저전력 고속 사물 인터넷을 위한 효율적인 믹스넷 기술에 대한 연구

전가혜 · 황혜정 · 이일구*

성신여자대학교

A Study on Efficient Mixnet Techniques for Low Power High Throughput Internet of Things

Ga-Hye Jeon · Hye-jeong Hwang · Il-Gu Lee*

Sungshin Women's University

E-mail : 20171988@sungshin.ac.kr / 20200974@sungshin.ac.kr / iglee@sungshin.ac.kr

요 약

최근 데이터가 모든 산업의 발전과 새로운 가치를 창출하는 촉매 역할을 하는 데이터 경제 사회로 전환되고 있으며, 코로나19로 인해 디지털 전환이 가속화되고 있다. 다가오는 지능형 사물인터넷 시대에 안전하고 효율적으로 데이터를 활용하기 어려운 중앙 집중형 시스템의 보안 문제점을 해결하기 위해 블록체인 및 믹스넷과 같은 분산형 시스템 이용 가능성이 크게 대두되고 있다. 블록체인은 데이터를 투명하고 분산된 형태로 관리하며 참여자들 간의 합의를 통해 데이터에 대한 신뢰성과 무결성을 보장하지만 데이터 투명성으로 인해 사용자의 프라이버시가 위협받는다. 한편, 프라이버시를 보호하기 위한 믹스넷 기술은 분산 네트워크에서 프라이버시를 보호하지만 비효율적인 전력 소비 효율과 처리속도 문제로 저가, 경량, 저전력 사물인터넷에 활용되기 어렵다. 본 논문에서는 종래의 믹스넷 기술의 한계점을 분석하고 저전력 고속 사물인터넷을 위한 믹스넷 기술 방식을 제안한다.

ABSTRACT

Recently data has been transformed into a data economy and society that acts as a catalyst for the development of all industries and the creation of new value, and COVID-19 is accelerating digital transformation. In the upcoming intelligent Internet of Things era, the availability of decentralized systems such as blockchain and mixnet is emerging to solve the security problems of centralized systems that makes it difficult to utilize data safely and efficiently. Blockchain manages data in a transparent and decentralized manner and guarantees the reliability and integrity of the data through agreements between participants, but the transparency of the data threatens the privacy of users. On the other hand, mixed net technology for protecting privacy protects privacy in distributed networks, but due to inefficient power consumption efficiency and processing speed issues, low cost, light weight, low power consumption Internet Hard to use. In this paper, we analyze the limitations of conventional mixed-net technology and propose a mixed-net technology method for low power consumption, high speed, and the Internet of things.

키워드

Mixnetwork, Internet of Thing, Blockchain, Privacy, Anonymity

Ⅰ. 서 론

중앙 집중형 시스템은 데이터의 위변조를 파악하기 어렵고, 문제 발생 시 전체 시스템을 사용할 수 없는 단일 지점 장애 문제가 제기되었다. 이러한 문제를 해결하는 방안으로 분산형 시스템의

* corresponding author

이용이 대두되고 있다. 대표적인 분산형 시스템으로는 블록체인 기술이 있다. 블록체인은 참여자들 간의 합의를 통한 거래내역이 기록된 거래 장부를 모든 참여자들이 가지고 있는 기술이다. 데이터를 투명하고 분산된 형태로 관리하여 데이터에 대한 신뢰성과 무결성을 보장한다. 이에 금융기관을 비롯하여 신원, 물류, 유통, 사물인터넷 등 산업과 생활 전반에 걸쳐 사용 영역이 점차 확장되고 있다. 하지만 데이터를 모든 참여자가 공유하는 과정에서 개인의 프라이버시 침해 문제가 발생할 수 있다. 기술의 발전으로 개인과 밀접한 데이터가 필요 이상으로 과도하게 수집되고 처리되어 프라이버시 내재화 (Privacy by Design)의 중요성이 커지고 있다. 특히 데이터 추적 기술은 개인의 민감정보 수집과 유출뿐만이 아니라 물리적 공격 수단으로 악용될 수 있으므로 추적방지 기술은 매우 중요하다. 따라서 블록체인과 같은 분산 환경에서의 추적을 방지하는 방안으로 믹스넷(Mixnet)의 적용을 제안한다. 2장에서는 믹스넷에 대해 알아보고 3장에서는 분산 환경에서의 믹스넷 적용 모델을 제시한 후 4장에서 결론과 향후 연구 방향을 제시한다.

II. 믹스넷

믹스넷은 패킷을 혼합하여 전달하는 라우팅 방식이다[2]. 믹스넷은 패킷 암호화, 패킷 혼합, 패킷 순서 재배치를 통해 추적을 방지한다. 이때, 추적이 어렵다는 것은 거래 내역이 포함된 패킷의 이동 경로를 파악하기 어렵다는 것뿐만 아니라 송·수신 노드 사이의 직접적인 연결을 확인할 수 없다는 것을 의미한다.

패킷 암호화는 이동 경로의 공개키를 활용한다. 이동 경로의 역순으로 암호화를 겹겹이 하고 마지막에는 송신 노드 바로 다음 경로 노드의 공개키로 암호화를 한다. 겹겹이 암호화된 패킷은 중간 이동 경로에 포함되어 패킷이 거쳐 간 노드라도 자신의 이전 노드와 자신 다음의 노드만 알 수 있다. 이때 패킷의 암호화나 복호화가 이뤄지더라도 동일한 규격을 유지하기 위해 Sphinx 기술을 이용하여 패킷의 길이와 같은 형태만으로도 정보를 유추하는 것을 방지한다[3].

