Journal of the Korea Convergence Society
Vol. 9. No. 9, pp. 83-88, 2018

ISSN 2233-4890
https://doi.org/10.15207/JKCS.2018.9.9.083

블록체인 합의 알고리즘과 공격 분석

김삼택
우송대학교 IT융합학부 교수

Analysis on Consensus Algorithms of Blockchain and Attacks

Sam-Taek Kim
Professor, Division of IT Convergence, Woosong University

요 약 블록체인은 중앙 집중화된 시스템이 아닌 분산화 된 시스템을 구현하는 데에 사용되는 기술로써, 익명성, 투명성 등을 특징으로 한다. 그러나 아직 블록체인을 상용화하기에는 고질적인 공격들이 존재한다. 본 논문에서는 이러한 블록체인을 구현하기 위해서 존재하는 대표적인 합의 알고리즘으로써 Bitcoin, Algorand, 그리고 IOTA를 소개하고, 각각의 합의 알고리즘들이 어떠한 방법으로 블록체인의 고질적인 공격들인 이중 지불 공격이나 시빌 공격을 해결하는지, 혹은 해결하지 못하고 있다면 어떤 방법으로 해결할 수 있는지를 소개한다. 뿐만 아니라 기존의 고질적인 공격이 가능한 새로운 시나리오를 제안한다.

주제어 : 블록체인, 합의 알고리즘, 이중 지불 공격, 시빌 공격, 암호화폐, 비트코인

Abstract The blockchain is the technique which is used in decentralized system instead of centralized system. Its characteristics are anonymous and transparency. However, there are still some traditional attacks. In this paper, we introduced some of the famous consensus algorithm with blockchain: Bitcoin, Algorand, and IOTA. Also, this paper talked about how each consensus algorithm tried to solve those traditional attacks such as double spending attack or sybil attack. Furthermore, if the consensus algorithm does not consider those attacks yet, then the author would introduce additional methods to solve those attacks. Furthermore, this paper proposed the new scenario that can make classical attacks be happened.

Key Words : Blockchain, Consensus algorithm, Double spending attack, Sybil attack, Cryptocurrency, Bitcoin

1. 서론

오늘날 집중화가 아닌 분산화를 통해 투명하고 익명성을 보장하는 블록체인 기술이 급격히 개발되고 있다. 2009년에 발표된 사토시 나카모토 비트코인 백서를 계기로 암호 화폐는 국내에서 큰 열풍을 불러일으키게 되었고, 현재는 블록체인 기술을 암호 화폐뿐만 아니라 사물인터넷, 물류, 금융 등 다양한 분야에 사용하고자 한다. 그러나 현재는 아직 블록체인 기술이 상용화되기 위해서 해결해야 할 한계점들이 많이 존재한다. 예를 들어 엄청난 수의 거래량을 처리할 수 있을 정도의 확장성, 다양한 블록체인들끼리 데이터를 주고받을 수 있는 상호 작용성, 빠른 속도 등의 문제들이 아직 남아있다. 그래서 오늘날엔 나름의 방법을 통해 위와 같은 다양한 문제들을 해결하기 위해 다양한 방법의 블록체인 합의 알고리즘이 개발되고 있다[1-4].

그러나 각각의 블록체인 합의 알고리즘은 다양한 취약점들을 가지고 있다. 해당 알고리즘이 가지고 있는 프로토콜 특징에 의한 전용 취약점도 있겠지만, 모든 블록체인 합의 알고리즘에서 나타날 수 있는 공용 취약점도

*This research is based support of 2018 Woosong University Academic Research Funding.
*Corresponding Author : Sam-Taek Kim(stkim@wsu.ac.kr)
Received August 10, 2018 Revised August 31, 2018
Accepted September 20, 2018 Published September 28, 2018

존재한다. 본 논문에서는 이러한 공용 취약점에 대해서 분석해보았다.

