Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.731

포그 기반 IoT 환경의 분산 신뢰 관리 시스템*

오 정 민,[1†] 김 승 주[2‡]
[1,2]고려대학교 정보보호대학원 (대학원생, 교수)

Distributed Trust Management for Fog Based IoT Environment*

Jungmin Oh,[1†] Seungjoo Kim[2‡]
[1,2]ICSP(Institute of Cyber Security & Privacy) School of Cybersecurity,
Korea University (Graduate student, Professor)

요 약

사물인터넷은 웨어러블 디바이스, 스마트폰 등의 많은 기기들이 통신하는 거대한 집단으로 네트워크 내 사물의 상호 연결은 기본적인 요구사항이다. 악성 기기와의 통신은 네트워크와 서비스를 악의적으로 손상시켜 품질에 영향을 줄 수 있기 때문에 신뢰할 수 있는 기기를 선택하는 것은 매우 중요하다. 그러나 IoT 기기의 이동성과 자원의 제약으로 신뢰 관리 모델을 만드는 것은 쉽지 않다. 중앙 집중 방식의 경우 독점 운영 및 단일 장애 지점, 기기 증가에 따른 자원 확장의 이슈가 있다. 분산 처리 방식은 기기가 서로 연결된 구조로 별도의 장비 추가 없이도 시스템을 확장 할 수 있으나, IoT 기기의 제한된 자원으로 데이터 교환 및 저장에 한계가 있으며 정보의 일관성을 보장하기 어렵다. 최근에는 포그 노드와 블록체인을 사용하는 신뢰 관리 모델이 제안되고 있다. 그러나 블록체인은 낮은 처리량과 속도 지연의 문제를 가지고 있어 동적으로 변화하는 IoT 환경에 적용하기 위해서는 개선이 필요하다. 따라서 본 논문에서는 사물인터넷을 위한 블록체인 기술인 IOTA를 적용하여 포그 기반 IoT 환경에서 신뢰할 수 있는 기기를 선택하기 위한 신뢰 관리 모델을 제안한다. 제안된 모델에서는 DAG(Directed Acyclic Graph) 기반 원장 구조를 통하여 신뢰 데이터를 위/변조 없이 관리하고 블록체인의 낮은 처리량과 확장성 문제를 개선한다.

ABSTRACT

The Internet of Things is a huge group of devices communicating each other and the interconnection of objects in the network is a basic requirement. Choosing a reliable device is critical because malicious devices can compromise networks and services. However, it is difficult to create a trust management model due to the mobility and resource constraints of IoT devices. For the centralized approach, there are issues of single point of failure and resource expansion and for the distributed approach, it allows to expand network without additional equipment by interconnecting each other, but it has limitations in data exchange and storage with limited resources and is difficult to ensure consistency. Recently, trust management models using fog nodes and blockchain have been proposed. However, blockchain has problems of low throughput and delay. Therefore, in this paper, a trust management model for selecting reliable devices in a fog-based IoT environment is proposed by applying IOTA, a blockchain technology for the Internet of Things. In this model, Directed Acyclic Graph-based ledger structure manages trust data without falsification and improves the low throughput and scalability problems of blockchain.

Keywords: Fog computing, IoT(Internet of Things), Trust management, Blockchain, Scabaility

Received(04. 12. 2021), Modified(06. 07. 2021), Accepted(07. 02. 2021)

* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술평가원의 지원을 받아 수행된 연구임 (No.2018-0-00532, 고등급(EAL6 이상) 보안 마이크로커널 개발)

† 주저자, jungmin48@gmail.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

I. 서 론

사물인터넷(Internet of Things)은 웨어러블 디바이스, 스마트 폰과 같이 무수히 많은 기기들이 종류에 관계없이 상호작용할 수 있는 거대한 집단이다. 사물인터넷은 인공지능(AI)의 발전으로 점점 더 자동화되고, 5G와 같은 빠른 무선 기술의 개발과 함께 사람들의 생활을 더욱 편리하게 만들어 주고 있다[1-3]. 네트워크에 연결된 IoT 기기는 2025년까지 전 세계적으로 250억 개를 넘어설 것으로 예상되며, 이때 인구는 약 80억 명으로 추산된다. 이는 개인 평균 12개 이상의 IoT 기기를 소유하거나 사용한다는 의미이다[4]. 이러한 스마트 기기들은 인간의 삶에 대한 데이터를 모니터링하고 수집할 수 있으며, 수집된 데이터를 집계, 융합, 처리 및 분석하여 다양한 서비스를 제공할 수 있도록 한다. 최근에는 스마트 의료, 스마트 팩토리와 같이 다양한 분야에서 IoT 기기를 활용하고 있으며, 이러한 서비스들을 통해 사물인터넷은 우리의 라이프 스타일을 획기적으로 변화시킬 것이다[5][6].

네트워크 내 기기의 상호 연결은 사물인터넷의 기본 요구 사항이다[7-9]. 그러나 현재 무수히 많은 기기가 생성되고 설치되고 있음에도 불구하고 실제로 연결되는 경우는 거의 없다. 이러한 이유로 사물인터넷의 폭발적인 성장에도 불구하고 스마트 라이프 시나리오는 여전히 해결해야 하는 과제가 많이 남아 있는 분야로 여겨지고 있다[10]. 사물인터넷은 각 장치가 다른 장치에 서비스를 요청하거나 제공할 수 있는 서비스 중심 아키텍처로 볼 수 있다. 만약 악성 기기와 통신을 하게 될 경우, 네트워크나 서비스를 악의적으로 손상시켜 서비스 품질에 영향을 줄 수 있기 때문에 신뢰할 수 있는 기기를 선택하는 것은 매우 중요하다. 그러나 안타깝게도 사물인터넷 환경은 거대한 크기의 네트워크, 기기의 이기종성과 이동성, 제한된 연산 자원과 저장 공간으로 인하여 신뢰 관리 모델을 만드는 것이 매우 어렵다. 또한 신뢰도 조작을 통한 기기 간 연결 제한 및 악성 서비스 제공자와의 연결과 같은 보안 문제 역시 IoT 기기의 신뢰 관리에서 해결해야 하는 중요한 과제이다.

일반적으로 신뢰 관리 시스템은 중앙 집중 방식과 분산 처리 방식으로 분류할 수 있다. 중앙 집중 방식은 모든 신뢰 데이터를 클라우드 서버와 같은 하나의 중앙 서버에 저장하고 처리한다. 이 방식은 일관된 정책 시행과 데이터 관리 측면에서 효율적일 수는 있으나 중앙 서버에 대한 단일 장애 지점(single point of failure)과 독점 운영의 문제가 발생할 수 있다. 또한 IoT 기기가 추가됨에 따라 서버의 자원에 대한 추가 확보 및 비용이 증가하게 된다. 반면에 분산 처리 방식의 경우 중앙 시스템이 필요하지 않고 기기 간의 연결로 시스템을 구축하기 때문에 별도의 장비 추가 없이도 새로운 IoT 기기가 시스템에 참여할 수 있다. 그러나 IoT 기기는 제한된 자원으로 인하여 시스템 내의 모든 노드와의 데이터 교환 및 저장을 수행하기가 어렵다는 단점이 있다. 최근 연구들에서는 IoT 기기의 신뢰 관리를 위해 포그 노드와 블록체인을 사용하는 모델들이 제안되고 있다. 신뢰 데이터의 저장과 처리를 포그 노드로 이관하여 IoT 기기의 자원 제약 문제를 해결하고, 포그 노드를 블록체인 네트워크에 참여 시켜 중앙 집중 방식의 문제를 해결한다. 그러나 블록체인은 데이터베이스의 일관성을 보장하기 위해 많은 시간이 요구되며, 그에 따라 처리량이 적기 때문에 IoT 기기가 생성하는 대량의 데이터를 처리하기에는 적합하지 않다. 블록체인을 통해 탈중앙화, 변조 방지 및 데이터 일관성의 요구사항을 만족한다고 해도 여전히 사물인터넷 환경에 적용하기에는 해결해야 할 문제가 남아 있다.

블록체인은 트랜잭션으로 구성된 블록이 체인 형태로 연결되어 저장되며, 블록이 이전 블록의 해시값을 포함함으로써 데이터의 불변성을 제공한다. 그러나 블록체인의 선형적인 구조로 인해 트랜잭션 수가 증가함에 따라 병목현상이 발생하게 되고, 이로 인해 체인에 추가되기까지 대기 시간이 증가한다. 이러한 문제를 개선하기 위해 방향성 비순환 그래프인 DAG 기반의 새로운 블록체인 모델들이 제안되었다. 이는 기존 체인 기반 모델이 한 번에 하나의 블록만 처리하는 순차적인 방식과는 다르게 동시에 여러 블록을 병렬로 처리하여 병목 현상을 해결하고 데이터가 추가되는 속도를 향상시킨다.

따라서 본 논문에서는 DAG 기반의 블록체인 모델을 사용하여 기존 블록체인 기반 솔루션의 문제점들을 개선하고, IoT 기기에 적합한 신뢰 관리 모델을 제안한다. 블록체인을 활용한 기존의 모델들의 경우 신뢰 관리 시스템에 대한 공격에 대해서는 제대로 고려하지 않고 일부 공격에 대해서만 고려되고 있다. 특히 포그 노드에 대한 신뢰는 프라이빗 블록체인을 사용하여 해결함으로써 탈중앙화 요구사항을 완전하게 달성하지 못한다. 이에 탈중앙화 목표를 달성하기 위하여 IOTA라는 퍼블릭 블록체인을 사용하여 시스템의 투명성과 공정성을 제공한다. 또한 기존 블록체

인의 선형 연결 방식이 아닌 DAG 구조를 사용함으로써 확장성을 개선한다. 이어지는 2장에서는 신뢰 관리 모델의 관련 연구를 살펴보고, 3장에서는 기존 연구를 분석하여 IoT 기기의 신뢰 관리 모델이 갖추어야 할 요구사항을 정의한다. 4장에서는 요구 사항을 충족하는 새로운 모델을 제안하며 5장에서는 제안된 모델이 앞서 정의한 요구사항을 만족하는지 분석한다. 마지막 6장에서는 전체 내용을 요약하며 논문을 마무리한다.

II. 관련 연구

최근 신뢰 관리 시스템에 관련된 연구에서는 포그 컴퓨팅과 블록체인을 적용하여 IoT 기기의 자원 제약의 문제와 분산 서버의 일관성 및 보안성 문제를 해결하려는 시도들이 많이 있다. 본 절에서는 이러한 신뢰 관리 시스템에 관련된 이전 연구를 살펴본다.

2.1 신뢰 관리 시스템

신뢰 관리는 다양한 종류의 기기가 다른 기기의 신뢰성에 대한 의견을 공유하고, 악성 기기와의 연결로 인한 오작동을 방지하도록 도와주는 역할을 한다. 그러나 기존의 인터넷 기반의 신뢰 관리 모델은 사물인터넷 환경에 적용하기에는 적합하지 않다. 이는 IoT 기기가 저 전력 및 저 용량으로 자원이 제한되어 있으며, 이기종간 이러한 제약사항이 다를 수 있기 때문이다. 일반 컴퓨터 시스템에 적합한 모델은 처리 및 저장 능력이 낮은 스마트 워치에서 동일한 성능으로 동작하지 않을 것이다[11][12]. 따라서 제한된 용량과 이기종성이라는 IoT 기기의 특성이 고려된 신뢰 관리 모델이 필요하다.

사물 인터넷은 기기 간에 서비스를 요청하거나 제공하는 서비스 중심 아키텍처로 볼 수 있다. 데이터를 안정적으로 전송하고, 서비스의 가용성에 대한 불확실성을 최소화하기 위해 서비스 제공자의 신뢰도를 효율적으로 평가하고 관리할 수 있어야 한다. 공격자는 악성 기기가 서비스 제공자로 선정되도록 다른 기기들과 공모하여 정직한 기기에 대한 부정적인 피드백을 제출하는 등의 악의적인 행동을 수행하여 시스템의 안정성과 정확성을 저해할 수 있다. 따라서 신뢰 관리 모델에서는 Bad mouthing attack, Bullet stuffing attack과 같은 신뢰 기반 공격에 대한 보호 방법이 함께 고려되어야 한다.

