이 일 구 교수 지도

석사학위 청구논문

분산 네트워크 환경에서의 보안 통신 방법

2023

성신여자대학교 대학원

미래융합기술공학과

박 나 은

분산 네트워크 환경에서의
보안 통신 방법

이 일 구 교수 지도

이 논문을 석사학위논문으로 제출함

2022년 11월

성신여자대학교 대학원
미래융합기술공학과
박 나 은

인 준 서

박나은의 석사학위 논문으로 인준함

2022년 11월

심사위원장 김 성 민 (서명 또는 인)

심 사 위 원 이 일 구 (서명 또는 인)

심 사 위 원 김 경 진 (서명 또는 인)

성신여자대학교 대학원

논문 개요

4차 산업 혁명과 함께 사물인터넷(IoT, Internet of Things), 무선 센서 네트워크(WSN, Wireless Sensor Network) 등 초연결 사회를 실현하기 위한 기술들이 활발히 연구되고 있다. 기존 유선 네트워크 대비 확장성이 뛰어나고 환경적 제약이 없어, 스마트 홈, 스마트 시티, 스마트 팩토리 등 여러 분야에서 적용할 수 있다. 그러나 여러 장치로 이루어진 광범위한 네트워크 연결이 이루어지면서 보안성, 사용성 측면에서의 성능 열화 문제가 발생한다. 이러한 문제를 해결하고자 망 분리 기술과 RAW(Restricted Access Window) 기술 등이 제안되어 이용되고 있다. 그러나 종래의 기술들은 보안성이 향상되면 사용성이 열화되고, 반대로 사용성이 향상되면 보안성이 열화되는 보안성-사용성 간 트레이드오프 관계가 존재하는 한계점이 있다. 본 논문에서는 보안성과 사용성을 동시에 향상하고 이기적 노드로 인한 성능 문제를 완화하고자 분산 네트워크 환경에서의 인증 모델과 네트워크 내 이기적 노드 대응 방법 두 가지 방법론을 제안한다. 실험 결과에 따르면 인증 모델에서는 지연 시간 요구사항 측면에서 종래 모델 대비 약 76% 높은 인증 수준을 보장함을 보였으며, 이기적 노드의 대응 모델에서도 이기적 노드의 자원 독점을 약 80% 완화할 수 있음을 증명했다.

목 차

표 차 례

그림 차례

Ⅰ. 서 론

최근 4차 산업 기술이 발전하면서 초연결 사회를 실현하기 위한 통신 기술들이 활발히 연구되고 있다. 그중에서도 사물인터넷(IoT, Internet of Things)과 무선 센서 네트워크(WSN, Wireless Sensor Network) 기술은 기존 유선 네트워크 인프라 대비 물리적, 환경적 제약이 없을 뿐 아니라, IoT 센서를 이용하여 다양한 산업 환경에도 적용할 수 있어서 확장성이 뛰어나다. 그러나 다양한 IoT 기기들과 센서들로 이루어진 광범위한 네트워크 연결이 활성화되면서 보안성, 통신 성능 등의 열화 문제가 대두되고 있다.

이러한 한계점을 해결하는 방법 중 망분리 기술과 RAW(Restricted Access Window) 기술이 연구되고 있다. 망분리 기술은 네트워크 연결망을 논리적, 물리적으로 분리하여 외부 네트워크에서의 접근을 차단하는 기술로, 외부 트래픽으로 인한 보안 위협을 차단해 높은 수준의 보안성을 유지할 수 있다. 그러나 분리망에 대한 사용자의 접근이 어렵고, 데이터 전송을 위해 이동식 스토리지를 이용하게 되는 경우 해킹 우려가 발생하므로 보안성과 사용성 간의 트레이드오프 관계가 발생한다. RAW 기술은 IEEE 802.11 ah 표준에서 사용되는 방식으로 임의 그룹이 각 슬롯을 할당받고, 할당받은 슬롯 내에서만 경쟁하게 되므로 네트워크 내 충돌 확률을 낮추고 스루풋은 향상할 수 있어 효율성이 뛰어나다. 그러나 네트워크 내부에 자원을 독점하는 이기적인 노드가 존재하게 되는 경우, RAW 기술은 기존과 같은 성능을 보장하지 못한다.

이처럼 종래에 많은 기술이 연구됐지만, 통신 모델에서 보안 문제를 반영하게 되는 경우 성능 열화를 초래할 수 있다. 본 연구에서는 대규모 네트워크 환경에서 보안성과 사용성을 보장하기 위한 2가지 기술을 제안한다.

첫째, 보안성을 위한 연구의 경우 분산 네트워크 환경에서 더 높은 보안성과 사용성 수준을 동시에 보장하기 위한 “안전한 네트워크 연결을 위한 분산 인증 메커니즘(DAM4SNC)”을 제안한다. DAM4SNC는 인증 성공 횟수와 거리에 따른 차등화된 인증 수준을 제공함으로써 보안 수준을 강화한다.

둘째, 사용성 측면 연구의 경우 이기적 노드에 대한 빠른 탐지와 대응을 위한 기술로써 이기적 노드 대응을 위한 “그룹핑 기반의 백오프 조정 방법”을 제안한다. 중앙 서버에서 임의로 연결된 노드들을 절반씩 그룹핑하고 선택된 그룹만 이기적 노드와 유사한 수준의 백오프 값을 가지도록 조정하여 경쟁함으로써 이기적 노드의 네트워크 자원 독점을 완화할 수 있다.

본 논문은 2개 PART로 구성된다. Ⅱ절 PART 1에서는 분산 네트워크 환경에서의 인증 모델을 제안하고, Ⅲ절 PART 2에서 네트워크 내 이기적 노드대응 방법을 제안한다. 마지막으로 Ⅳ절에서는 두 연구를 요약하며 논문을 마무리한다.

Ⅱ. PART 1: 분산 네트워크 환경에서의 인증 모델

1. 서론

최근 사이버 보안 사고의 피해 규모와 심각성이 증가하고 있으며, 이에 따라 점점 지능화되는 보안 위협에 대응하여 중요 정보를 보호하기 위한 시스템 개발이 필요하다[1]. 이러한 요구사항을 해결하기 위해 정부에서는 국가정보보호 기본지침을 통해 망 분리라는 개념을 도입했다[2].

망 분리란 기업망과 외부 인터넷망을 논리적, 물리적으로 분리하는 기술, 환경을 의미하며, 인터넷 연결망을 원천적으로 차단하여 외부의 공격을 차단하는 것을 말한다[3]. 그러나 모바일 저장 매체를 사용하여 사용자 또는 다른 네트워크 간에 분리된 네트워크에서 데이터를 전달하면 보안 수준이 저하되고 시스템의 보안 취약성이 발생할 우려가 있다[4, 5]. 따라서 이러한 한계를 극복하기 위해 네트워크 연결 기술이 필요하다.

현재의 네트워크 연결 개념은 논리적, 물리적 네트워크 분리 및 연결 방식을 이용한다. 따라서 사용성 혹은 보안성 중 하나가 강화되면 다른 하나가 약해지는 문제가 발생한다[5, 6]. 이러한 트레이드오프 문제는 네트워크 사용자의 수와 네트워크 접속 빈도가 증가함에 따라 서비스 품질과 보안 성능에 큰 영향을 미칠 수 있어 해결해야 할 중요한 문제점이다[6]. 따라서 기존 기술의 한계점을 극복하기 위해 분리된 네트워크와 같은 보안 수준을 유지하면서 사용성을 향상할 수 있는 네트워크 연결 솔루션이 필요하다.

본 연구에서는 네트워크 연결 기술의 트레이드오프 문제를 해결하고, 분산 네트워크 환경에서 더 높은 보안성과 사용성 수준을 동시에 보장하기 위한 “안전한 네트워크 연결을 위한 분산 인증 메커니즘(DAM4SNC)”을 제안한다. 분산 노드 간의 주기적인 인증을 기반으로 분리된 네트워크와 통신함

으로써 기존의 중앙집중식 네트워크 연결 솔루션의 사용성과 보안성 측면의 비효율성을 해결한다. 연결 네트워크의 분산 노드는 신뢰할 수 있는 노드와 주변 노드 간 주기적인 인증을 시도함으로써 인증 성공 횟수와 거리(홉 수)에 따라 인증 수준을 차등화하여 보안 수준을 강화할 수 있다.

논문의 주요 기여점은 다음과 같다.

1) 분산 환경에서 망 분리 기술의 본질적인 트레이드오프 문제를 제시하고 이를 개선하기 위한 효과적이고 간단한 모델 DAM4SNC를 제안한다.

2) DAM4SNC는 별도의 네트워크에서 안전한 통신 구조를 도입하고 있다. 실험 결과 DAM4SNC는 프레임 집성 및 트러스트 노드 기술을 적용하지 않는 종래 방식 대비 같은 인증 수준에서 모든 경우에서 제안 방식의 지연 시간 측면의 상대적 효율성(REP, Relative efficiency of proposed scheme)이 약 420% 이상임을 증명했다.

논문은 다음과 같이 구성된다. 2장에서는 제안된 DAM4SNC 기술과의 비교를 위한 선행연구, 기술 및 한계점에 대해 분석한다. 3장에서는 제안하는 DAM4SNC 기술에 관해 설명하고, 4장에서는 실험 환경 및 시뮬레이션 결과에 관해 설명한다. 마지막으로 5장에서는 논문의 결론과 향후 연구에 대해 제시하고 마무리한다.

2. 관련 연구

본 장에서는 제안하는 기술에 기반을 두는 배경 기술과 선행연구들을 분석했다.

1) 배경 기술

다중 요소 인증은 둘 이상의 인증 방식을 조합하여 인증에 사용하는 방식이다[7, 8, 9]. 기존의 단일 인증 방식은 단순 개인정보 유출이나 악의적인 해킹을 통한 보안 위협이 내재되어 있다[10, 11]. 그러나 다중 요소 인증을 사용하면 여러 인증 프로세스를 복합적으로 사용하므로 보안성을 강화할 수 있다[9]. 다중 요소 인증을 사용하면 인증 프로세스의 수에 따라 사용자가 수행해야 하는 인증의 수도 증가하기 때문에[7], 보안성은 향상될 수 있으나 이용자의 편의성은 저하되는 트레이드오프 관계가 존재한다.

통신 과정에서 데이터 처리의 지연 시간을 줄이기 위해 프레임 집계(Frame aggregation) 기법이 연구되었다. 프레임 집계 기술은 패킷 또는 프레임 수준에서 적용하여 수행할 수 있는 기술로서, 여러 패킷 또는 프레임을 하나의 큰 묶음으로 결합하여 전송한다[12, 13, 14]. 집계 기술이 인터넷 프로토콜 또는 응용 계층에서 수행되는 경우 패킷 집계로 분류되고, 물리 계층 혹은 중간 접근 제어 계층과 같은 하위 계층에서 수행될 때는 프레임 집계로 분류된다.

프레임 집계의 작동 메커니즘은 Fig. 1과 같다. 프레임 집계를 수행하지 않고 통신하면 REQ(Request Packet)를 수신하는 즉시 적절한 RES(Response Packet)을 전송한다. 그러나 프레임 집계 기술을 적용할 경우, 여러 요청 패킷을 결합하여 하나의 큰 묶음으로 전송할 수 있으므로 하나의 응답 패킷으로도 응답할 수 있다. 따라서 이러한 기술은 집계 방식이 적용되지 않은 통신 환경보다 지연 시간 측면에서 상당한 개선을 기대할 수 있다.

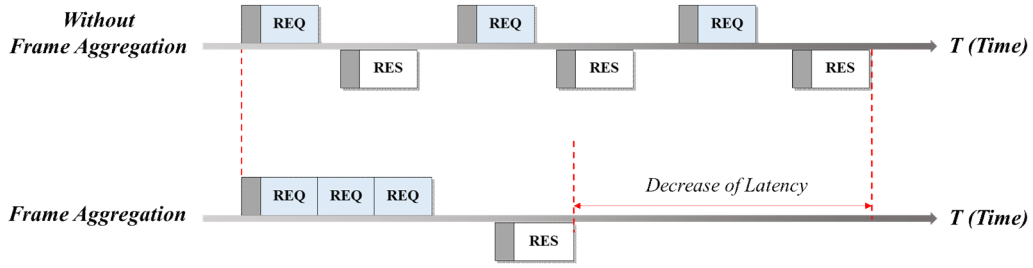


FIGURE 1. Frame Aggregation

프레임 집계 기술은 전송 프레임을 제어와 부분 재전송을 더 효율적으로 수행, 보장하기 위해 여러 프레임을 하나의 큰 프레임으로 통합할 수 있다. 이 기술은 차세대 무선 네트워크를 위해 제안된 바 있으며 전송 시간과 오버헤드 측면 모두 줄일 수 있는 장점이 입증된 바 있다[14, 15, 16, 17].

2) 선행연구 분석

미국 연방 금융 기관 심사 위원회 및 국립 표준 기술 연구소와 같은 국가 기관에서는 신뢰할 수 있는 도메인과 신뢰할 수 없는 도메인을 분리하여 네트워크를 보호할 것을 권장하고 있다[18, 19]. 그러나 분리된 네트워크의 보안 패치 및 서비스를 위해서는 네트워크 연결이 필수적이다. 특히, 네트워크 간의 데이터 교환에 USB와 같은 하드웨어 미디어가 사용됨에 따라 지연 성능 및 보안이 저하될 우려가 있다[4, 5].