패킷 혼합은 여러 패킷을 모아 섞는 것이다. 이때 최대한 많은 패킷을 함께 섞는 것이 중요하다. 패킷이 많을수록 패킷을 특정하기 어렵고 이동 경로의 경우의 수가 많아져 추적이 어려워지기 때문이다. 그러므로 많은 패킷을 모은 후 가짜 패킷을 만들어 함께 섞는다[4]. 가짜 패킷을 만들어 사용하면 추적가능성이 낮아질 뿐만이 아니라 패킷이 모이는 데 걸리는 시간을 줄일 수 있다.

패킷 순서 재배치는 패킷의 송신 순서의 역순으로 수신하면서 재배열하는 것이다. 패킷이 송신된 순서대로 수신된다면 송·수신 노드의 연결 구조를 파악할 수 있다.

표 1. 주요 믹스넷 비교

Techniques	Using Fake packet	Low Latency	Using Block chain
SG-Mixes[2]	O	X	X
Vuvuzela[4]	O	X	X
Nym network[5]	O	O	O

믹스넷을 분산 환경에 적용하기 위한 시도로는 표1과 같은 Nym network가 있다[5]. 하지만 Nym network의 구조는 Mix server가 별도로 존재하고 해당 서버를 사용하기 위한 Client를 검증하기 위한 방식으로만 블록체인을 사용하고 있어서 확장성이 제한되고 복잡성이 증가하는 문제가 있다.

III. 분산환경에서의 믹스넷 적용 모델

본 연구에서 제안하는 모델은 분산 환경에 믹스넷을 적용하여 개별 노드가 Client이자 Mix server가 된다. 그러므로 Nym network와 같이 별도의 Mix server가 존재하지 않는다. 개별 노드에서 패킷 암호화, 패킷 혼합, 패킷 순서 재배치를 모두 수행한다. 다른 노드에서 수신한 패킷들은 가짜 패킷과 함께 다음 노드로 이동한다. 해당 과정은 수신 노드에 패킷이 도착할 때까지 반복되며, 네트워크 전체적으로 이뤄진다.

가짜 패킷을 추가하는 것은 익명성을 높이지만 처리 속도 저하를 발생시킨다. 기존 믹스넷은 참여자가 증가함에 따라 가짜 패킷 생성 및 처리 과정에 지연이 발생한다. 하지만 분산 환경에 적용 시 익명성 보장에 필요한 가짜 패킷을 여러 노드들이 나눠서 생성하기 때문에 처리 속도를 줄일 수 있다.

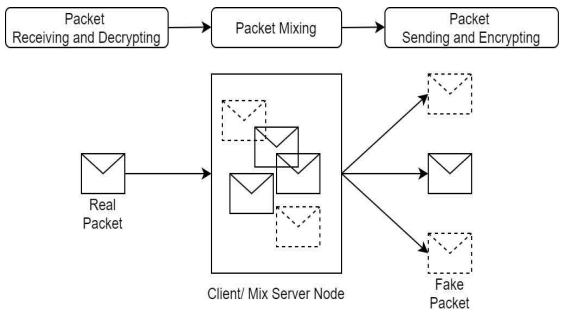

그림1. 가짜 패킷 조절 가능한 믹스넷

또한 기존 믹스넷은 실제 패킷수를 고려하지 않고 가짜 패킷을 생성한다. 이 역시 참여자가 증가함에 따라 처리 속도를 저하시켜 믹스넷의 확장성을 저하시킨다. 본 연구에서 제안한 모델은 네트워크 상황에 따라 가짜 패킷량을 조절한다. 그림1과 같이 네트워크 상황에 따라 가짜 패킷수를 제어하여 일정한 익명성과 처리 속도를 보장한다. 이는 네트워크 복잡도를 낮춰 IoT와 같은 저전력 모델의 확장성을 높인다.

이처럼 믹스넷을 분산 환경에 적용한 결과, 공공거래장부에 거래 내역 자체는 존재하지만 이 거래 내역을 이용하여 거래자를 특정하거나 거래 과정 추적은 어렵다. 이는 거래 참여자의 익명성을 보장한다.

Ⅳ. 결 론

분산 환경은 데이터를 공유하여 데이터의 무결성과 신뢰성을 제공한다. 하지만 그 과정에서 개인의 프라이버시 침해 문제가 발생할 수 있다. 프라이버시를 보호하기 위해 분산 환경에 믹스넷 적용을 제안한다. 개별 노드들은 Client이자 Mix server가 되어 별도의 Mix server가 필요하지 않다. 가짜 패킷을 분산하여 생성하므로 처리 속도를 빠르게하며, 네트워크 상황에 따라 가짜 패킷량을 조절하여 일정 수준의 익명성과 처리 속도를 보장한다. 향후 제안 모델의 시뮬레이션을 구현하여 추적 불가능성과 처리 속도 향상 입증할 것이다.

Acknowledgement

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아 수행된 연구임.

References

[1] Bitcoin: A peer-to-peer electronic cash system : https://bitcoin.org/bitcoin.pdf

[2] D. Kesdogan, J. Egner and R. Büschkes, “Stop- and- Go-MIXes Providing Probabilistic Anonymity in an Open System”, Springer, Vol. 1525, pp. 83-98, Nov. 1998.

[3] G. Danezis and I. Goldberg, “Sphinx: A Compact and Provably Secure Mix Format”, in 30th IEEE Symposium on Security and Privacy, May. 2009

[4] J. V. D. Hooff, D. Lazar, M. Zaharia and N. Zeldovich, “Vuvuzela: scalable private messaging resistant to traffic analysis”, in SOSP '15: Proceedings of the 25th Symposium on Operating Systems Principles, pp. 137-152, Oct. 2015.

[5] A. The Nym Network : https://nymtech.net/nym-whitepaper.pdf