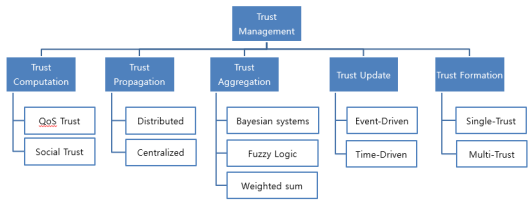


Fig. 1. 5 five design dimensions of trust system

효과적인 신뢰 관리를 위해서는 ①신뢰 구성(trust composition), ②신뢰 전파(trust propagation), ③신뢰 업데이트(trust update), ④신뢰 형성(trust formation), ⑤신뢰 집계(trust aggregation) 등의 설계 요소를 충족해야 한다[13]. 신뢰 구성에서는 신뢰도 계산에 필요한 속성을 결정한다. 이 정보는 서비스 품질(Quality of Service) 또는 사회 관계 정보일 수 있다. 신뢰 전파는 신뢰 값에 대한 연산과 저장이 어떻게 처리되는가에 따라 중앙 집중 방식과 분산 처리 방식으로 나눌 수 있다. 신뢰 업데이트는 신뢰 정보가 업데이트되는 빈도에 대한 것으로 이벤트 중심 또는 시간 중심 방식이 있다. 신뢰 형성은 신뢰 구성에서 결정된 신뢰 속성을 결합하는 방식으로 신뢰는 단일 속성 또는 다중 속성으로 형성될 수 있다. 마지막으로 신뢰 집계는 직접 상호작용을 통해 평가한 신뢰 데이터와 다른 기기로부터 제출된 데이터를 통합하는 방법으로 가중 합계, 베이지안 추론, 퍼지 로직, 회귀 분석 등이 사용된다.

앞서 설명한 것과 같이 신뢰 관리 시스템은 신뢰 전파 방식에 따라 중앙 집중 방식과 분산 처리 방식의 두 개의 그룹으로 분류할 수 있다. 중앙 집중 방식은 모든 신뢰 데이터를 클라우드 서버와 같은 하나의 중앙 서버에 저장하고 처리한다. 이 방식은 일관된 정책 시행과 데이터 관리 측면에서 효율적일 수는 있으나 중앙 서버에 대한 단일 장애 지점과 독점 운영의 문제가 발생할 수 있다. 또한 IoT 기기가 추가됨에 따라 서버 자원에 대한 추가 확보 및 비용이 증가하게 된다. 반면에 분산 처리 방식의 경우 중앙 시스템이 필요 하지 않

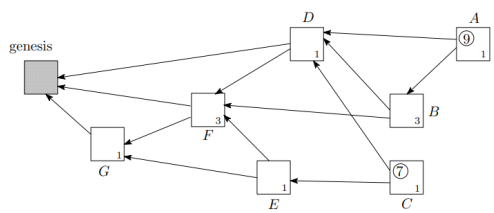


Fig. 2. Directed Acyclic Graph of IOTA[26]

고 기기 간의 연결로 시스템을 구축하기 때문에 별도의 장비 추가 없이도 새로운 IoT 기기가 시스템에 참여할 수 있다. 그러나 IoT 기기는 제한된 자원으로 인하여 시스템 내에 있는 다른 노드들과의 데이터 교환 및 저장에 한계가 있으며, 저장소가 분산되어 있기 때문에 일관된 정보를 제공하기가 어렵다는 단점이 있다. 이러한 문제점들을 개선하기 위하여 최근 연구들에서는 포그 노드와 블록체인을 사용하는 모델들이 제안되고 있다[14-17]. 신뢰 데이터의 저장과 처리를 포그 노드로 이관하여 IoT 기기의 자원 제약 문제를 해결하고, 포그 노드를 블록체인 네트워크에 참여 시켜 중앙 집중 방식의 문제를 해결한다.

2.2 DAG기반 블록체인(Blockchain)

중앙 집중 방식의 문제를 해결하기 위한 방안으로 블록체인이 유망한 솔루션으로 떠오르고 있다. 블록체인은 데이터를 여러 군데 나누어 저장하는 데이터 분산 처리 기술로 일정 주기에 따라 거래 내역을 정렬해 블록에 저장하고, 이 블록을 이전 블록들에 체인 형태로 연결한다[18]. 블록체인은 탈중앙화, 투명성, 불변성의 특징으로 다양한 분야에서 폭넓게 연구 및 적용되고 있다. 가장 대표적인 블록체인으로는 비트코인과 이더리움이 있다.

그러나 현재의 비트코인과 이더리움 시스템은 사용자가 크게 증가함에 따라 확장성의 문제를 겪고 있다. 특히 처리량과 지연은 사용자 경험에 중요한 영향을 미친다. 기존의 블록체인 네트워크는 현재의 블록이 전체 네트워크의 모든 노드들에 전파될 수 있도록 블록 크기(block size)와 블록 간격(block interval)을 제한한다. 이로 인해 초당 처리할 수 있는 트랜잭션 수에 제한이 있어 기존의 중앙 집중 방식에 비해 매우 낮은 수준의 처리량을 제공한다[23]. 예를 들어 비자카드는 초당 거래 처리량이 4,000TPS 이상인 반면, 비트코인은 7TPS, 이더움은 30TPS로 대규모 트랜잭션 처리가 필요한 시나리오를 만족시키기에는 어려움이 있다[24][25].

또한 기존의 블록체인 시스템은 사용자와 채굴자가 구분되어 있어 사용자가 자신의 트랜잭션을 블록에 포함시키기 위해서는 채굴자를 선출하여 검증하고 그 대가로 수수료를 지불한다. 그러나 네트워크를 통해 전송되는 거래의 수가 증가함에 따라 채굴자들은 가장 높은 수수료를 제공하는 거래를 선택하려 하고, 이로 인해 거래 비용이 급증하고 대기 시간이 길어지는 문제가 발생한다. 이러한 문제를 해결하기 위해 차세대 블록체인으로 DAG 구조를 기반으로 한 새로운 유형의 블록체인들이 제안되고 있다.

2.2.1 DAG(Directed Acyclic Graph)

블록체인을 사용하면 데이터가 체인 형태로 연결됨에 따라 저장된 데이터의 불변성과 추적 가능성이라는 이점을 얻을 수 있다. 그러나 선형적으로 연결되는 구조는 트랜잭션 처리량을 저하시킨다. 이러한 기존 블록체인 시스템의 낮은 처리량과 확장성 문제를 개선하기 위해 IOTA[26], Byteball[27], Nano[28] 등의 DAG 기반의 새로운 블록체인 모델이 제안되었다. DAG는 방향성 비순환 그래프로 연속으로 이어지는 방향성을 가진 네트워크 연결 방법을 말한다. DAG은 네트워크 내의 노드가 새 트랜잭션을 추가하려는 경우, 이 전에 생성된 두 개 이상의 다른 트랜잭션을 찾아 유효성을 검사하고 연결함으로써 전체 네트워크를 확장한다. 이러한 설계로 인해 네트워크에서 트랜잭션을 확인하는 역할이 기존 채굴자에서 네트워크의 각 노드로 이전된다[29]. 이는 블록 생성을 위한 리더 선출을 기다리지 않기 때문에 트랜잭션이 빠르게 확인될 수 있으며, 네트워크의 모든 노드가 트랜잭션을 확인하는 데 적극적으로 참여하도록 장려한다. 이로 인해 검증자에게 지불해야 할 수수료가 없어 실제 거래 수수료를 최저 수준으로 유지 할 수 있도록 도와준다[30][31].

이와 같이 DAG의 트랜잭션은 여러 곳에서 동시다발적으로 추가되기 때문에 속도가 빠르며, 사용자가 많아진다 해도 트랜잭션의 승인이 지연되거나 병목현상이 발생하지 않는다. 오히려, 사용자가 늘어 트랜잭션이 많아질수록 검증의 신뢰도와 속도는 증가한다. 다시 말해 DAG은 기존 블록체인 모델이 한 번에 하나의 블록만 처리하는 순차적인 방식과는 다르게 동시에 여러 블록을 병렬로 처리하여 병목 현상을 해결하고, 데이터가 추가되는 속도를 향상시킨다[32].

2.2.2 IOTA

IoT 기기는 매 밀리 초마다 엄청난 양의 데이터를 생성하고 있으며, 스마트 교통이나 의료와 같은 응용분야의 경우에는 실시간성이 요구되고 있다. 그러나 기존의 블록체인은 이러한 방대한 데이터를 실시간으로 처리할 수 없어 사물 인터넷과 블록체인의 통합을

어렵게 한다[33]. 대표적인 DAG 기반 블록체인 중 하나인 IOTA는 사물인터넷을 위해 고안된 분산 원장 기술로 네트워크의 확장성과 거래 수수료와 같은 기존 블록체인의 문제를 개선한다.

IOTA 아키텍처의 구성요소는 다음과 같다.

- Tangle: 네트워크의 모든 노드에 복제되는 공개 원장이다. 데이터는 트랜잭션이라는 객체에 저장되어 Tangle에 추가되며, 추가된 이후에 트랜잭션 변경은 불가능하다.
- 클라이언트: Tangle에 추가할 트랜잭션을 생성하여 노드에 보내는 역할을 수행한다.
- 노드: 네트워크를 구성하는 핵심 요소로 트랜잭션의 발행 및 유효성 검사를 수행하고, 트랜잭션의 무결성을 보장한다.
- 트랜잭션: 교환할 데이터 또는 IOTA 토큰이 포함된 페이로드이다.
- 제네시스 트랜잭션: 초기에 모든 IOTA 토큰을 보유한 첫 번째 트랜잭션이다.

IOTA에서는 새로운 트랜잭션을 추가하기 위해서 이전 두 개의 거래를 승인하고 소량의 작업 증명을 수행하는 방식으로 거래를 검증한다. 그래프의 시작점인 제네시스 트랜잭션은 모든 트랜잭션에 의해 직간접적으로 승인되며, 다른 거래에 의해 아직 승인되지 않은 새로 들어오는 트랜잭션을 팁(tip)이라고 부른다. 다른 트랜잭션에 의해 승인을 받을 때마다 해당 트랜잭션의 Weight는 증가하며, Weight가 높을수록 보다 높은 신뢰도를 가진다고 판단할 수 있다. 별도의 채굴자가 없이 처리되어 트랜잭션이 수수료 없이 발행될 수 있어 소액거래가 용이하며, 원장 활동이 활발할수록 검증도 활발하게 이루어지기 때문에 참여하는 노드가 많으면 많을수록 속도가 빨라진다는 장점을 가지고 있다.

새로운 트랜잭션을 추가하기 위해 아직 승인되지 않은 트랜잭션인 팁을 선택하기 위해서 마르코프 체인 몬테카를로(Markov chain Monte Carlo)라고 불리는 팁 선택 알고리즘을 사용한다. 마르코프 체인 몬테카를로 알고리즘은 몇 개의 랜덤 워커(random walker)를 Tangle 내부에 배치하고, 이 랜덤 워커가 그래프의 끝부분을 향하게 하여 마지막에 워커들이 멈춘 팁을 선택하여 승인함으로써 새로 들어오는 거래를 Tangle에 추가한다. 이 팁 선택 알고리즘은 기존에 승인된 트랜잭션이 아닌 아직 승인되지 않은 트랜잭션을 선택하도록 하여 승인되지 않은 트랜잭션의 개수가 증가하는 것을 방지하고 네트워크를 안정적으로 유지할 수 있도록 한다. 또한, 노드는 트랜잭션을 승인하는 동안 충돌하는 트랜잭션이 존재하는지 확인하여 이중 지출 트랜잭션이 발생하는 것을 방지한다[34]. 기존 IOTA 구현에서는 네트워크의 안정성을 위하여 코디네이터(coordinator) 노드를 운영한다. 코디네이터에서 생성되는 트랜잭션을 마일스톤(milestone)이라고 하며, 마일스톤에 의해 참조되고 승인된 트랜잭션을 신뢰하도록 한다. 이러한 코디네이터는 네트워크 보안을 보장하는 동시에 단일 장애 지점을 나타낸다. 이는 IOTA가 완전한 탈중앙화 네트워크가 되는 것을 제한한다.