이러한 문제를 해결하기 위해 네트워크 연결 시스템이 고안되었으며, 분리된 네트워크 시스템 간에 데이터를 교환하고 서비스를 상호 연결하기 위해 네트워크 간 데이터 전송 시스템이 도입되었다. 그러나 데이터는 분리된 도메인과 연결된 도메인 간에도 교환되어야 하므로 네트워크 간 데이터 전송 시스템에서 보안은 별도의 네트워크와 같은 수준으로 유지되어야 하는 특성

이 있다. 네트워크 간 데이터 전송 기술이 활발히 연구되고 있지만[20, 21], 대부분의 연구에서는 사용성과 보안성을 동시에 고려하지 않는다[22, 23]. 네트워크의 크기와 밀도가 커질수록 기존의 중앙집중식 인증 및 네트워크 연결 기술의 구조적 한계로 인해 보안성 및 사용성이 저하된다. 따라서 사물인터넷 기반의 고밀도 네트워크 시대에는 안전하고 효율적인 인증 및 네트워크 연결 기술이 요구된다[24, 25].

대부분의 기존 IoT 연결 시스템은 중앙집중식 클라이언트-서버 모델로 구성되어 서비스를 제공하는 구조이다[26, 27]. 그러나 IoT의 고유한 특성으로 인해 여러 장치가 동시에 연결되어 동시에 통신하는 경우 중앙 서버에 오버헤드가 발생할 위험이 있다. 이는 다음과 같은 여러 문제점을 수반한다.

1) 네트워크 트래픽과 클라이언트 수가 증가하면 시스템 성능이 저하되고 병목 현상이 발생할 우려가 있다[28, 29, 30, 31].

2) 클라이언트-서버 모델은 중앙집중식 구조이기 때문에 중앙 서버에 문제가 발생하거나 권한이 없는 사용자가 중앙 서버의 계정을 탈취하면 같은 네트워크에 속한 모든 클라이언트에 영향을 미친다[28, 32, 33].

이러한 중앙집중식 네트워크 문제를 해결하기 위해 분산 네트워크 기술이 연구되는 추세다[34, 35, 36, 37]. 기존 중앙집중식 시스템의 보안을 강화하고, 외부 클라우드 서비스의 프라이버시 문제를 해결하며, 데이터 무결성 및 보안성을 향상하는 분산 시스템이 제안되었다[34]. 시큐어 셸 알고리즘의 암호화된 데이터가 블록체인 네트워크에 입력되면 네트워크에서 검증을 수행하여 빠른 트랜잭션 속도와 데이터 저장 효율성을 제공할 수 있다. 그러나 이 연구는 블록체인 네트워크만을 기준으로 성능을 평가한다는 점에서 한계가 있다. 블록체인을 이용한 분산 병원 네트워크에 대한 새로운 분산 인증 방법을 제안하고 중앙집중식 시스템을 위한 정보보호 기술을 도입한 또 다른

연구[35]에서는, 모델의 효율성을 스루풋과 오버헤드, 응답 시간으로 분석하고 우수성을 입증하고 있다. 그러나 제안, 실험 환경이 블록체인과 의료 시스템에 한정된다는 한계점이 존재한다.

분산 알고리즘 측면에서도 다양한 연구가 제안되었다. 확장성을 위해 중앙집중화 솔루션을 도입하고[36], P2P 인프라의 성능과 보안 측면에서 P2P(Peer-to-Peer) 분산 아키텍처와 하이브리드 아키텍처를 비교했다[36]. 그러나 C-RAN(Cloud Radio Access Networks) 환경에서 베이스밴드 기능 (BBUs, baseband functionalities)에서 BBU 호텔 문제를 해결하지 못하거나[36], 특정 악의적인 공격이 발생했을 때 네트워크에 미치는 영향만을 분석하였다는 한계점이 존재한다[37].

기존 연구들은 제한된 분야에서 문제를 해결하거나 블록체인 네트워크와 같은 특정 환경에서만 제안된 기술을 사용할 수 있다는 한계가 있었다. 본 연구에서는 모든 환경에서 일반적으로 사용할 수 있는 분산 네트워크에 대한 인증 방법을 분석한다.

3. 분산 네트워크 환경에서의 인증 모델

기존 네트워크 연결 시스템은 보안보다는 성능과 편의성을 고려한 구조로 설계되어 솔루션의 구성과 관리가 복잡하고 어려워서 네트워크 분리 효과가 떨어진다. 이에 따라 네트워크 연결 시스템의 취약성으로 인한 보안 사고를 방지하기 위해 사용성과 보안성을 동시에 제공하는 네트워크 연결 시스템의 필요성이 대두되고 있다.

본 절에서는 분산 네트워크 환경에서 높은 보안성과 사용성을 보장하는 DAM4SNC와 프레임 형식 및 동작 방식에 관해 설명한다.

1) DAM4SNC

DAM4SNC는 분산 네트워크 환경에서 안전한 네트워크 연결을 보장한다. 연결된 네트워크의 분산된 노드 간의 인증을 통해 분리된 네트워크와 통신하여 중앙집중식 제어 방식의 기존 네트워크 연결 솔루션의 비효율성을 극복할 수 있다. 본 연구에서 설계한 DAM4SNC 구성은 Fig. 2와 같다.

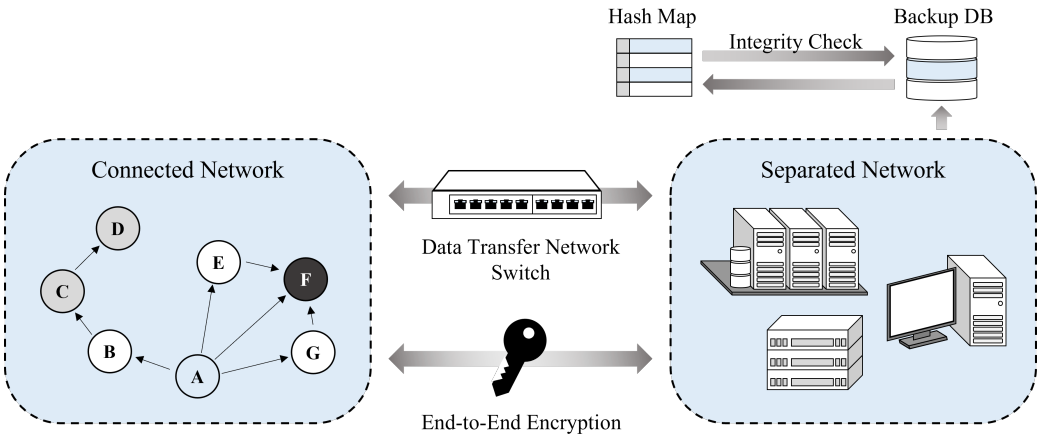


FIGURE 2. Structure of DAM4SNC

Fig. 2에서 각 노드는 내부 네트워크와 외부 네트워크가 분리된 분산 네트워크 환경에서 보안을 강화하기 위해 식별 및 인증을 수행한다. DAM4SNC는 네트워크를 연결하고 분리한다. 네트워크 간 스위치를 통해 악성 트래픽이 감지되면 분리된 네트워크로의 연결을 차단한다. 네트워크는 논리적으로 분리되므로, 신뢰 수준이 높을수록 액세스가 더 어려워지고 네트워크는 위협으로부터 보호되며 인증 결과의 무결성이 유지된다. 또한, 읽기와 쓰기가 모두 가능한 별도의 네트워크와 달리 쓰기만 가능한 백업 데이터베이스와 별도로 저장된 해시맵을 통해 노드 손상을 탐지할 수 있다.

2) 주기적 메모리 증명 및 신뢰 전파 모델

Fig. 3은 신뢰 노드(A)와 일반 클라이언트 노드(B-G))로 구성된 연결된 분산 네트워크의 구성이다.

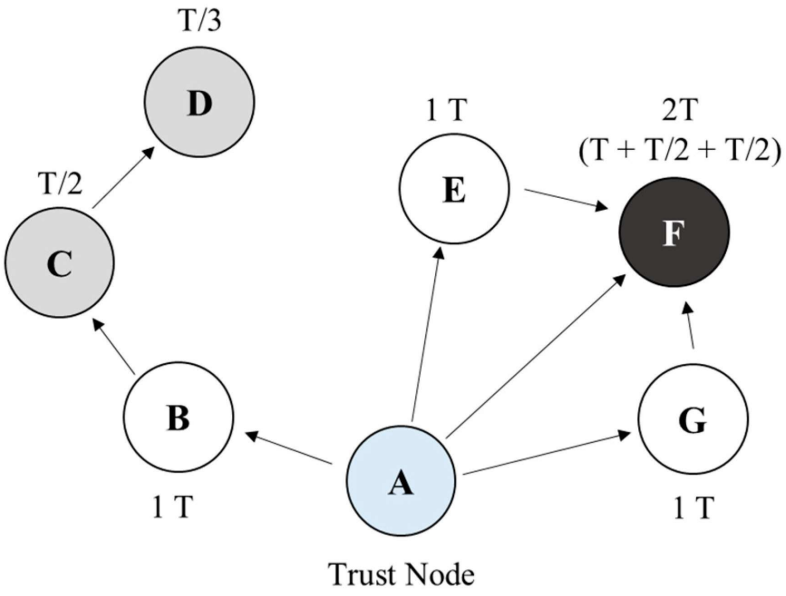


FIGURE 3. Operation of trust level

본 논문에서는 네트워크 내에 신뢰 노드가 최소 1개 이상이 존재하는 것으로 가정한다. 다른 노드와 달리 신뢰 노드(A)는 관리자가 직접 관리하고 액세스하는 노드로서, 로컬 네트워크에는 하나의 신뢰 노드만 존재한다. 관리자는 신뢰할 수 있는 내부 네트워크의 데이터 보호 담당자 또는 공개적으로 신뢰할 수 있는 인증 기관의 직원과 같이 특정 수준의 권한을 가진 직원이 담당한다. 이러한 모델의 신뢰 노드는 주기적으로 노드에 접근하여 악의적 접근이나 무결성 침해 여부를 확인하고 문제 발생 시 즉시 복구함으로써 관리자에 의해 보호될 수 있다고 가정한다. 클라이언트 노드는 신뢰 및 주변 노드와 자신의 신원을 주기적으로 확인하여 신뢰 수준을 높이거나 유지한다. 분산 노드는 업데이트된 신뢰 수준을 단위 시간 동안 저장하는 주변 노드에 주기적으로 자신의 신원을 확인한다.

Fig. 3 환경을 예로 들면, 노드 F는 A로부터 인증을 받는 신뢰 노드 A, E, G를 통해 인증함으로써 인증 수준을 향상한다. 인증 수준은 신뢰 수준 T로 표시한다. 노드가 신뢰 노드로부터 직접 인증을 받으면 1T의 신뢰 수준을 받는다. 신뢰 노드로부터 인증을 받은 노드로부터 인증을 받으면 신뢰 노드와의 홉 수(h)에 반비례하는 T/(w · h)의 인증 레벨을 수신한다. 본 연구에서는 평가 모델을 단순화하기 위해 w를 1로 설정하여 모델링 및 시뮬레이션을 적용하였다. 여기서 w는 가중치로, 신뢰 수준의 비율을 결정하는 계수로 이용한다. 분산 노드가 인접 노드를 통한 인증에 성공하면 신뢰 노드로부터의 거리가 멀어지기 때문에 가중치는 감소하게 된다. 예를 들어, 노드 D는 신뢰 노드 A로부터 3홉만큼의 거리에 있는 노드 C로부터 인증을 받기 때문에 T/3의 인증 레벨을 얻는다. 노드가 분산 네트워크 환경에서 인접 노드로부터 다중 인증을 수신하는 경우 인증 레벨은 다중 인증 결과의 합에 따라 결정된다. 예를 들어, Fig. 3 환경에서, 클라이언트 노드 E 및 G는 1T의 신뢰 수준을 갖는다. 노드 F는 신뢰 노드 A로부터 인증 수준 T를 수신하고 이웃 노드 E 및 G로부터 인증 수준 T/2를 수신한다. 따라서, 노드 F의 레벨은 2T(=1T + T/2 + T/2)가 될 수 있다.

3) 프레임 구조

노드가 정의된 인증 수준에 도달하면, 네트워크 연결 시스템은 각 노드의 암호화된 데이터, 해시값, 신뢰 수준으로 하나의 프레임을 생성한다. 생성된 프레임은 프레임 집계 기술을 이용하여 집계 프레임을 구성한 후 분리된 네트워크에 전송한다. 전송된 프레임의 구조는 Fig. 4와 같다.

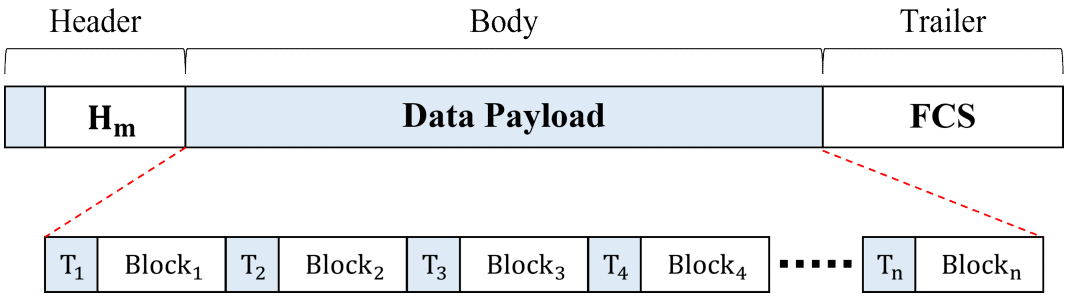


FIGURE 4. Structure of transmitted frame in DAM4SNC

프레임은 헤더(Header), 바디(Body), 트레일러(Trailer)로 구성된다. 헤더에는 각 블록의 해시값이 저장되는 해시 맵(Hm)이 포함된다. 바디 영역은 각 노드의 n개의 암호화된 데이터와 트러스트 맵 Tn 값의 조합으로 구성된다. 트러스트 맵은 인증에 성공했을 때 얻어지는 인증 결과로서 HMAC (Hash-Based Message Authentication Code) 알고리즘을 통해 인증 결과의 무결성을 검증한다. HMAC 알고리즘은 특수한 형태의 MAC(message authentication code) 기능으로, 발신자와 수신자가 공유하는 비밀키를 이용하여 해시함수를 통해 입력된 메시지를 처리할 수 있는 대표적인 암호화 알고리즘이다[38]. 사전에 공유한 비밀키를 이용하여 각 값을 계산하고 전송된 HMAC 값과 비교함으로써 데이터의 위·변조 여부를 검증함으로써 데이터 무결성을 확보할 수 있다[39]. 여러 노드의 데이터를 하나의 프레임으로 그룹화하여 전송하므로 중앙집중식 네트워크 연결 솔루션 환경에서 개별 인증 시스템보다 짧은 실행 시간을 기대할 수 있으며 트레일러에는 프레임 체크 시퀀스를 포함하여 오류 감지에 사용한다.

