

산업용 IoT의 데이터 보안성 향상을 위한 Raft 합의 알고리즘 기반 데이터 분산 서비스

장민희¹, 이재민², 김동성^{*}

금오공과대학교 IT융복합공학과^{1,2,*}

{unimini27¹, ljmpaul², dskim^{*}}@kumoh.ac.kr

Data Distribution Service based Raft Consensus Algorithm For Improving Data Security of Industrial IoT

Min-Hui Jang¹, Jae-Min Lee², Dong-Seong Kim^{*}

Kumoh National Institute of Technology

Dept. of IT Convergence Eng^{1,2,*}

요약

본 논문은 산업용 IoT의 데이터 보안성 향상을 위한 블록체인 기반 데이터 분산 서비스를 제안한다. 산업용 IoT(IIoT, Industrial Internet of Things) 환경은 ICBM(IoT, Cloud Computing, Big data, Mobile) 기술을 융복합하여 산업의 생산성과 수익성을 개선하는 자동화 중심의 대규모 분산 시스템이다. 이를 유연하게 운영하기 위해서는 각 산업용 장비가 가진 프로토콜 모두 호환이 가능하고 실시간 상태 메시지 공유가 가능해야 한다. 이러한 네트워크의 상호운용성 향상을 위하여 DDS 미들웨어 기반 플랫폼이 연구되었으나 외부의 침입으로 인한 데이터의 위·변조가 발생하면 데이터의 신뢰성을 보장할 수 없다. 본 논문에서는 데이터 무결성과 보안성을 보장하기 위해 Raft 합의 알고리즘을 활용한 산업용 IoT의 미들웨어를 제안하고자 한다.

I. 서론

산업용 IoT(IIoT, Industrial Internet of Things) 환경은 ICBM(IoT, Cloud Computing, Big data, Mobile) 기술을 융복합하여 산업의 생산성과 수익성을 개선하는 자동화 중심의 대규모 분산 시스템이다. 이러한 환경은 산업용 장비와 운영시스템 간 혹은 산업용 장비 간 생산 정보를 실시간, 양방향으로 주고받음으로써 유동적으로 제어하여 운영할 수 있다[1]. 산업용 IoT 환경을 유연하게 운영하기 위해서는 각 장비가 가진 프로토콜 모두 호환이 가능하고 실시간으로 상태 메시지를 주고받을 수 있어야 한다. 기존연구에서는 이러한 요구사항을 만족하기 위해 대규모 산업용 장비의 신뢰성, 실시간성을 보장하기 위하여 DDS(Data Distribution Service) 미들웨어를 결합한 시스템이 연구되고 있다[2]. 이러한 시스템은 산업용 장비의 생산데이터, 사고 및 고장과 생산중단을 최소화하기 위한 유지관리 데이터를 포함하고 있다. 따라서 외부의 침입으로 인한 데이터의 위·변조가 발생하면 데이터의 신뢰성을 보장할 수 없으므로 이러한 데이터를 활용한 유동적인 생산계획을 진행할 수 없으며 오동작, 중단 등의 사고로 인한 막대한 인명, 자산 피해 등이 발생할 수 있다[3].

본 논문에서는 산업용 IoT 네트워크 환경에 블록체인을 활용하여 각 노드에서 발생하는 데이터의 보안성을 향상하는 방안을 제안한다. 제안된 시스템은 DDS를 통해 노드 및 운영시스템 간 상호작용으로 전력 데이터를 실시간으로 파악하여 탄력적인 전력 공급량을 조절할 수 있다. 이러한 데이터는 폐쇄형 네트워크 환경의 DDS에 적용하기 적합한 Raft 합의 알고리즘 기반 Private 블록체인 네트워크를 통해 관리함으로써 데이터의 기밀성, 신뢰성, 무결성을 확보할 수 있도록 한다.

II. 기존 연구의 문제점 분석

기존의 산업용 IoT 인프라의 상호운용성을 위한 DDS 플랫폼 구성은 그림 1과 같다. 해당 시스템은 산업용 IoT를 구성하는 산업용 IoT 장비