2.2.3 탈중앙화 IOTA(포스트 코디네이터)

일반적으로 분산 원장 기술의 보안 메커니즘은 성숙한 네트워크를 전제하기 때문에 초기 단계에서는 의도한 대로 작동하기에 충분히 견고하지 못하다는 한계가 있다. 이에 초기 단계에서는 다양한 부트스트래핑(bootstrapping) 보안 조치를 채택하여 네트워크의 성장을 보조한다. IOTA도 초기의 네트워크를 훼손하려는 공격자에 대한 위험을 고려하여 중앙 집중식 코디네이터에 의존한 보안 메커니즘을 제공하였다. 그러나 이는 일시적인 조치로 현재 IOTA 재단에서는 탈중앙화를 달성하기 위하여 코디네이터를 제거하는 Coordicide 프로젝트를 진행하고 있다[35].

기존 버전에서는 코디네이터가 마일스톤 트랜잭션을 발행하고, 마일스톤에 의해 승인되고 연결된 트랜잭션만 유효한 것으로 간주함으로써 트랜잭션 간의 충돌을 해결하였다. 따라서 Coordicide 프로젝트에서 가장 중요한 것은 코디네이터가 없이도 충돌을 해결할 수 있는 합의 메커니즘이다. 이를 위해 IOTA에서는 선호하는 트랜잭션에 투표하는 메커니즘을 사용하며, 모든 노드는 메시지에 서명하고 투표를 하는데 사용할 고유 식별자(ID)를 가진다. 그러나 투표 시스템에서 노드의 식별자에만 의존하면 노드가 여러 개의 식별자를 생성하여 중복 투표를 하는 Sybil attack에 취약해 질 수 있다. 따라서 IOTA에서는 노드에 대한 평판 시스템인 '마나(Mana)'를 제안한다. 마나는 트랜잭션을 전송함으로써 노드에 부여되는 크레딧으로 유효한 트랜잭션을 전파하여 얻을 수 있다.트랜잭션에 노드 식별자를 추가하여 전송된 트랜잭션에 비례하여 마나를 축적한다. 마나는 얻기는

어렵지만 잃기는 쉽도록 설계되어 노드가 정상적으로 동작하도록 장려하고, 악의적인 행동을 하는 노드에 대해서는 처벌 메커니즘으로 마나를 회수한다. 획득한 마나는 네트워크에 트랜잭션이 추가되는 속도를 제어하고 충돌 트랜잭션 합의를 위한 투표에 사용된다.

IOTA는 스팸을 방지하기 위해 노드 당 최대 트랜잭션 속도를 설정하고 있으며, 트랜잭션 속도는 작업증명(Proof-of-Work)을 기반으로 최근 발행된 트랜잭션 건수, 마나 등의 요소에 따라 조절된다. 마나 양이 많은 노드는 평판이 낮은 노드 대비 적은 양의 작업증명이 요구되어 더 많은 트랜잭션을 추가할 수 있다. IOTA의 작업증명은 기존 블록체인에서 리더 노드를 선출하기 위해 수행하는 것과는 다르게 가장 빠르게 완료한 노드만 트랜잭션을 추가할 수 있는 것이 아니기 때문에 채굴 경쟁으로 이어지지 않고, 사물인터넷 환경을 고려하여 많은 양의 에너지가 필요하지 않도록 설계되어 있다[35].

충돌 트랜잭션에 대한 합의를 위한 투표 진행시에도 보유한 마나의 양에 따라 투표에 가중치를 부여한다. 따라서 좋은 행위자는 네트워크에 더 큰 영향을 미칠 수 있다. 충돌이 발생하면 노드는 셀룰러 오토마타(cellular automata)[36] 알고리즘에 기반 하여 합의에 도달할 때까지 이웃 노드들과 해당 트랜잭션에 대한 의견을 반복적으로 교환한다. 셀룰러 오토마타는 다른 합의 알고리즘에 비해 매우 높은 수준의 병렬화를 달성할 수 있다는 장점이 있다[37]. 이때 항상 같은 이웃 노드와 의견 교환이 이루어진다면 이는 공격 경로를 나타낼 수 있다. 따라서 이웃 노드는 무작위로 선출되며, 추가적으로 마나 기반 평판을 통합하여 보안을 향상시킨다. 노드는 평판이 비슷한 이웃과의 연결을 선호한다. 이로 인해 공격자가 이웃으로 간주되려면 높은 평판을 얻기 위해 많은 비용을 지불해야한다. 이러한 메커니즘으로 시간이 지남에 따라 정직한 노드가 보유한 마나의 양은 자연스럽게 증가하고, 네트워크는 점점 더 안전해진다. [35]에서는 10,000개의 노드 기준 128개의 충동 트랜잭션이 있는 케이스에 대해 시뮬레이션을 수행하여 몇 초 만에 합의에 도달하는 것을 확인하였다.

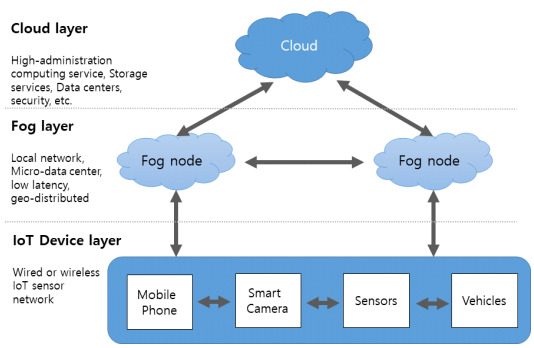


Fig. 3. The architecture of Fog computing

이처럼 IOTA는 탈중앙화, 데이터 변조 방지 및 일관성 보장 등의 특징과 함께 빠른 속도와 확장성까지 제공할 수 있어 IoT 포그 컴퓨팅 기반 신뢰 관리 모델에 적합한 솔루션이라고 할 수 있다.

2.3 포그 컴퓨팅(Fog computing)

포그 컴퓨팅은 스토리지, 통신, 컴퓨팅 자원을 사용자와 가까운 장소에 배치하여 데이터가 생성되는 기기의 근거리에서 처리함으로써 지연 시간과 대역폭 사용을 줄이며 신뢰성을 높이는 분산 컴퓨팅 기술이다. 데이터가 생성되는 기기와 클라우드 서버 사이에 포그 노드를 배치하고 지연 시간에 민감한 서비스들을 포그 노드로 이전하여, 클라우드 서버의 개입 없이 빠르게 서비스를 제공한다. 또한 기기가 생성 또는 수집한 데이터에 대한 임시적인 저장 및 실시간 분석을 수행한다. 이후 적절한 데이터 필터링을 거쳐 상위 계층인 클라우드에 데이터를 전달함으로써 글로벌 분석 및 장기 보관이 될 수 있도록 도와준다.

기존 클라우드 기반의 중앙 집중식 신뢰 관리 모델에는 여러 가지 문제점들이 있다. 운영 독점으로 인한 데이터 조작 및 단일 장애 지점을 비롯하여 IoT 시스템의 동적 특성을 제대로 처리할 수 없다. 또한, 이 모델에서는 모든 장치가 단일 중앙 서버와 상호작용하기 위해 에너지를 소비하고, 통신 대역폭을 사용하기 때문에 병목 현상이 발생할 수 있다.

[38-40]에서는 분산처리 방법으로 IoT 기기 계층에서 수행되는 신뢰 관리 모델을 제안하였으나 컴퓨팅과 에너지 자원이 제한된 IoT 기기에서는 신뢰 계산, 전파, 업데이트 및 저장과 같은 기능을 제대로 제공할 수 없다. 또한, 블록체인 네트워크 내의 모든 데이터를 저장하기 위한 충분한 저장 공간을 가지고 있지 않기 때문에 IoT 기기를 직접 블록체인에 참여시키는 것은 현실적인 솔루션이라고 할 수 없다. 이렇게 제한된 자원 문제를 해결하기 위하여 [12][41]에서는 IoT 기기에서 수집된 데이터를 포그 노드로 전달하여 처리 및 저장하도록 하는 모델을 제안하였다.

포그 노드가 IoT 기기의 자원 한계를 해결할 수 있다고 해도 블록체인이 사용하는 합의 알고리즘 수행에 따른 낮은 트랜잭션 처리량과 높은 지연 시간으로 인해 여전히 IoT 시나리오에서 블록체인을 적용하는 것은 어려운 문제로 남아 있다. 또한 IoT 기기와 연결된 포그 노드가 전달된 데이터를 제대로 처리할 것이라는 신뢰가 보장되어야 한다. 이전 연구를 살펴보면 프라이빗(private) 또는 컨소시엄 블록체인(consortium blockchain)을 사용하여 이 문제를 해결하고자 했다. 그러나 이러한 경우, 네트워크에 참여하는 노드를 사전에 알고 있고, 해당 노드를 신뢰하는 것이기 때문에 블록체인을 적용하는 것이 과연 효과적인 방법인가에 대해 다시 살펴볼 필요가 있다[42]. 또한 완전한 탈중앙화가 아니기 때문에 여전히 독점 운영을 통한 데이터 조작이 가능하다. 따라서 보다 공정성 있는 신뢰 모델을 구현하기 위해서는 누구든지 네트워크에 참여하여 데이터 운영에 대한 감사를 할 수 있는 퍼블릭 블록체인(public blockchain)을 사용하는 것이 적합하다. 다만, 이 경우 악의적인 공격자 역시 네트워크에 참여할 수 있기 때문에 Selective Forwarding attack[43]과 같은 공격으로부터 방어할 수 있는 메커니즘이 제공되어야 한다.

III. 신뢰 관리 시스템 요구사항

앞서 관련 연구에서 본 것과 같이 블록체인과 포그 컴퓨팅 기술을 적용하여 신뢰 관리시스템의 안정성을 높이기 위한 시도들이 많이 있다. 본 절에서는 IoT 환경의 분산 신뢰 관리 시스템이 갖추어야할 요구사항을 정의하고, 이를 기반으로 기존 연구를 분석한다.

3.1 IoT 기기 신뢰 관리 모델 요구사항 정의

R1. 탈중앙화(decentralization)

중앙 집중 방식은 중앙에서 한 번에 관리가 가능하기 때문에 운영이 용이하고 비용도 절감할 수 있다는 장점이 있다. 그러나 중앙에서 모든 것을 처리하기 때문에 데이터가 조작되거나 운영 독점, 단일 장애 지점의 문제가 발생할 수 있다. 따라서 신뢰 관리 시스템은 탈중앙화 방식을 통하여 신뢰 관리가 투명하게 운영되어야 한다[44].

R2. 변조 방지(tamper-proofing)

신뢰 데이터의 변조는 신뢰 관리 시스템의 기본이 무너지는 매우 치명적인 문제이다. 따라서 수집된 데이터가 절대 조작될 수 없도록 데이터 변조 방지가 보장되어야 한다[43-45][47].

R3. 일관성(consistency)

스마트 시티와 같은 개방적인 대규모 IoT 환경에서는 IoT 기기의 이동성으로 네트워크의 참여와 제거가 빈번하게 이루어진다. 따라서 분산 신뢰 관리 모델에서 일관된 데이터베이스 관리는 매우 중요한 요구사항이 된다. 하나의 지점에서 낮은 신뢰도를 부여받은 IoT 기기가 다른 지점으로 이동하여 악의적인 동작을 계속 수행할 수 있다. 이러한 문제가 발생하는 것을 방지하기 위해서 IoT 기기의 신뢰도는 네트워크 전체에서 동일하게 저장되어 관리되어야 한다[6][12][44].

R4. 적시성(timeliness)

IoT 기기의 신뢰도는 기기의 과거 동작을 기준으로 평가된다. 기기의 동작은 시간이 지남에 따라 변경될 수 있기 때문에 최신 상태의 데이터를 사용해야 보다 정확한 연산 결과를 얻을 수 있다. 블록체인을 사용하는 경우 이를 달성하기 위해서는 단위 시간 내의 처리량, 응답 속도와 같은 확장성 문제도 함께 고려되어야 한다[6][44][48].

R5. IoT 기기 자원 최적화 (IoT device resource optimization)

신뢰 관리를 위해서는 신뢰 구성, 집계, 전파 및 업데이트와 같은 다양한 프로세스가 수행되어야 한다. 그러나 IoT 장치는 제한된 자원으로 인하여 네트워크 내의 모든 장치에 대한 신뢰 평가를 처리하고 저장하기 어렵다. 따라서 기기의 수행능력에 맞게 프로세스가 분배될 수 있도록 해야 한다[6].