4. 성능 평가

본 절에서는 제안된 DAM4SNC 모델과 기존의 중앙집중식 네트워크 연결 기술 모델을 시뮬레이션을 통해 구현한다. 시뮬레이션 결과를 바탕으로 제안된 모델의 유효성을 기존 기술과 비교하여 검증하였다.

1) 실험 환경

제안한 DAM4SNC 기법과 기존 기법의 성능을 파이썬 3으로 구현된 같은 시뮬레이션 환경에서 비교 분석하였다. 시뮬레이션 모델에서는 기존 기법에 대해 전형적인 중앙집중식 기법[40]의 핵심 기능을 구현하였다. 이 두 가지 방법에 대한 시뮬레이터는 3.80GHz Intel Core™ i7-10700K CPU와 32GB RAM이 장착된 PC 환경에서 구현했다. 각 모델에 대한 의사 코드는 Algorithm 1-3에 표현되어 있다.

제안된 아이디어를 기존의 방법과 효과적으로 비교하기 쉽도록 인증과 관련된 핵심 기능만을 구현하여 비교하였다. 시뮬레이션 모델에서 기존 연구 방법론[40]과 같은 방법으로 지연 시간과 인증 수준을 측정하였다. 시뮬레이션에서 네트워크는 무작위로 분산된 노드로 구성된다. 하나의 중앙 노드가 다른 노드를 인증하고 연결하는 종래 모델과 DAM4SNC 메커니즘에 의해 분산 인증되어 연결되는 제안하는 모델을 구축하여 실험했다. 구현한 시뮬레이션 환경에서 DAM4SNC의 핵심 기능을 비활성화시켰을 때 기존 방식과 같은 성능 결과를 보이는 것을 확인한 후 DAM4SNC 기능을 활성화하여 성능을 평가하였다.

ALGORITHM 1.

Pseudo code for DAM4SNC authentication

INPUT: Number of nodes, Target security level each node

1. iterate (node size increases):
2. randomly set target security levels for all nodes (level 1 - 3)
3. **while** (until all nodes reach the target security level and transmit data):
4. // do authentication method(function)
5. authentication( )

OUTPUT: Latency

ALGORITHM 2.

Pseudo code for DAM4SNC authentication function

INPUT: Pseudo code for DAM4SNC authentication function

```
1  def authentication ():
2    randomly sample N1~i (nodes to authenticate)
3    randomly sample M1~j (nodes to be authenticated)
4    Tm = Tm + (Tn/hop) // parallel and simultaneous authentication
5    if Tm == target_level:
6      transfer datam
```

OUTPUT: Latency

ALGORITHM 3.
Pseudo code for CON authentication

INPUT: Number of nodes, Target security level each node

```
1  iterate (node size increases):
2    set target security levels for all nodes
3    // each group of target levels has
4    // the same number of nodes of the ones of DAM4SNC's)
5  while (until all nodes reach the target security level and transmit data):
6    randomly choose N (nodes to be authenticated)
7    Tn = Tn + 1
8    if Tn == target_level:
9      transfer datan
```

OUTPUT: Latency

Algorithm 1-3은 각각 제안된 DAM4SNC와 기존의 중앙집중식 인증 방법의 시뮬레이션을 위한 의사 코드이다. CON은 기존의 중앙집중식 네트워크 모델이며[40], 기존의 중앙집중식 인증 방법은 데이터 통신을 위해 프레임 집계 및 신뢰 노드를 사용하지 않는다.

DAM4SNC 모델은 노드 간 분산 인증을 통해 신뢰 수준을 누적하여 시스템이 요구하는 보안 수준을 얻을 수 있다. 실험에서는 목표 보안 수준을 무작위로 3단계로 설정하였고 레벨 1-3에 도달하려면 각각 2, 5, 10단계 인증이 필요하다고 가정했다. DAM4SNC 모델에서의 인증을 고려할 때, 분산 노드는 인접 신뢰 또는 인증 노드를 통해 인증을 받고, 인증된 분산 노드는 인접 노드에 대한 분산 인증을 수행한다. 즉, 시뮬레이션에서는 기존 모델의 경우 노드 간 데이터 전송만 수행하고, 제안된 DAM4SNC의 경우 신뢰 수준 할당 및 프레임 집합을 수행하면서 노드 간 데이터 전송을 구현한다. 모든 노드에 대해 순차적인 인증을 적용하는 기존의 중앙집중식 방식

과 달리, 제안하는 방식은 지정된 시간 동안 반복 루프에서 각 노드를 인증한다. 인증된 노드의 신뢰 수준은 인증된 각 노드의 홉 수에 따라 T/h에 의해 결정된다. 최종 신뢰 수준은 지정된 시간 동안 주변 노드로부터 인증을 받은 신뢰 수준의 합을 기반으로 결정된다. 목표 보안 수준에 도달하면 노드는 프레임을 스위치로 보내고, 전송된 프레임은 지정된 시간 동안 스위치에 버퍼링 되어 집계되면서 분리된 네트워크로 동시에 전송할 수 있다. 논문에서는 노드 수에 따른 지연 시간을 비교하기 위해 Algorithm 1~3과 같이 고정된 단계로 노드 수를 늘리면서 실험을 수행하여 결과를 비교했다.

Algorithm 3에서 보이는 기존의 중앙집중식 모델에서도 DAM4SNC 시뮬레이터와 같이 노드의 수를 늘리면서 시뮬레이션을 반복하며, 보안 수준은 DAM4SNC 모델과 같은 수준으로 설정하였다. 종래 모델은 DAM4SNC와 다르게 홉 수를 기반으로 계산되지 않는다. 따라서 연결 스위치에서 n−factor 인증을 위해 n 인증을 수행하며, 목표 보안 수준을 획득하면 데이터가 전송된다.

제안된 DAM4SNC의 성능을 같은 실험 환경에서 기존 방식과 비교하기 위해 100개에서 1000개까지 연결된 네트워크의 노드 수를 100개 단위로 늘리면서 지연 시간을 측정하였다.

각 모델에 필요한 각 보안 수준별 도달 기간은 두 모델을 시뮬레이션하여 분석할 수 있다. 이는 DAM4SNC 모델의 평가 지표로 사용되었다. 각 노드가 다중 요소 인증을 적용하면 인증 횟수에 비례하여 노드의 보안성이 높아지므로, 같은 전송 횟수를 갖는 각 노드의 전송 시간을 결정할 수 있다.

각 모델의 대기 시간은 각 노드가 인증 요청을 시작한 시점부터 최종 인증이 완료된 시점까지로 정의하였고 각 인증 수준의 지연 시간을 고려하여 두 모델 간의 보안 수준에 따른 지연 시간의 차이를 분석하였다.

2) 실험 결과 및 분석

실험에서는 [40]의 기존 방법과 제안된 DAM4SNC를 같은 시뮬레이션 환경에서 구현하였다. DAM4SNC의 집계 및 신뢰 수준과 같은 차별화된 기능을 비활성화하여 기존 성능을 구현했다. 노드의 수를 100개에서 1,000개까지 100개씩 증가시키면서 지연 시간과 각 보안 수준의 지연 시간을 측정하여 출력하는 과정을 1,000번 반복하고 평균을 계산하여 그래프로 나타내었다.

연결된 네트워크의 노드 수를 100개에서 1,000개까지 100개 일괄적으로 증가시켰을 때의 지연 시간을 비교한 결과는 Fig. 5와 같다.

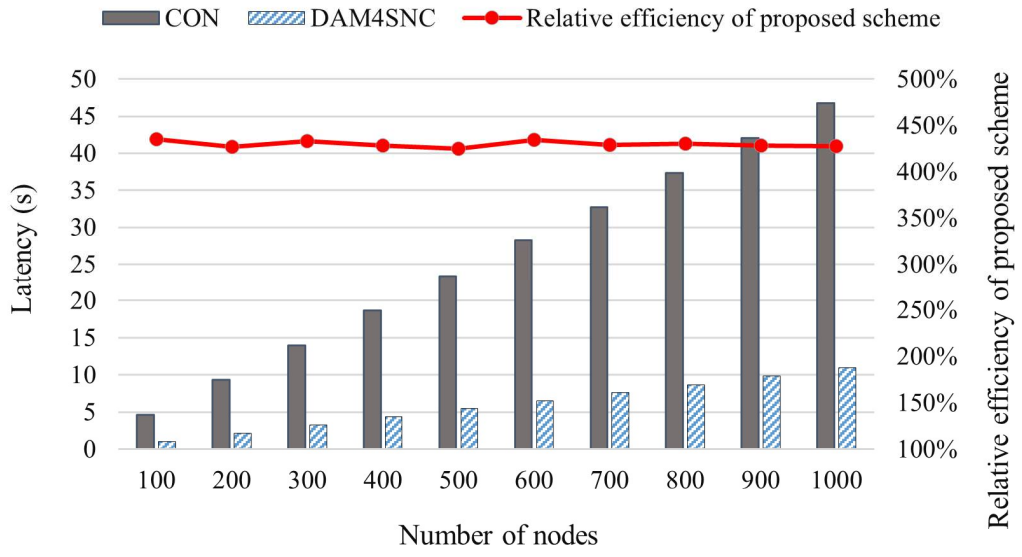


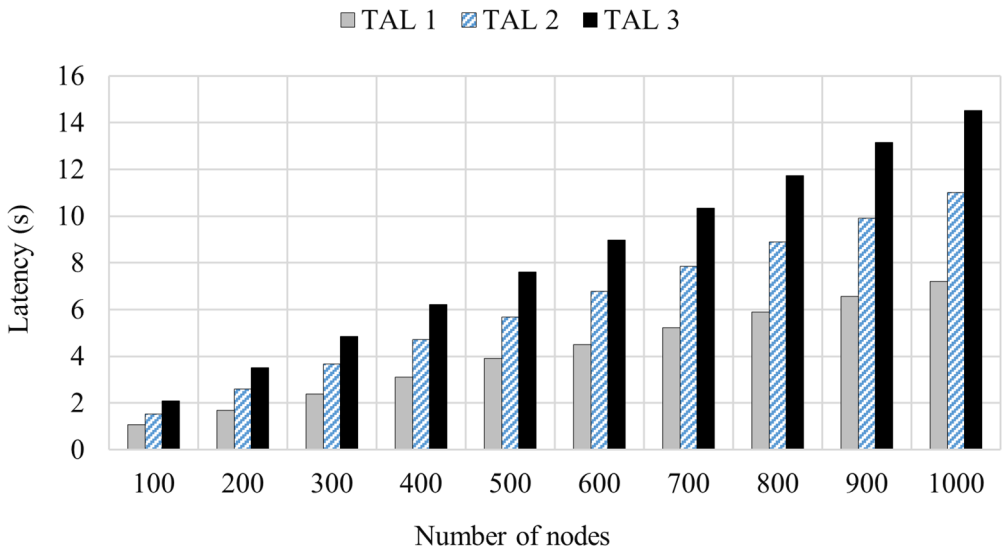
FIGURE 5. Comparison between the DAM4SNC and CON models

Fig. 5를 고려하여 제안하는 기법의 상대적 효율성은 아래 수식(1)과 같이 정의되었다.

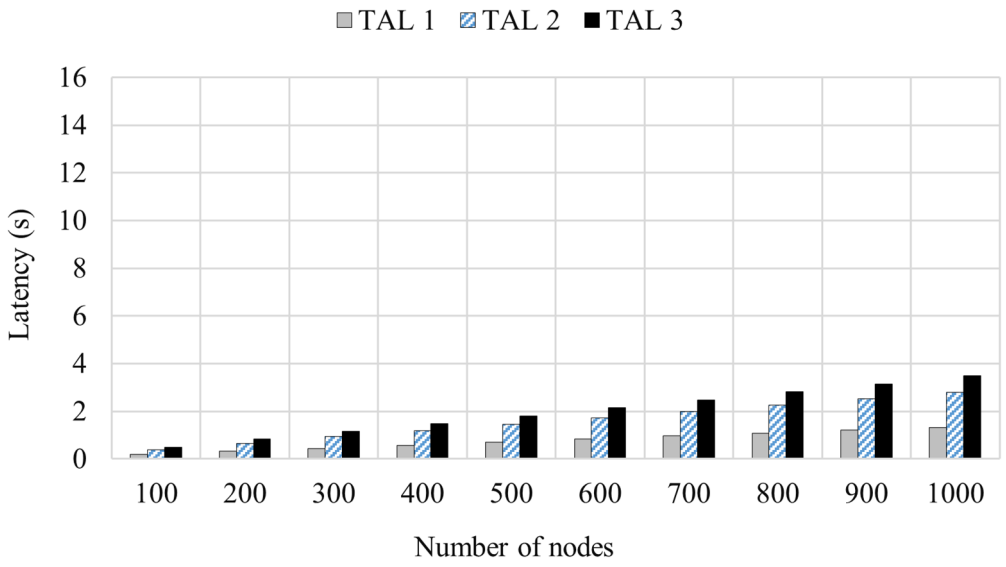
$$REP(Relative\ efficiency\ of\ proposed\ scheme) = \frac{CON's\ Latency}{DAM4SNC's\ Latency} \times 100 \quad (1)$$

실험 결과와 같이 노드가 100개와 200개일 때 기존 모델의 평균 지연 시간은 4.66초와 9.32초였다. 그러나 DAM4SNC를 적용한 경우 지연 시간은 각각 1.07초와 2.18초로 감소했다. 마지막으로 노드 수를 1000개로 늘렸을 때 기존 모델과 DAM4SNC는 각각 46.76초, 10.93초로, DAM4SNC는 약 230초 정도 더 낮은 지연 시간을 보였다.

