



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

이 일 구 교수 지도  
석사학위 청구논문

고신뢰 · 고효율 네트워크를 위한  
동적 릴레이 전송 기법

2024

성신여자대학교 대학원  
미래융합기술공학과  
전 유 란

고신뢰 · 고효율 네트워크를 위한  
동적 릴레이 전송 기법

이 일 구 교수 지도

이 논문을 석사학위 논문으로 제출함

2023년 11월

성신여자대학교 대학원  
미래융합기술공학과  
전 유 란

# 인 준 서

전유란의 석사학위 논문으로 인준함

2023년 11월

심사위원장..... 김 성 민..... (서명 또는 인)

심 사 위 원..... 임 연 섭..... (서명 또는 인)

심 사 위 원..... 이 일 구..... (서명 또는 인)

성신여자대학교 대학원

## 논문 개요

WiFi 기술은 고성능·고효율 무선 네트워크를 실현하기 위해 세대를 거듭하며 발전하고 있다. 최근 시작된 IEEE(Institute of Electrical and Electronics Engineers) 802.11bn 표준화 과정에서 차세대 WiFi 기술은 데이터 처리율, 서비스 응답 속도, 지연, 파워 소모량을 획기적으로 개선하여 고신뢰성(Ultra High Reliability, UHR)을 보장하는 것을 목표로 진화하고 있다. 그러나 최근 WiFi를 탑재한 정보통신(Information Technology, IT) 제품 시장 규모의 성장과 함께 무선랜(Wireless Local Area Network, WLAN)의 보안 위협이 증가하고 있음에도 불구하고, 보안성 향상을 위한 표준화 노력이 미흡한 상황이다. 본 연구에서는 무선 단말이 패킷의 보안 요구사항과 지연 요구사항을 인지하여 적응적으로 릴레이 전송(Adaptive Relay Transmission, ART)을 수행하는 전송 기법을 제안한다. ART는 저지연 전송이 요구될 경우, 단일 홉 전송하는 직접(direct) 전송 방식으로 전송하고, 강한 보안이 요구될 경우, 짧은 홉 전송하여 도청 확률을 줄이는 릴레이(relay) 전송 방식을 사용한다. 또한, 저지연과 강한 보안이 동시에 요구되는 상황에서는 데이터 처리율, 에너지 효율성, 보안을 종합적으로 고려하는 전송 방식을 결정하여 네트워크의 신뢰성을 향상시킨다. 실험 결과에 따르면, ART는 지연 허용 네트워크(Delay Tolerant Network, DTN) 환경에서 항상 direct 전송하는 direct 모델 대비 신뢰 네트워크 에너지 효율을 13.1배 개선하였으며, 보안 위협이 큰 네트워크 환경에서 항상 relay 전송하는 relay 모델과 동일한 수준의 정보유출량을 보였다. 또한, ART는 노드 밀집도가 큰 네트워크 환경에서 direct 모델보다 네트워크 처리율을 212.4% 개선하였으며, 네트워크 간섭이 큰 상황에서도 15.4 Mbps의 링크 처리율을 보이며, 간섭의 영향이 가장 적음을 입증하였다.

# 목 차

논문 개요	
I. 서론	1
II. 관련 연구	5
III. 고신뢰 · 고효율 네트워크를 위한 동적 릴레이 전송 기법	12
1. ART의 구조와 동작	12
2. ART의 전송 방식 결정 방법	15
1) direct 전송과 relay 전송 방식	15
2) ART의 전송 방식 결정 방법	16
IV. 평가지표	18
1. 보안성	19
1) 도청자 공격에 대한 대응	19
2) 정보유출량	19
2. 에너지 효율	21
3. 처리율	25
V. 평가 및 분석	26
1. 네트워크 모델	26
2. 네트워크 상황에 따른 성능 비교	28
1) 지연 허용 네트워크 환경에서의 성능 비교	28
2) 보안 위협이 큰 네트워크 환경에서의 성능 비교	33
3) 시뮬레이션 라운드 수에 따른 네트워크의 배터리 수명	
비교	35
4) 노드 밀집도가 큰 네트워크 환경에서의 성능 비교	36

5) 간섭이 큰 네트워크 환경에서의 성능 비교 ..... 41

VI. 결론 ..... 46

참고문헌

ABSTRACT(영문초록)

## 표 차 례

Table 1. Related work on transmission method .....	5
Table 2. Transmission table of ART(HT/HR) .....	17
Table 3. The descriptions of notations .....	18

## 그림 차례

FIGURE 1. Energy model and radio block diagram of ART .....	12
FIGURE 2. Packet frame structure of ART .....	14
FIGURE 3. Flowchart of transmission algorithm of ART .....	17
FIGURE 4. Network structure of simulation .....	26
FIGURE 5. Network energy efficiency vs. ratio of delay tolerant packets .....	29
FIGURE 6. Link throughput vs. ratio of delay tolerant packets .....	31
FIGURE 7. Network throughput vs. ratio of delay tolerant packets · .....	32
FIGURE 8. Information leakage vs. the number of eavesdropping nodes in network .....	33
FIGURE 9. Remaining energy level vs. simulation rounds .....	35
FIGURE 10. Network energy efficiency vs. the number of the active other nodes .....	36
FIGURE 11. Link throughput vs. the number of the active other nodes .....	38
FIGURE 12. Network throughput vs. the number of the active other nodes .....	39
FIGURE 13. Network energy efficiency vs. interference range of the active other nodes .....	41
FIGURE 14. Link throughput vs. interference range of the active	

other nodes ..... 42

FIGURE 15. Network throughput vs. interference range of the  
active other nodes ..... 44

## I. 서론

5세대(5th Generation, 5G) 이동 통신 기술이 널리 보급되어 활용되면서 사물인터넷(Internet of Things, IoT) 장치 간의 원격 통신뿐 아니라 증강현실(Augmented Reality, AR), 가상현실(Virtual Reality, VR), 메타버스와 같은 가상환경에서 통신하는 애플리케이션들이 기하급수적으로 증가하고 있다. 이처럼, 방대한 양의 데이터를 처리하기 위한 안정적인 저지연 통신(Ultra Reliability and Low Latency Communication, URLLC)이 요구되고 있으며, 많은 양의 데이터를 실시간으로 안전하게 전송하기 위한 다양한 기술들이 개발되고 있다 [1].

대표적인 근거리 무선 통신 기술인 WiFi 기술은 전 세계 모바일 트래픽의 약 67%를 처리할 정도로 필수적인 통신 인프라 기술로 활용되고 있다 [2]. 또한, 무선 네트워크 환경에서 안전하고 효율적인 통신 서비스 환경을 제공하기 위해 세대별 WiFi 기술의 표준화 노력이 적극적으로 이루어지고 있다. WiFi 4세대는 높은 처리율(High Throughput, HT), 5세대는 매우 높은 처리율(Very High Throughput, VHT), 6세대는 높은 효율성(High Efficiency, HE), 7세대는 극도로 높은 처리율(Extremely High Throughput, EHT), 그리고 8세대는 무선 장치의 보안 취약점을 공격하는 네트워크 환경이나 간섭 환경에서도 효율적이고 신뢰할 수 있는 초고신뢰(Ultra High Reliability, UHR) 통신 환경을 제공하는 것을 목표로 하고 있다. WiFi 7은 802.11be에 도입된 특성들에 기반하여 표준화를 완료하고, 2024년부터 상용화를 목표로 하고 있으며, WiFi 8은 2023년 11월 스터디 단계를 마무리하고, 표준화 시작 단계에 있다.

WiFi 8에서는 다중 액세스 포인트(Multi-Access Point, Multi-AP), 다중 링크(multi-link), 다중 사용자(multi-user), 전송 기회(Transmission Opportunity, TXOP) 시간 공유, 릴레이(relay) 전송 기술의 표준화를 통해 네

트위크의 신뢰성을 극대화한다 [3]. 특히, relay 전송 기술은 액세스 포인트로 동작하지 않는 스테이션(non-Access Point Station, non-AP STA)이 relay 전송을 수행하는 스테이션(Relay Station, Relay STA)으로 동작함으로써 직접(direct) 전송 기술보다 저비용으로 광범위 통신이 가능하다 [4]. multi-link를 활용하여 relay 통신을 수행하면, 지연에 민감한 정보와 지연이 허용되는 정보를 구분한 후 서로 다른 링크로 전송하여 서비스 품질(QoS, Quality of Service) 개선이 가능하다 [5]. 또한, relay 통신 시 multi-AP 노드, multi-user 노드, relay STA 노드 간의 TXOP 정보를 교환하면 안정적인 저지연 통신이 가능하다 [6]. 이처럼 relay 전송 기술을 multi-AP, multi-link, TXOP 시간 공유 기술과 함께 활용하면, 간섭을 최소화한 저비용, 고효율 통신이 가능하며 통신 범위 확장이 가능하다. 따라서, WiFi 8에서는 UHR 보장을 위해 relay 전송 기술 관련 표준화가 필수적이다.

또한, WiFi 8에서 중점적으로 다루고 있는 UHR을 달성하기 위해서는 에너지 효율과 데이터 처리율 간의 트레이드오프(trade-off) 문제와 보안 위협 문제를 고려해야 한다. 높은 데이터 처리율을 달성하기 위해서는 제한된 시간 안에 더 많은 데이터를 전송해야 하므로, 저지연성과 데이터 손실률 모두 개선해야 한다. 그러나 저지연성을 보장하기 위해서는 짧은 시간 동안 큰 파워를 사용하여 데이터를 전송해야 하는데, 이때 많은 에너지를 소모하게 되고, 일부 노드는 전력 제약으로 인해 패킷을 전송하지 못하는 문제가 발생한다. 즉, 패킷이 요구하는 지연성을 고려하여, 요구되는 수준만큼의 최적의 전송 파워를 사용하는 것이 매우 중요하다. 또한, WiFi를 탑재한 정보 통신(Information Technology, IT) 제품의 수가 증가함에 따라 무선랜의 보안 취약점을 타겟으로 하는 공격이 증가하고 있다 [7]. 그러나 최근까지 WiFi는 높은 데이터 처리율, 간섭 최소화, 에너지 효율성에 초점을 맞춰 발전하고 있으며, 패킷 통신의 보안성은 고려하지 못하고 있다. 즉, 종래의 WiFi는 보안 요

구사항을 만족하지 못하더라도 고속 전송률, 저지연, 저전력 성능 요구사항을 만족하면 고신뢰 프로토콜로 간주되어 왔다. 그러나 WiFi 8에서 추구하는 UHR 목표를 달성하기 위해서는 보안과 성능을 모두 고려한 표준 기술 개발이 필수적으로 요구된다.