R6. 기기 증가에 따른 확장성(scalability)

IoT 기기는 계속 증가하고 있고, 네트워크에 연결되어 더 많은 데이터가 생성, 전달된다. 이러한 특징은 앞서 적시성의 요구사항을 만족시키기 어렵게 하며, 데이터 저장 공간의 부하 문제를 야기 시킨다. 따라서 증가하는 기기에 확장 가능한 시스템을 구축하여 이런 문제들을 해결할 수 있어야 한다[6][34].

R7. 신뢰 기반 공격에 대한 안정성(resiliency against trust based Attack)

신뢰 관리 시스템에 대하여 다음과 같은 공격들이 이루어질 수 있다. 이러한 공격들은 신뢰 관리 시스템의 정확성을 훼손하고 나아가 네트워크 전체에 악영향을 미칠 수 있다. 따라서 신뢰 관리 시스템 설계 시에는 이러한 공격에 대한 고려가 이루어져야 한다.

- A1. Bad mouthing attack: 정직한 노드의 평판을 손상시키는 공격이다. 노드의 평가를 악의적으로 나쁘게 제출하여 해당 노드의 신뢰도를 손상시킨다. 자신 또는 협력관계에 있는 노드들이 서비스 제공자로 선택될 수 있도록 악성 노드와 협력하는 공모 공격(collusion attack)의 한 형태이다[6][12][44][47][49-51].
- A2. Ballot stuffing attack: 이 공격은 Bad mouthing attack과 반대로 자신과 협력 관계에 있는 노드에 대하여 좋은 평가를 제출하여 해당 노드가 서비스 제공자로 선정될 가능성을 높이는 공격이다. 다른 악성 노드와 협력하여 서로의 평판을 높일 수 있으며, 이는 신뢰 관리 시스템의 정확성을 떨어트린다[6][47][49-51].
- A3. On-off attack: 신뢰 관리 시스템에 의하여 악성 노드로 분류가 되면 서비스 제공자로 선택되는 확률이 매우 떨어지게 된다. 이러한 상황을 피하기 위하여 정상 동작과 악성 동작을 랜덤하게 수행하며 악성 노드로 분류되지 않은 상태를 유지하여 다른 악성 노드와 결탁하여 담합 공격을 수행할 수 있다[12][47][49].
- A4. Self-promoting attack: 악성 노드가 자신에 대한 좋은 평판을 제출하여 서비스 제공자로 채택된 후, 그다음 불량하거나 오작동하는 서비스를 제공할 수 있다[12][49][50][51].
- A5. Sybil attack: 네트워크 내의 하나의 노드가 여러 개의 ID를 생성한 후, 실제 여러 개의 노드가 평가한 것처럼 특정 노드에 대해 다수의 신뢰도를 제출하여 해당 노드의 신뢰도에 영향을 끼칠 수 있다[12][43].
- A6. Selective forwarding attack: 이 공격은 신뢰 값 전파를 포그 노드로 위임하였을 경우에 발생할 수 있는 공격이다. 만약 포그 노드가 협력하는 IoT 기기가 있는 경우, 해당 노드에 대해서 긍정적인 영향을 미치는 데이터만 전파하여 신뢰 관리 시스템의 정확성을 떨어트릴 수 있다[43].

3.2 기존 연구 분석

기존의 연구가 위에서 정리한 요구사항을 만족하고 있는지 파악하기 위하여 분석 작업을 진행하였다. 관련된 논문을 검색하기 위하여 대표적으로 알려진 ACM[52], Elsevier[53], IEEE[54], Springer[55]의 4가지 출판사를 선정하여, 'Trust', 'Block chain'의 키워드로 검색하였고, 추가적인 정보가 필요한 경우 Google scholar[56]를 활용하였다. 논문을 검색한 결과, ACM 10건, Elsevier 28건, IEEE 138건, Springer 50건이 검색되었다. 이 중 상세한 내용이 포함되지 않거나 중복된 논문들을 제거한 후 최종적으로 11편을 선별하여 분석하였다. 분석된 결과는 [Table 1]에 정리하였으며, 요구사항을 만족하는 경우는 'O', 불만족하는 경우는 'X'로 표기하였다. 그리고 탈중앙화를 위하여 블록체인을 사용하였으나 프라이빗 또는 컨소시엄 블록체인을 사용한 경우와 같이 요구사항을 완전하게 만족시키지 못하는 경우에는 '△'로 표기하였다.

[16]은 IoT 기기-포그 노드의 2계층 아키텍처를 제안한다. IoT 기기가 포그 노드에 주기적으로 평판 값을 전달하고 포그 노드에서 이를 블록체인에 추가하여 네트워크의 모든 포그 노드에서 동일한 데이터를 관리한다. 필요한 신뢰 데이터는 가장 가까이에 있는 포그 노드에 요청하여 받음으로써 응답 지연을 개선하고자 하였다. 이 모델에서 IoT 기기와 포그 노드는 네트워크에 자유롭게 추가 및 제거할 수 있으며 서로 다른 소유자에 의해 관리될 수 있다. 각 노드 간의 데이터 공유는 블록체인을 통해 이루어지며, 탈중앙화, 변조방지, 일관성을 제공한다. 그러나 중앙집중 모델 대비 확장성을 제공하기 위하여 블록체인을 사용하였으나 네트워크에 참여하는 노드가 많아지고, 그에 따라 거래가 많아지면 블록 추가 및 합의에 많은 시간이 소요되어 데이터의 업데이트가 적시에 되지 않는다는 한계점을 가지고 있다.

[21]은 P2P 네트워크에 적용할 수 있는 블록체인 기반의 일반화된 평판 시스템을 제시하고 있다. 평판 점수 제출 시, 타임스탬프(timestamp)와 수신한 파일의 MAC(Message Authentication Code) 값을 포함하도록 하여 평판 점수가 실제 상호작용 기반에 기초한 것임을 증명하도록 하여 거짓된 평가를 제출함으로써 발생할 수 있는 문제를 해결하고, IP 주

Table 1. Compliance requirements of Existing Studies

	R1	R2	R3	R4	R5	R6	R7. Resiliency against TBA					
							A1	A2	A3	A4	A5	A6
[16]	O	O	O	O	O	X	O	O	O	O	X	X
[21]	O	O	O	X	X	X	O	O	O	O	O	X
[33]	O	X	O	O	O	O	X	X	X	X	X	X
[44]	△	△	O	O	O	X	X	X	O	O	O	O
[45]	△	△	O	O	O	X	X	X	X	X	X	O
[46]	△	△	O	O	O	X	X	X	O	O	O	O
[47]	△	△	O	O	O	X	O	O	O	X	O	O
[58]	O	O	O	O	O	X	O	O	O	O	O	O
[59]	△	△	O	△	O	X	X	X	X	O	O	O
[60]	△	△	O	O	O	X	X	X	O	O	O	O
[63]	△	△	O	O	O	△	O	O	O	O	O	O

소 기반의 식별자를 사용하여 Sybil attack을 방지한다. 그리고 보증금(deposit) 제도를 사용하여 부정직한 행동을 제한하고, 검증자에 대한 보상으로 사용한다. 블록체인 기반 네트워크는 초당 처리할 수 있는 트랜잭션 수에 제한이 있다는 점을 개선하기 위하여 블록 확인 시간을 10분에서 5분으로 변경하는 방법을 제안하였다. 그러나 블록 간격은 현재 생성된 블록이 다음 새로운 블록이 생성되기 전에 네트워크의 모든 노드에 전파됨을 보장하기 위한 설정으로 블록체인 네트워크의 안정성을 유지하기 위해서는 블록 크기와 간격의 균형을 유지하는 것이 중요하다. 노드의 수가 증가하는 경우 5분 이내에 모든 노드에 전파되지 못하고 결국 블록체인 네트워크의 안정성을 해칠 수 있다. 이는 지속 가능한 해결 방법이라고 할 수 없고, 여전히 확장성의 한계를 가지고 있다.

[33]은 IoT P2P 네트워크의 신뢰 관리 모델로 블록체인이 가지고 있는 지연, 네트워크 오버헤드와 같은 확장성 문제를 해결하기 위해 Holochain[57]을 적용한 모델을 제안한다. Holochain은 P2P 네트워크에서 분산 애플리케이션을 구축하기 위해 개발된 블록체인으로 기존 블록체인의 확장성 문제를 로컬 스토리지와 분산 해시 테이블 기술을 통하여 개선한다. IoT 기기가 생성하는 대량의 데이터를 처리하기 위해 분산 해시 테이블(distributed hash table)을 사용하여 분산 스토리지에서 데이터 검색을 가속한다. 데이터베이스의 일관성을 유지하기 위해 네트워크의 모든 노드가 블록체인의 복사본을 가지고 있어야 하는 기존의 구조는 네트워크의 대역폭과 시스템의 확장성에 부정적인 영향을 미치기 때문에 각 노드는 자신의 데이터를 로컬체인 형태로 저장한 다음, 분산 해시 테이블을 통해 실제 데이터의 해시값을 네트워크의 다른 모든 노드와 공유한다. 그러나 블록체인은 데이터가 체인에 한번 추가되면 변경이 불가능한 반면, Holochain은 로컬 체인내의 데이터 업데이트가 가능하다. 따라서 악성 노드 또는 공격자에 의해 손상된 노드가 있는 경우, 신뢰 데이터를 변경하여 IoT 기기의 신뢰도를 조작하는 신뢰 기반 공격을 수행할 수 있다.

[44]는 블록체인을 활용한 차량 네트워크의 신뢰 관리 모델을 제안하였다. 차량 ID 번호를 각 차량의 식별자로 사용함으로써 Self-promoting attack이나 Sybil attack과 같이 가짜 식별자를 이용하여 수행될 수 있는 공격으로부터 시스템을 보호한다. 신뢰 데이터의 저장과 처리를 노변 장치(Road Side Unit)로 이관하여 차량의 자원 제약 문제를 해결하고, 블록체인을 사용하여 신뢰 관리 모델의 탈중앙화, 변조방지, 일관성을 제공하고자 했다. 그리고 블록에 포함된 신뢰 값의 절대 값 합을 기반으로 작업증명을 수행하여, 더 많은 신뢰 값을 가지고 있는 노드가 채굴자로 선정되어 신뢰 값에 대한 변화가 빠르게 반영되도록 하였다. 제안된 모델에서는 다른 차량에 대한 평가 결과가 브로드캐스팅 되는 것이 아니라 근거리에 있는 노변 장치에 전달되는 구조로 '노변 장치는 신뢰할 수 있다'는 것이 전제조건이다. 해당 논문에서는 블록체인 네트워크에 참여하는 노변 장치가 네트워크 사업자에 의해 주기적으로 보안 검사가 이루어

지기 때문에 노변 장치에 대한 공격은 짧은 기간에만 유효하다고 설명하고 있다. 이는 노변 장치가 일부 사업장에 의해서 관리되는 폐쇄형 블록체인으로 완전한 탈중앙화라고 할 수 없다. 악의적인 노드가 없이 참여하는 모든 노드를 신뢰할 수 있다면 쓰기 권한이 공유된 데이터베이스가 보다 적합한 솔루션일 수 있다[42]. 블록체인은 신뢰가 형성되어 있지 않는 노드들이 합의 메커니즘을 통해 동일한 데이터베이스를 유지하는 것으로 연산과 저장소에 대한 오버헤드가 발생한다.

[45]는 무선 센서 네트워크(wireless sensor network)에 블록체인을 적용하여 스마트 컨트랙트 실행을 통해 악성 노드 탐지 프로세스에 대한 공정성과 추적성을 제공한다. 해당 모델에서는 컨소시엄 블록체인을 적용하여 권한을 가진 조직에서 인증기관(certificate authority)역할을 수행하는 노드와 검증 노드(verification node)를 사전에 지정하여 운영한다. 이는 이해관계가 맞는 조직 간의 공모를 통하여 특정 기기의 평판 향상을 위하여 다수의 ID를 생성하여 배포하고 자신들에게 유리하게 데이터를 조작하여 운영할 가능성이 있다. [46][60]에서 제안된 모델에서도 프라이빗 블록체인을 사용하여 악성 노드에 의해 네트워크가 손상되는 것을 해결하고자 하였다. 그러나 프라이빗과 컨소시엄 블록체인은 네트워크 참여를 허가해주는 중앙의 기관이 필요하기 때문에 블록체인의 기본 이념인 탈중앙화 네트워크와 거리가 있다. 사전에 선정된 기관이 얼마나 투명하고 신뢰도가 높은지에 따라 네트워크의 안정성이 결정되며, 자신에게 유리하도록 블록체인을 운영할 가능성이 존재하기 때문에 이로 인한 시스템의 투명성과 공정성이 저하된다.