본 논문의 2장에서는 모든 블록체인 합의 알고리즘의 공용 취약점으로써 이중 지불 공격(Double Spending Attack)과 시빌 공격(Sybil Attack)과 네트워크 공격을 소개한다. 3장에서는 오늘날의 대표적인 블록체인 기술로써 비트코인, 알고랜드, 아이오타에 대해 간단히 소개하고, 각각의 기술들이 어떠한 방법으로 이중 지불 공격이나 시빌 공격을 해결하려고 노력하였는지, 혹은 해당 합의 알고리즘들이 미처 위의 공격들을 고려하지 못했다면 어떤 방법으로 해결할 수 있을지 그 알고리즘을 제안하였다.

2. 블록체인 공격

블록체인에는 어떤 합의 알고리즘을 사용하는지에 상관없이 항상 취약한 공격들이 존재한다. 이 부분에선 블록체인 내에 나타나는 고질적인 공격들을 소개하겠다.

2.1 이중 지불 공격(Double spending Attack)

이중 지불 공격은 동일한 코인에 대해 두 번 이상의 서로 다른 거래가 나타나는 공격이다. 예를 들어 공격자 앨리스(Alice)가 가지고 있는 5 BTC를 밥(Bob)에게 주었다는 거래 하나와, 5 BTC를 모두 캐럴(Carol)에게 주었다는 또 다른 거래를 동시에 생성하는 것을 이중지불이라고 할 수 있다. Fig. 1 에서 블록체인에서의 이중 지불 공격 시나리오는 다음과 같을 수 있다. 앨리스가 밥에게 5 BTC를 지불하고 인형을 사려고 한다고 가정해 보자. 처음에 앨리스는 밥에게 5 BTC를 주었다는 거래를 만든다. 그러나 코인이 해당 계좌로 잘 들어갔는지 여부를 확실히 하기 위해서는 대략 1시간이 걸린다. 그러므로 밥의 입장에선 아직 정확하게 앨리스의 5 BTC가 본인 계좌로 들어왔는지 확신할 순 없지만, 앨리스가 그러한 내용의 거래를 생성하였으니까 돈이 들어올 것이라 믿고 앨리스에게 인형을 건네준다. 그런데 동시에 앨리스는 밥에게 보냈다고 했던 5 BTC를 캐럴에게 보내는 거래를 몰래 생성한다. 만약 앨리스가 캐럴에게 5 BTC를 건네준 거래를 포함하는 블록이 후에 실제 블록체인에 올라가게 된다면 밥은 인형을 이미 앨리스에게 주었지만 5 BTC를 받지 못하였으므로 사기를 당하게 된 것이다. 이러한 것이 이중 지불 공격 시나리오이다[1,3,5,11].

2.2 시빌 공격(Sybil Attack)

시빌 공격은 블록체인에서 활동할 노드를 누구나 만들 수 있을 때 나타날 수 있는 공격으로써 한 명의 공격자가 여러 개의 가짜 노드들을 많이 만들어 블록체인의 네트워크를 장악하도록 하는 공격이다. 이는 누구나 네트워크에 쉽게 참여하고 빠져나올 수 있는 특성을 가진 블록체인에게 특히 취약한 공격이다. 예를 들어 주어진 여러 개의 블록들 중에 투표자의 과반수가 선택한 블록이 블록체인에 올려 진다고 가정해보자. 이 때 시빌 공격자는 전체 네트워크의 노드 개수보다 더 많은 가짜 노드들을 생성하여 공격자가 원하는 블록에 찬성하는 투표를 하도록 할 수 있다. 그렇게 되면 공격자가 원하는 거래의 내용이 마음대로 블록체인에 올라가게 된다[1,4].

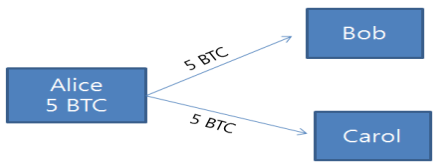

Fig. 1. Scenario of double spending attack

2.3 네트워크 공격들

이 외에도 네트워크 공격이 존재한다. 라우팅 공격(Routing Attack) 혹은 이클립스 공격(Eclipse Attack)이 그 예이다[2,4]. 이는 공통적으로 블록체인의 네트워크를 분리시켜 피해자와 연결된 네트워크만 외부로부터 고립시킴으로써 피해자에게 옳지 않은 메시지를 보내거나 비정상적인 데이터를 보내는 것이 특징이다. 이러한 네트워크 공격 또한 모든 블록체인 프로토콜에서 존재할 수 있다. 그러나 사실상 이러한 공격들은 블록체인 합의 알고리즘과는 상관없이 네트워크상에서 해결해야 하는 문제이기 때문에 이 논문의 주제에 벗어나므로 네트워크 공격은 생략하겠다.