따라서 수식 1에 따라 계산된 제안 방식의 상대 효율(REP)은 모든 경우에 약 420% 이상의 결과를 보였다. 목표 인증 레벨 (TAL, Target Authentication Level)을 기준으로 지연 시간의 차이를 확인할 수 있다. Fig. 6 (a),(b)는 각각 기존 모델과 DAM4SNC 모델의 레벨에 따른 지연 시간 변화 그래프이다.



(a)



(b)

FIGURE 6. Latency based on TAL: (a) CON and (b) DAM4SNC models

Fig. 6 (a),(b)에서 기존 모델과 DAM4SNC 모델의 TAL은 TAL 1~3으로 표현했다. TAL 1~3은 각각 2, 5, 10단계 인증이 필요한 것으로 가정했다.

노드 수가 1,000개인 경우 TAL 1~3을 사용한 기존 모델의 평균 지연 시간은 각각 7.20초, 11.01초, 14.51초였다. 반면 DAM4SNC 모델을 적용한 경우 평균 1.33초, 2.79초, 3.48초의 짧은 지연 시간을 보였다.

Fig. 6 (a)의 기존 모델은 TAL이 증가하면 인증 횟수가 증가하기 때문에 보안 수준에 비례하여 지연 시간이 증가한다. 이는 더 높은 다단계 인증이 필요함을 의미한다. 그러나 Fig. 6 (b)의 DAM4SNC 모델은 보안 수준과 무관하게 수준별 지연 시간이 유사한 수준으로 증가한다. 이는 주어진 대기 시간 요구사항에 대해 제안된 방법이 기존 방법보다 높은 인증 수준을 보장할 수 있음을 의미한다. Fig. 7은 각 모델에 필요한 지연 시간에 따른 TAL 달성 정도를 나타낸 그래프이다.

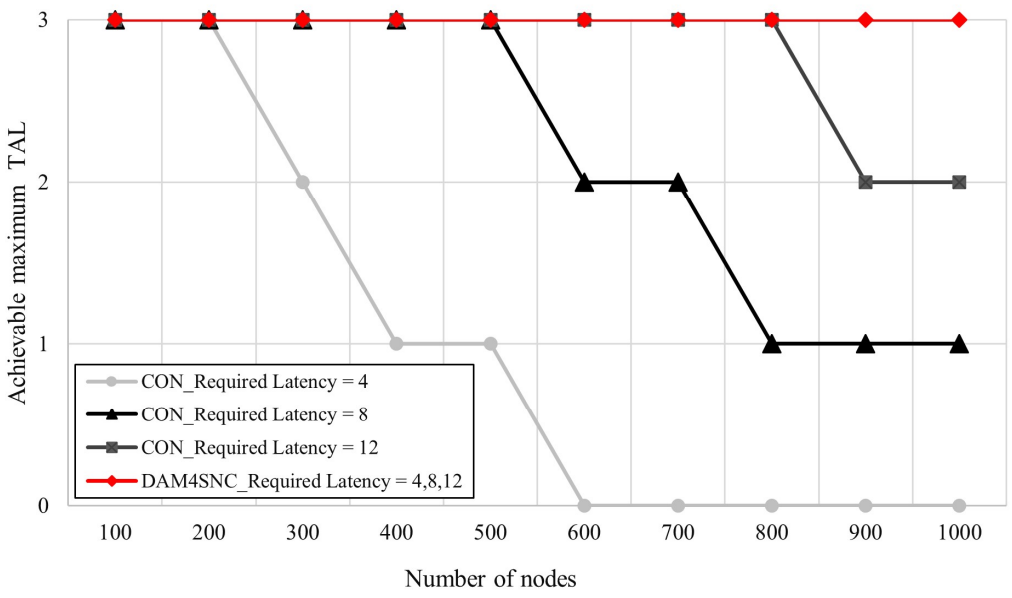


FIGURE 7. Achievable maximum TAL for the required latency conditions for each model

Fig. 7은 각 모델에 필요한 대기 시간 조건에 대해 달성 가능한 최대 TAL을 계산한 결과이다. 달성 가능한 최대 TAL은 종래 모델이 기존 모델에서 요구되는 대기 시간에 대해 우수한 성능을 보인다. 예를 들어, 요구되는 지연 시간이 12인 경우 기존 모델은 노드가 900개 이상일 때부터 TAL 3 수준을 달성할 수 없다. 이에 비해 DAM4SNC는 요구되는 지연 시간이 4인 경우에도 모든 경우에 TAL 3을 달성할 수 있었다. 즉 DAM4SNC는 제한된 지연 시간 환경에서도 기존 모델보다 높은 보안 수준을 달성할 수 있음을 증명했다. 네트워크의 많은 노드가 스위치에 데이터 처리 요청(읽기/쓰기)을 보낼 때 각 노드는 인증을 위한 각 요청에 대한 해당 응답을 보내야 하므로 요청 및 응답과 같은 관리 프레임 오버헤드를 생성하여 총 스루풋이 열화된다. 그러나 제안된 DAM4SNC 방식을 사용하면 노드 간 분산 인증을 통해 인증 수준을 높여 인증 중에는 관리 프레임을 수신하지 않고 마지막 데이터 포인트를 전송할 때만 관리 프레임을 수신한다. 따라서 관리 프레임의 수에 대한 오버헤드를 낮추고 프레임 집계 방식을 통해 스루풋이 향상될 수 있어 지연 시간과 스루풋 간의 트레이드오프 관계를 해결할 수 있다.

5. 결론 및 향후 연구

본 연구에서는 기존의 중앙집중식 네트워크 연결 방식의 한계를 분석하고 이러한 한계를 극복하기 위해 DAM4SNC 모델을 제안한다. 사이버 공격의 지속적인 발생으로 인해 외부의 보안 위협에 대한 대응책이 요구되고 있으며, 이러한 외부 위협을 차단하기 위한 네트워크 분리 기술이 설계되었다. 그러나 망분리 기술은 업무 처리의 비효율성 문제가 있으며, 이를 해결하기 위해 개발된 망 연결 모델은 효율성을 우선시하기 때문에 보안성이 부족한 한계점이 존재한다.

DAM4SNC 모델은 연결된 네트워크의 노드가 병렬로 분산 인증을 수행하고 프레임 집계 프로토콜을 사용하여 별도의 네트워크에서 데이터베이스에 액세스하기 때문에 기존의 중앙집중식 네트워크 연결 모델의 비효율성을 개선할 수 있다. DAM4SNC의 분산 인증은 신뢰 전파에 기반을 둔 다단계 인증의 효과가 있으며 해시맵 배열을 이용하여 악성코드 트래픽, 정보 위변조 탐지, 암호화 저장 단계 등을 수행함으로써 분산 네트워크 환경에서 안전한 인증이 가능하다. 따라서 DAM4SNC 모델은 기존의 중앙집중식 네트워크 연결 모델보다 향상된 보안성을 갖춘 네트워크 환경을 제공할 수 있다.

본 연구의 한계점은 실제 네트워크 환경 기반 실험이 아닌 파이썬 기반의 시뮬레이터를 구축하여 실험한 것으로, 실제 네트워크 환경이 반영되지 않았다. 더불어 네트워크 내 트러스트 노드가 필수적으로 존재한다고 가정하였으므로, 트러스트 노드가 명확히 존재하지 않는 환경에서는 트레이드오프 관계를 해소하지 못한다는 한계점이 있다. 따라서 본 연구의 후속 연구로 실제 네트워크 통신 환경이 반영된 조건에서 DAM4SNC에 대한 성능을 분석한다. 그리고 보편화 된 환경에서 DAM4SNC의 보안 및 성능 트레이드오프를 최적화하기 위한 환경 및 조건을 수학적 모델링 및 시뮬레이션을 통해 분석할 계획이다.

Ⅲ. PART 2: 네트워크 내 이기적 노드 대응 방법

1. 서론

소형 디바이스 간의 무선 연결을 활성화하고자, 무선 센서 네트워크(WSN)가 도입되었다[41]. WSN은 복잡한 유선 인프라를 구축하지 않고도 다양한 센서를 이용하여 네트워크에 연결할 수 있고, 기존 유선 인프라 대비 물리적, 환경적 제약이 없고 확장성 측면에서 뛰어난 장점이 있다[42]. 이에 따라 최근 여러 분야에서의 IoT 기기의 연결이 급증하면서 WSN는 더욱 주목받고 있다. 특히, 의료, 국방, 농업, 환경 등 여러 분야에 적용 가능한 센서를 이용하여 일상에서부터 인간의 접근이 어려운 산간지역이나 산업 인프라까지 폭넓게 이용될 수 있다[43].

WSN를 이용하는 경우 환경에 따라 연결되는 센서 노드의 수가 수천, 수만에 이르기까지 방대한 규모의 네트워크가 구성될 수 있으나 가용성이 보장되어야 한다. 그리고 공급 가능한 에너지가 제한적이기 때문에 통신 및 데이터 처리 등의 주요 기능을 제외한 기능에서의 에너지 소모를 최소화하여 제한된 자원을 효율적으로 이용하는 것이 중요하다[44].

네트워크 자원을 효율적으로 관리하기 위해, 여러 메커니즘이 연구, 적용되고 있다. 그중에서도 IEEE 802.11 ah 표준에서는 제한된 액세스 윈도우(RAW, Restricted Access Window) 메커니즘을 이용한다. RAW 메커니즘은 스테이션을 그룹화하여 그룹별 액세스를 RAW 슬롯이라는 제한된 시간 간격으로 규제하여 동작시키는 그룹 기반의 경합 메커니즘이다. 각 그룹의 스테이션은 EDCA(Enhanced Distributed Channel Access) 프로토콜을 이용하여 할당된 RAW 슬롯 기간 동안 액세스할 수 있다. 따라서 다수의 스테이션 전체가 경쟁하지 않고 슬롯 내 스테이션만 경쟁에 참여하게 되므로 충돌 확률을 줄이고 스루풋과 에너지 효율성을 향상할 수 있다[45, 46].

그러나 네트워크 내에 이기적 노드가 존재하는 경우 네트워크 내 노드들의 스루풋은 급격히 낮아진다. 이기적 노드는 악의적으로 더 많은 자원을 이용하기 위해 정상적으로 작동하는 노드의 패킷을 폐기하거나 액세스 기회를 독점하는 등의 동작을 수행한다. 이로 인해 다른 노드들은 패킷을 재전송하거나 채널 액세스 기회가 적어지면서 자원을 낭비하게 된다. 따라서 이기적 노드의 수가 일정 수준 이상 증가하게 되면 네트워크 운영 및 효율성에 심각한 피해를 줄 수 있다[47]. 그러나 이기적 노드는 정상적인 노드의 동작에 직접 개입하지 않고 전송 채널을 독점하거나 정상 노드의 접근 기회를 박탈하고[48], 정상 노드로 위장하여 동작하기 때문에 이를 탐지하기 어렵다. 따라서 이기적 노드에 대한 빠른 탐지와 대응을 위한 기술이 중요해지고 있다.

본 논문에서는 이러한 문제점을 해결하고자 이기적 노드 대응을 위한 그룹핑 기반의 백오프 조정 방법을 제안한다. 특정 노드가 백오프 값을 임의로 낮게 조정하여 네트워크 자원을 독점하는 경우, 중앙 서버는 이를 감지하고 다른 일반적인 노드들에 이기적 노드와 유사한 수준의 백오프 값을 설정하도록 신호를 보내는 방식으로 동작한다. 그러나 모든 노드의 백오프 값을 낮게 조정할 경우, 네트워크 전체의 스루풋이 저하될 수 있으므로, 중앙 서버에서 마음대로 연결된 노드들을 그룹핑 하여 그룹별 차례대로 백오프 값을 변경할 수 있도록 한다. 차례로 선택된 그룹만 이기적 노드와 유사한 수준의 백오프 값을 가지도록 변경하여 경쟁함으로써 이기적 노드의 네트워크 자원 독점을 완화할 수 있다.

본 논문의 기여점은 다음과 같다.

1) 이기적 노드에 효율적으로 대응함으로써 네트워크의 통신 안정성을 보장하고 스루풋을 유지할 수 있다.

2) 기존 네트워크 동작 구조에서 크게 벗어나지 않고 백오프 조정 알고리즘만 도입할 수 있다.

3) Netsim 시뮬레이터를 이용하여 실제 네트워크와 유사한 환경을 구성하여 제안 기술을 검증하였다.

4) 실험 결과, 제안하는 기술을 적용했을 때 이기적 노드의 스루풋을 약 80% 감소시키는 결과를 보였다.

본 논문은 다음과 같은 내용으로 구성된다. 2장에서 관련 선행연구를 분석하고, 3장에서는 본 연구를 통해 제안하는 기술을 소개한다. 4장에서는 Netsim 시뮬레이터를 이용하여 제안하는 기술을 실험, 검증하고 결과를 분석한다. 5장에서는 향후 연구 제안 및 결론에 관해 서술한다.