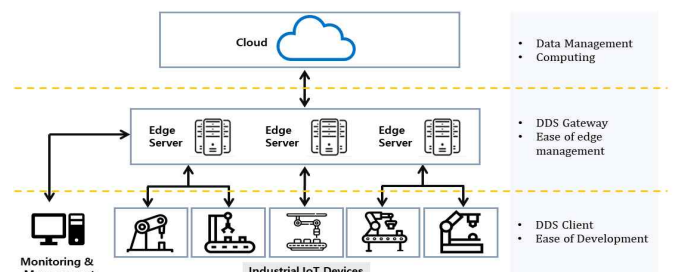


그림 1 IIoT의 엣지 컴퓨팅 플랫폼 기반의 데이터 분산 서비스에서 DDS Client, IoT 서버에서 DDS Gateway, 클라우드에서 Database 환경으로 구성된다. 산업용 장비는 생산 데이터가 발생할 시, 해당 서버로 전송하고 모니터링 시스템에서는 Database를 포함한 클라우드에 저장된 데이터를 활용하여 모니터링 한다[3]. 그러나 이러한 시스템은 외부의 침입이 발생하였을 때 데이터의 위·변조에 대한 위험과 소비자의 전력 소비 패턴과 같은 정보의 유출에 대한 대처방안이 부족하다. 이는 산업 환경을 실시간으로 파악하여 생산 전략을 탄력적으로 조절하고 실시간 설비 모니터링을 통해 유지보수를 해야 하는 산업용 IoT 환경에서 데이터의 무결성을 보장할 수 없을 경우 치명적인 문제가 발생할 수 있음을 의미한다.

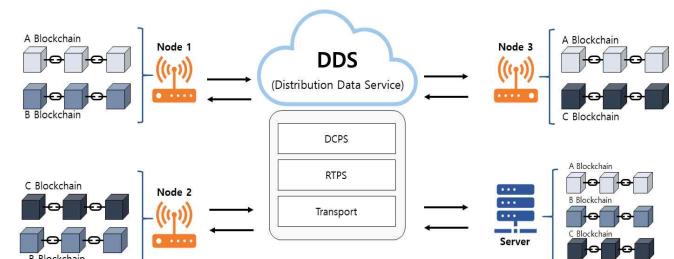


그림 2 합성 전투 시스템의 데이터 보안성 향상을 위한 블록체인 기법 구성도 따라서 [4]에서는 DDS 미들웨어 기반 네트워크 환경에서 그림 2와 같이 다수의 센서 및 장비들로 구성되고, 실시간성과 보안성이 요구되는 합

정 전투 시스템의 대용량 데이터의 보안성을 향상하는 PBFT 합의 알고리즘 기법을 제안하고 있다. 그러나 해당 연구에서 채택한 PBFT 합의 알고리즘은 합의 과정에서 발생하는 중복 확인과 인증 절차에서 총 노드 수 N 에 대해 발생하는 네트워크 통신 횟수는 N^2 가 된다. 이는 노드의 수가 증가함에 따라 복잡도도 증가해 합의를 도출하기 어렵다는 것을 뜻한다.

III. 데이터 보안 향상을 위한 Raft 합의 알고리즘 기반 DDS 아키텍처

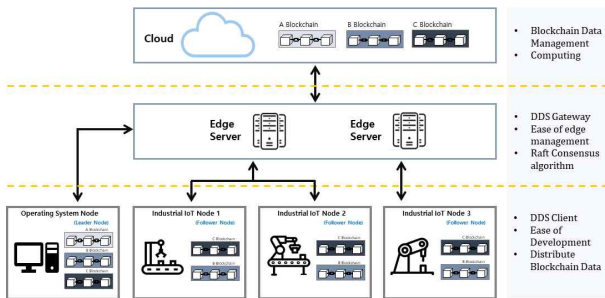


그림 3 데이터 보안 향상을 위한 Raft 합의 알고리즘 기반 DDS 아키텍처

본 논문에서 제안하는 산업용 IoT의 데이터 보안성 향상을 위한 Raft 합의 알고리즘 기반 DDS 아키텍처는 그림 3과 같이 구성된다. 제안하는 시스템 아키텍처는 산업용 IoT를 구성하는 산업용 장비에서 DDS Client, 이러한 장비를 관리하는 서버에서 DDS Gateway, Database 기반 Cloud로 구성된다. 이로써 산업용 장비, 운영시스템 간 논리적 통신이 가능하다.

산업용 장비에서 발생하는 데이터는 합의 알고리즘을 통하여 산업용 인프라를 구성하는 모든 노드와 합의 과정을 진행한 후 블록체인에 저장하여 분산 저장하도록 한다. 이때 사전에 허가받는 노드만 네트워크 참여가 가능하며 폐쇄형 네트워크 환경에 용이한 Private 블록체인의 Raft 합의 알고리즘과 DDS 미들웨어를 활용하고자 한다. 본 논문에서 제안하는 DDS 기반 Raft 합의 알고리즘을 통한 블록체인 생성과정은 다음과 같다. Raft 합의 알고리즘 과정은 크게 Propose, Request & Response, Commit, Apply로 구성된다. Leader 노드는 Log 및 Meta 데이터를 Append Entry 메시지로 Transaction 정보를 전송하여 각 노드는 동기화 과정을 진행한다. 이때 Topic을 생성하고 해당 Topic을 구독하고 있는 Follow 노드로 전송할 수 있도록 한다. Commit의 성공 여부 파악 후 Heartbeat Topic을 통해 Leader 노드와 Follower 노드는 주기적으로 동작 중지가 없음을 확인하고 이때 Follower 노드는 전송받은 Commit 데이터에 대한 Log 값을 통해 새로 추가할 블록을 blockchain 데이터에 추가하도록 한다.