본 연구에서는 무선 센서 네트워크 환경에서의 고신뢰성을 보장하기 위해 패킷의 지연 요구사항과 보안 요구사항을 고려하여 direct 전송 방식과 relay 전송 방식을 동적으로 사용하는 적응형 릴레이 전송(Adaptive Relay Transmission, ART) 방식을 제안한다. 제안하는 ART는 direct 전송을 통해 저지연성을 보장하고, relay 전송을 통해 보안성을 향상시킨다. 또한, direct 전송 방식과 relay 전송 방식을 동적으로 적용함으로써 애플리케이션에서 요구되는 수준만큼의 최적의 자원을 사용하고, 성능과 보안을 최적화하여 통신의 신뢰성을 향상시킨다.

본 논문의 주요 기여점은 다음과 같다.

- 첫째, 네트워크 상황을 인지하여 보안과 성능을 최적화하는 고신뢰·저지연 동적 릴레이 전송 방식을 제안한다.
- 둘째, 기존 장치(legacy device)와 후방 호환성(backward compatibility)을 유지하면서 고신뢰·저지연 전송 방식을 지원하는 패킷 프레임 구조를 제안한다.
- 셋째, MATLAB 환경에서 무선랜 환경을 구성한 후 제안하는 ART 방식과 종래의 방식을 구현하고, 네트워크의 밀집도, 간섭, 패킷의 요구사항이 변화함에 따른 비신뢰 네트워크 에너지 효율, 신뢰 네트워크 에너지 효율, 링크 처리율, 네트워크 처리율, 정보유출 정도를 평가하였다.

본 논문의 구성은 다음과 같다. II 장에서는 선행연구를 분석하고, III 장에서는 제안하는 모델인 동적 릴레이 전송 방식을 설명한다. IV 장에서는 보안, 에너지 소모량, 처리율을 비교하고 분석하기 위한 평가지표를 설명하며, V 장

에서는 평가 결과를 분석한다. VI장에서는 결론을 맺는다.

## II. 관련 연구

무선 센서 네트워크에서 전송 방식은 큰 전송 파워로 단일 홉 전송하는 direct 전송 방식과 작은 전송 파워로 다중 홉 전송하는 relay 전송 방식이 있다. direct 전송 방식은 데이터를 빠르게 전송할 수 있지만, 파워 소모량이 크며, relay 전송 방식은 지연이 크지만, 짧은 홉으로 전송하기 때문에 파워 소모량이 작다. 즉, direct 전송 방식과 relay 전송 방식은 네트워크 상황에 따라 전송 효율이 달라진다. 따라서, direct 통신 환경과 relay 통신 환경을 동시에 고려하고, 네트워크 상황에 적응적으로 동작하여 전송 효율을 높이는 동적 (Adaptive) 전송 방식이 연구되고 있다. Table 1은 relay 전송 방식과 adaptive 전송 방식의 기여점과 한계점을 분석한 결과이다. 또한, 각 연구에서 중점적으로 개선하고자 하는 성능들을 에너지, 지연, 보안 관점에서 분류하였다.

Table 1. Related work on transmission method

Transmission method	Ref	Contribution	Limitation	Main features		
				Energy	Latency	Security
Relay	[8]	<ul style="list-style-type: none"> <li>• 통계학습 기반 반 분산형 적응 네트워크 접근 메커니즘을 제안하여 네트워크 오버헤드를 개선함</li> </ul>	<ul style="list-style-type: none"> <li>• 제안하는 방식은 패킷의 지연만을 고려하므로 자원 제약적인 IoT 환경에 적용하기 어려움</li> </ul>	x	√	x
	[9]	<ul style="list-style-type: none"> <li>• 유연한 파장 분할 다중화 기반 네트워크 제어 평면 아키텍처를 제안하여 지연을 최적화함</li> </ul>	<ul style="list-style-type: none"> <li>• 패킷의 보안 요구 사항과 다양한 네트워크 상황을 고려하지 못함</li> </ul>	√	√	x
	[10]	<ul style="list-style-type: none"> <li>• 가장 큰 에너지 잔량을 갖는 노드를 relay 전송 노드로서 선택하는 라우팅 방식을 제안하여 네트워크의 배터리 수명을 개선함</li> </ul>	<ul style="list-style-type: none"> <li>• 에너지 잔량이 큰 노드가 relay 전송 노드로 선택되므로, 악의적인 노드의 배터리 소모 공격에 취약함</li> </ul>	√	√	x

		<ul style="list-style-type: none"> <li>고신뢰 요구사항을 갖는 네트워크 상황을 가정하여 성능 평가를 수행함</li> </ul>	√	√	x	
[11]	<ul style="list-style-type: none"> <li>분산 학습 자동화 알고리즘을 사용하여 QoS를 최적화하고, 종단 간 지연과 에너지 소모량을 개선함</li> </ul>	<ul style="list-style-type: none"> <li>패킷의 보안 요구사항을 고려하지 못함</li> </ul>				
[12]	<ul style="list-style-type: none"> <li>에너지, 통신 경로(link) 노드의 배터리 수명 및 지연 지표를 고려하는 군집화 기반 지연 인식 relay 전송 노드 선택 방법을 제안함</li> </ul>	<ul style="list-style-type: none"> <li>데이터와 네트워크를 보호하는 데 필요한 보안 조치를 명시하지 않음</li> </ul>	√	√	x	
[13]	<ul style="list-style-type: none"> <li>계층적 군집화 기법과 에너지 수확 기술을 통합하여 이종 무선 센서 네트워크의 에너지 효율성을 향상시키는 relay 전송 방식을 제안함</li> </ul>	<ul style="list-style-type: none"> <li>이종 장치에 제안 프로토콜을 적용하는 데 있어 기밀성과 데이터 무결성에 대한 고려가 필요함</li> <li>노드를 다양한 군집으로 분류하여 관리하는 복잡성으로 인해 대규모 배포 상황에 적용하기 어려움</li> </ul>	√	x	x	
[14]	<ul style="list-style-type: none"> <li>무선 센서 네트워크에서 상황에 따라 경로를 조정할 수 있는 보안 라우팅 방식을 제안함</li> </ul>	<ul style="list-style-type: none"> <li>전송 지연에 대한 고려가 필요함</li> <li>높은 보안 수준을 유지하기 위한 추가적인 자원 소모를 고려하지 못함</li> </ul>	√	x	√	
Adaptive	[15]	<ul style="list-style-type: none"> <li>여러 개의 모바일 싱크 노드를 사용하여 direct 및 relay 전송을 결정하는 방식을 제안하고, 에너지 효율과 배터리 수명을 개선함.</li> </ul>	<ul style="list-style-type: none"> <li>다양한 싱크 노드의 이동성을 위한 오버헤드가 발생함</li> <li>동적 라우팅 과정에서 발생할 수 있는 보안 위협을 고려하지 못함</li> </ul>	√	x	x

[16]	<ul style="list-style-type: none"> <li>• 협력적인 단말 간 직접 통신 (device-to-device, D2D) 네트워크를 위한 동적 라우팅 접근 방식을 제안함</li> </ul>	<ul style="list-style-type: none"> <li>• 다양한 동적 네트워크의 변수들을 적용하지 못함</li> <li>• D2D 네트워크에서 협력적으로 라우팅하는 노드들의 보안 영향을 고려하지 못함</li> </ul>	√	√	x
[17]	<ul style="list-style-type: none"> <li>• 다양한 센서의 데이터를 수집하고, 패킷 결합 기술을 활용하는 라우팅 방식을 제안하여 전송 효율을 높임</li> </ul>	<ul style="list-style-type: none"> <li>• 서로 다른 센서가 동작함에 따른 보안 영향을 평가하지 못함</li> </ul>	√	√	x
[18]	<ul style="list-style-type: none"> <li>• 단일 홉 네트워크와 다중 홉 네트워크 환경을 고려하는 해시 기반 키 관리 메커니즘을 제안함</li> </ul>	<ul style="list-style-type: none"> <li>• 해시 기반 메커니즘을 적용함에 따른 처리 복잡성이 증가함</li> </ul>	√	√	√

Muhammad Ahmad Raza [8]은 네트워크의 자원 제약과 오버헤드를 고려하여, 통계학습 기반의 적응적 네트워크 접근 메커니즘을 제안하고, 지연이 허용되지 않는 패킷과 지연이 허용되는 패킷이 공존하는 네트워크에서의 효율적인 전송을 도모했다. 장치의 전송 이력을 학습하여 지연을 줄이고 다양한 패킷을 효과적으로 관리함으로써 산업용 사물인터넷(Industrial Internet of Things, IIoT) 네트워크의 자원 효율성을 개선하였다. 실험에 따르면, 종래 방식 대비 채널 활용 측면에서 효율적임을 입증하였으나, 제안하는 방식은 패킷의 지연을 우선적으로 고려하여 서비스 응답 시간 개선에 초점을 맞추고 보안과 에너지 효율을 분석하지 못했다.

Francesco Palmieri [9]은 5G 통신의 신뢰성을 보장하고, 지연을 줄이기 위해 파장 분할 다중화 기반 네트워크 제어 평면 구조를 제안했다. 제안하는 아키텍처를 통해 실시간 라우팅의 지연 및 차단(blocking)을 최소화하고, 전송 경로의 신뢰성을 보장할 수 있었다. 이 연구는 5G 통신의 신뢰성과 지연 최적

화를 수행했지만, 패킷의 보안 요구사항과 네트워크 상황을 고려하지 못하여 현실적인 네트워크 환경에 적용할 수 없었다.

Y. Harold Robinson [10]은 무선 센서 네트워크의 배터리 수명을 개선하기 위해 에너지 사용량을 고려하여 최적의 relay 전송 노드를 선택하는 동적 라우팅 프로토콜(Dynamic Routing Protocol, DRP)을 제안하였다. 제안하는 DRP는 에너지 잔량이 가장 큰 노드를 relay 전송 노드로 선택하여 패킷 전송률을 높인다. DRP는 종래 연구 대비 네트워크 배터리 수명을 개선하였으며, 배터리가 고갈되어 데이터를 전송할 수 있는 경로가 존재하지 않는 네트워크의 공백 노드 문제를 개선하였다. 이 연구는 서비스 지연과 에너지를 종합적으로 고려하여 상대적으로 유연한 네트워크 환경을 보장하지만, 노드의 배터리 잔량에 의존하는 노드 선택 방식을 적용하기 때문에 악의적인 노드의 배터리 소모 공격에 취약하다.