2. 선행연구 분석

본 절에서는 이기적 노드를 탐지할 때, 백오프 값을 이용하지 않는 경우와 이용하는 경우로 구분하여 선행연구들을 분석한다.

1) 백오프 값을 이용하지 않는 경우

Muhammad Fayza외 5인 연구[47]에서는 모바일 애드혹 네트워크(MANET, Mobile ad-hoc network) 환경에서 이기적 노드가 네트워크 운영에 심각한 위협을 초래한다는 점에 주목하여, consumption to contribution(C2C) 정보를 이용한 이기적 노드 검출 방법을 제안했다. 논문에서는 제안 기술의 검증을 위해 ns-2를 이용하여 노드의 통신 속도와 이기적 노드의 수를 랜덤하게 변경하며 30개 이상의 case를 만들어 실험을 진행했다. 경로 탐색 프로세스에 참여하여 다른 패킷을 폐기하는 경우와 경로 탐색 프로세스에 참여하지 않고 경로 요청(RREQ, Route Request) 제어 패킷을 폐기하는 두 가지 공격 유형으로 나누어 실험을 진행하였으며 기존의 Observation-based Cooperation Enforcement in Ad hoc Networks(OCEAN) 방식과 비교하여 제안 방식을 비교했다. 실험 결과 경로 탐색 프로세스에 참여하는 공격자 유형의 경우 OCEAN보다 탐지율, 탐지 시간 측면에서 성능 향상을 보였다. 그러나 경로 탐색 프로세스에 참여하지 않는 공격자 유형에서는 오히려 OCEAN보다 성능이 열화되는 결과를 보여, 제한적인 환경에서의 성능 개선만 보였다.

MANET 환경에서 이기적 노드를 식별하기 위한 또 다른 연구로, Lincy E. Jim외 2인의 연구[49]에서는 인공 면역 시스템(AIS, Artificial Immune System)의 원리를 활용한 인공 면역 시스템 기반 알고리즘(AISBA, Artificial Immune System Based Algorithm)을 제안했다. Route Error로 인해 송신 노드가 ACK 패킷을 수신하지 못하게 되면 위험 신호를 발생시켜 원인 노드를 탐지한다. 저자들은 제안 알고리즘의 성능을 검증하고자 시뮬레이션을 통

해 AISBA와 선행 기술인 SAODV(Secure AODV, Ad hoc On-demand Distance Vector)[50]와 비교했다. 실험 결과 이기적 노드의 탐지율이 SAODV의 경우 평균 85.34%였으나 ASIBA는 평균 93.41%로 성능의 개선을 보였고 이기적 노드로 인한 패킷 드롭과 네트워크 내 Router Error까지 식별할 수 있음을 증명했다. 그러나 이 연구는 실험에 이용한 데이터 세트 등의 상세한 설명이 부족해 실험을 재현, 비교하기 어렵다는 한계점이 있다.

2) 백오프 값을 이용하는 경우

W. F. Fihri 외 3인의 연구[51]에서는 인지 라디오 네트워크(CRN, Cognitive Radio Network) 환경에서 Media Access Control(MAC) 계층을 대상으로 하는 백오프 조작 공격(BMA, Backoff Manipulate Attack)을 분류, 예측하기 위한 서포트 벡터 머신(SVM, Support Vector Machine) 기반 모델을 제안했다. 백오프를 조작하여 유휴 채널을 독점하는 이기적 노드가 포함된 네트워크의 패킷 스루풋과 지연 시간의 정보를 입력 값으로 사용하였으며 BMA 공격이 수행되었을 때, 백오프 값 변경으로 인한 패킷 전송 및 평균 지연 및 스루풋을 분석한다. 분석한 결과를 모델링한 후, Decision Tree, K-Neighbors, Na□ve Bayes 등의 기계 학습 알고리즘과의 비교를 통해 제안 방식의 성능을 검증했다. 실험 결과 SVM에서 RBF(Radial Basis Function) 커널을 이용했을 때 탐지 정확도의 향상을 보였다. 탐지 속도 측면에서도 다른 기계 학습 알고리즘을 사용했을 때보다 높은 성능을 보였으며, 가장 오랜 시간이 소요된 랜덤 포레스트 알고리즘과 비교했을 때, 탐지 속도가 약 37% 향상되었다. 그러나 이 논문의 실험 환경의 경우 1253개의 정상 노드와 273개의 이기적 노드를 포함한 데이터 세트를 훈련 데이터로 이용했고, 472개의 노드를 학습 데이터로 이용한 결과이나, 만약 데이터 세트의 크기가 매우 큰 경우에 RBF 커널을 이용한 SVM 기반 모델의 분류 속도가 크게 열화될 수 있다는 한계점이 존재한다.

Fatima Salma Sadek 외 3인의 연구에서는 무선 센서 네트워크 환경에서 이기적인 노드를 식별하는 방법을 제안했다[48]. 이기적인 노드는 정상 노드로 위장하여 동작하기 때문에 기존 탐지 방식으로는 검출이 어렵다. 이 연구에서는 시뮬레이션 환경에서 이기적인 노드를 통한 공격을 실행시킨 후, 정상 노드와 매개 변숫값의 평균을 비교하여 이기적인 노드로 분류할 수 있는 기준을 정의했다. 이때 백오프 값을 조작하여 해당 노드의 패킷 스루풋을 최대로 증가시키는 이기적인 노드의 동작은 통상적으로 정상 노드보다 많은 패킷을 송신한다는 점을 이용한다. 이기적인 노드를 5, 10, 15, 20개 배치하여 각각 실험을 진행하고 결과를 비교했다. 네트워크 트래픽을 분석한 결과, 이기적인 노드에서 전송하는 패킷의 수가 나머지 모든 정상 노드에서 전송하는 패킷의 수보다 많게 나타났고, 99.5%의 탐지 효율성을 달성했다. 하지만 배치한 이기적인 노드의 수가 적은 경우, 정상 노드와 이기적인 노드의 매개변수 평균값에 큰 차이가 나타나지 않는다. 이기적인 노드 공격이 소규모로 발생하고 있는 경우, 이를 공격으로 분류하기 어렵다는 한계점이 있다.

Georgiev Yuliyan의 연구[52]에서는 이기적으로 동작하는 스테이션을 별도의 이기적인 그룹에 배치하여 정상 스테이션으로부터 격리하는 이기적인 동작 완화기법 SSQPA(Selfish Station Quarantine Punishment Algorithm)을 제안했다. 특정 스테이션이 SSQPA에 의해 탐지되면 해당 스테이션은 이기적인 스테이션으로 분류되고 정상 스테이션과 다른 RAW 그룹에 배치된다. 이를 통해 이기적인 스테이션에 의한 정상 스테이션의 스루풋 감소 및 패킷 손실을 줄였다. 제안하는 알고리즘의 성능을 증명하기 위해 ns-3 네트워크 시뮬레이터를 이용한 실험을 진행했다. 60초간 실험을 진행하며 UDP, TCP 펌웨어, TCP IP 카메라를 대상으로 채널 액세스를 위한 경쟁을 시도했다. 실험 결과를 평가하기 위해 이기적인 스테이션의 비율 대비 공정성과 스루풋, 패킷 손실량을 이용했으며 기존 방식과 비교했을 때, SSQPA 알고리즘을 적용한

경우 손실되는 패킷의 수가 감소했다. 그러나 SSQPA는 탐지 알고리즘이 정해진 임계값 요구사항을 충족하는 경우에만 성능 효율성을 보이게 되므로 환경적 제약이 존재한다.

Table 1은 앞서 설명한 선행연구들을 정리한 표이다.

TABLE I Comparison of previous studies

Study	Backoff	Method	Weakness
Muhammad Fayza et al. [47]	X	• C2C 정보를 이용하여 MANET 환경에서 이기적인 노드를 검출하는 방법을 제안 • 경로 탐색 프로세스에 참여하여 다른 패킷을 폐기하는 동작을 수행하는 공격자와 RREQ 제어 패킷을 폐기하는 공격자로 구분하여 시뮬레이션 진행	거짓 긍정(FP)으로 탐지되는 경우가 많아, 상황에 따라 성능이 열화될 수 있음
Lincy E. Jim et al. [49]	X	• MANET 환경에서 이기적인 노트를 식별하는 방법으로 AIS의 원리를 활용한 AISBA 알고리즘을 제안 • 종래 방식과 비교했을 때, 탐지율이 향상되었으며, 이기적인 노드로 인한 패킷 드롭 및 현재 네트워크에 존재하는 route error를 식별할 수 있음을 증명	실험에 이용한 데이터 세트에 대한 소개가 포함되어 있지 않아 재현이 어려움
Wassim Fassi Fihri et al. [51]	O	• CRN 환경에서 MAC 계층을 대상으로 하는 BMA 공격을 분류하고 예측하기 위해 SVM 기반 모델을 제안 • SVM 분류기를 Polynomial 커널과 RBF 커널을 이용하는 경우로 구분하여 실험을 진행	데이터 세트의 크기가 매우 커질 경우, RBF 커널을 이용한 SBM 기반 모델의 분류 속도가 매우 느려질 수 있음

Fatima Salma Sadek et al. [48]	O	• 무선 센서 네트워크 환경에서 이기적인 노드를 식별하는 방법을 제안 • 정상 노드와 매개변수 값의 평균을 비교하여 이기적인 노드로 분류할 수 있는 기준을 정의 후, 실험을 진행하여 99.5%의 탐지 효율성 달성	배치한 이기적인 노드의 수가 적은 경우, 정상 노드와 이기적인 노드의 매개변수 평균값에 큰 차이가 나타나지 않음
Georgiev Yuliyan et al, [52]	O	• 이기적으로 동작하는 스테이션을 별도의 이기적인 그룹에 배치하여 정상 스테이션으로부터 격리하는 이기적인 동작 완화기법인 SSQPA 알고리즘을 제안 • 60초간 실험을 진행하며 UDP, TCP 펌웨어, TCP IP 카메라를 대상으로 채널 액세스를 위한 경쟁을 시도	상황에 따라 정상적으로 로그가 수집되지 않는 상황 발생

Table 1과 같이, 이기적 노드를 탐지하고 대응하기 위해 다양한 방법론이 연구되었으나 환경적 제약이 존재해 특정 환경에서만 성능 향상을 보이는 경우가 많았다. 따라서 본 논문에서는 종래 802.11 ah 모델의 구조를 유지하면서도 이기적 노드를 탐지하고 효율적으로 대응할 수 있는 백오프 조정 방법을 제안한다.

3. 네트워크 내 이기적 노드 대응 방법

본 절에서는 종래의 802.11 ah 모델에서 발생할 수 있는 이기적 노드 문제를 해결하기 위한 방법론을 제안한다.

기존의 네트워크 모델에서는 Fig. 8과 같이, 노드 간 프레임을 전송할 때에 충돌이 발생한 경우 노드별로 계산된 랜덤 백오프 값만큼 대기한 후 재전송하는 구조로 동작한다.

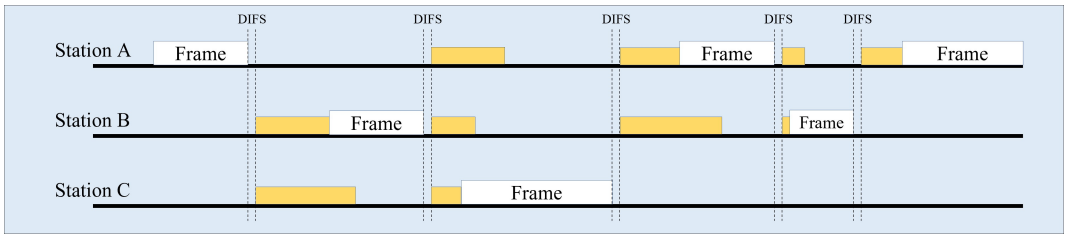


FIGURE 8. Normal random backoff communication

그러나 Fig. 9과 같이, 특정 노드가 백오프 값을 고의로 낮게 설정하는 경우, 다른 노드와의 경쟁에서 승리하는 빈도가 높아진다. 따라서 이기적 노드는 계속해서 네트워크 자원을 점유하고 있으므로 다른 노드의 스루풋이 낮아지는 문제가 있다.

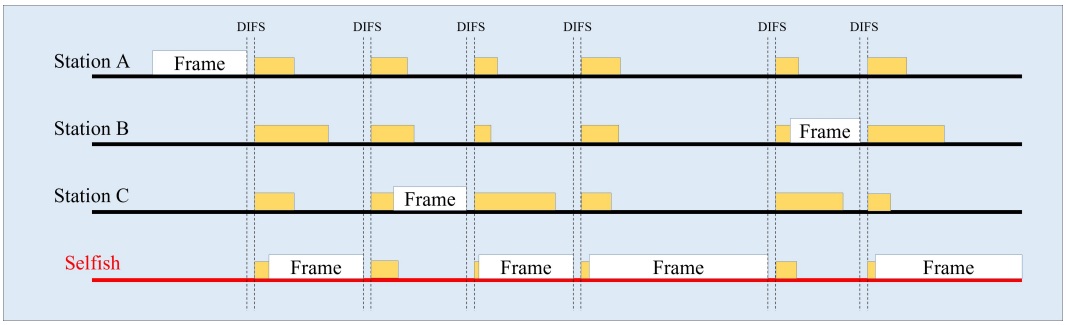


FIGURE 9. Random backoff communication with selfish nodes

따라서 본 논문에서는, 이기적 노드로 인한 스루풋 저하 문제에 대응하고자 백오프 조정 방법을 제안한다. 이기적 노드가 고의적으로 낮은 백오프를 설정하여 네트워크 자원을 점유하는 경우, 같은 네트워크에 포함된 나머지 노드들의 백오프를 이기적 노드와 유사한 수준으로 낮게 조정하여 유사한 조건에서 경쟁할 수 있도록 조정한다.