[47]에서는 시스템을 IoT 기기 계층, 시스템 관리 계층, 애플리케이션 계층으로 모델링하였다. 이 모델의 핵심 부분은 신뢰 관리자(trust manager), 인증자(authenticator), 블록체인 채굴 노드가 포함된 시스템 관리 계층이다. 신뢰 관리자는 IoT 기기로부터 받은 신뢰도를 계산하고 집계한 후 채굴 노드로 전달하여 블록체인에 저장한다. 블록체인의 특성에 따라 저장된 데이터에 대한 변조 방지와 일관성을 제공하고, 기록된 정보를 추적하여 On-off attack을 수행한 노드를 식별할 수 있다. 그러나 논문에서 사용하는 멀티체인(multichain)은 프라이빗 블록체인이며, 신뢰 관리자와 인증자는 구역별로 나누어져 있어 해당 구역 내의 단일 장애 지점이 될 수도 있어 완전한 탈중앙화를 제공한다고 할 수 없다.

[58]에서는 이더리움의 스마트 컨트랙트를 사용하여 포그 노드의 신뢰도를 평가하는 모델을 제안하고 있다. 먼저 IoT 디바이스가 포그 노드와 상호 작용 후 해당 포그 노드의 신뢰 정보를 트랜잭션에 담아 스마트 컨트랙트를 실행시킨다. 스마트 컨트랙트는 사전에 정의된 계산식을 이용해 포그 노드의 평판을 계산하고, 계산된 결과는 오프체인 데이터베이스에 업데이트된다. 제안된 모델에서는 오프체인 데이터베이스를 사용하여 포그 노드의 신뢰 데이터와 로그를 저장하여 저장소에 대한 부담을 줄이고, 보증금 정책을 사용하여 참여하는 IoT 기기가 포그 노드에 대한 평가를 정직하게 수행하도록 하여 장려함으로써 Bad mouth attack이나 Bullet stuffing attack을 방어한다. 또한 트랜잭션은 모든 노드에 전파되기 때문에 악의적인 목적을 가진 채굴 노드가 일부 트랜잭션을 누락시키는 Selective forwarding attack에 대해서도 보호가 된다. 그러나 IoT 기기의 수가 증가함에 따라 전달되는 신뢰 데이터의 양도 많아지고, 그에 따라 블록체인에서 처리해야 하는 트랜잭션이 증가하면 블록 추가 및 합의에 많은 시간이 소요되는 확장성의 문제가 발생할 수 있다.

[59]에서는 IoT 기기의 데이터를 저장하고 악의적인 동작을 분류할 수 있는 IoT-블록체인 인프라의 동작 모니터링 아키텍처를 제안했다. 제안된 아키텍처에서는 영역별로 기기의 동작을 저장하기 위하여 로컬 블록체인을 구성한다. 이를 위해 영역별로 인증기관 역할을 담당하는 마스터 노드를 지정하고, 그룹 아이디를 만들어 하위 노드들에 서명 티켓을 전달하여 인증한다. 기기 간의 모든 종류의 통신은 트랜잭션으로 간주하며, 트랜잭션 수가 사전 정의된 블록 크기에 도달하면 마스터 노드가 새 블록을 만들어 로컬 블록체인에 추가한다. 사전에 지정된 마스터 노드는 해당 영역의 중앙 기관이 되어 단일 장애 지점이 되거나 데이터가 조작될 가능성이 있다. 또한 트랜잭션의 수가 정의된 블록 크기에 도달하지 못할 경우 블록체인에 추가되기까지의 지연이 발생할 수 있다.

[63]에서는 데이터 계층, 블록체인 계층 및 애플리케이션 계층의 세 가지 핵심 계층을 포함하는 신뢰 아키텍처를 제안하였다. 데이터 계층은 센서로 구성되어 있으며, 데이터를 수집하고 수집된 데이터를 트랜잭션에 담아 게이트웨이로 전송한다. 블록체인 계층에서는 게이트웨이가 프라이빗 블록체인 네트워크에 참여하여 블록 생성, 검증, 합의 과정을 수행한다.

해당 논문에서는 프라이빗 블록체인을 사용함으로써 게이트웨이 노드는 이미 네트워크에 참여하기 위한 권한을 가지고 있기 때문에 블록 생성을 위해 경쟁할 필요가 없으며, 주기적인 간격으로 블록을 생성한다. 또한 게이트웨이의 평판을 관리하여 평판이 좋은 경우 공격 가능성이 낮으므로 해당 노드에서 생성된 블록의 경우 적은 수의 트랜잭션을 검증하도록 하여 검증 프로세스의 계산 비용과 지연시간을 개선하였다. 그러나 블록체인에서 블록 간격은 현재 생성된 블록이 다음 새로운 블록이 생성되기 전에 네트워크의 모든 노드에 전파됨을 보장하기 위한 설정이다. 따라서 노드 간에 패킷이 전달되는 시간은 고려하지 않고 검증 속도만으로 블록의 생성되는 간격을 조절하는 것은 블록체인 네트워크의 안정성을 해칠 수 있다.

기존의 연구를 살펴보면 블록체인을 사용함으로써 탈중앙화, 변조 방지, 일관성과 같은 요구사항은 비교적 쉽게 달성되고 있는 것으로 보여 진다. 그러나 블록체인의 확장성 문제에 대해서는 대부분의 연구에서 다루고 있지 않다. 신뢰 관리 시스템에 대한 공격에 대해서도 [58]을 제외하고는 일부 공격에 대해서만 고려되고 있다. 특히 포그 노드에 대한 신뢰는 고려되고 있지 않거나, 탈중앙화와 트레이드오프가 발생하는 프라이빗 블록체인을 사용하여 해결한다. 따라서 본 논문에서는 탈중앙화를 달성하기 위하여 퍼블릭 블록체인을 사용하여 시스템의 투명성과 공정성을 제공하고자 한다. 또한 블록체인의 처리량 관점에서 확장성을 개선하고, 신뢰 관련 공격으로부터 시스템을 안전하게 지킬 수 있는 신뢰 관리 모델을 제안한다.

IV. IOTA기반 시스템 모델 제안

본 절에서는 포그 컴퓨팅 기반 사물인터넷 환경에서 상호 작용하는 IoT 기기의 신뢰도를 평가하고, 저장하는 신뢰 관리 모델을 제안한다. 3절에서 정의한 요구사항 중 탈중앙화, 데이터 무결성, 일관성을 위하여 블록체인 기술을 적용한다. 기존 블록체인 시스템의 낮은 처리량과 확장성, 높은 비용의 문제를 해결하기 위하여 본 논문에서는 DAG 기반 블록체인 시스템인 IOTA를 기본 모델로 사용하여 신뢰 데이터에 대한 투명성과 일관성을 보장한다.

제안하는 분산 신뢰 관리 모델은 [Fig.4]과 같다. IoT 기기는 클라이언트, 포그 노드는 Tangle 네트워크를 구축하는 IOTA 노드의 역할을 한다. IoT 기기 간의 상호작용을 통하여 신뢰도를 도출하고, 계산된 결과를 트랜잭션에 추가하여 포그 노드로 전달한다. 포그 노드는 전달받은 트랜잭션을 Tangle에 추가한다. 이 후, Tangle에 저장된 데이터를 기반으로 IoT 기기의 최종 신뢰도를 계산한다. 주요 절차는 다음과 같이 나눌 수 있다.

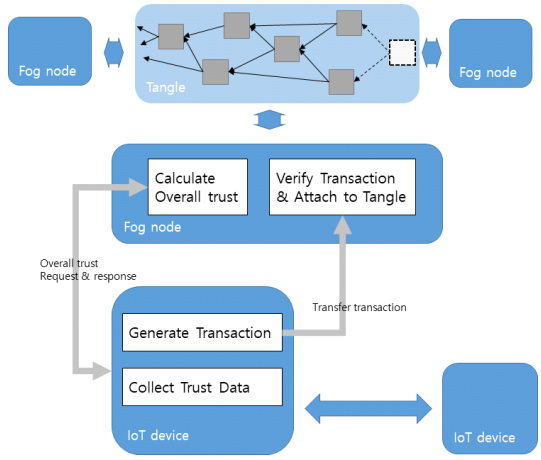


Fig. 4. Proposed system architecture

4.1 신뢰 데이터 수집 및 평가

계정은 마스터키(master key) 역할을 하는 시드(seed)를 기반으로 주소(address)를 생성하며, 이를 통해 IoT 기기를 식별할 수 있다. IoT 기기는 다른 기기와의 상호작용에 기반 하여 ▲Ownership, ▲Friendship, ▲Honesty 관점으로 대상 기기의 신뢰도를 계산한다. Friendship은 상호작용에 기반하여 "성공 연결 요청 수/모든 요청의 성공 최대 연결 수"로 계산하며, Honesty는 주어진 시간 동안 직접 관찰한 결과를 기반으로 평가되는 항목으로, 일정 기간 이상 징후 감지 규칙(재전송, 반복, 지연 등)을 사용하여 의심스러운 동작의 개수를 기반으로 평가한다[49][61]. 마지막 Ownership은 기기 소유자에 대한 항목으로 동일한 소유자의 기기인 경우에는 신뢰할 수 있다고 판단한다[49][62]. 이렇게 수집된 데이터를 수식 (1)을 통해 결합하여 상호작용에 대한대상 기기의 신뢰도 $T_{ij}^{connect}$ 도출한다.

$$T_{ij}^{connect} = \alpha \cdot T_{ij}^{Friendship} + \beta \cdot T_{ij}^{Honesty} + (1-\alpha-\beta) \cdot T_{ij}^{Ownership} \quad (1)$$

4.2 트랜잭션 생성

앞에서 계산된 직접 신뢰도를 포함하는 IOTA 트랜잭션을 생성하여 포그 노드로 전달한다. 트랜잭션을 생성하기 위해서는 IOTA 코어 클라이언트 라이브러리를 사용한다. 가장 먼저 트랜잭션을 보낼 노드를 선택한다. 이 노드는 IOTA 네트워크에 대한 진입점이 된다. 다음으로 Tangle에 연결하기 위해서는 두 개의 팁 트랜잭션의 해시값이 필요하다. 이를 위해서 클라이언트는 노드에 팁 선택 프로세스 수행을 요청한다. 모든 IOTA 노드는 팁 선택 알고리즘(tip selection algorithm)을 포함하고 있으며 Weight를 기준으로 유효성을 판단하여 팁 트랜잭션을 선택한다. 신규 트랜잭션을 생성하기 위해서는 작업 증명을 수행해야 한다. 그러나 자원이 충분하지 않은 IoT 기기의 경우 로컬 작업 증명(local PoW) 수행에 오랜 시간이 걸릴 수 있다. IOTA는 IoT 환경에 적합한 솔루션 제공을 목표로 하고 있어 클라이언트가 아닌 포그 노드에서 작업 증명을 수행할 수 있는 옵션을 제공하고 있다. 따라서 본 논문에서는 원격 작업 증명(remote PoW)을 통해 IoT 기기의 자원 사용을 최소화한다. 마지막으로 시드로부터 파생된 개인키(private key)를 이용하여 트랜잭션을 서명한 후, 트랜잭션이 Tangle에 연결될 수 있도록 포그 노드로 전송한다.

4.3 Tangle 트랜잭션 추가

IoT 기기로부터 트랜잭션을 수신한 포그 노드는 다음의 과정을 거쳐 Tangle에 트랜잭션을 추가한다. 앞의 트랜잭션 생성 단계에서 작업 증명을 포그 노드로 이관하였다. 작업 증명은 퍼즐을 풀기 위해 컴퓨팅파워가 소비되었다는 증명이다. IOTA 트랜잭션은 스팸 트랜잭션을 보내지 못하도록 하기 위해 작업증명을 요구한다. 작업 증명 알고리즘은 수행하기 어렵지만 검증하기 쉽다는 특징을 가지고 있으며, 이때 난이도는 최소 중량 크기(minimum weight magnitude)로 정의된다. 이 작업은 트랜잭션 내 모든 필드의 해시값을 구하는 것으로, 해시값이 최소 중량 크기와 동일한 0의 개수로 끝날 때까지 논스(nonce) 값을 증가시키며 해시값 계산을 반복한다. 비트코인과는 다르게 IOTA의 작업증명은 사물인터넷 환경을 고려하여 많은 양의 에너지가 필요하지 않도록 설계되어 있다[35].

