폼을 구성하여 IoT 인증 기능을 수행함으로써 IoT 인증 시스템의 탈중앙화, 인증 데이터의 무결성을 확보할 수 있다. 또한, 안전성 분석 내용을 살펴보면 Sensor node에서는 경량 연산만을 이용하여 인증 기능을 수행하기에 저성능 기기적용에 적합함을 확인할 수 있다. 추가적인 연구로써 Sensor node ID 등록 및 검증 트랜잭션에 대한 블록체인 성능 시험 및 평가 연구를 진행할 계획이다.

REFERENCES

[1] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system

for IoT," Computers & Security, Vol. 78, Sep. 2018.
[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, 2008.
[3] 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.
[4] 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.
[5] A. Moinet, B. Darties, and J. L. Baril, "Blockchain based trust & authentication for decentralized sensor networks," arXiv preprint arXiv:1706.01730, 2017.
[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] A. A. Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data," International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, 2018.
[11] D. Duc, and K. Kim, "Defending RFID authentication protocols and against DoS attacks," Computer Communications, Journal of Computer Communications, 2011.
[12] 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.
[13] M. Stamp, Information Security Textbook(Principles and Practice) 1st Ed., NY: John Willey & Sons Inc., 2005.
[14] 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.
[15] J. Lee, "BIDaas: Blockchain Based ID As a Service," IEEE Access, Vol. 6, 2018.
[16] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," M.Sc. Thesis, University of Guelph, Canada, June 2016.
[17] V. Buterin, "A next-generation smart contract and decentralized application platform," White paper, 2014.
[18] C. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, 1949.

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 currently taking PhD course in Computer Science and Engineering from Kyungpook National University. 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.

Kijun Han received the B.S. degree in Electrical Engineering from Seoul National University, Korea, in 1979. M.S. degree in Electrical Engineering from KAIST, Korea, in 1981, and M.S. and Ph.D. degrees in Computer Engineering from University of Arizona, USA in 1985 and 1987, respectively. He is currently a Professor in School of Computer Science and Engineering, Kyungpook National University. He is interested in Network systems, IoT, and Wireless sensor network.