그러나 모든 노드의 백오프를 낮게 조정하게 될 경우, 좁은 범위에서의 랜덤 백오프 값으로 인해 충돌이 심화 될 수 있다. Fig. 10은 정상 노드들의 백오프 값의 절반으로 조정한 이기적 노드가 존재할 때의 스루풋 값과 모든 노드를 이기적 노드의 백오프와 같게 설정했을 때의 스루풋을 비교한 결과이다.

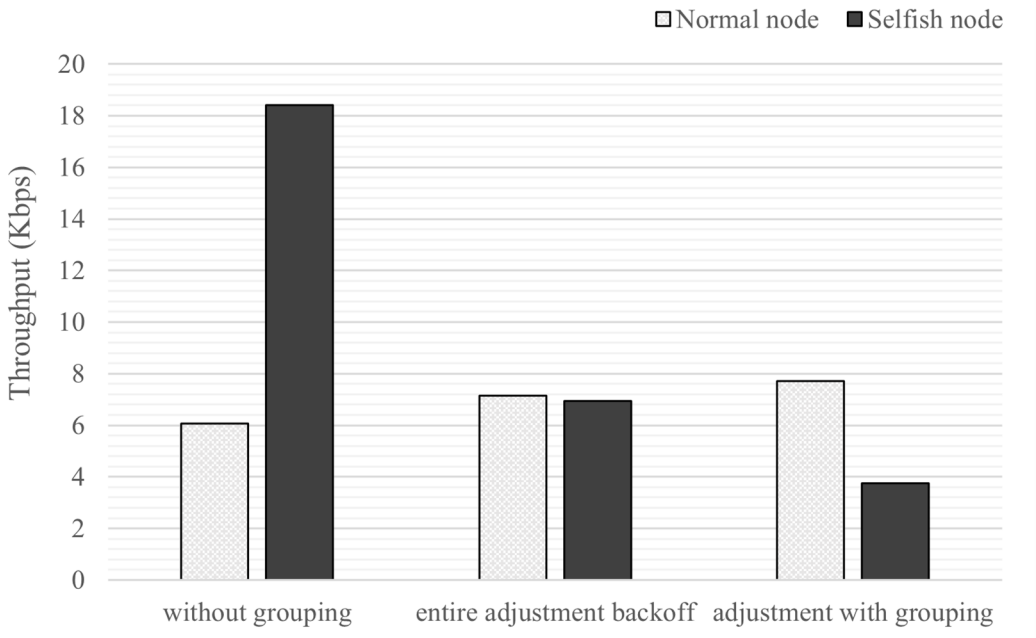


FIGURE 10. Comparison of throughput per backoff adjustment unit

실험은 이후 4. 성능 평가 절에서 설명할 환경인 Netsim 시뮬레이터를 이용하여 진행했다. 정상 통신을 수행하는 노드 10개와 백오프 값을 최소치로 조정하여 동작하는 이기적 노드 1개를 구성하여 총 1,000초 동안 통신을 수행한 결과이다. 실험 결과 이기적 노드만 동작하는 공격 환경(without grouping)에서는 정상 노드 10개의 평균 스루풋이 약 6.06Kbps, 이기적 노드의 스루풋은 18.4Kbps였다. 이에 대응하기 위해서 전체 노드의 백오프 값을 공격자가 설정한 최소치로 변경한 환경(entire adjustment backoff)과 5개의 노드는 공격자와 같은 값으로 조정하고, 5개의 노드는 조정하지 않은 환경(adjustment with grouping) 환경을 비교했다. 모든 노드가 변경된 환경에서는 정상 노드가 7.13Kbps, 이기적 노드가 6.95Kbps로 이기적 노드의 스루풋이 약 62% 저하된 것을 보인다. 그러나 5개의 노드만 조정한 환경에서는 정상 노드가 7.72Kbps, 이기적 노드가 3.74Kbps로 약 79%의 스루풋을 저하시킬 수 있다. 더불어 정상 노드들의 평균 스루풋도 세 환경 중 가장 높은 스루풋을 보이며, 공격자와 같은 값으로 조정된 그룹의 스루풋은 9.09Kbps로 가장 높았다.

따라서, 전체 노드의 백오프 값을 변경하는 환경보다 그룹 단위로 백오프 값을 변경하는 것이 스루풋 측면에서 더 효율적임을 보였다. 이에 그룹 기반의 백오프 변경을 통한 이기적 노드 대응 방법을 제안한다.

제안하는 방법의 전반적인 구조는 Fig. 11과 같다.

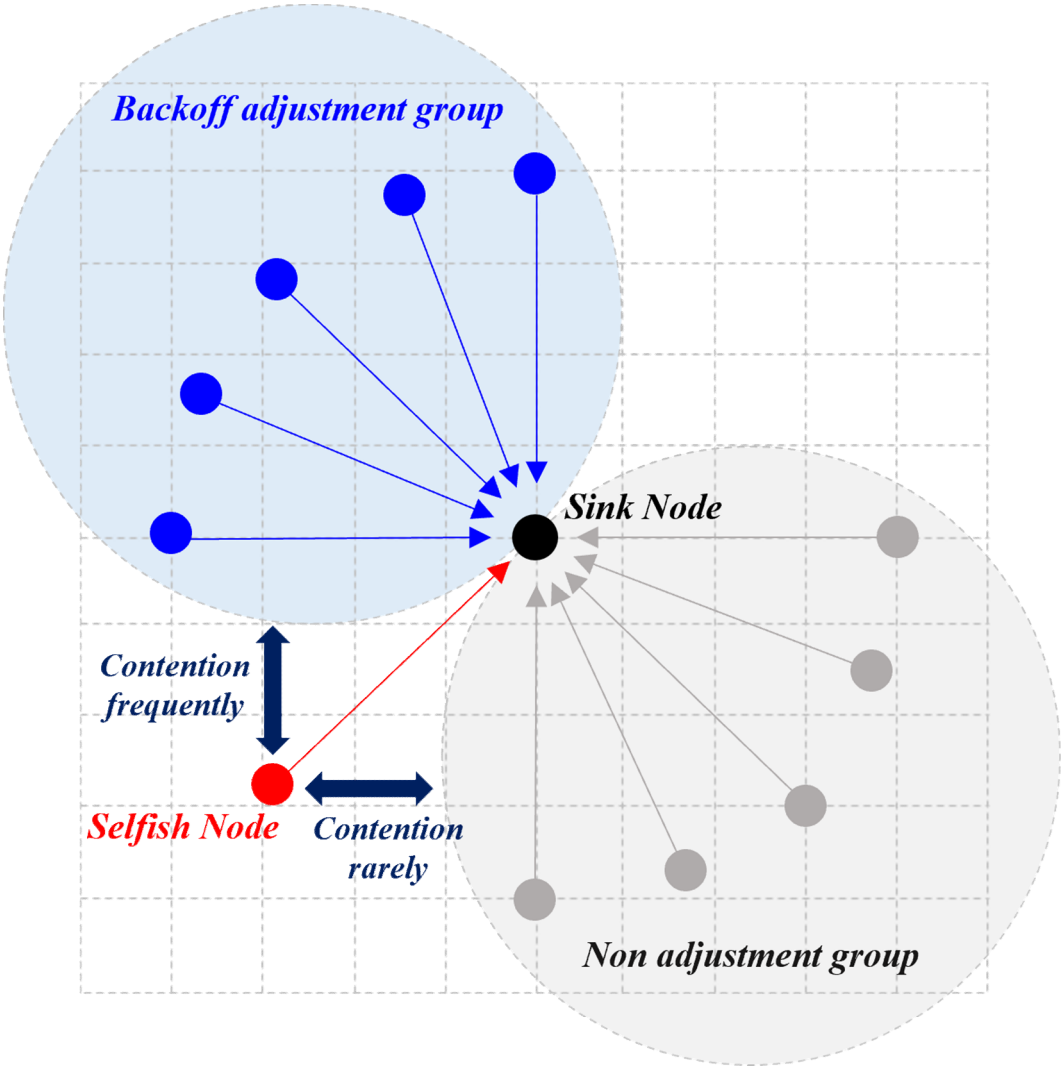


FIGURE 11. Structure of group based backoff adjustment technique

Fig. 11과 같이, 이기적 노드 존재를 감지하게 되는 경우 전체 노드를 균등하게 나누어 그룹핑한다. 이후, 각 그룹이 차례대로 이기적 노드와 유사한 수준의 백오프로 조정하여 해당 그룹과 이기적 노드가 공정한 환경에서 경쟁할 수 있도록 한다.

4. 성능 평가

본 절에서는 제안하는 모델의 검증을 위한 실험 환경 및 평가 방법에 관해 설명한다.

1) 실험 환경

실험은 Windows 10, INTEL(R) CORE(TM) I7-10700K CPU@3.80GHz 환경에서 Netsim Standard 13.2.x64버전을 이용하여 실험 환경을 구성한 후 진행하였으며, Wireless Sensor Network[53] 환경에서 ZIGBEE 통신 환경을 구축했다. 실험에 사용한 세부 설정은 Table II와 같다.

TABLE II Simulation Environment

Layer	Category	value
Network layer	Protocol	IPv4
Datalink layer	Protocol	IEEE 802.15.4
	Max CSMA BO	4
	Max Backoff Expo	5
	Min Backoff Expo	3
	Max Frame Retries	3
Physical layer	Frequency	2400MHz
	Data Rate	250kbps

실험에 사용한 네트워크 구성은 Fig. 12와 같다.

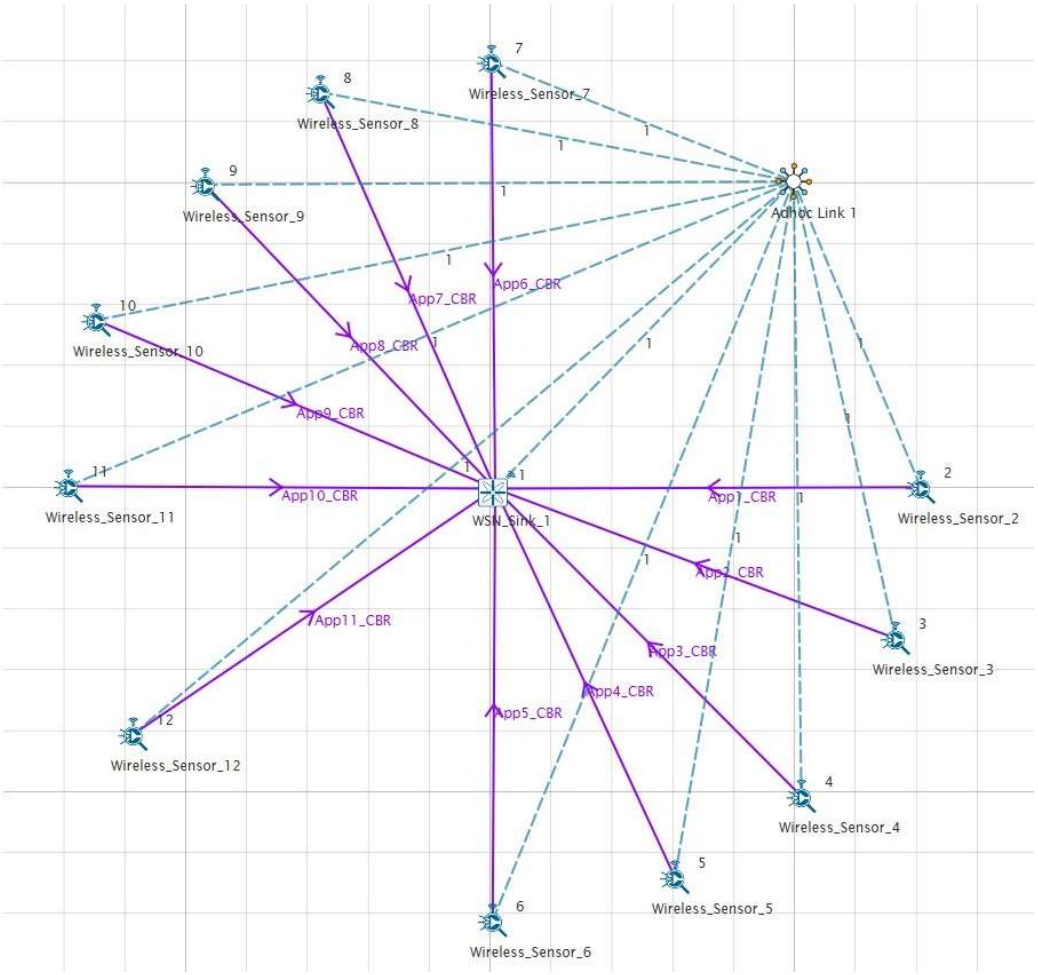


FIGURE 12. Experimental network structure

10개의 노드가 1,000초 동안 통신하는 환경을 구성하였다. 공격자 환경에서는 공격자 노드를 1개 더 추가하여 10개의 정상 노드와 1개의 공격자 노드가 통신하는 환경으로 구성했다. 공격자 노드의 경우 기존에 설정된 백오프 값을 최소치로 조정한 후에 통신하는 환경으로 수정한 후 통신하도록 구성했다.

제안 환경의 경우 10개의 정상 노드를 5개씩 A, B 그룹으로 할당하였으며 그 중 A 그룹의 백오프 값을 공격자 노드와 같게 설정한 후 통신하도록 한다.

노드 간 통신의 경우 10개 혹은 11개의 무선 센서 노드가 중앙의 WSN_Sink 노드로 데이터를 전송하도록 구성되었으며, CBR 타입의 UNICAST 방식을 이용하여 통신한다.