작업 증명이 끝나면 노드는 로컬 데이터베이스에 트랜잭션을 추가하여 Tangle에 연결한다. 트랜잭션이 동시에 모든 노드에 전달되는 것이 아니기 때문에 각 노드의 로컬 데이터베이스는 서로 다른 트랜잭션을 가질 수 있다. 다른 분산 시스템과 마찬가지로 이웃 노드들과 데이터베이스를 동기화하여 단일 소스를 형성한다. 하나의 노드가 트랜잭션을 받으면 이웃 노드에 가십을 시도하고, 합의 알고리즘을 통해 충돌을 해결하여 최종적으로 모든 노드가 동일한 데이터베이스를 가지게 된다.

4.4 최종 신뢰도 계산

IoT 기기는 다른 기기와 연결하기 전에 포그 노드에 대상 기기의 신뢰도를 요청할 수 있다. 포그 노드는 Tangle에 저장된 데이터를 기반으로 IoT 기기에 대한 최종 신뢰도를 계산한다. 먼저 대상 기기와의 상호 작용에 대해 평가된 직접 신뢰도(direct trust)와 주변 기기에 의해서 평가된 간접 신뢰도(indirect trust)를 아래의 수식(2)을 이용하여 최종 신뢰도(overall trust)를 계산하고, 이를 IoT 기기에 반환한다.

$$T_{ij}^{overall} = \alpha \cdot T_{ij}^{direct} + (1-\alpha) \cdot T_{ij}^{indirect} \quad (2)$$

아래의 수식(3)은 직접 신뢰도 산출을 위한 계산식으로 cw는 누적 중량(cumulative weight)을 나타내고, Thr은 임계값(threshold)을 나타낸다.

$$T_{ij}^{direct} = \sum (T_{ij}^{connect} \cdot (1 - cw/Thr)) \quad (3)$$

트랜잭션의 누적 중량은 값이 클수록 다른 노드들로부터 많은 승인을 받은 것으로 신뢰할 수 있는 데이터라는 의미이다. 그러나 트랜잭션의 누적 중량은 시간의 흐름에 따라 지속해서 증가하지만 반대로 실제 기기의 신뢰도는 하락할 수 있다. 예를 들어, 악성 기기가 초기에 높은 신뢰도를 확보하기 위해 정상적인 동작을 수행하다가 이후에 원래의 목적을 달성하기 위해 악의적인 동작을 수행하거나, 공격자에 의해 기기가 손상되어 오동작 할 수 있다. 따라서 과거의 평가보다는 최근 상호작용에 대한 평가 결과에 더 많은 가중치를 부여하여 계산한다.

아래의 수식(4)은 주변 기기들에 의해 평가된 간

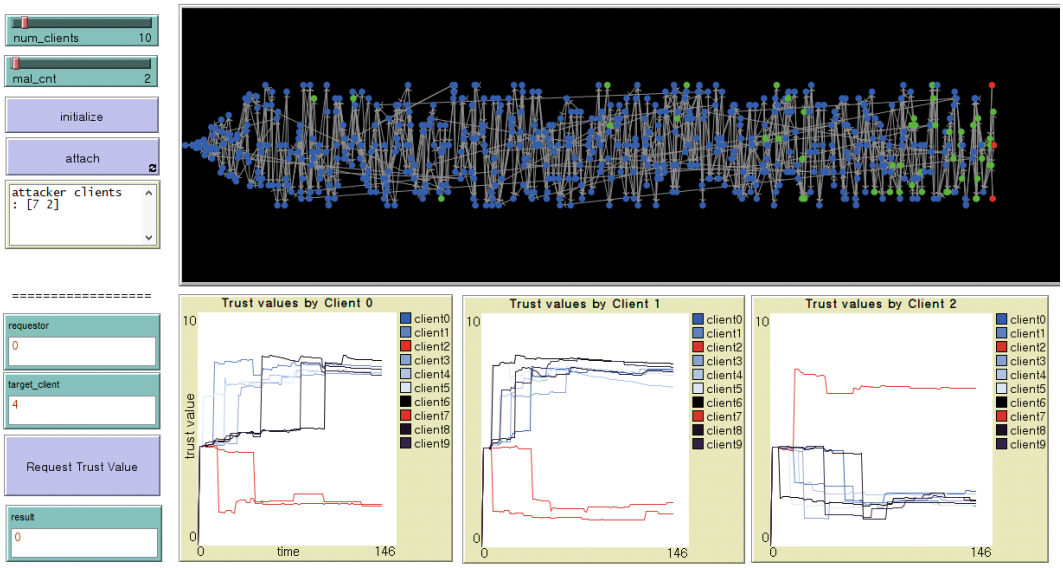


Fig. 5. Simulation GUI

접 신뢰도 산출을 위한 계산식이다.

$$T_{ij}^{indirect} = \sum_{k} (T_{ik}^{direct} * T_{kj}^{direct}) \quad (4)$$

주변 기기가 정직한 기기인 경우에는 올바른 신뢰도를 제출하지만, 악성 기기라면 점수를 조작하여 Bad mouthing attack이나 Ballot stuffing attack을 수행할 수 있다. 따라서 해당 기기에 대한 신뢰도에 따라 제출된 점수에 가중치를 부여하여 이러한 공격으로부터 방어한다. 만약 해당 기기에 대한 직접 신뢰도가 0이라면, 제출된 신뢰도는 전체 점수에 영향을 주지 못한다.

V. 시스템 분석

5.1 시뮬레이션 결과

본 절에서는 제안한 모델의 시뮬레이션 수행 결과를 보인다[Fig. 4]. 앞서 제시한 수식을 통해 계산된 신뢰도를 기반으로 네트워크 내의 손상된 클라이언트 검출 가능 여부를 파악한다. 시뮬레이션은 NetLogo [64] 시뮬레이터를 사용하여 Tangle 네트워크를 구축하였으며, [65]의 시뮬레이션 모델을 참고하였다. 본 논문에서 제안하는 모델은 신뢰도 계산 시 누적 중량을 사용하기 때문에 정확도를 높이기 위하여 기존 시뮬레이션의 update-cw 과정을 수정하여 실제 승인된 트랜잭션에 한하여 누적 중량이 증가되도록 개선하였다. 시뮬레이션이 수행되면 클라이언트의 신뢰 데이터를 트랜잭션에 추가하여 저장하도록 로직을 추가하였다. 제안된 모델에서는 클라이언트의 요청에 의해서 대상 기기의 최종 신뢰도 계산하나, 시뮬레이션에서는 트랜잭션 추가에 따른 변화를 파악하기 위하여 단위 기간(tick)마다 계산하여 그 결과를 그래프로 나타낸다. 앞서 서술한 것과 같이 최종 신뢰도는 간접 신뢰도를 제공하는 주변 기기의 신뢰도에 영향을 받는다. 신뢰도를 요청하는 기기와 간접 신뢰도를 제공하는 기기 사이의 관계에 따라 최종 신뢰도가 상대적으로 다르게 나타나게 된다. 본 시뮬레이션에서는 3개의 기기를 임의로 선정하여 각 기기에게 전달되는 최종 신뢰도 변화를 관찰 및 분석하였다. 그래프 결과를 직관적으로 파악하기 위하여 정상 클라이언트의 신뢰도는 파란색 실선으로 표시하고, 악성 클라이언트의 신뢰도는 빨간색으로 표시하였다. 시뮬

Table 2. Key parameters

Parameters	Values
Client number	20
MWM (minimum weight magnitude)	8
Thr	300
weight of direct trust value	0.6
weight of direct trust value	0.4

레이션에 사용된 주요 파라미터는 〔Table 2〕와 같다.

〔Fig.6〕〔Fig.7〕〔Fig.8〕는 악성 클라이언트를 각각 2개, 5개, 10개 배치하였을 때, 네트워크 내의 전체 클라이언트의 신뢰도를 그래프로 보여준다. 악성 클라이언트의 수가 전체의 50%까지 증가하여도 신뢰도 계산에는 영향을 미치지 못하며, 정상 클라이언트와 악성 클라이언트를 구분한다.

다음으로는 네트워크 규모에 따른 악성 노드 탐지 여부를 파악하기 위하여 참여하는 클라이언트의 수를 증가시켜 시뮬레이션을 진행하였다. 클라이언트의 수는 20개부터 50개까지 10 단위로 증가시켰고, 악성