Habib Mostafaei [11]은 종래 QoS 라우팅 방식의 지연과 에너지 문제를 해결하기 위해 분산 학습을 활용한 라우팅 방법을 제안했다. 소수의 신뢰 노드를 택한 후 데이터를 전송하는 분산 알고리즘을 활용하여, QoS 요구사항들을 최적화했다. 네트워크 혼잡도와 신뢰성 요구사항이 변화함에 따른 평가를 수행했으며, 종단 간 지연과 에너지 소모량 모두 종래 라우팅 방식보다 우수했다. 그러나 이 연구는 고신뢰 요구사항을 가정한 평가를 수행하여 현실적인 네트워크 상황을 고려했다고 보기 어렵다. 또한, 패킷의 QoS 요구사항만을 고려하여, 보안 위협으로 인해 신뢰성이 저하되는 상황을 고려하지 못했다.

P. Suman Prakash [12]은 무선 센서 네트워크 환경에서 지연을 고려하는 relay 전송 노드 선택 메커니즘을 제안하였다. 또한, relay 전송 노드 선택 과정을 최적화하기 위해 노드의 거리, 에너지 효율, 링크의 배터리 수명 및 지연 지표에 기반하여 군집화를 수행하였다. 이 방법은 에너지 소모량을 관리하고 통신 지연을 줄여 네트워크의 효율성과 서비스 응답 속도를 향상하는 데 기여

하였지만, 데이터와 네트워크를 보호하는 데 필요한 보안 조치를 명시하지 않았다.

Antar Abdul-Qawy [13]는 계층적 군집화 기법과 에너지 수확 기술을 활용하여 이기종 무선 센서 네트워크의 에너지 효율성을 향상시키는 프로토콜을 제안했다. 이 방법은 에너지 잔량과 주변 노드와의 근접성을 함께 고려하여 군집화를 수행함으로써 데이터 전송 효율과 에너지 효율을 개선했다. 그러나 제안 모델은 노드를 네트워크 에너지, 혼잡도 등의 기준에 따라 다양한 군집으로 분류를 수행하여 관리하기 때문에 복잡성이 크며, 대규모 배포 상황에 적용하기에는 어렵다.

Qiong Shi [14]은 악의적인 노드가 존재하는 무선 센서 네트워크 환경에서 전송 경로를 조정하여 보안성을 개선하는 라우팅 방법을 제안했다. 이 방법은 이전의 패킷 전송 경로를 분석하여 relay 전송 노드의 공격확률에 기반한 신뢰값을 도출하고, 신뢰값이 큰 노드에 패킷을 전송한다. 또한, 네트워크의 변수들을 최적화하여 최적의 라우팅 경로를 선택하고, 패킷 손실률과 에너지 소모량을 개선하였다. 그러나 제안하는 방법은 전송 지연의 최적화를 수행하지 않으며, 개별 노드의 신뢰값 계산 과정에 따른 추가적인 자원 소모가 발생할 수 있다.

Bilal R. Al-Kaseem [15]은 여러 모바일 싱크노드를 사용하여 무선 센서 네트워크에서 최적의 전송 경로를 결정하며, 네트워크 내 전체 노드의 에너지 효율을 관리하는 방식을 제안했다. 제안하는 방식은 모바일 싱크노드로부터 수집한 주변 노드의 정보를 활용하여 경로를 결정함으로써 네트워크의 배터리 수명을 연장하고 에너지 효율을 개선했지만, 모바일 싱크노드를 별도로 관리함에 따른 오버헤드가 발생한다. 또한, 라우팅 과정에서 발생할 수 있는 도청이나 데이터 가로채기와 같은 잠재적인 위협으로부터 보호하기 위한 보안 조치를 고려하지 못했다.

Praveen Kumar Devulapalli [16]은 대규모 협력 D2D 네트워크를 위해 중단 간 지연과 에너지 효율을 고려하는 동적 라우팅 방식을 제안했다. 이 방식은 노드들의 지리적 위치에 기반하여 군집화를 수행하며, 노드 간의 협력적인 통신 방식을 활용하여 정보를 전송한다. 실험 결과에 따르면, 에너지 효율, 지연, 비트 수신 에러율을 개선하여 D2D 네트워크 성능을 향상시켰다. 그러나 제안 방식은 네트워크 동기화를 완전히 고려하지 못해 실제 네트워크 환경에 적용하기 어렵다. 또한, D2D 네트워크에서 협력 노드 간 데이터의 무결성과 기밀성에 대한 고려가 필요하다.

L.-L. Hung [17]은 에너지 효율을 개선하기 위해 센서의 배터리 수명을 개선하는 라우팅 체계를 제안했다. 다양한 센서들이 서로 다른 센서들의 이벤트 데이터를 수집하고 중계하며, 같은 방향으로 전송되는 패킷을 결합하여 목적지 노드로 전송함으로써 네트워크의 유연성을 향상시켰다. 이를 통해 전체 네트워크의 에너지 소모량을 줄이고, 센서 노드의 긴 배터리 수명을 유지했다. 그러나 서로 다른 유형의 센서가 동작함에 따라 보안의 위협이 증가할 수 있는 문제가 있다.

A.B. Feroz Khan [18]은 IoT 환경 내 단일 홉 네트워크뿐만 아니라 다중 홉 네트워크를 고려하는 해시 기반 키 관리 방법을 제안했다. 데이터 암호화 통신 시에 노드를 인증하는 방법을 단일 홉과 다중 홉 라우팅 시나리오에 적용하였으며, 패킷 손실률을 줄이기 위해 다중 홉 라우팅 방법을 활용하였다. 실험 결과에 따르면, 패킷 손실률, 지연, 에너지 소모량 관점에서 종래 방식 대비 성능이 개선됨을 시뮬레이션을 통해 입증했다. 그러나 해시 기반 메커니즘을 적용함에 따라 처리 복잡성이 증가할 수 있으며, 악성 노드의 악의적인 행위를 재밍 공격으로 한정하여 실제적인 공격 시나리오를 적용하기 어렵다.

종래의 연구들은 공통적으로 에너지 효율성, 지연성, 보안 간의 상관관계를 분석하지 못했으며, 이 중 일부 지표만 개선하는 데 초점을 맞췄다. 세 가지

지표를 모두 고려하기 어려운 이유는 에너지와 지연성 간의 trade-off 문제와 보안 기능을 추가하는데 복잡도와 비용이 증가하는 문제가 있기 때문이다. 그러나, 고신뢰·고효율 네트워크를 위해서는 에너지 효율, 지연성 그리고 보안을 필수적으로 고려하여 시스템을 설계해야 한다.

### Ⅲ. 고신뢰 · 고효율 네트워크를 위한 동적 릴레이 전송 기법

본 장에서는 미디어 액세스 제어(Media Access Control, MAC) 계층, 물리(Physical, PHY) 계층 관점에서 ART 동작 구조와 최적의 전송 방식을 결정하기 위한 ART의 동작 원리를 설명한다.

#### 1. ART의 구조와 동작

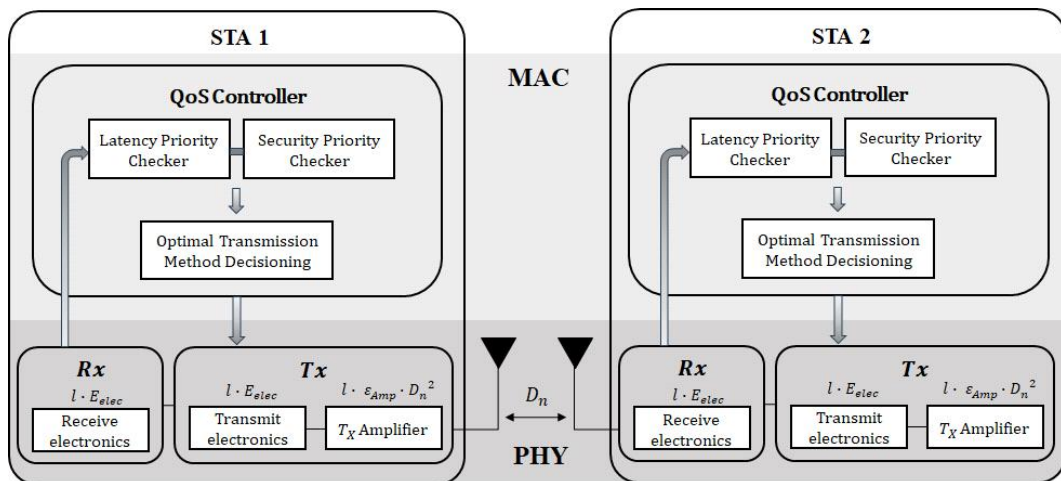


FIGURE 1. Energy model and radio block diagram of ART

Fig. 1은 제안하는 모델의 에너지 모델과 라디오 블록다이어그램을 나타낸 그림이다 [19]. MAC 계층에서는 스테이션(Station, STA) 1이 수신한 패킷을 처리하고, 패킷 요구사항을 확인하여 최적의 전송 방식을 결정하며, PHY 계

층에서는 결정된 전송 방식을 사용하여 STA 1에서 STA 2로 패킷을 전송한다. 또한, STA 2는 수신한 패킷의 요구사항을 확인하여 최적의 전송 방식을 결정하여, 다른 STA에 패킷을 전송한다. 본 연구에서 STA는 액세스 포인트 스테이션(Access Point Station, AP STA)과 비 액세스 포인트 스테이션(non-AP STA)을 포함하는 개념으로 정의하며, AP STA는 중계기 역할을 수행할 수 있는 노드이고, non-AP STA는 중계기 역할을 수행할 수 없는 노드를 말한다. 전송 방식은 direct 전송 방식과 relay 전송 방식 중 한 가지 전송 방식이 선택되는데, direct 전송 방식이 선택되는 경우에 출발지(source) STA에서 AP STA로 패킷을 direct 전송하며, relay 전송 방식이 선택되는 경우에는 source STA에서 non-AP STA로 relay 전송하여 최종적으로 AP STA에 패킷을 전달한다. QoS 컨트롤러는 디지털 기저대역(digital baseband) 시스템의 일부분으로 패킷의 지연과 보안 요구사항에 기반하여 우선순위를 확인하는 지연 우선순위 체커(latency priority checker), 보안 우선순위 체커(security priority checker)로 구성된다. latency priority checker는 패킷의 지연 요구사항에 따라 지연에 민감한(delay sensitive) 패킷인지, 지연이 허용되는(delay tolerant) 패킷인지 확인하고, security priority checker는 보안 요구사항에 따라 강한 보안(strong security)을 요구하는 패킷인지, 약한 보안(weak security)을 요구하는 패킷인지 확인한다. QoS 컨트롤러는 latency priority checker와 security priority checker가 확인한 패킷 요구사항을 고려하여 direct 전송 방식과 relay 전송 방식 중 한 가지 방식을 전송 방식으로 결정한다.