2) 실험 결과 및 분석

제안하는 모델의 평가는 각 노드의 스루풋 평균과 공정성을 기준으로 비교하였다. 실제 네트워크 환경에서는 이기적 노드가 가진 백오프 값을 다른 노드들이 알 수 없으므로, 백오프 수치를 조금씩 줄여가면서 최적의 결과를 도출하게 된다. 논문에서는 백오프 수치를 기본값부터 최소 수치까지 조정하면서 총 5개의 세트를 정의하였다. 정의한 단계는 Table III과 같다.

TABLE III Backoff adjustment set

value	SET 1	SET 2	SET 3	SET 4	SET 5
Max CSMA Backoff	4	3	2	1	1
Max Backoff Expo	5	4	3	3	3
Min Backoff Expo	3	3	3	3	3
Max Frame Retries	3	4	5	6	7

Table III의 단계에서, Netsim 시뮬레이터에서 기본적으로 설정되는 기본값은 SET 1이며, 실험을 위해 이기적 노드로 설정한 노드는 SET 4의 값으로 설정하여 실험했다. SET 5의 경우 SET 4와 비교하여 직접적인 백오프 값의 차이는 없으며, 통신 실패까지 시도할 최대 프레임 재전송 횟수를 정하는 Max Frame Retries 수치만 변경된 것으로, SET 4보다 약간의 성능 향상을 기대할 수 있다.

Fig. 13은 제안 방식의 백오프 조정 그룹이 단계적으로 백오프 수치를 줄이면서 통신을 시도하였을 때의 결과이다.

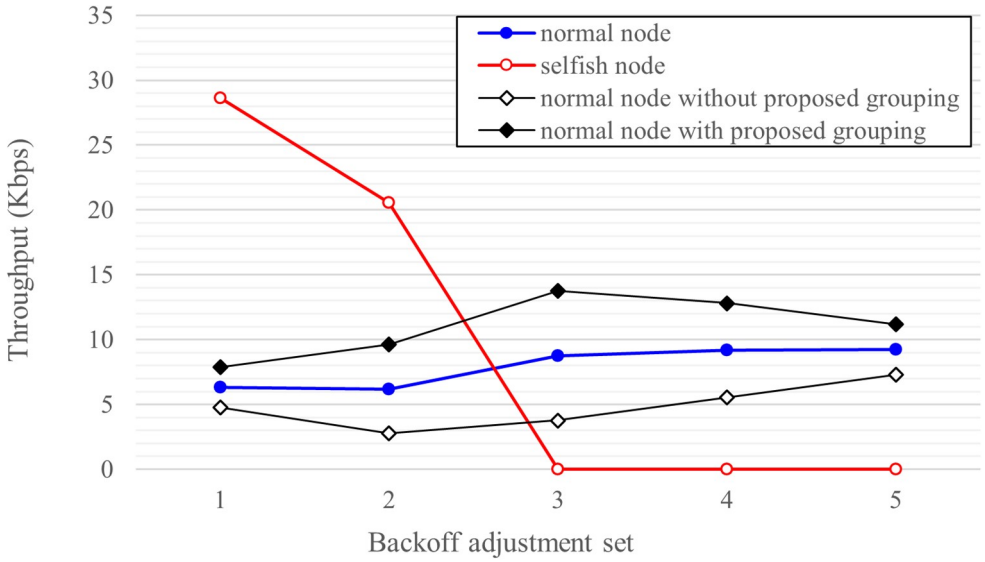


FIGURE 13. Comparison throughput each backoff adjustment set

Fig. 13에서 확인할 수 있듯이 제안하는 모델에서의 백오프 조정 그룹의 백오프 수치가 공격자와 유사한 수준인 SET 4에 가까워질수록 제안 방식의 성능이 향상되는 것을 확인할 수 있었다. 백오프 값에 직접적인 영향은 없지만, 실패 선언까지 시도할 최대 프레임 전송 횟수를 조정한 SET 5에서는 SET 4보다 약 0.77%의 스루풋이 향상되는 것을 보였다. 실험 결과 이기적 노드의 백오프 값과 유사한 수준으로 접근할수록 이기적 노드를 제외한 나머지 통신 노드들의 스루풋이 향상되는 것을 보였다. 따라서 백오프 조정 그룹의 수치가 공격자와 같은 수준에 도달하였을 때 달성할 수 있는 성능을 비교 분석하였다. 성능 분석은 정상적으로 통신하는 노드 전체, 이기적 노드가 수행하는 공격을 수행하는 공격자 노드, 제안하는 환경에서는 백오프 값을 조정한 그룹의 노드와 조정하지 않은 그룹의 노드 4개의 분류로 나누어 결과를 확인하였다.

4개 분류별 결과를 제안하는 모델을 적용한 네트워크 환경과 그렇지 않은 종래 환경의 결과를 비교하였다. 노드별 스루풋 평균을 비교한 결과는 Fig. 14와 같다.

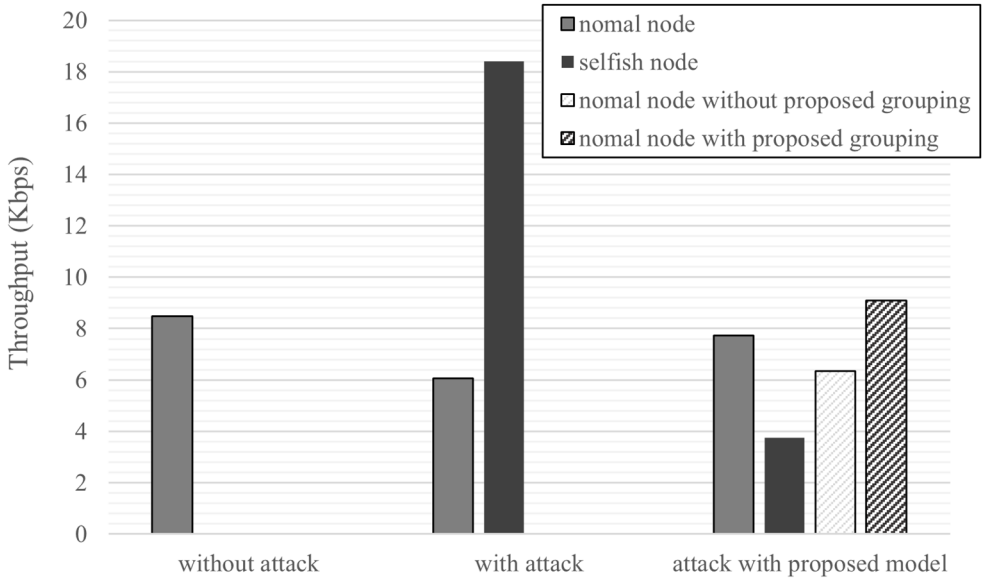


FIGURE 14. Comparison of throughput each environment

Fig. 14와 같이, 노드 별 스루풋의 평균에서는 공격이 발생하지 않는 환경의 경우 전체 노드들의 스루풋 평균이 8.48Kbps로 측정된다. 하지만 이기적 노드의 개입으로 자원을 독점하는 환경에서는 정상 노드는 6.07Kbps로 약 28.4%의 스루풋이 감소하고 이기적 노드의 스루풋은 18.40Kbps로 정상 노드보다 약 2배 이상의 스루풋을 보인다. 그러나 제안하는 방법인 그룹 기반의 백오프 조정 방식이 적용된 네트워크 환경에서는, 정상 노드들의 전체 스루풋은 7.72Kbps로 약 9%의 감소만 보였으며 백오프를 조정한 그룹은 9.09Kbps, 조정하지 않은 그룹은 6.35Kbps로 백오프를 조정하지 않은 그룹

에서도 공격이 발생하지 않은 환경보다 약 25%의 스루풋이 감소하면서 전체 노드가 종래 방식보다 더 높은 스루풋을 보장하는 것을 증명했다. 특히, 이기적 노드의 스루풋은 3.74Kbps로 감소하면서 약 80%의 스루풋이 감소했다.

제안 모델이 적용된 네트워크 환경은 이기적 노드가 존재해도 약 28.3% 감소하는 종래 환경 대비 약 9%의 감소량을 보였으며, 이기적 노드의 스루풋은 큰 폭으로 감소시키며 이기적 노드의 자원 독점을 완화하는 모습을 보였다.

노드별 공정성을 비교한 결과는 Fig. 15와 같다.

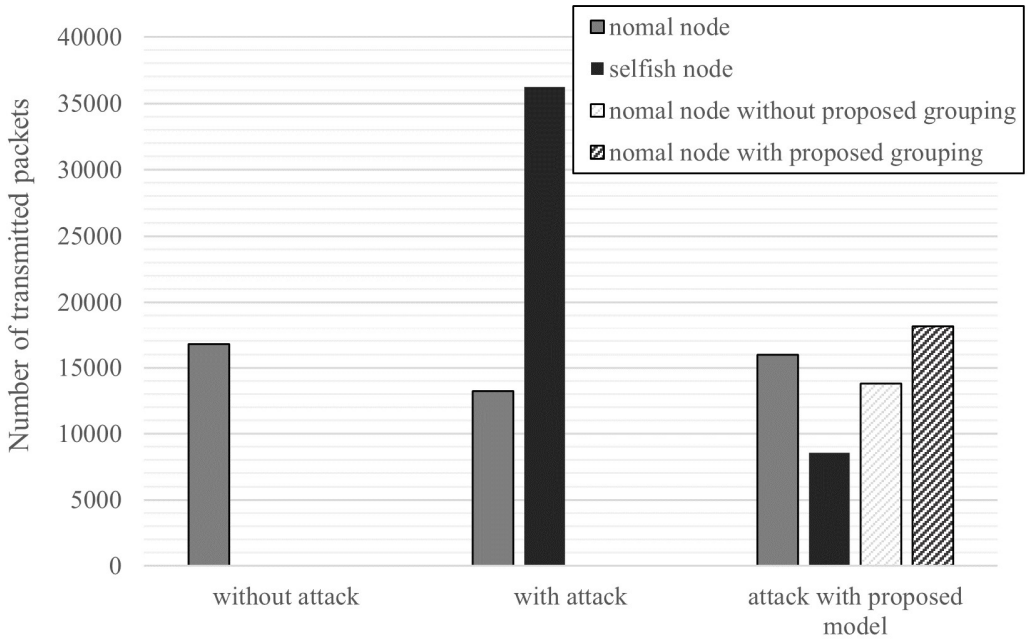


FIGURE 15. Comparison of fairness each environment

노드 별 공정성은 각 노드가 통신 기회를 가져간 지표인 패킷 전송 횟수를 이용하여 비교하였다. 실험 결과, 공격이 발생하지 않은 정상 환경에서는 노드들의 평균 패킷 전송 횟수가 16,790회였으나 공격이 발생하면 정상 노드는 13,217회, 이기적 노드는 36,255회로 정상 노드는 약 21%가 감소했다. 그러

나 제안하는 기법을 적용한 환경에서는 10개 정상 노드들의 평균 패킷 전송 횟수가 15,987회로 공격이 발생하지 않은 환경에 비해 약 4.7% 정도의 감소량만 보이며, 36,255회였던 이기적 노드는 8,548회로 약 76%의 큰 감소 폭을 보였다.

5. 결론 및 향후 연구

네트워크 내에 이기적 노드가 존재할 때, 네트워크에서 적절히 대응하지 못하면 나머지 노드들의 스루풋이 급격히 낮아져 사용성 침해의 우려가 있다. 그러나 이기적 노드는 정상 노드들의 동작에 직접 개입하지 않고 채널을 독점하거나 정상 노드로 위장하여 동작하기 때문에 탐지하기 어렵다. 본 연구에서는 이러한 문제점을 해결하고자 이기적 노드에 대응하기 위한 그룹핑 기반의 백오프 조정 방법을 제안하였다. 이기적 노드 존재가 파악되면 중앙 서버는 나머지 노드들을 절반씩 그룹화하여 백오프 값을 조정한다. 조정 과정을 반복적으로 수행함에 따라 최적의 수치에 도달하게 된 경우 이기적 노드와 유사한 수준의 백오프 값을 가지고 경쟁할 수 있음으로써 이기적 노드의 네트워크 자원 독점을 완화할 수 있다. 더불어, 특정 환경조건이나 정보를 이용하지 않고 일반적인 네트워크 환경에서 백오프 값만 조정하여 이기적 노드에 대한 대응이 가능해 환경조건에 제약을 받지 않는다는 기여점이 있다. 백오프 조정 방식의 성능을 평가하기 위해 Netsim Standard 13.2 시뮬레이터를 이용하여 제안 모델이 적용된 환경과 적용되지 않은 환경을 구축하여 비교하였다. 실험 결과 이기적 노드의 백오프 값과 같은 수준까지 조정되었을 때, 제안 모델이 적용되지 않은 환경에서는 정상 노드들이 약 28.4%의 스루풋이 감소하였으나 제안 모델을 적용할 경우 정상 노드는 약 9%만 감소했다. 또한, 이기적 노드는 제안 모델을 적용했을 때 약 80%의 스루풋이 감소하여 이기적 노드가 존재해도 이기적 노드의 자원 독점을 완화하면서도 기존 성능을 유지할 수 있음을 보였다. 하지만, 본 연구의 시뮬레이션 모델링은 각 센서 노드의 위치나 개별적인 성능, 특성을 고려하지 않고 일관된 성능을 가진 10개의 센서가 존재하는 환경에서 진행되었다. 그리고 실험의 단순성을 위해 그룹핑 대상의 노드를 이분법적으로 나누고, 1명의 공격자를 두었기 때문에 실제 다양한 종류, 성능이 연결된 센서 네트워크와는 차이가 있을 수 있

다. 향후 연구로는 각 노드의 통신 환경 및 스루풋 등을 학습하여 우선순위 기반의 그룹화를 상세하게 수행함으로써 성능 최적화를 수행하고자 한다.