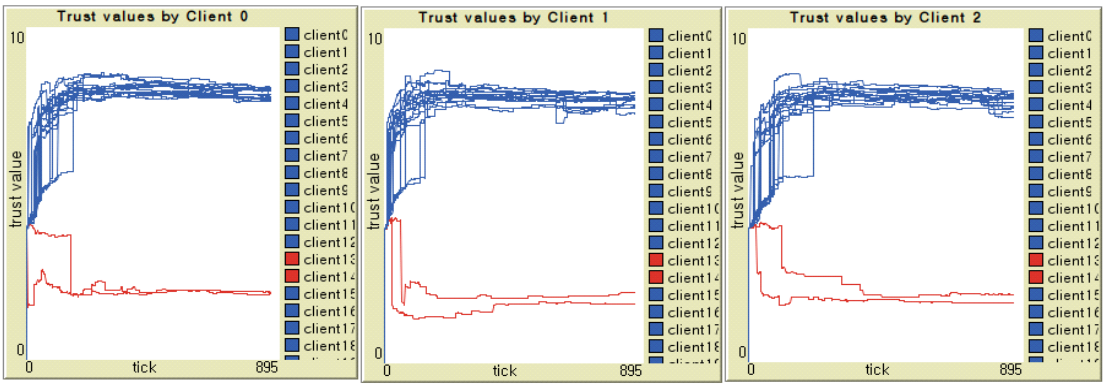


Fig. 6. Trust values of clients in networks with 2 malicious clients

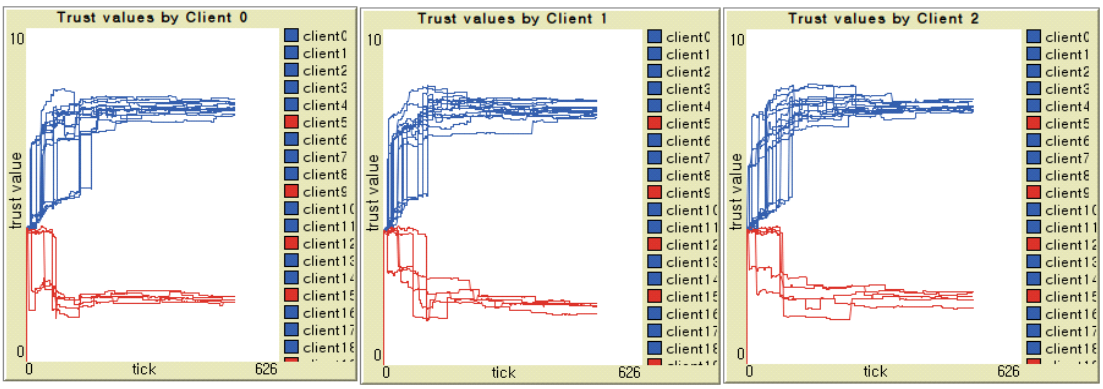


Fig. 7. Trust values of clients in networks with 5 malicious clients

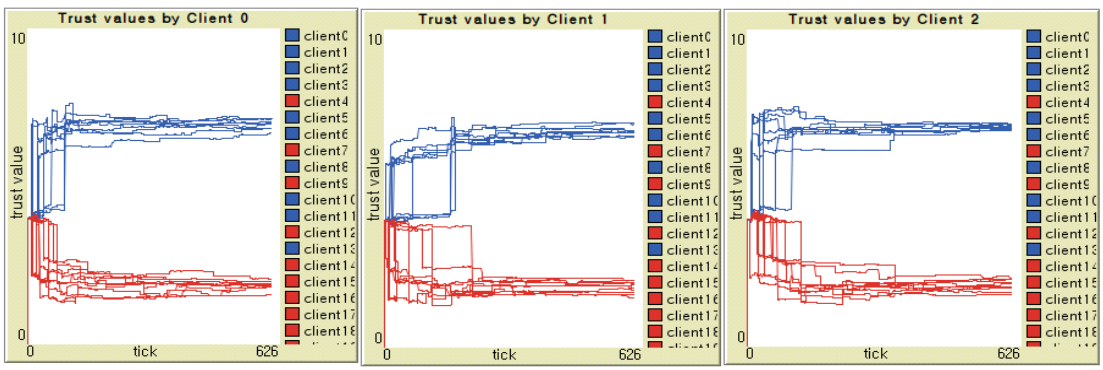
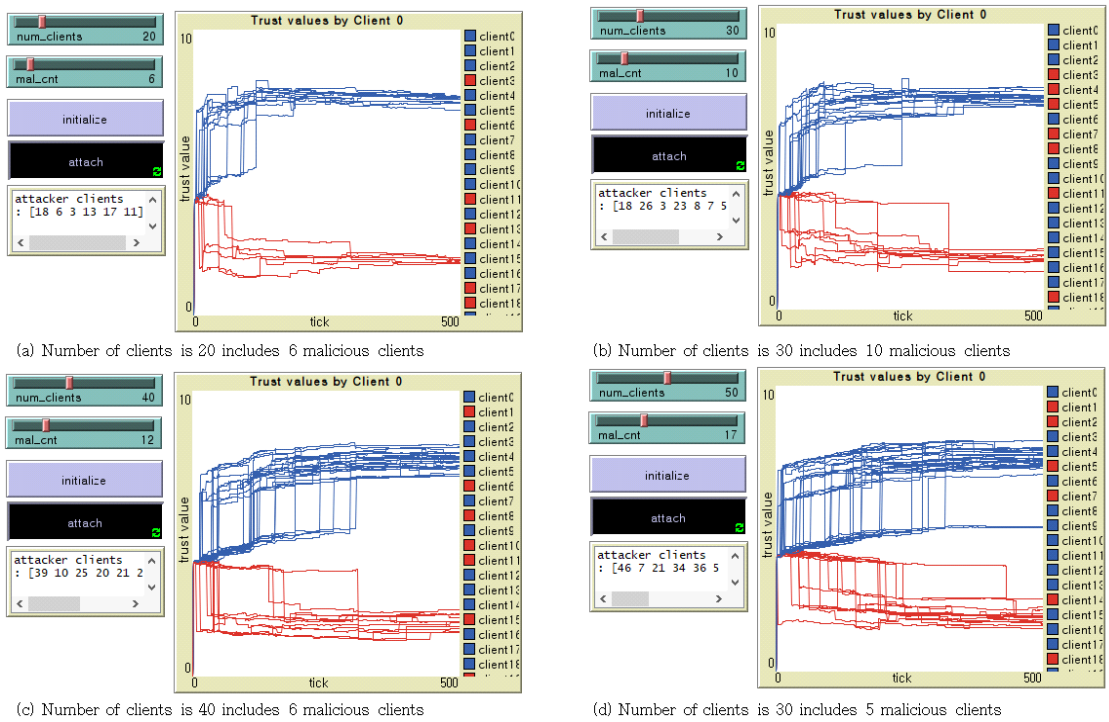


Fig. 8. Trust values of clients in networks with 10 malicious clients



(a) Number of clients is 20 includes 6 malicious clients

(b) Number of clients is 30 includes 10 malicious clients

(c) Number of clients is 40 includes 6 malicious clients

(d) Number of clients is 30 includes 5 malicious clients

Fig. 9. Malicious client identification by increasing number of clients in networks

클라이언트는 전체의 1/3 수준을 유지하도록 설정하였다. [Fig.9]는 이에 대한 결과를 나타낸다. 참여하는 클라이언트의 수가 증가함에 따라 기기와의 상호작용을 기반으로 부여되는 직접 신뢰도가 최종 신뢰도에 반영되는 속도가 늦어진다. 그러나 직접 상호작용이 없음에도 주변 클라이언트들이 제출한 간접 신뢰도를 통해 악성 클라이언트가 식별이 가능함을 확인할 수 있다.

5.2 시스템 요구사항 적합성 분석

본 절에서는 제안된 신뢰 관리 시스템이 3절에 정의한 요구사항을 어떻게 만족시키는지 분석한다.

1. 탈중앙화

IOTA는 초기 단계에서 부트스트래핑 보안 조치로 공격자에 대한 위험으로부터 네트워크를 보호하기 위하여 중앙 집중식 코디네이터에 의존한 보안 메커니즘을 제공한다. 그러나 이는 일시적인 조치로 포스트 코디네이터 단계에서는 코디네이터를 제거하고, 노드에 대해 마나 평판 시스템과 투표 메커니즘을 구현하여 탈중앙화를 달성한다.

2. 변조방지

Tangle의 가장 기본적인 속성 중의 하나는 불변성(immutability)으로 트랜잭션이 Tangle에 연결된 후에는 변경할 수 없다. 이러한 불변성은 해시 알고리즘의 특성으로 만족된다. IOTA에서는 트랜잭션의 모든 필드에 대해 해시값이 생성된다. 그리고 각 트랜잭션은 두 개의 이전 트랜잭션과 연결된다. 따라서 트랜잭션을 변경하면 직접 또는 간접적으로 연결된 트랜잭션이 모두 무효가 되기 때문에 변조가 불가능하다.

3. 일관성

노드는 로컬 데이터베이스에 트랜잭션을 추가하여 Tangle에 연결한다. 트랜잭션이 동시에 모든 노드에 전달되는 것이 아니기 때문에 각 노드의 로컬 데이터베이스는 서로 다른 트랜잭션을 가질 수 있다. 다른 분산 시스템과 마찬가지로 이웃 노드들과 데이터베이스를 동기화하여 단일 소스를 형성한다. 하나의 노드가 트랜잭션을 받으면 이웃 노드에 가십을 시도하고,

합의 알고리즘을 통해 충돌을 해결하여 최종적으로 모든 노드가 동일한 데이터베이스를 가짐으로써 일관성을 제공한다.

4. 적시성

적시성은 상호 작용의 결과를 기반으로 신뢰도를 업데이트하는 부분과 Tangle로 부터 최종 신뢰도를 받아오는 부분으로 나누어 분석한다.

먼저 신뢰도 업데이트 시에는 특정 기기 1대와 직접 상호 작용 후 수집한 데이터를 바탕으로 신뢰도를 계산한다. 여기에서는 수집된 정보에 대한 가중치 합 연산으로 연산의 복잡도가 낮으며, 1대의 기기에 대한 점수를 계산하는 것으로 네트워크 내의 기기의 수가 증가하여도 영향을 받지 않으며 일정한 연산량과 시간이 소모된다. 계산이 완료되면 트랜잭션을 생성하여 Tangle에 업데이트한다. DAG의 트랜잭션은 여러 곳에서 동시다발적으로 추가가 가능하기 때문에 대기할 필요 없이 빠르게 업데이트를 할 수 있으며, 사용자가 많아진다 해도 트랜잭션의 승인이 지연되거나 병목현상이 발생하지 않는다. 만약 공격자에 의해 오동작하는 기기가 발생하면 해당 정보는 Tangle에 빠르게 업데이트되어 공유될 수 있다. DAG은 기존 체인 기반 모델이 한 번에 하나의 블록만 처리하는 순차적인 방식과는 다르게 동시에 여러 블록을 병렬로 처리하여 병목 현상을 해결하고, 데이터가 추가되는 속도를 향상시켜 신뢰 데이터의 적시 업데이트를 제공한다.

다음으로 Tangle에 저장된 정보를 통합하여 최종 신뢰도를 계산하여 IoT 기기에 반환 부분이다. 트랜잭션이 Tangle에 빠르게 추가되기 때문에 최종 점수 계산에 최신의 정보가 사용될 수 있다. 또한, 정보를 통합하는 연산을 IoT 기기가 아닌 컴퓨팅 자원이 충분한 포그 노드에서 진행하여 최종 신뢰도를 빠르게 연산하여 IoT 기기에 전달할 수 있다.

5. IoT 기기 자원 최적화

컴퓨팅과 에너지 자원이 제한된 IoT 기기에서의 연산을 최소화하고, 데이터 연산과 저장 작업을 포그 노드로 이관하여 IoT 기기의 자원을 최적화 한다. IoT 기기에서 수집된 신뢰 데이터를 포그 노드로 전달하여 처리한다. 포그 노드는 IOTA 노드로서 원격 작업 증명과 팁 선택 알고리즘 수행하고 Tangle 데이터베이스를 저장하는 역할을 한다.

6. 기기 증가에 따른 확장성

IOTA에서는 새로운 트랜잭션을 Tangle에 추가하기 위해서 이전 두 개의 거래를 승인하고 소량의 작업 증명을 수행해야 한다. 따라서 트랜잭션을 추가하는 원장 활동이 활발할수록 검증도 활발하게 이루지고, 참여하는 노드가 많으면 많을수록 트랜잭션의 검증 속도는 빨라진다. 즉, IoT 기기의 수가 늘어 트랜잭션이 많아질수록 검증의 신뢰도와 속도가 향상되므로 기기 증가에 따른 확장성 문제가 해소된다.

7. 신뢰 기반 공격에 대한 안정성

각 IoT 기기는 IOTA 계정의 주소를 통해 식별이 가능하다. 신뢰 데이터 제출 시에 기기의 주소를 확인하여 평가를 수행한 기기와 평가를 받는 기기가 일치하는 경우 유효하지 않은 것으로 처리함으로써 Self-promoting attack을 방어할 수 있다. 트랜잭션은 IoT 기기에서 코어 클라이언트 라이브러리를 사용하여 생성된다. 포그 노드는 트랜잭션의 유효성을 검증하고 Tangle에 추가할 수 있으나 트랜잭션을 생성하거나 서명하지는 못한다. 따라서 신뢰 데이터에 대한 변경은 IoT 기기에서만 이루어질 수 있다. 이때, 공격자의 IoT 기기가 다른 기기의 신뢰도를 조작하기 위하여 거짓 데이터를 전달할 수 있다. 그러나 수식(4)와 같이 최종 신뢰도 계산 시, 신뢰 데이터를 전달하는 기기의 신뢰도에 따라 가중치가 부여되기 때문에, 신뢰도가 낮은 IoT 기기가 전달한 데이터는 최종 신뢰도에 큰 영향을 끼치지 못하며, 이를 통해 Bad mouthing attack과 Ballot stuffing attack을 방어할 수 있다.

포드 노드에는 IOTA 노드 식별자가 주어지고, 노드가 정직하게 동작하도록 '마나' 기반 평판 시스템을 통해 각 노드의 평판을 관리한다. 마나는 트랜잭션을 전송함으로써 노드에 부여되는 크레딧으로 유효한 트랜잭션을 전파하여 얻을 수 있다. 보유한 마나의 양이 많을수록 네트워크에 더 많은 트랜잭션을 추가할 수 있으며, 충돌 트랜잭션 합의를 위한 투표에서도 큰 영향을 미칠 수 있다. 마나는 얻기는 어렵지만 잃기는 쉽도록 설계되어 악의적인 행동을 하는 노드에 대해서는 마나를 회수하여 처벌한다. 이러한 노드의 평판 관리를 통해 노드가 정직하게 동작하도록 장려하고, 임의의 트랜잭션만 전달하는 Selective forwarding attack을 방어할 수 있다.

VI. 결 론

사물인터넷은 무수히 많은 기기들이 종류에 관계없이 상호작용하며 인간의 삶에 대한 데이터를 모니터링하고 수집하고, 수집된 데이터를 집계, 융합, 처리 및 분석하여 다양한 서비스를 제공할 수 있는 거대한 집단이다. 그리고 각 장치가 다른 장치에 서비스를 요청하거나 제공할 수 있는 서비스 중심 아키텍처로 볼 수 있다. 악성 기기와 통신을 하게 될 경우, 네트워크나 서비스를 악의적으로 손상시켜 서비스 품질에 영향을 줄 수 있기 때문에 신뢰할 수 있는 기기를 선택하는 것은 매우 중요하다. 최근 연구에서는 IoT 기기의 신뢰 관리를 위해 포그 노드와 블록체인을 사용하는 모델들이 제안되고 있다. 신뢰 데이터의 저장과 처리를 포그 노드로 이관하여 IoT 기기의 자원 제약 문제를 해결하고, 포그 노드를 블록체인 네트워크에 참여시켜 중앙 집중 방식의 문제를 해결한다. 그러나 블록체인은 데이터베이스의 일관성을 보장하기 위하여 많은 시간이 요구되고 있으며, 그에 따라 처리량이 낮기 때문에 IoT 기기가 생성하는 대량의 데이터를 처리하기에는 적합하지 않다.