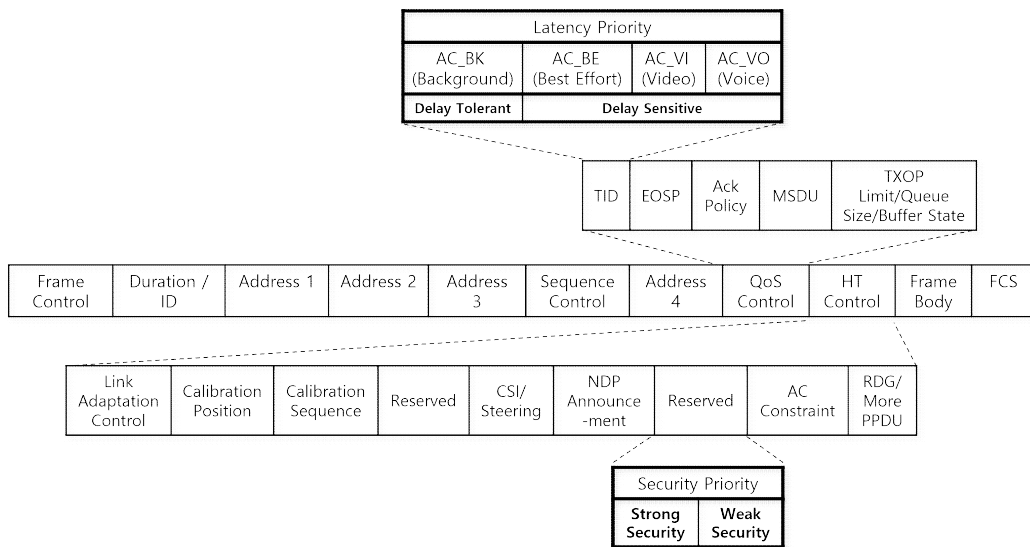


FIGURE 2. Packet frame structure of ART

Fig. 2는 제안하는 모델의 패킷 프레임 구조를 나타내며, IEEE(Institute of Electrical and Electronics Engineers) 802.11 무선랜 표준의 패킷 프레임 구조를 기반으로 하고 있다. 제안하는 패킷 프레임은 트래픽 아이디(Traffic Identifier, TID) 필드를 재활용하여 지연이 허용되는 트래픽과 지연에 민감한 트래픽을 구분할 수 있도록 하고 예약된(reserved) 비트를 security priority 필드로 활용한다는 점에서 종래의 패킷 프레임 구조와 차이가 있다. 강한 보안을 요구하는 패킷은 security priority 필드에 1로 입력되며, 약한 보안을 요구하는 패킷은 0으로 입력된다. 또한, 종래의 QoS Control 필드를 통해 지연이 허용되는 패킷인지, 지연에 민감한 패킷인지 확인한 후, latency priority 필드 값을 채운다. QoS Control 필드의 서브 필드인 TID 필드에는 액세스 카테고리(Access Category, AC)값이 입력되며, 지연 요구사항에 따라 AC\_background, AC\_best effort, AC\_video, AC\_voice로 나뉜다. 이 중 AC\_background 트래픽은 지연과 처리율의 제약을 받지 않는 트래픽을 의미

하므로 이는 지연이 허용되는 패킷으로 볼 수 있다 [20]. 따라서, latency priority checker는 TID 필드 값이 AC\_background라면 지연이 허용되는 패킷, 그렇지 않으면 지연에 민감한 패킷으로 간주한다. 지연에 민감한 패킷은 latency priority 필드 값이 1이며, 지연이 허용되는 패킷은 그 값이 0이다. latency priority checker와 security priority checker는 각각 latency priority와 security priority 필드 값을 확인하고, QoS 컨트롤러는 패킷의 요구사항을 고려하여 direct 전송 방식과 relay 전송 방식 중 한 가지 방식을 선택한다.

## 2. ART의 전송 방식 결정 방법

본 장에서는 패킷 전송 방식인 direct 전송 방식과 relay 전송 방식의 trade-off 관계를 분석하고, 지연 및 보안 요구사항에 기반하여 relay 전송 방식과 direct 전송 방식 중 한 가지 방식을 전송 방식으로 결정하는 알고리즘을 설명한다.

### 1) direct 전송과 relay 전송 방식

패킷을 전송하는 방식에는 direct 전송 방식과 relay 전송 방식이 있다. direct 전송 방식은 단일 홉을 통해 전송하는 방식으로, 패킷을 빠르게 전송할 수 있지만, 긴 홉으로 장거리 전송하기 때문에 파워 소모량이 크다. 따라서, direct 전송 방식은 에너지 잔량이 충분한 환경에서 서비스 응답 속도를 개선할 수 있다. relay 전송 방식은 다중 홉 전송 방식으로 노드에서 노드로 relay 전송하며, relay 전송 노드는 전송 링크 내에서 패킷을 전달하는 용도로만 사용된다. relay 전송 방식은 여러 홉을 거쳐 패킷을 전송하기 때문에 지연이 크지만, 짧은 홉을 사용하여 근거리 전송을 하므로 파워 소모량이 작다. 또한, 보안 관점에서 짧은 홉으로 전송하는 relay 전송 방식은 패킷 전송 반경이 좁아서 도청자 공격이나 위변조 공격에 상대적으로 안전하다. 반면에 장거리 전

송하는 direct 전송 방식은 악의적인 노드가 전송 반경 안에 들어올 확률이 높아서 도청자 공격이나 위변조 공격에 취약하다. 제안하는 ART는 direct 전송 방식과 relay 전송 방식의 지연, 보안, 에너지 성능을 고려하여 패킷의 요구사항에 따라 최적의 전송 방식을 결정한다.

## 2) ART의 전송 방식 결정 방법

Fig. 3은 ART의 전송 알고리즘을 보여주는 흐름도이다. ART는 애플리케이션 상황을 지연 요구사항과 보안 요구사항의 우선순위가 각각 높은 경우와 낮은 경우로 분류한다. 지연에 민감하면서 강한 보안을 요구하는 패킷을 전송할 때는 지연과 보안 요구사항에 따른 우선순위가 각각 높은 경우이며, 지연이 허용되고, 약한 보안을 요구하는 패킷을 전송할 때는 각 요구사항의 우선순위가 모두 낮은 경우이다. latency priority 필드 값과 security priority 필드 값의 XOR 연산한 결과가 1이라면, 두 요구사항의 우선순위가 서로 다른 상황을 말한다. 이때, latency priority 값이 security priority 값보다 크다면, 지연에 민감하고, 약한 보안을 요구하는 패킷을 전송하는 경우이므로, 저지연성을 보장하기 위해 direct 전송하고, security priority 값이 더 크다면, 지연이 허용되고, 강한 보안을 요구하는 패킷을 전송하는 경우이므로 relay 전송한다. 또한, latency priority 값과 security priority 값의 XOR 연산 결과가 0이라면, 두 요구사항의 우선순위가 동일한 상황이며, 지연과 보안 요구사항의 우선순위가 모두 높거나, 모두 낮은 경우를 의미한다. 이 경우에는 처리율을 우선적으로 고려하는 높은 처리율(High Throughput, HT) 모드와 신뢰성을 우선적으로 고려하는 높은 신뢰성(High Reliability, HR) 모드로 동작한다. 즉, 지연과 보안 요구사항의 우선순위가 동일한 경우, HT 모드에서는 처리율을 극대화하기 위해 direct 전송 방식을 사용하며, HR 모드에서는 에너지 효율성, 보안, 처리율을 종합적으로 개선하기 위해 relay 전송 방식을 사용한다.

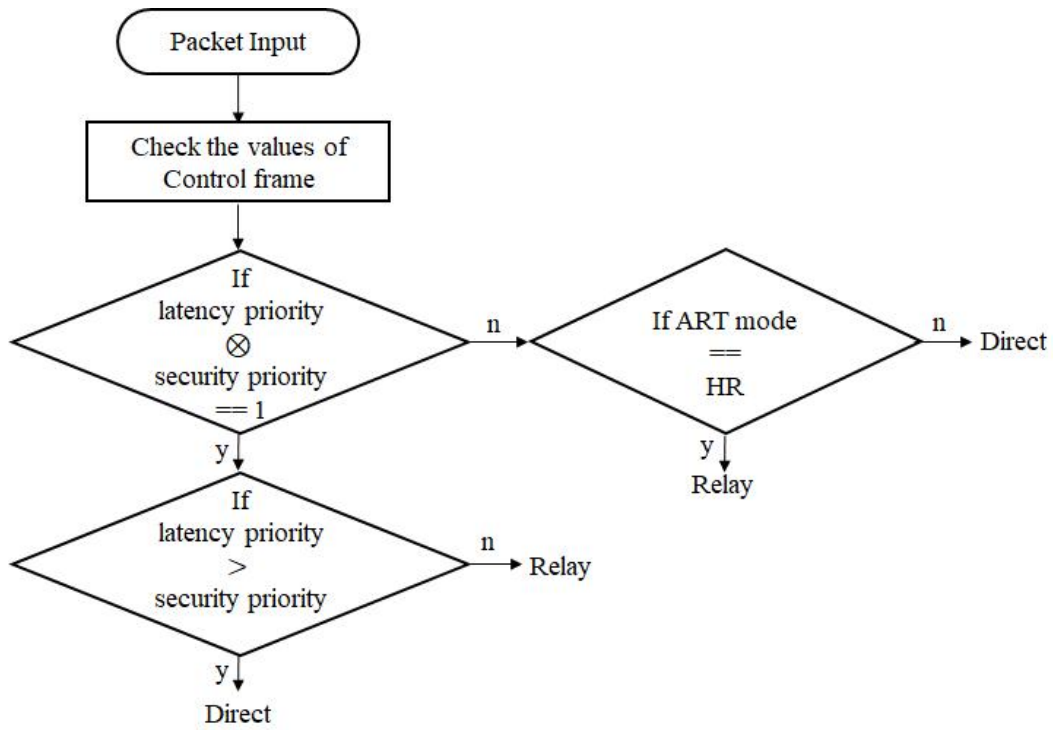


FIGURE 3. Flowchart of transmission algorithm of ART

이러한 동작 원리에 따른 전송 방식을 Table 2에 정리하였다.