V. 결론

4차 산업 혁명과 함께 초연결 기술을 실현하기 위한 사물인터넷, 무선 센서 네트워크 기술들이 활발히 연구되고 있으며 네트워크의 보안성과 사용성을 향상하기 위한 연구들이 함께 진행되고 있다. 본 연구에서는 네트워크에서 발생하는 보안성, 사용성 간 트레이드오프 문제를 해결하고자 두 가지 방법론을 제안하였다.

분산 네트워크 환경에서 더 높은 보안성과 사용성 수준을 동시에 보장하기 위한 “안전한 네트워크 연결을 위한 분산 인증 메커니즘(DAM4SNC)”을 제안하였으며 실험 결과 같게 주어진 지연 시간 요구사항에서 제안 모델이 종래 방식보다 더 높은 인증 수준을 보장할 수 있음을 보였고, 제안 모델의 상대 효율성(REP) 측면에서도 높은 결과를 보였다.

이기적 노드 대응을 위한 그룹핑 기반의 백오프 조정 방법에서도 제안 모델을 적용했을 때, 이기적 노드가 존재하는 환경을 기준으로 종래 방법보다 더 적은 스루풋이 감소하는 것을 보였다. 또한, 이기적 노드의 자원 독점은 큰 폭으로 완화할 수 있음을 보여 제안 방식의 성능을 입증했다.

ACKNOWLEDGMENTS

본 논문의 PART 1: 분산 네트워크 환경에서의 인증 모델은 2022년 1월 MDPI Sensors에 게재된 내용을 보완하여 작성되었습니다[54].

본 논문들을 지도해주신 이일구 교수님과 PART 1 연구 구체화를 위한 논의와 시뮬레이션 평가, 관련 연구 분석에 기여해 준 공저자 박소현, 오예솔, 문정현 학생, PART 2: 네트워크 내 이기적 노드 대응 방법 연구를 위한 관련 연구 분석에 기여해 준 김서이 학생에게 감사드립니다.

참고 문헌

[1] Alqahtani, H.; Sarker, I.H.; Kalim, A.; Minhaz Hossain, S.M.; Ikhlaq, S.; Hossain, S. Cyber Intrusion Detection Using Machine Learning Classification Techniques. In Proceedings of the International Conference on Computing Science, Coummunication and Security, Gujarat, India, 26-27 March 2020; pp. 121-131.

[2] Jaehyeok, H.; Youngin, Y.; Gimin, H.; Jaeyeon, L. Secure file transfer method and forensic readiness by converting file format in network segmentation environment. J. Inf. Secur. Cryptogr. 2019, 29, 859-866.

[3] Liu, D.; Chang, X.; Wan, S.; Tang, J.; Cheng, Y. Turing Machine-based cross-network isolation and data exchange theory model. IEEE Access 2019, 7, 125732-125746.

[4] Hou, Y.; Such, J.; Rashid, A. Understanding security requirements for industrial control system supply chains. In Proceedings of the 2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Montreal, QC, Canada, 28 May 2019; pp. 50-53.

[5] Lin, Y.; Lin, L. Design and realization of a computer security control circuit for local area network. In Proceedings of the 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, 5-7 July 2019; pp. 9-12.

[6] Sunil, C.; Anil, K.; Ned, S.; David, M.W. Conceptualizing the Secure Internet of Things. In Demystifying Internet of Things Security; Apress: Berkeley, CA, USA, 2020.

[7] Weijia, J.; Wanlei, Z. Distributed Network Systems: From Concepts to Implementations; Springer: Boston, MA, USA, 2004; Volume 15.

[8] Jacomme, C.; Kremer, S. An extensive formal analysis of multi-factor authentication protocols. In Proceedings of the 2018 IEEE 31st Computer Security Foundations Symposium (CSF), Oxford, UK, 9-12 July 2018; pp. 1-15.

[9] Ignacio, V.; Angelica, C.; Alfonso, R. Authentication schemes and methods: A systematic literature review. Inf. Softw. Technol. 2018, 94, 30-37.

[10] Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Netw. 2019, 33, 82-88.

[11] Nag, A.K.; Roy, A.; Dasgupta, D. An adaptive approach towards the selection of multi-factor authentication. In Proceedings of the 2015 IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, 7-10 December 2015; pp. 463-472.

[12] Akyurek, A.S.; Rosing, T.S. Optimal packet aggregation scheduling in wireless networks. IEEE Trans. Mob. Comput. 2018, 17, 2835-2852.

[13] Taguchi, Y.; Kawashima, R.; Nakayama, H.; Hayashi, T.; Matsuo, H. PA-Flow: Gradual packet aggregation at virtual network I/O for efficient service chaining. In Proceedings of the 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Hong Kong, China, 11-14 December 2017; pp. 335-340.

[14] Wang, P.; Petrova, M. Cross talk MAC: A directional MAC scheme for enhancing frame aggregation in mm-wave wireless personal area networks. In Proceedings of the 2016 IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur, Malaysia, 23-27 May 2016; pp. 602-607.

[15] Karmakar, R.; Chattopadhyay, S.; Chakraborty, S. Impact of IEEE 802.11n/ac PHY/MAC high throughput enhancements on transport and application protocols-A survey. IEEE Commun. Surv. Tutor. 2017, 19, 2050-2091.

[16] Rahman, H.; Ahmed, N.; Hussain, I. Comparison of data aggregation techniques in Internet of Things (IoT). In Proceedings of the 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 23-25 March 2016; pp. 1296-1300.

[17] Zhou, X.; Boukerche, A. AFLAS: An adaptive frame length aggregation scheme for vehicular networks. IEEE Trans. Veh. Technol. 2016, 66, 855-867.

[18] Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A. Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev. 2); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2015.

[19] Federal Financial Institutions Examination Council. FFIEC Information Technology Examination Handbook Information Security; Federal Financial Institutions Examination Council: Arlington, WV, United States, 2016.

[20] Lim, M. Directly and indirectly synchronous communication mechanisms for client-server systems using event-based asynchronous communication framework. IEEE Access 2019, 7, 81969-81982.

[21] Mundada, Y.; Ramachandran, A.; Feamster, N. SilverLine: Data and network isolation for cloud services. In Proceeding of the 3rd HotCloud, Portland, OR, USA, 14-15 June 2011.

[22] Qi, Z.; Wu, Y.; Hang, F.; Xie, L.; He, Y. A Secure Real-time Internal and External Network Data Exchange Method Based on Web Service Protocol. In Proceeding of the 2020 International Symposium on Computer Engineering and Intelligent Communications (ISCEIC), Guangdong, China, 7-9 August 2020; pp. 184-187.

[23] Feng, X.; Sicheng, T.; Gongliang, L.; Yang, X.; Yizheng, T. Research on Cross-network Exchange Method of Enterprise Application Business Process Data. J. Phys. Conf. Ser. 2020, 1693, 012037.

[24] De Freitas, M.B.; Rosa, L.; Cruz, T.; Simões, P. SDN-Enabled Virtual Data Diode. In Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2018; Volume 11387.

[25] Cao, J.; Yu, P.; Ma, M.; Gao, W. Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network. IEEE Internet Things J. 2018, 6, 1561-1575.

[26] Mahalle, P.N.; Shinde, G.; Shafi, P.M. Rethinking Decentralised Identifiers and Verifiable Credentials for the Internet of Things. In Internet of Things, Smart Computing and Technology: A Roadmap Ahead; Part of the Studies in Systems, Decision and Control book series (SSDC); Springer: Cham, Switzerland, 2020.

[27] Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. 2020, 135, 106382.

[28] Nguyen, H.; Marendy, P.; Engelke, U. Collaborative framework design for immersive analytics. In Proceeding of the 2016 Big Data Visual Analytics (BDVA), Sydney, Australia, 22-25 November 2016; pp. 1-8.

[29] Idris, M.Y.; Stiawan, D.; Habibullah, N.M.; Fikri, A.H.; Abd, R.M.R.; Dasuki, M. IoT smart device for e-leaming content sharing on hybrid cloud environment. In Proceeding of the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 19-21 September 2017; pp. 1-5.

[30] Kawato, T.; Higashino, M.; Takahashi, K.; Kawamura, T. Proposal of e-learning system integrated P2P model with client-server model. In Proceeding of the 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 22-25 January 2019; pp. 1-6.

[31] Shi, C.; Zhang, Y.; He, R. Design and implementation of a P2P r esource sharing system based on metadata catalog. In Proceeding of the 2016 9th International Symposium on Computational Intellige nce and Design (ISCID), Hangzhou, China, 10-11 December 2016; pp. 78-81.

[32] Choi, S.; Lee, J.H. Blockchain-based distributed firmware update architecture for IoT devices. IEEE Access 2020, 8, 37518-37525.

[33] Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. Big Data Cogn. Comput. 2 020, 4, 28.

[34] Cha, J.; Singh, S.K.; Kim, T.W.; Park, J.H. Blockchain-empower ed cloud architecture based on secret sharing for smart city. J. In f. Secur. Appl. 2021, 57, 102686.

[35] Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; C hoo, K.K.R.; Aledhari, M. Decentralized Authentication of Distribute d Patients in Hospital Networks Using Blockchain. IEEE J. Biomed. Health Inform. 2020, 24, 2146-2156.

[36] Khorsandi, B.M.; Tonini, F.; Raffaelli, C. Centralized vs. distribut ed algorithms for resilient 5G access networks. Photon. Netw. Com mun. 2019, 37, 376-387.

[37] De As□s L□pez-Fuentes, F. Decentralized Online Social Network Architectures. In Social Networks and Surveillance for Society; Spr inger: Berlin/Heidelberg, Germany, 2019; pp. 85-100.

[38] Sihite, A.B.; Susanti, B.H. Second preimage attack method on various MAC constructions and its application with AES-128. In Proceeding of the 2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 23-24 August 2016; pp. 37-42.

[39] Jiang, S.; Zhu, X.; Wang, L. An efficient anonymous batch authentication scheme based on HMAC for VANETs. IEEE Trans. Intell. Transp. Syst. 2016, 17, 2193-2204.

[40] Ålvarez, I.; Moutinho, L.; Pedreiras, P.; Bujosa, D.; Proenza, J.; Almeida, L. Comparing Admission Control Architectures for Real-Time Ethernet. IEEE Access 2020, 8, 105521-105534.

[41] Cena, Gianluca, et al. "Evaluating and modeling IEEE 802.15. 4 TSCH resilience against Wi-Fi interference in new-generation highly-dependable wireless sensor networks." Ad Hoc Networks 106 (2020): 102199.

[42] Khan, Tayyab, et al. "ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs." Future Generation Computer Systems 125 (2021): 921-943.

[43] Sah, Dinesh Kumar, et al. "EDGF: Empirical dataset generation framework for wireless sensor networks." Computer Communications 180 (2021): 48-56.

[44] Nayak, Padmalaya, et al. "Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities." Measurement 178 (2021): 108974.

[45] Tian, Le, et al. "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11 ah research." Journal of Network and Computer Applications 182 (2021): 103036.

[46] Sangeetha, U., and A. V. Babu. "Service differentiation in IEEE 802.11 ah WLAN under restricted access window based MAC protocol." Computer Communications 172 (2021): 142-154.

[47] Fayaz, Muhammad, et al. "Counteracting selfish nodes using reputation based system in mobile Ad Hoc networks." Electronics 11.2 (2022): 185.

[48] Sadek, Fatima Salma, et al. "Identifying Misbehaving Greedy Nodes in IoT Networks." Sensors 21.15 (2021): 5127.

[49] Jim, Lincy E., Nahina Islam, and Mark A. Gregory. "Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes." Computers & Security 113 (2022): 102538.

[50] Zapata, Manel Guerrero. "Secure ad hoc on-demand distance vector routing." ACM SIGMOBILE Mobile Computing and Communications Review 6.3 (2002): 106-107.

[51] Fihri, Wassim Fassi, et al. "A Machine Learning Approach for Backoff Manipulation Attack Detection in Cognitive Radio." IEEE Access 8 (2020): 227349-227359.

[52] Georgiev, Y.; Verhoeven, R.; Meratnia, N. Selfish Behavior in IEEE 802.11ah Networks: A Detection Algorithm and Mitigation Strategies. Sensors 2022, 22, 4472. https://doi.org/10.3390/s22124472

[53] Tetcos, NetSim, https://www.tetcos.com/index.html

[54] Park, N.-E.; Park, S.-H.; Oh, Y.-S.; Moon, J.-H.; Lee, I.-G. Distributed Authentication Model for Secure Network Connectivity in Network Separation Technology. Sensors 2022, 22, 579. https://doi.org/10.3390/s22020579

ABSTRACT

Secure communication technique in distributed networks

Na Eun Park
Department of Future Convergence Technology Engineering
Graduate School of
Sungshin Women's University

Along with the 4th industrial revolution, technologies to realize a hyper-connected society, such as the Internet of Things (IoT) and Wireless Sensor Networks (WSN), are being actively researched. It has excellent scalability and no environmental restrictions compared to existing wired networks. Therefore, it can be applied in various fields, such as smart homes, smart cities, and smart factories. However, performance deterioration in security and usability occurs as many network connections are made of multiple devices. Network separation technology and RAW (Restricted Access Window) technology have been proposed and used to solve this problem. However, conventional technologies have a limitation in that a trade-off relationship exists between security and usability, in which usability deteriorates when security improves, and security deteriorates when usability improves. In this paper, we propose two methodologies: an authentication model in a distributed network environment and a method for dealing with selfish nodes in the network to simultaneously improve security and usability and alleviate performance problems caused by selfish nodes.

Experimental results show that the authentication model guarantees an authentication level of about 76% higher than the conventional model in terms of latency requirements and that the selfish node's resource monopoly can be alleviated by about 80% in the response model of the selfish node.