3. 암호화폐의 합의 알고리즘 방어 법

일반적으로 암호 화폐들은 이중 지불 공격을 방어하기 위해서 어떠한 블록을 블록체인에 올릴 것인지를 합의하는 합의 알고리즘을 통해 해결한다. 본 장에서는 고

질적인 블록체인의 공격들에 대해서 대표적인 블록체인 합의 알고리즘들은 각각 어떠한 방법으로 이를 방어하고자 하는지, 혹은 만약 어떠한 공격에 대해 저항성이 없다면, 이를 보완하기 위해서 어떠한 새로운 방법이 있는지를 알아보겠다.

3.1 비트코인(Bitcoin)

Proof of Work(PoW)는 대표적으로 비트코인이 사용하고 있는 합의 알고리즘이다. Fig. 2 에서는 PoW를 통해 생성된 블록들이 어떤 구조로 블록체인에 추가되는지를 보여준다. PoW에선 마이너들이 많은 양의 해시 파워를 소모하여 주어진 퍼즐을 풀게 되고, 먼저 퍼즐을 정확하게 푼 마이너가 비로소 블록체인에 올릴 새로운 블록을 생성할 수 있게 된다[2,3].

비트코인의 경우 이러한 PoW 때문에 많은 양의 컴퓨팅파워를 가지고 있지 못하면 쉽게 이중 지불 공격을 가할 수 없다. 이중 지불을 수행하기 위해서는 공격자가 자신이 만든 거래들을 포함하는 블록들을 생성시킬 수 있어야 하는데, 그러기 위해서는 많은 양의 해시파워를 통해 주어진 문제를 가장 먼저 풀어야 하므로 엄청난 전력이 필요하기 때문이다. 그럼에도 불구하고 여전히 비트코인은 의도적인 블록 포크(fork)를 일으키는 이기적인 채굴기법 공격(Selfish Mining Attack)이나, 전체 해시파워량의 51%를 공격자가 차지하는 51% 공격 등을 통해 다양한 방법으로 이중 지불 공격이 가능하다. 이러한 이중 지불 공격을 막기 위해서는 한 마이너가 전체 컴퓨팅파워의 과반수이상을 가지지 못하는 정책을 만들어야 한다. 그럼으로써 공격자가 만든 이중 지불된 거래를 포함하는 블록을 쉽게 생성하지 못하도록 해야 한다.

비트코인은 시빌 공격에 상대적으로 취약하지 않다. 왜냐하면 공격자가 가짜 노드들을 많이 만들어도 특정량의 해시파워를 가지고 있지 못하다면 어차피 얻을 수 있는 이득이 없기 때문이다. 공격하기 위해서 많은 컴퓨팅 파워를 필요로 하므로 오히려 그만큼의 파워를 가지고 있다면 정상적으로 행동하는 것이 더 큰 이득일 수 있다. 이러한 경제적인 작용 때문에 시빌 공격은 비트코인에서 일어나기 어렵다.

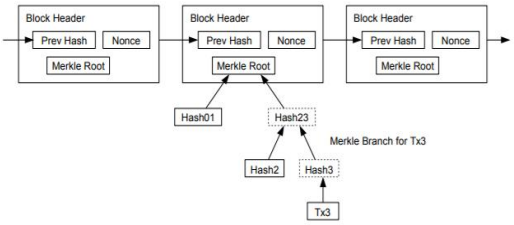

Fig. 2. Overview of Blockchain with PoW

3.2 알고랜드(Algorand)

Byzantine Agreement Consensus 계열 합의 알고리즘 중에서 오늘날 각광받고 있는 것은 알고랜드이다. 알고랜드는 Verifiable Random Function(VRF)를 통한 cryptographic sortition을 통해 위원회(committee)를 무분별하고, 사적으로, 그러나 다른 노드들과의 상호 작용 없이 독립적으로 뽑아 블록체인에 올려 질 새로운 블록들에 대해 위원회 노드들이 투표를 하도록 한다. Fig. 3은 cryptographic sortition을 통해서 선발된 노드들이 메시지를 전파하는 모습을 보여준다. 알고랜드의 경우, 이러한 프로토콜을 사용하기 때문에 블록체인에 대한 포크가 일어날 순 없으므로 이중 지불 공격에 대해서는 어느 정도 저항성을 가진다[7-9].