Table 2. Transmission table of ART(HT/HR)

Case of application	Requirements of packet	Transmission method	
		ART_HT	ART_HR
1	Delay tolerant and strong security	Relay	
2	Delay sensitive and weak security	Direct	
3	Delay tolerant and weak security	Direct	Relay
4	Delay sensitive and strong security	Direct	Relay

## IV. 평가지표

본 장에서는 제안 모델의 성능 검증에 활용되는 평가지표인 에너지 효율성, 처리율, 보안 성능을 분석한다. 링크 내부에서 전송하는 노드(STA nodes)와 링크 외부에서 전송하는 노드(Other nodes)로 나누어 각 노드의 성능을 계산한 후, 링크 성능과 네트워크 성능을 분석하였다. 각 평가지표 분석 시 사용한 파라미터와 이에 대한 설명은 Table 3과 같다.

**Table 3. The descriptions of notations**

Notation	Description
$(x_n, y_n)$	The location of node
$D(n, n+1)$	The distance between $n_{th}$ and $n+1_{th}$ node ( $m$ )
$H$	The number of transmission hops
$E_{Network}$	Total energy consumption of network ( $J$ )
$E_{STAs}$	Total energy consumption of STA nodes ( $J$ )
$E_{Others}$	Total energy consumption of Other nodes ( $J$ )
$l$	Packet length ( $bit$ )
$E_{elec}$	Energy consumption of the circuit ( $J/bit$ )
$\epsilon_{amp}$	Energy consumption of Tx amplifier ( $J/bit/m^2$ )
$K$	The number of other nodes
$E$	The number of eavesdropping nodes
$r$	The interference range of Other nodes ( $m$ )
$R$	The number of rounds in simulation
$d_r$	The data rate ( $bps$ )
$T$	Total transmission time in simulation ( $sec$ )
$E_r$	Remaining energy level of the node ( $J$ )

## 1. 보안성

제안하는 ART 모델은 패킷의 보안 요구사항을 인지한 후 적응적으로 릴레이 전송을 수행하여 보안성을 개선한다. 제안하는 모델이 종래 모델 대비 도청 확률을 줄여 도청자 공격에 상대적으로 안전함을 보이고, 정보유출량 지표를 활용하여 보안성을 평가한다.

### 1) 도청자 공격에 대한 대응

도청자 공격은 악의적인 공격자가 통신 채널에 침투하여 패킷의 내용을 가로채거나 위변조하는 공격을 말한다. 현존하는 암호화 방식은 완벽하게 안전하다고 볼 수 없으며, 공격자가 패킷 도청 후 무차별 대입 공격(brute force attack)을 복합적으로 활용한다면, 도청한 패킷을 복호화하는 것이 가능하다. 그뿐만 아니라, 최신 네트워크 프레임의 헤더 정보들은 고속 처리와 저지연 서비스를 지원하기 위해 암호화되지 않은 상태로 무선 전송되며, 네트워크 기술이 발전할수록 저전력 고효율 전송을 위해 단말의 고급 정보들이 헤더에 더 많이 포함되고 있다. 따라서, 패킷에 강한 암호화를 적용하는 것도 중요하지만, 패킷이 도청자에게 노출될 확률을 줄이는 것도 매우 중요하다. ART는 패킷 내 입력된 보안 요구사항을 확인하고, 강한 보안을 요구하는 패킷이라면, 릴레이 전송을 수행한다. 적응형 릴레이 전송을 통해 보안이 중요한 패킷은 근거리 전송함으로써 중요 정보의 도청 확률을 줄인다. 단, 여기서 릴레이 노드는 신뢰할 수 있는 노드이며, 릴레이 전송이 끝난 후에는 데이터를 즉시 폐기한다고 가정한다.

### 2) 정보유출량

본 연구에서는 제안하는 방식과 종래방식의 보안성을 정량적으로 비교하기 위해 정보유출량을 계산한다. 정보유출량은 수식 (1)을 통해 도청된 패킷 수와

패킷의 길이를 곱하여 구했으며, 도청된 패킷 수는 하나의 패킷 전송 시, 몇 개의 도청자 노드에 패킷이 도청되었는지를 계산하였다. Algorithm 1은 도청된 패킷 수를 구하는 과정을 나타낸 의사코드(pseudo-code)이다. 송신 노드의 전송 반경 안에 도청자 노드가 포함되는지 여부에 따라 도청 여부를 결정한다. 즉, 도청자 노드와 송신 노드 간의 거리가 전송 반경보다 작을 때 도청자 노드가 전송 반경 안에 있는 것으로 간주한다. 또한, 송신 노드가 패킷을 전송해야 패킷의 도청이 가능하므로, 송신 노드의 에너지 잔량이 0보다 크고, 도청자 노드가 전송 반경 안에 들어올 경우, 도청되었다고 판단한다. 패킷이 도청되는 상황은 STA nodes가 패킷을 전송할 때 도청을 당하는 경우와 Other nodes가 패킷 전송할 때 도청을 당하는 경우로 나뉜다. STA 노드의 패킷 전송 시 도청된 패킷 수와 Other nodes의 패킷 전송 시 도청된 패킷 수를 합하여 전체 네트워크 내에서 도청된 패킷 수를 계산한다.

$$Information\ leakage(bit) = Total\ number\ of\ eavesdropped\ packets \times l \quad (1)$$

---

**Algorithm 1** Pseudo-code of calculating the number of eavesdropped packets

---

**Input:**  $H, E, K, E_r, r$

**Output:** eavesdropped\_network

---

```

for i = 1 to H do           ▷ Packet transmission of STA nodes
  for j = 1 to E do       ▷ Eavesdropping attack of eavesdropping nodes
    if  $E_r(n_i) > 0$  and  $D(n_i, n_j) < D(n_i, n_{i+1})$  then
      eavesdropped_link += 1;
    end if
  end for
end for

for i = 1 to K do         ▷ Packet transmission of other nodes
  for j = 1 to E do       ▷ Eavesdropping attack of eavesdropping nodes
    if  $E_r(n_i) > 0$  and  $D(n_i, n_j) < r$  then
      eavesdropped_others += 1;
    end if
  end for
end for

```

eavesdropped\_network = eavesdropped\_link + eavesdropped\_others;

**return** eavesdropped\_network

---

## 2. 에너지 효율

전체 네트워크의 에너지 소모량 ( $E_{Network}$ )은 STA nodes의 에너지 소모량 ( $E_{STAs}$ ) 과 Other nodes의 에너지 소모량 ( $E_{Others}$ )을 합하여 계산하며, 이는 수식 (3)에서 정의한다. 수식 (2)는  $(x_n, y_n)$ 와  $(x_{n+1}, y_{n+1})$  위치에 있는 두 노드 간의 거리를 계산하는 수식이며, STA nodes의 에너지 소모량을 계산하기 위해 사용된다. Fig. 1의 에너지 모델을 참고하여 수식 (4)의  $E_{STAs}$ 을 구하였으며, 하나의 패킷 전송 시 송신 에너지와 수신 에너지를 합하여 계산한다. 송신 에너지는 송신 시 회로에서 소모하는 에너지와 증폭기에서 소모하는 에너지를 포함하며, 수신 에너지는 수신 시 회로에서 소모하는 에너지로 구할 수 있다. 이때, 송신 증폭기에서 소모하는 에너지는 STA nodes 간의 전송 반경의 제곱에 비례하여 증가하기 때문에, 전송 반경이 송신 에너지 소모에 미치는 영향은 매우 크다. 따라서, 장거리 전송하는 direct 전송 방식이 근거리 전송하는 relay 전송 방식보다 큰 에너지를 소모하게 된다. 또한, direct 전송할 때 단일 홉 전송하므로, 한 번의 송신 에너지와 수신 에너지를 소모하며, relay 전송 시에는 송신 에너지와 수신 에너지가 홉의 개수  $H$ 번 만큼 소모된다. 수식 (5)는 Other nodes의 에너지 소모량 ( $E_{Others}$ )을 구하는 수식으로, 송신 에너지만을 고려하기 때문에 송신 증폭기와 송신 회로의 에너지 소모량을 계산한다. 이때, 송신 증폭기의 에너지 소모량은 Other nodes의 전송 반경 ( $r$ )의 제곱에 비례하여 증가한다.

$$D(n, n+1) (m) = \sqrt{(x_{n+1} - x_n)^2 + (y_{n+1} - y_n)^2} \quad (2)$$

$$E_{Network} (J) = E_{STAs} + E_{Others} \quad (3)$$

$$E_{STAs} (J) = \begin{cases} l \times (2 \times E_{elec} + \epsilon_{amp} \times D^2) & \text{if Direct} \\ l \times (2 \times H \times E_{elec} + \epsilon_{amp} \times \sum_{n=1}^H D^2) & \text{if Relay} \end{cases} \quad (4)$$

$$E_{Others}(J) = \sum_{n=1}^K l \times (E_{elec} + \epsilon_{amp} \times r^2) \quad (5)$$

수식 (6)과 (7)은 각각 비신뢰 네트워크 에너지 효율과 신뢰 네트워크 에너지 효율을 나타낸다. (6)과 (7)의 에너지 효율 모두 네트워크 내에서 성공적으로 수신한 패킷의 양을 에너지 소모량으로 나누어 계산하지만, 패킷의 수신 성공 여부를 판단하는 기준이 다르다. 수식 (6)에서는 송신 노드의 에너지 잔량이 매우 작거나 수신 노드가 간섭을 받았을 때 패킷 수신이 실패했다고 판단하며, (7)에서는 패킷이 도청자 노드로부터 도청을 받았을 때에도 패킷 수신이 실패했다고 판단하여 패킷의 도청 여부를 추가로 검사한다. 즉, 비신뢰 네트워크 에너지 효율은 전송 중간에 도청이 되어도 목적지까지 패킷을 전송하면 패킷을 성공적으로 수신한 경우라고 판단하기 때문에 신뢰성을 평가하기 어렵다. 반면, 신뢰 네트워크 에너지 효율은 패킷 수신 성공 여부를 결정할 때, 처리율, 에너지 효율, 정보유출량을 모두 고려하므로, 네트워크의 신뢰성을 평가하는 지표로 볼 수 있다.

$$\begin{aligned} & \text{Unreliable network energy efficiency (bpJ)} \\ & = \frac{\text{The number of packets successfully received in unreliable network} \times l}{E_{Network} \times R} \quad (6) \end{aligned}$$

$$\begin{aligned} & \text{Reliable network energy efficiency (bpJ)} \\ & = \frac{\text{The number of packets successfully received in reliable network} \times l}{E_{Network} \times R} \quad (7) \end{aligned}$$