이러한 방안은 단순 고장이 발생한 노드뿐만 아니라 악의적 노드가 발생하여도 PBFT 합의 알고리즘을 통해 과반수의 데이터를 기반으로 판단하기 때문에 전체 데이터의 신뢰성을 보장할 수 있다. 또한 블록체인 데이터는 위·변조에 대한 위험이 없으므로 데이터의 무결성을 보장하여 산업용 IoT 인프라를 구성하는 시스템을 안정적으로 운영할 수 있다.

VI. 모의실험 및 성능 평가

그림 4는 합의 알고리즘 및 DDS 미들웨어를 적용한 후 데이터 전송 지연 시간을 비교한 그래프이다. 수평축은 노드 개수이고 수직축은 트랜잭션 데이터를 전송하는데 걸린 지연 시간을 나타낸다. PBFT 합의 알고리즘은 네트워크에 참여하는 모든 노드에 합의를 위한 통신이 이루어져야 하여 노드의 수가 증가할수록 복잡도도 증가해 지연을 나타냄을 보인다. Raft 합의 알고리즘은 이에 비해 비교적 적은 지연을 보인다. 또한 기존 연구에서 제안한 기법은 데이터 공유 횟수를 줄여 PBFT만을 이용한 데이터 공유 기법보다 10배 적은 속도를 보인다. 그러나 PBFT 합의 알고리즘

의 복잡성으로 인해 Raft 알고리즘과 비슷한 속도를 보이고 있으며, 노드 수가 광범위하게 증가하게 되면 Raft 알고리즘보다 높은 지연 시간을 나타낼 것으로 예상된다. 본 논문에서 제안하는 기법은 4가지 기법 중 가장 낮은 지연 시간을 나타내며 이로써 데이터의 무결성과 실시간성 모두 만족할 수 있음을 알 수 있다.

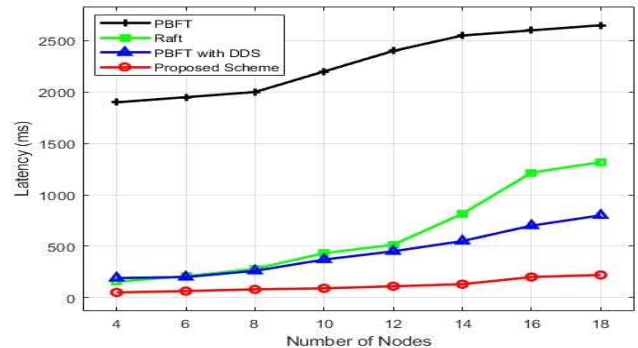


그림 4 합의 알고리즘 및 DDS를 적용한 합의 알고리즘의 지연 시간 비교

VI. 결론 및 향후 연구

본 논문에서는 산업용 IoT 인프라를 구성하는 장비들에서 발생하는 데이터를 DDS 도메인을 통한 Raft 합의 알고리즘의 합의 과정으로 블록체인화 하여 데이터의 신뢰성 및 무결성을 확보하였다. 또한 성능분석을 통해 실시간성을 충족함을 보여주었다.

향후 연구로는 제안한 기법을 바탕으로 산업용 장비와 운영시스템 간 혹은 산업용 장비 간 상호작용을 통한 데이터를 빅데이터화 후 머신러닝 기법에 적용하여 산업망 환경을 유연하게 운영하고 예측할 수 있는 방안을 고려해 볼 것이다.

ACKNOWLEDGMENT

본 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원사업으로 수행된 연구(2018R1A6A1A03024003) 및 과학기술정보통신부 및 정보통신기획평가원의 Grand ICT연구센터지원사업의 연구결과로 수행되었으며(IITP-2020-2021-0-01612), 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2019R1F1A1064055).

참고 문헌

- [1] Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu and Hongbo Zhu, "Blockchain for the IoT and industrial IoT: A review", IEEE Transactions on Smart Grid, Vol. 10, 2020
- [2] J.H Cha, J.M Lee and D.S Kim, "Data Distribution Service based on Edge Computing Platform of Industrial IoT", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 1164-1165, Aug. 2020
- [3] J.H Cha, J.W Lee, J.M Lee and D.S Kim, "Real-time Middleware Application and Trend Study for Civil and Military ICT Convergence Technologies", The Journal of The Korean Institute of Communication Sciences, pp. 47-54, Sep. 2020
- [4] J.W Lee, J.M Lee, D.S Kim and J.W Kim, "Design of Blockchain Scheme for Improving Data Security of Naval Combat Systems", Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 72-73, 2020