알고랜드는 시빌 공격에 대해서도 방어할 수 있는 대책을 가지고 있다. 새로운 블록을 투표할 위원회를 랜덤하게 구성할 때, 알고랜드는 VRF 함수와 Proof of Stake(PoS)를 혼합하여 구성한다. 즉, 알고랜드 지분을 많이 가진 노드들이 위원회의 구성원으로써 뽑힐 확률이 더 많게 하면서 동시에 무분별하게 위원회를 동적으로 구성한다는 것이다. 이렇게 함으로써, 공격자, 혹은 공격자가 만든 가짜 노드들이 알고랜드 네트워크에서 상당한 양의 지분을 가지고 있지 못하다면 위원회의 구성원으로써 선발되기가 매우 어려우므로, 가짜 노드들도 무용지물이 된다.

또한 사실상 공격자들이 알고랜드의 지분을 많이 가지고 있다면 시빌 공격을 통해서 얻을 수 있는 이득보다 알고랜드의 안전성을 보장해 알고랜드의 가치를 올리는 것이 더 큰 이득이 될 수 있기 때문에, 굳이 공격을 하지 않을 것이다[6,7,14].

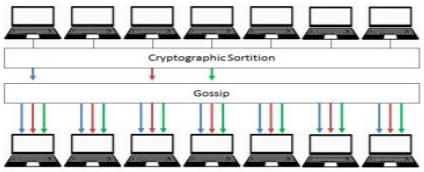

Fig. 3. Overview of Algorand with randomly selected committee with cryptographic sortition

3.3 아이오타(IOTA)

아이오타는 다른 암호 화폐들과는 다르게 새로운 구조의 데이터 저장 방식을 통해 블록체인을 구현한다. 주로 다른 블록체인들의 형태는 하나의 체인으로 이루어져 있지만, 아이오타는 방향성 비 사이클 그래프(Directed Acyclic Graph : DAG)의 구조를 통해 블록체인을 만든다. 그러므로 거래 처리 속도나 확장성이 비트코인과 같은 단일 체인보다는 더 좋은 이점이 있다.

아이오타의 경우엔 이중 지불 공격에 대해서 확률적으로 막을 수 있다고 주장한다. 탱글을 아이오타의 블록체인이라고 할 때, 탱글에는 여러 개의 체인이 존재할 수 있다. Fig. 4는 탱글의 이론적인 모습이다. 탱글에는 여러 개의 체인으로 이루어져있으므로 포크가 일어날 확률이 단일 체인보다 농후하다. 그러나 설사 이중 지불 된 거래가 탱글에 존재한다고 해도 확률적인 인식에 따라 이중 지불된 거래가 속한 서브탱글은 결국 버려지게 될 것이라고 아이오타 백서는 주장하고 있다[9,10]. 그러나 현재는 그러한 확률 식이 정립된 상태가 아니고, Parasite Chain Attack 이나 Splitting Attack 등을 통해 이중 지불 공격이 가능한 상태이다.