Algorithm 2는 수식 (7)의 신뢰 네트워크에서 성공적으로 패킷을 수신한 횟수를 구하는 pseudo code이다. 네트워크 내에서 모든 패킷의 수신 성공 횟수를 계산하므로, STA nodes와 Other nodes의 패킷 수신 성공 횟수를 합하여 계산하였다. STA nodes의 패킷 전송 시에는 Other nodes의 간섭을 받으며, 패킷을 수신하는 STA nodes가 Other nodes의 간섭 반경 내에 포함될 경

우 간섭으로 인해 패킷 수신 에러가 발생한다. 따라서, 패킷을 송신하는 STA nodes와 Other nodes 간의 거리가 Other nodes의 간섭 반경과 STA nodes의 전송 반경을 합한 것보다 클 때, 간섭을 받지 않는다. 또한, Other nodes의 패킷 전송 시에는 STA nodes의 간섭을 받으며, 외부의 Other nodes가 STA nodes의 간섭 반경 내에 포함될 경우, 간섭으로 인한 패킷 수신 에러가 발생한다. 따라서, Other nodes와 간섭을 주는 STA nodes 간의 거리가 Other nodes의 전송 반경과 STA nodes의 간섭 반경을 합한 것보다 클 때, 간섭을 받지 않는다. 또한, 도착되었는지 여부를 판단할 때, Algorithm 1과 동일하게 패킷 전송 반경 내에 도착자 노드가 포함될 때 도착되었다고 판단한다. 즉, 송신 노드와 도착자 노드 간의 거리가 전송 반경보다 작을 때 도착되었다고 판단하며 안전한 패킷 전송에 실패한다. 따라서, 패킷 송신 노드의 에너지 잔량이 0이 아니고, 패킷을 수신하는 노드가 간섭을 받지 않으며, 전송 중에 도착을 받지 않는다면 패킷을 성공적으로 안전하게 전송하였다고 간주한다.

---

**Algorithm 2** Pseudo-code of calculating the number of successfully received packets in reliable communication

---

**Input:**  $R, H, K, E_r, r$   
**Output:** received link, received\_network

---

```

for  $i = 1$  to  $H$  do           ▷ Packet transmission of STA nodes
  for  $j = 1$  to  $K$  do           ▷ Interference of other nodes
    for  $k = 1$  to  $E$  do         ▷ Eavesdropping attack of eavesdropping nodes
      if  $E_r(n_i) > 0$  and  $D(n_i, n_j) > r + D(n_i, n_{i+1})$  and  $D(n_i, n_k) > D(n_i, n_{i+1})$  then
        packet received = 1;
      else
        packet received = 0;
        Stop transmitting if interfered with one of other nodes
      end if
    end for
  end for
  received_link += packet received;
end for

for  $i = 1$  to  $K$  do           ▷ Packet transmission of other nodes
  for  $j = 1$  to  $H$  do           ▷ Interference of STA nodes

```

---

---

```

for k = 1 to  $E$  do    ▷ Eavesdropping attack of eavesdropping nodes
  if  $E_r(n_i) > 0$  and  $D(n_i, n_j) > r + D(n_i, n_{i+1})$  and  $D(n_i, n_k) > r$  then
    packet received = 1;
  else
    packet received = 0;
    Stop transmitting if interfered with STA nodes
  end if
end for
end for
  received_others += packet received;
end for

received_network = received_link + received_others;
return received_link, received_network

```

---

### 3. 처리율

패킷의 전송 효율을 확인하기 위해 처리율 지표를 활용하였다. 처리율은 총 전송 시간 동안 전송에 성공한 패킷의 양으로 정의하였고, 링크 처리율과 네트워크 처리율을 각각 계산하여 평가했다. 총 전송 시간 ( $T$ )은 라운드마다 전송 지연(transmission delay)을 구한 후 합산하였으며, (8)은 총 전송 시간을 구하는 수식을 나타낸다. 수식 (9)의 링크 처리율은 전송 링크 내부의 STA nodes가 성공적으로 전송한 패킷 수를 총 전송 시간으로 나누어 계산하였고, 수식 (10)의 네트워크 처리율은 STA nodes와 Other nodes가 성공적으로 전송한 패킷 수를 총 전송 시간으로 나누어 계산하였다.

$$T(sec) = \sum_{n=1}^R H \times \frac{l}{d_r} \quad (8)$$

$$Link\ throughput\ (bps) = \frac{\text{The number of successfully received packets in link} \times l}{T} \quad (9)$$

$$Network\ throughput\ (bps) = \frac{\text{The number of successfully received packets in network} \times l}{T} \quad (10)$$

## V. 평가 및 분석

ART 모델을 평가하기 위해 MATLAB 기반 시뮬레이터를 구현하여 802.11n 표준 무선랜 환경을 모델링했다.

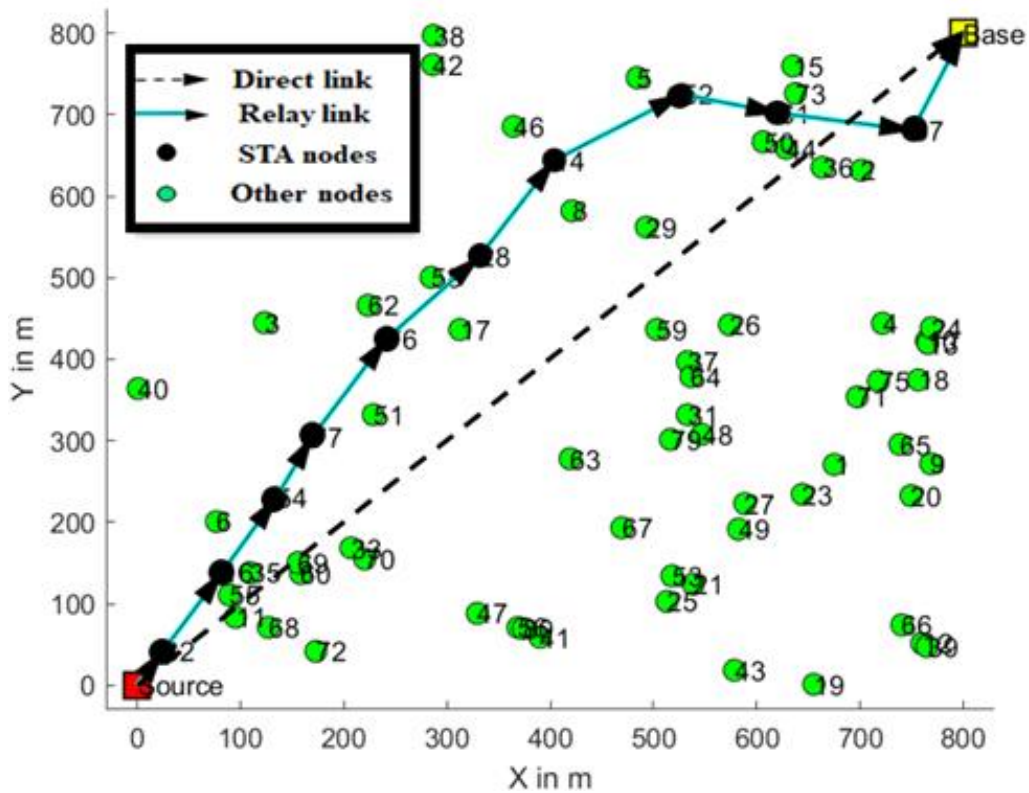


FIGURE 4. Network structure of simulation

### 1. 네트워크 모델

Fig. 4는 본 연구에서 수행한 시뮬레이션의 네트워크 구조를 나타낸다. 반경이 800m인 네트워크에서 80개의 non-AP STA와 1개의 AP STA가 존재하는 구조이다. 이때, non-AP STA는 source STA 혹은 relay STA로 동작하며, AP STA는 기지국 액세스 포인트(base station Access Point, base AP)로

동작한다. 시뮬레이션 라운드마다 source STA에서 base AP로 direct 전송 링크와 relay 전송 링크 중 하나의 링크를 사용하여 패킷을 전송한다. 검은색 점선 화살표와 하늘색 실선 화살표는 각각 direct 전송 링크와 relay 전송 링크를 나타내며, 검은색 원과 초록색 원은 각각 STA nodes와 Other nodes를 나타낸다. STA nodes는 source STA와 relay STA를 포함한 링크 내부의 STA 노드들을 나타내며, Other nodes는 링크 외부의 STA 노드들을 나타낸다. direct 전송 시에는 source STA에서 base AP로 단일 홉 전송하며, relay 전송 시에는 source STA에서 base AP까지 relay STA를 사용하여 다중 홉 전송한다. 시뮬레이션에서 base AP의 위치는 고정되며, base AP를 제외한 STA nodes와 Other nodes의 위치는 라운드마다 동적으로 변한다. 따라서, relay 전송 경로는 라운드마다 새롭게 결정되며, 다익스트라 알고리즘(dijkstra algorithm)을 사용하여 결정된다. dijkstra algorithm은 송신 노드와 수신 노드 사이의 거리가 최단 거리가 되도록 경로를 결정하는 알고리즘으로, 패킷 전송 거리를 최소화함으로써 에너지 효율적으로 패킷을 전송할 수 있다 [21].

## 2. 네트워크 상황에 따른 성능 비교

본 장에서는 지연 허용 네트워크, 보안 위협이 큰 네트워크, 노드 밀집도가 큰 네트워크, 간섭이 큰 네트워크 환경 조건에서 시뮬레이션을 수행하고, 비신뢰 네트워크 에너지 효율, 신뢰 네트워크 에너지 효율, 링크 처리율, 네트워크 처리율, 정보유출량, 네트워크 수명을 측정하였다. 시뮬레이션이 시작되면 라운드마다 링크 내에서 패킷이 생성되며, 패킷은 지연이 허용되면서 약한 보안을 요구하는 패킷, 지연이 허용되면서 강한 보안을 요구하는 패킷, 지연에 민감하면서 약한 보안을 요구하는 패킷, 지연에 민감하면서 강한 보안을 요구하는 패킷, 총 4가지 유형의 패킷으로 구성된다. 제안하는 ART\_HT 모델과 ART\_HR 모델, 그리고 패킷의 요구사항을 고려하지 않고 항상 relay 전송하는 relay 모델과 항상 direct 전송하는 direct 모델과의 성능 비교를 수행하였다.