이에 본 논문에서는 기존 연구를 분석하여 IoT 기기의 신뢰 관리 모델이 갖추어야 할 요구사항을 정의하고, 사물인터넷 환경에 맞는 분산 신뢰 관리 시스템을 제안하였다. 기존 블록체인 기반 시스템의 한계점을 개선하기 위하여 방향성 비순환 그래프인 DAG 기반의 IOTA를 적용하였다. 기존 블록체인이 한 번에 하나의 블록만 순차적으로 처리하는 방식이었다면, DAG 기반의 IOTA에서는 동시에 여러 트랜잭션을 병렬로 처리하여 병목 현상을 해결하고, 데이터 추가 속도를 개선하였다. 또한 네트워크에 참여하는 포그 노드를 '마나' 기반의 평판 시스템을 통해 관리하고, 최종 신뢰도 계산 시, 평가자에 해당하는 기기의 신뢰도에 따라 가중치를 부여함으로써 신뢰 기반 공격을 방어하였다.

IoT 기기는 계속 증가하고 있으며 그에 따라 시스템의 확장성은 반드시 고려해야 할 사항이다. IOTA는 사물 인터넷을 위한 분산 원장으로 DAG 구조를 사용하여 IoT 기기와 트랜잭션 증가에 대한 확장성 문제를 효과적으로 해결 할 수 있는 솔루션이다. 또한 기존의 중앙 노드 역할을 하는 코디네이터를 제거함으로써 탈중앙화의 특징을 만족하여 투명성과 공정성이 중요한 신뢰 관리 시스템에 적합하다.

References

[1] Afif Osseiran, Jose F Monserrat, and Patrick Marsch. 2016. 5G mobile and wireless communications technology. Cambridge University Press.

[2] Rappaport, Theodore S., et al. "Overview of millimeter wave communications for fifth-generation (5G) wireless networks-With a focus on propagation models," IEEE Transactions on antennas and propagation 65.12, pp. 6213-6230, 2017.

[3] Shariatmadari, Hamidreza, et al. "Machine-type communications: current status and future perspectives toward 5G systems," IEEE Communications Magazine 53.9, pp. 10-17, 2015.

[4] Elbouanani, Salim, My Ahmed El Kiram, and Omar Achbarou. "Introduction to the Internet of Things security: Standardization and research challenges," 2015 11th International Conference on Information Assurance and Security(IAS). IEEE, pp. 32-37, 2015.

[5] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE communications surveys & tutorials 17.4, pp. 2347-2376, 2015.

[6] Kouicem, Djamel Eddine, et al. "A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things," IEEE Transactions on Dependable and Secure Computing 2020.

[7] S. Gill, P. Chawla, P. Sahni, and S. Kaur, "An effective and empirical review on Internet of Things and real-time applications," in Advances in Computer and Computational Sciences. Heidelberg, Germany: Springer, pp. 159 - 167, 2018.

[8] B. Guidi and L. Ricci, "Aggregation

techniques for the Internet of Things: An overview," in The Internet of Things for Smart Urban Ecosystems. Heidelberg, Germany: Springer, pp. 151 - 176, 2019.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347 - 2376, 4th Quart, 2015.

[10] G. Hunt. 2018. Introducing Microsoft Azure Sphere: Secure and power the intelligent edge. Retrieved Feb. 17, 2019 from https://azure.microsoft.com/en-us/blog/introducing-microsoft-azure-sphere-secure-and-power-the-intelligent-edge/

[11] A. Altaf, H. Abbas, F. Iqbal, and A. Derhab, "Trust models of Internet of smart things: A survey, open issues and future directions," J. Netw. Comput. Appl., vol. 137, pp. 93 - 111, Jul. 2019.

[12] Pourghebleh, Behrouz, Karzan Wakil, and Nima Jafari Navimipour. "A comprehensive study on the trust management techniques in the internet of things," IEEE Internet of Things Journal 6.6, pp.9326-9337, 2019.

[13] Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems," Computer Communications 97, pp. 1-14, 2017.

[14] J. Guo and I.-R. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems", 2015 IEEE International Conference on Services Computing, pp. 324-331, 2015.

[15] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks", IEEE Internet of Things Journal, pp. 1-1, 2018.

[16] D. E. Kouicem, A. Bouabdallah and H. Lakhlef, "An Efficient Architecture for Trust Management in IoE Based Systems of Systems", 2018 13th Annual Conference on System of Systems Engineering (SoSE), pp. 138-143, 2018.

[17] P. K. Sharma, M.-Y. Chen and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT", IEEE Access, vol. 6, pp. 115-124, 2018.

[18] Pilkington, Marc. Blockchain technology: principles and applications. Research handbook on digital transformations. Edward Elgar Publishing, 2016.

[19] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review (2008): 21260.

[20] Antonopoulos, Andreas M., and Gavin Wood. Mastering ethereum: building smart contracts and dapps. O'reilly Media, 2018.

[21] Dennis, Richard, and Gareth Owen. "Rep on the block: A next generation reputation system based on the blockchain," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). IEEE, 2015.

[22] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform," white paper 3.37 2014.

[23] Zhou, Qiheng, et al. "Solutions to scalability of blockchain: A survey," IEEE Access 8, pp. 16440-16455, 2020.

[24] E. K. Kogias, P. Jovanovic, N. Gailly,

I. Khoffi, L. Gasser, and B. Ford, “Enhancing bitcoin security and performance with strong consistency via collective signing,” in Proc. 25th USENIX Security Symp. USENIX Secur., pp. 279 - 296, 2016.
[25] Scalability of Bitcoin. Sep. 1, 2019. https://en.bitcoin.it/wiki/Scalability
[26] S. Popov, "The tangle", 2018, https://iota.org/IOTA_Whitepaper.pdf.
[27] A. Churyumov, "Byteball: A decentralized system for storage and transfer of value", 2016, https://byteball.org/Byteball.pdf.
[28] C. LeMahieu, "Nano: A feeless distributed cryptocurrency network", 2018, https://nano.org/en/whitepaper.
[29] Huang, Junqin, et al. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," IEEE Transactions on Industrial Informatics 15.6 (2019): 3680-3689.
[30] Yang, Di, et al. "A review on scalability of blockchain," Proceedings of the 2020 The 2nd International Conference on Blockchain Technology. 2020.
[31] Park, Seongjoon, and Hwangnam Kim. "DAG-based distributed ledger for low-latency smart grid network," Energies 12.18. 2019, 3570.
[32] Yang, Wenhui, et al. "LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks," IEEE Transactions on Vehicular Technology 69.6, pp. 5749-5759, 2020.
[33] Frahat, Rzan Tarig, Muhammed Mostafa Monowar, and Seyed M. Buhari. "Secure and scalable trust management model for IoT P2P network," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). IEEE, 2019.
[34] M. Bhandary, M. Parmar and D. Ambawade, "A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle," 2020 5th International Conference on Communication and Electronics Systems (ICCES), COIMBATORE, India, pp. 827-832, 2020.
[35] Popov, Serguei, et al. "The coordicide," Accessed Jan (2020): 1-30.
[36] Codd, Edgar F. Cellular automata. Academic press, 2014.
[37] NKN Lab. NKN: a Scalable Self-Evolving and Self-Incentivized Decentral ized Network, 2018. https://www.nkn.org/doc/NKN Whitepaper.pdf
[38] Azad, Muhammad Ajmal, et al. "M2m-rep: Reputation system for machines in the internet of things," Computers & Security 79, pp. 1-16, 2018.
[39] F. Bao and I.-R. Chen, “Dynamic trust management for Internet of Things applications,” in Proc. Int. Workshop Self-Aware Internet Things, pp. 1 - 6, 2012.
[40] F. Bao, I.-R. Chen, and J. Guo, “Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems,” in Proc. IEEE 11th Int. Symp. Auto. Decentralized Syst. (ISADS), pp. 1 - 7, Mar. 2013.
[41] Wang, Bo, et al. "A reliable IoT edge computing trust management mechanism for smart cities," IEEE Access 8, pp. 46373-46399, 2020.
[42] Wüst, Karl, and Arthur Gervais. "Do you need a blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018.
[43] Otte, Pim, Martijn de Vos, and Johan Pouwelse. "TrustChain: A

Sybil-resistant scalable blockchain," Future Generation Computer Systems 107, pp. 770-780, 2020.
[44] Yang, Zhe, et al. "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things Journal 6.2, pp. 1495-1505, 2018.
[45] She, Wei, et al. "Blockchain trust model for malicious node detection in wireless sensor networks," IEEE Access 7, pp. 38947-38956, 2019.
[46] Cinque, Marcello, Christian Esposito, and Stefano Russo. "Trust management in fog/edge computing by means of blockchain technologies," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018.
[47] Lahbib, Asma, et al. "Blockchain based trust management mechanism for IoT," 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019.
[48] Kochovski, Petar, et al. "Trust management in a blockchain based fog computing platform with trustless smart oracles," Future Generation Computer Systems 101, pp. 747-759, 2019.
[49] Alemneh, Esubalew, et al. "A two-way trust management system for fog computing," Future Generation Computer Systems 106, pp. 206-220, 2020.
[50] Chen, Ray, Jia Guo, and Fenye Bao. "Trust management for service composition in SOA-based IoT systems," 2014 IEEE wireless communications and networking conference (WCNC). IEEE, 2014.
[51] Chen, Ray, Fenye Bao, and Jia Guo. "Trust-based service management for social internet of things systems," IEEE transactions on dependable and secure computing 13.6, pp. 684-696, 2015.
[52] ACM, https://dl.acm.org/
[53] Elsevier, https://www.sciencedirect.com
[54] IEEE, https://ieeexplore.ieee.org/
[55] Springer, https://www.springer.com
[56] Google scholar, https://scholar.google.co.kr
[57] Eric Harris-Braun, Nicolas Luck, Arthur Brock, "Holochain. Scalable agent-centric distributed computing," DRAFT (ALPHA 1) - 2/15/2018. https://whitepaperdatabase.com/wp-content/uploads/2018/08/holochain-HOT-whitepaper.pdf.
[58] Debe, Mazin, et al. "IoT public fog nodes reputation system: A decentralized solution using Ethereum blockchain," IEEE Access 7, pp. 178082-178093, 2019.
[59] Ali, Jawad, et al. "Blockchain-based smart-IoT trust zone measurement architecture," Proceedings of the International Conference on Omni-Layer Intelligent Systems. 2019.
[60] Cinque, Marcello, et al. "Blockchain-empowered decentralised trust management for the Internet of Vehicles security," Computers & Electrical Engineering 86 (2020): 106722.
[61] Chen, Ray, Jia Guo, and Fenye Bao. "Trust management for service composition in SOA-based IoT systems," 2014 IEEE wireless communications and networking conference (WCNC). IEEE, 2014.
[62] Atzori, Luigi, Antonio Iera, and

Giacomo Morabito. "Siot: Giving a social structure to the internet of things," IEEE communications letters 15.11, pp. 1193-1195, 2011.
〔63〕 Dedeoglu, Volkan, et al. "A trust architecture for blockchain in IoT," Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. 2019.
〔64〕 U. Wilensky, "NetLogo," Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, Illinois, 1999.
〔65〕 M. Bottone, F. Raimondi and G. Primiero, "Multi-agent based simulations of block-free distributed ledgers", 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 585-590, 2018.

〈저자소개〉

오 정 민 (Jungmin Oh) 정회원
2004년~2009년: 건국대학교 컴퓨터공학부 학사
2009년~2010년: 티맥스 코어 연구원
2010년~현재: LG전자 선임 연구원
2019년~현재: 고려대학교 정보호대학원 석사과정
〈관심분야〉 FIDO, IoT 보안, 블록체인

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: 고려대학교 사이버국방학과/정보호대학원 정교수
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년: 4차산업혁명위원회 위원: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2020년~현재: 합동참모본부 정책자문위원회 자문위원
〈관심분야〉 보안공학 및 보안내재화 방법론, 보안성 평가/인증, RMF A&A, 암호학 및 블록체인