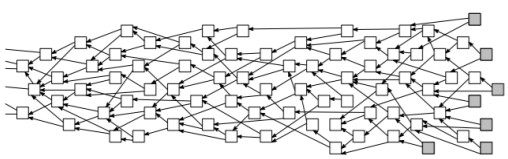

Fig. 4. Overview of Tangle

4. 아이오타(IOTA) 이중 지불 공격시나리오

아이오타가 앞으로 이중 지불에 대해서 저항성을 갖기 위해서는 먼저 이중 지불된 거래가 속한 서브탱글을 확률적으로 버릴 수 있는 식이 확실하게 정립되어야 한다. 또한, 본 논문에서는 백서에서 언급한 시나리오 이외에 여러 개의 서브 탱글 중에 어떤 서브 탱글을 선택할 확률 뿐만 아니라 팁 선택 알고리즘(tip selection algorithm)을 수행시키는 시작점에 따른 이중 지불 공격 시나리오를 제안하였다. 예를 들어 만약 Fig. 5에서와 같이 음영으로 표시된 왼쪽의 파란색 사각형이 원래의 거래라고 한다면, 공격자가 파란색 거래에 대해서 이중 지불 된 거래를 생성하여 그림에서의 오른쪽의 초록색 사각형과 같은 위치에 놓았다고 하자. 이론적으로는, 팁 선택 알고리즘을 통해서 서브탱글 중 하나를 선택하는 과정에서 팁 선택 알고리즘을 수행시키는 시작점에서부터 탱글의 끝 부분까지 탱글에 있는 거래들의 타당성을 모두 체크하기 때문에 이중 지불 된 거래들이 함께 같은 서브탱글에 있을 수 없다. 그러나 아이오타의 풀 노드들은 자기만의 팁 선택 알고리즘을 가질 수 있으므로, 팁 선택 알고리즘의 시작점을 파란색과 초록색 사이에 두게 하여, 거래들의 타당성을 확인하는 과정에서 이중 지불된 거래들이 함께 위치할 수 없도록 할 수 있다. 이러한 시나리오가 가능하니, 팁 선택 알고리즘의 시작점이 안전한 곳에 위치하도록 하는 알고리즘이 추가적으로 개발되어야 한다.

아이오타는 시빌 공격이 어느 정도 가능하다. 공격자가 탱글에 여러 개의 가짜 팁들을 만들어 공격자가 원하는 거래를 선택하도록 할 수 있다. 그러나 아이오타에서도 탱글에 거래를 올리려면 소량의 해시 파워를 통해 PoW를 거쳐야하기 때문에 가짜 거래를 무한히 만들 수는 없다. 아이오타가 시빌 공격에 대해 큰 저항성을 가지기 위해서는 알고랜드나 비트코인과 같이 아무나 함부로 거래를 생성하거나, 팁 선택 알고리즘을 수행시키지 못하고 일정량의 지분을 가지고 있거나, 혹은 네트워크에서 가장 힘이 센 노드를 선택하여 그들만 새로운 거래를 생성하거나 팁 선택 알고리즘을 수행하도록 해야 한다[12,13,15].

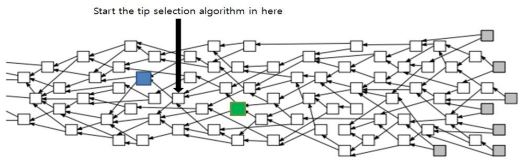

Fig. 5. Scenario when the double spending attack can be happened with the start point of tip selection algorithm

아래의 알고리즘과 같이 아이오타의 이중 지불 공격 시나리오는 미리 원래 거래와 이에 대해 이중 지불된 거래를 탱글에 올린 후, 새로운 팁이 끝에 생성될 때 팁 선택 알고리즘이 실행되는 시작점을 기본 거래와 이중 지불 된 거래 사이 중 랜덤한 위치의 어느 곳으로 고정시킨다.

```
procedure attack_scenario
```

```
new_tip = GenerateNewTip()
positionOne = original_transaction.position
positionTwo = double_spent_transaction.position
srand(unsigned int)time(NULL)
starting_point =
rand()%(positionTwo-positionOne+1)+positionOne
result = tip selection algorithm(starting_point)
if result = true    then
  //attack succeed!
else
  //attack fail!
```

Algorithm 1 : attack_scenario

```
procedure tip selection algorithm(starting_point)
```

```
point = starting_point
while(point<= tip.position)
   // validate conflicted transaction
    if there is conflic then
    return false
    else
    point ++
return true
```

Algorithm 2 : tip selection algorithm

그런 후에 팁 선택 알고리즘을 수행시킨다. 팁 선택 알고리즘에서는 시작점에서 시작하여 이중 지불 된 거래가 없는 지 확인한다. 시작점이 원래의 거래와 이중 지불된 거래 사이에 위치하므로 거래들을 확인하는 과정에서 원래의 거래와 이중 지불된 거래는 공존할 수 없게 된다. 그러므로 사용자는 아무런 문제가 없다고 여기고 팁 선택 알고리즘의 반환 값을 참(True)으로 두게 될 것이다.