### 1) 지연 허용 네트워크 환경에서의 성능 비교

본 장에서는 링크 내 지연이 허용되는 패킷 발생 비율이 증가함에 따른 direct, relay, ART\_HT, ART\_HR 모델의 성능을 측정하였다. 이때, 활성화된 Other nodes의 수는 20, Other nodes의 간섭 반경은 20m로 고정하여 시뮬레이션을 수행하였다. 지연이 허용되는 패킷의 발생 비율이 높은 경우는 DTN 상황을 나타내며, 지연이 허용되는 패킷의 발생 비율이 낮을 경우는 지연에 민감한 네트워크(Delay Sensitive Network, DSN)를 나타낸다. 제안하는 모델의 패킷 요구사항은 보안과 지연 두 가지 요소를 고려하기 때문에 지연이 허용되는 패킷은 지연이 허용되면서 강한 보안을 요구하는 패킷과 지연이 허용되면서 약한 보안을 요구하는 패킷으로 구성된다. direct 모델과 relay 모델은 패킷의 요구사항을 고려하지 않는 모델이기 때문에 패킷의 요구사항 수준이

변화하여도 일정한 결과를 보인다. 반면에 패킷의 요구사항을 고려하는 ART\_HT 모델과 ART\_HR 모델은 패킷의 지연 요구사항이 변화함에 따라 요구사항에 맞춰 동작 모드를 결정함으로써 성능과 보안을 최적화한다.

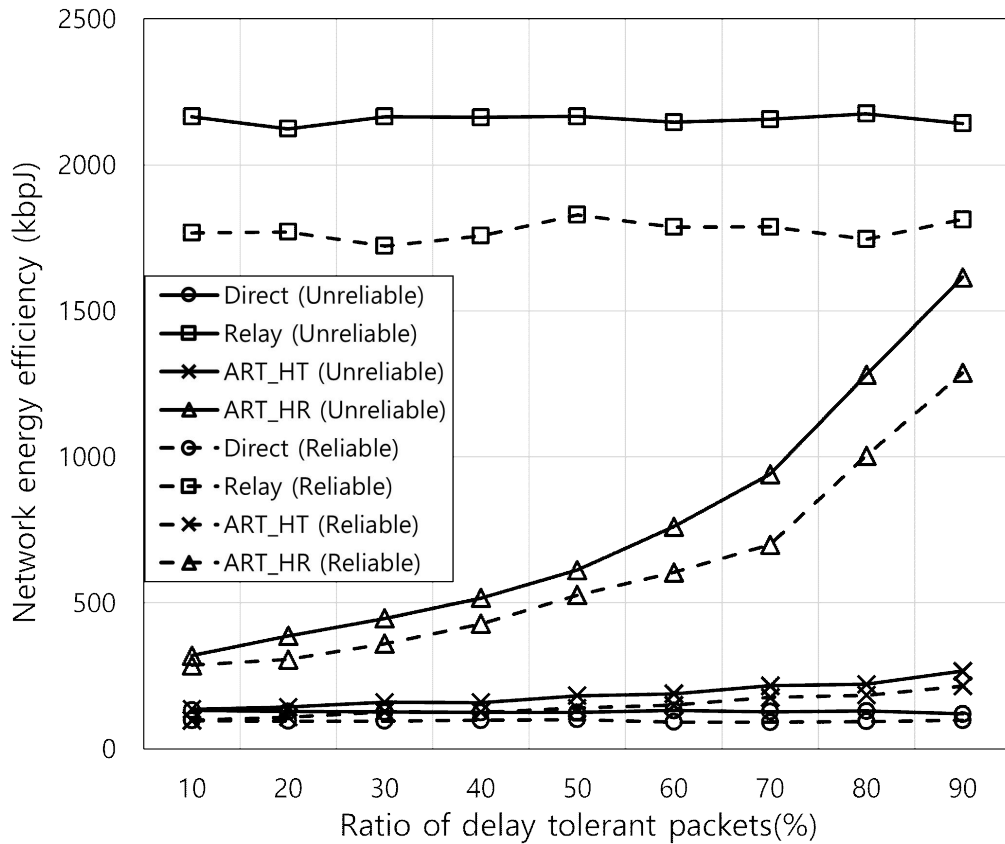


FIGURE 5. Network energy efficiency vs. ratio of delay tolerant packets

Fig. 5는 링크 내 지연이 허용되는 패킷의 발생 비율이 증가함에 따른 네트워크 에너지 효율을 나타내며, 신뢰 통신 환경을 고려하는 신뢰 네트워크 에너지 효율과 신뢰 통신 환경을 고려하지 않는 비신뢰 네트워크 에너지 효율을 측정하였다. 신뢰 네트워크 에너지 효율은 패킷의 도착으로 인한 전송 실

패 횟수까지 고려하므로 비신뢰 네트워크 에너지 효율보다 낮은 에너지 효율을 보인다. direct, relay, ART\_HT, ART\_HR 모델의 신뢰 네트워크 에너지 효율은 비신뢰 네트워크 에너지 효율보다 각각 24.6%, 17.6%, 20.7%, 20% 더 낮은 효율을 보였다. 신뢰 네트워크 에너지를 비신뢰 네트워크 에너지 효율과 비교했을 때, direct 모델이 가장 큰 성능 저하를 보였으며, relay 모델이 가장 성능 저하가 작았다. 신뢰 통신 환경을 고려할 때와 고려하지 않을 때 모두 에너지 효율은 항상 근거리 전송하는 relay 모델이 가장 높았으며, 항상 장거리 전송하는 direct 모델이 가장 낮았다. 또한, ART\_HR 모델의 신뢰 네트워크 에너지 효율은 DTN 환경에서 ART\_HT, direct 모델보다 5.9배, 13.1배 개선되었다. 이는 ART\_HR 모델이 ART\_HT 모델, direct 모델보다 relay 전송 횟수가 많기 때문이며, relay 전송을 통해 에너지 효율성을 개선함을 입증하였다.

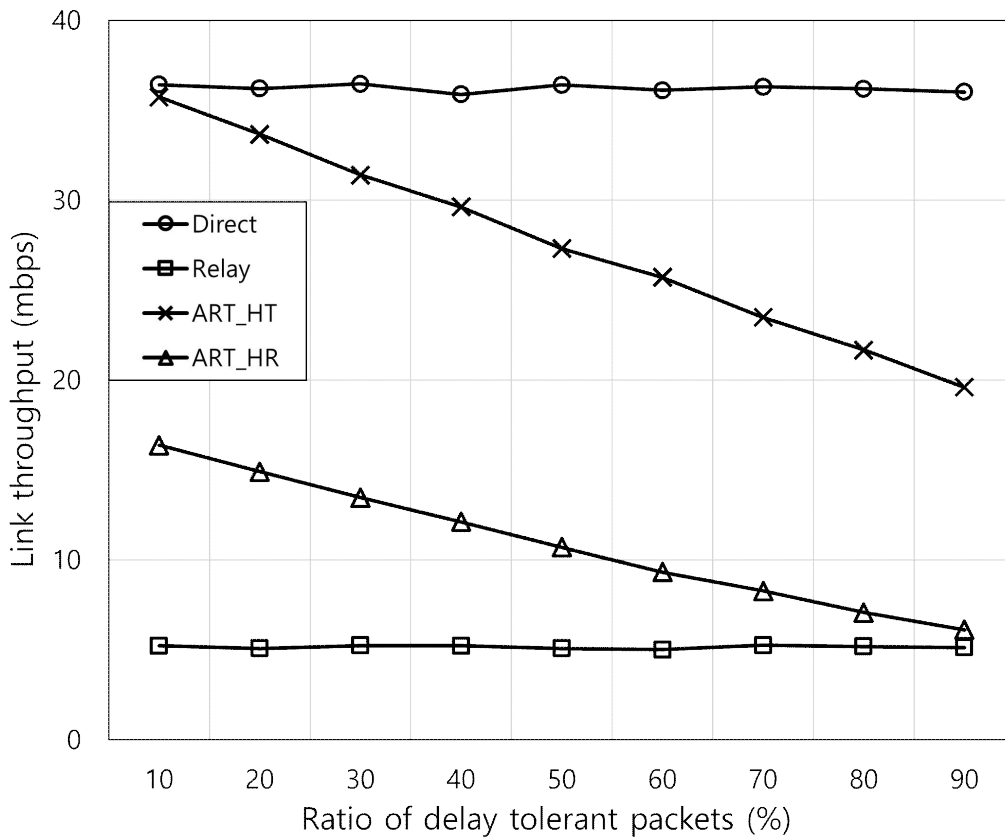


FIGURE 6. Link throughput vs. ratio of delay tolerant packets

Fig. 6은 지연이 허용되는 패킷의 발생 비율이 변화함에 따른 링크 처리율을 나타낸다. 링크 처리율은 전송 링크 내 STA nodes의 데이터 처리율을 합하여 계산했다. 실험 결과에 따르면 direct, ART\_HT, ART\_HR, relay 모델 순으로 링크 처리율이 높았다. relay 전송 횟수가 많아질수록 비교적 많은 홉을 거쳐 패킷을 전송하기 때문에 링크 처리율은 relay 모델이 가장 낮은 성능을 보였다. 또한, ART\_HT, ART\_HR 모델은 지연이 허용되는 패킷의 발생 비율이 증가할수록 relay 전송 횟수가 증가하기 때문에 링크 처리율은 낮아지며, 처리율을 우선적으로 고려하는 ART\_HT 모델은 direct 전송 횟수가 상대적으로 많아서 ART\_HR 모델보다 개선된 링크 처리율을 보였다.