위 공격은 팁 선택 알고리즘의 시작점을 제네시스 블록(Genesis block)으로 두면 해결될 수 있을 것이다. 다만 그럴 경우 안정성은 올라갈지 몰라도 성능이나 효율이 떨어질 수 있다.

5. 결론

분산화 시스템을 지향하는 블록체인 기술은 오늘 날에 다양한 한계점을 극복하고 많은 분야에 활용되기 위해서 여러 가지 합의 알고리즘들을 통해 개발되고 있다. 그러나 이러한 합의 알고리즘들에는 공통적으로 해결해야 할 공격들이 존재한다. 이중 지불 공격, 시빌 공격, 네트워크 공격 등이 그 예이다. 본 논문에서는 다양한 합의 알고리즘들이 어떤 방법으로 위의 공격들을 해결했는지 분석하였고, 미처 해결하지 못한 공격들에 대해서는 저자가 어떤 방법으로 해결할 수 있을지 소개하고, 해당 합의 알고리즘에서 고질적인 공격이 가능한 새로운 시나리오를 제안하였다. 특히 알고랜드 에서는 팁 선택 알고리즘을 수행시키는 시작점에 따른 이중 지불 공격 시나리오를 제안하였다.

향후 연구 방향은 안전성도 높으면서 동시에 성능도 향상된 최적의 팁선택 알고리즘개발과 이를 접목시킨 IoT 시스템 취약점 분석이다.

REFERENCES

[1] J. R. Douceur.(2002). The Sybil attack. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA.

[2] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In Proceedings of the 24th Usenix Security Symposium, Washington, DC. 129 - 144.

[3] S. Nakamoto. (2008) . Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[4] C. Decker and R. Wattenhofer. (2013). Information propagation in the Bitcoin network. In Proceedings of the 13th IEEE International Conference on Peer-to-Peer Computing.

[5] I. Eyal and E. G. Sirer. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Proceedings of the 2013

Financial Cryptography and Data Security Conference.
[6] D. Mazières. (2014). The Stellar consensus protocol: A federated model for internet-level consensus. https://www.stellar.org/papers/stellarconsensus-protocol.pdf
[7] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. (2017). "Algorand: Scaling byzantine agreements for cryptocurrencies," in Proeedings. 26th ACM Symp. Operating Syst. Principles, 51 - 68.
[8] M. Castro and B. Liskov. (1999). "Practical byzantine fault tolerance," in Proceeding. 3rd USENIX Symp. Operating Syst. Des. Implementation, 173 - 186.
[9] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, (2017). "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '17. ACM, 195 - 209.
[10] S. Bag, S. Ruj, and K. Sakurai, (2016). "Bitcoin block withholding attack :Analysis and mitigation," IEEE Transactions on Information Forensics and Security, 99, 1 - 12.
[11] G. Karame, E. Androulaki, and S. Capkun. Double-Spending (2012). Fast Payments in Bitcoin. In Proceedings of ACM CCS 2012.
[12] S, Popov, The Tangle, https://iotatoken.com/IOTA_Whitepaper.pdf
[13] bitcoinj. Working with micropayment channels. https://bitcoinj.github.io/working-with-micropayments
[14] J. Chen and S. Micali. (2017). Algoland. Technical report, URL http://arxiv.org/abs/1607.01341
[15] S. H. Hong & S. H. Park (2017). The Research on Blockchain-based Secure IoT Authentication. *The Korean Journal of The Korea Convergence Society, 8(11),* 57-62.

김 삼 택(Sam-Taek Kim) [정회원]

- 1987년 8월 : 중앙대학교 중앙대학원 전자계산학과 (이학 석사)
- 2005년 2월 : 중앙대학교 중앙대학원 컴퓨터공학과 (공학 박사)
- 1990년 5월 ~ 1995년 2월 : LG연구소 전임연구원
- 1995년 3월 ~ 현재 : 우송대학교 IT융합학부 교수
- 관심분야 : 무선/유선 네트워킹, VoIP, 모바일 컴퓨팅, IoT, Big Data, USN, Blockchain