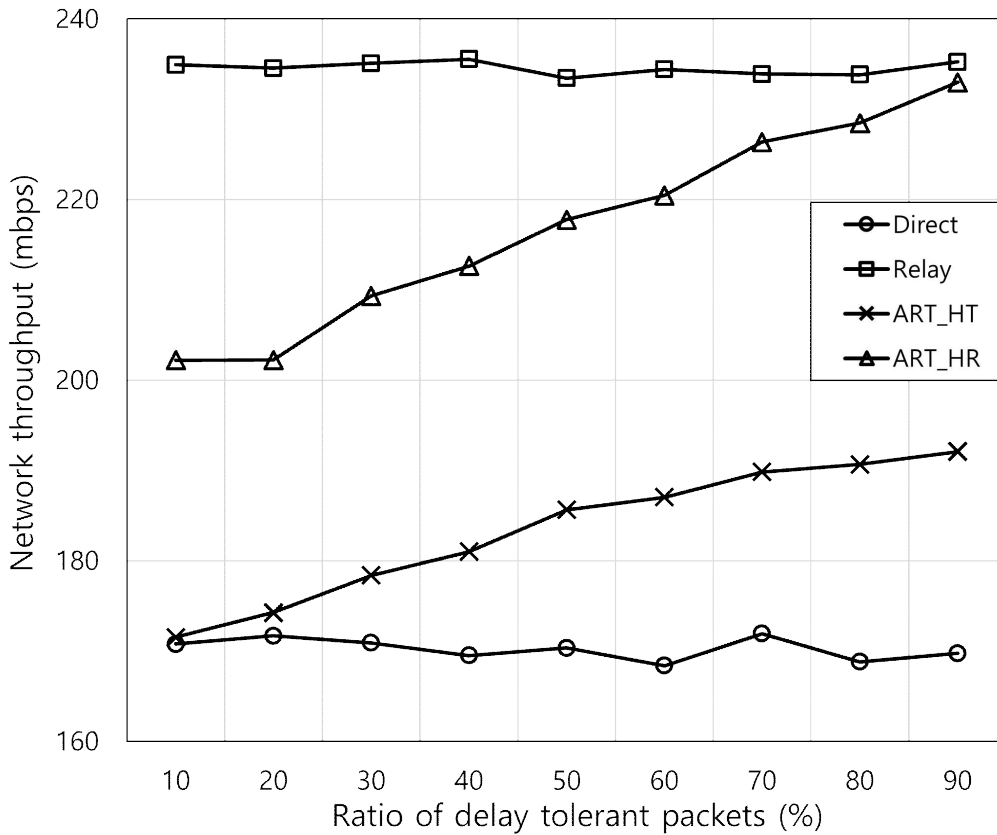


FIGURE 7. Network throughput vs. ratio of delay tolerant packets

Fig. 7은 지연이 허용되는 패킷의 발생 비율이 변화함에 따른 네트워크 처리율을 나타낸다. 네트워크 처리율의 경우, direct 모델은 전송 반경이 길어서 외부 노드에 미치는 간섭의 영향이 크므로, 가장 낮은 네트워크 처리율을 보였다. 또한, relay 모델은 전송 반경이 짧으므로, 외부 노드에 미치는 간섭의 영향이 작아서 가장 높은 네트워크 처리율을 보였다. ART\_HT, ART\_HR 모델은 지연이 허용되는 패킷이 증가할수록 relay 전송 횟수가 증가해서 네트워크 처리율이 개선되며, ART\_HR 모델이 ART\_HT 모델보다 높은 네트워크 처리율을 보였다. 또한, DTN 환경에서 ART\_HT 모델은 링크 처리율을 크게 향상시켰고, ART\_HR 모델은 네트워크 처리율을 크게 향상시켰다.

2) 보안 위협이 큰 네트워크 환경에서의 성능 비교

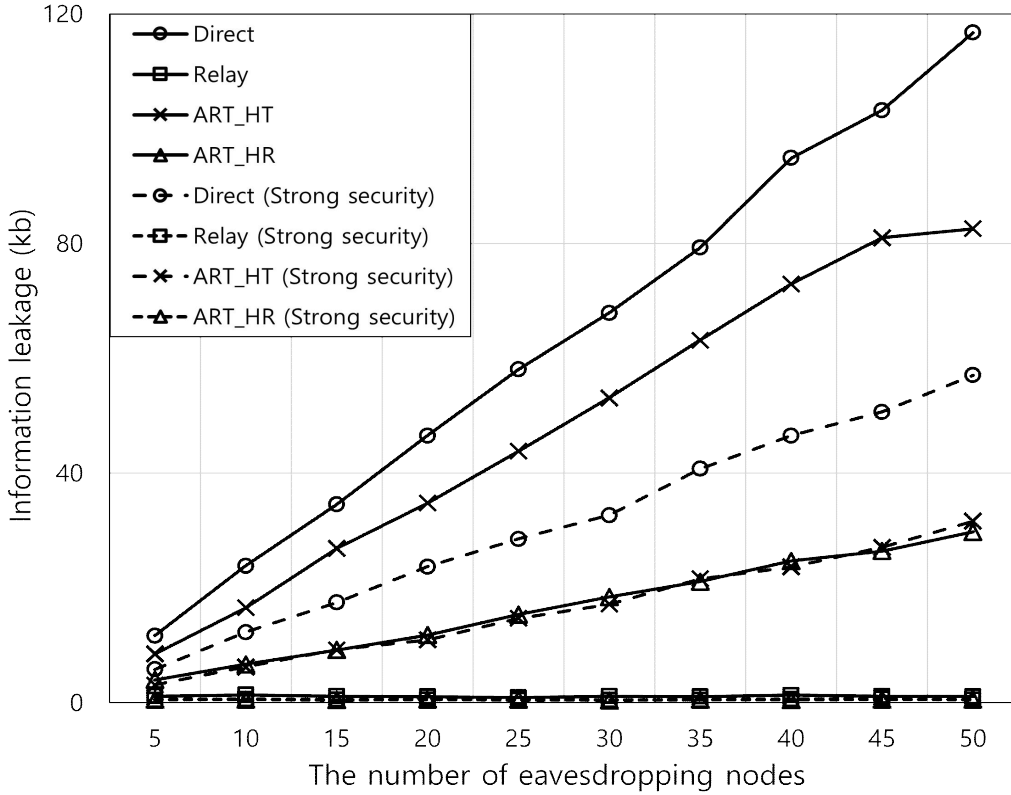


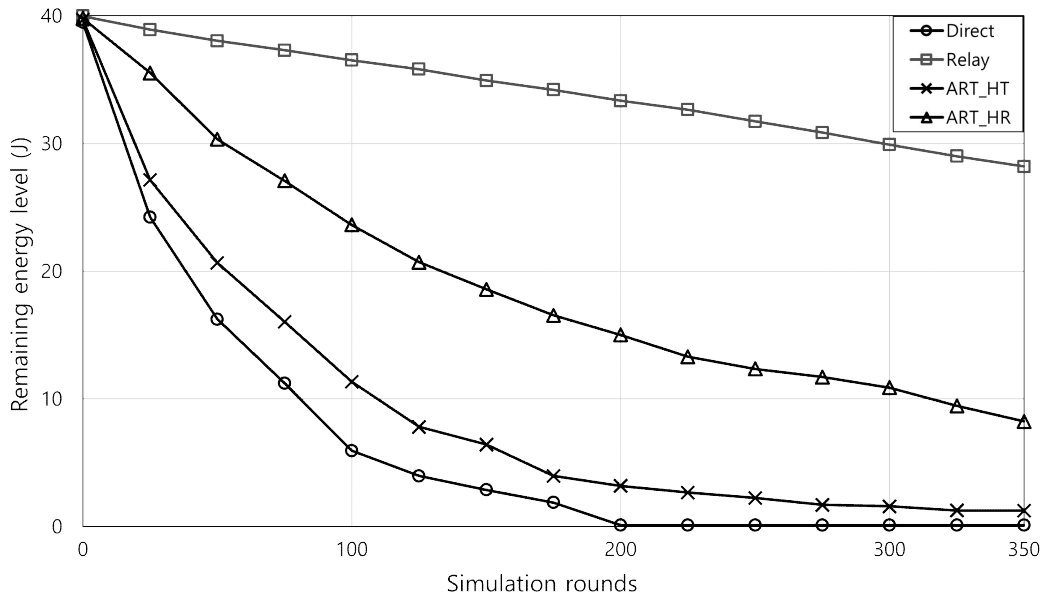
FIGURE 8. Information leakage vs. the number of eavesdropping nodes in network

Fig. 8은 네트워크 내 도청자 노드의 수가 증가함에 따른 모든 패킷의 정보유출량과 강한 보안을 요구하는 패킷의 정보유출량을 나타낸 그래프이다. 강한 보안을 요구하는 패킷의 정보유출량은 점선 그래프로 표현하였다. 도청자 노드의 수가 증가할수록 패킷의 도청 확률은 높아지며, 이에 따라 정보유출량은 증가한다. direct 모델은 STA nodes가 패킷을 장거리 전송함에 따라 도청자 노드가 STA nodes의 전송 반경 내에 위치할 확률이 높다. 따라서, direct 모델의 정보유출량이 가장 많았다. 반면에, relay 모델은 STA nodes가

패킷을 근거리 전송함에 따라 도착 확률을 줄일 수 있어서 상대적으로 정보유출량이 적었다. ART\_HR 모델은 보안 요구사항을 고려하여 강한 보안을 요구하는 패킷은 relay 전송한다. 따라서, 보안 위협이 큰 네트워크에서 ART\_HT, direct 모델보다 정보유출량이 적었다. ART\_HT 모델의 경우, 보안을 고려하지 않고, 처리율을 우선적으로 고려하기 때문에 relay 모델과 ART\_HR 모델보다 정보유출량이 많았다.

약한 보안과 강한 보안을 요구하는 모든 패킷의 정보유출량은 relay 모델이 ART\_HR 모델보다 14.4배 작은 정보유출량을 보였다. 그러나 강한 보안을 요구하는 패킷의 정보유출량은 ART\_HR 모델이 relay 모델과 동일한 정보유출량을 보였다. 이는 ART\_HR 모델이 강한 보안을 요구하는 패킷을 모두 relay 전송하기 때문이며, 보안 위협이 큰 네트워크 환경에서도 고신뢰 보안을 유지한다.

### 3) 시뮬레이션 라운드 수에 따른 네트워크의 배터리 수명 비교



**FIGURE 9. Remaining energy level vs. simulation rounds**

Fig. 9는 시뮬레이션 라운드 수에 따른 네트워크의 에너지 잔량 변화를 나타낸다. 총 350번의 라운드 동안 시뮬레이션을 수행하였으며, 활성화된 Other nodes의 수와 간섭 반경은 각각 20, 20m로 설정하였다. 또한, 링크 내에서 발생하는 지연에 민감한 패킷과 지연이 허용되는 패킷의 발생 비율은 1:1로 고정하여 성능평가를 수행하였다. 에너지 잔량이 0이 되는 순간, 네트워크 내에서 모든 노드의 에너지가 고갈되어 더 이상 패킷을 송수신할 수 없으므로, 이 순간의 라운드 수는 네트워크의 수명을 나타낸다. 네트워크 수명은 relay, ART\_HR, ART\_HT, direct 순으로 길었다. direct 모델의 에너지 잔량이 가장 큰 폭으로 감소하여 약 200번째 라운드에서 에너지가 모두 고갈되었으며, 해당 지점에서의 relay, ART\_HR, ART\_HT 모델은 각각 전체 에너지의 16.5%, 62.4%, 92%의 에너지 사용량을 보였다.

#### 4) 노드 밀집도가 큰 네트워크 환경에서의 성능 비교

본 장에서는 네트워크 내에서 전송을 수행하는 Other nodes의 수를 변화함에 따른 direct, relay, ART\_HT, ART\_HR 모델의 성능을 측정하였다. Other nodes의 간섭 반경은 20m, 링크에서 발생하는 지연에 민감한 패킷과 지연이 허용되는 패킷의 발생 비율은 1:1로 고정한 조건에서 성능을 평가하였다.

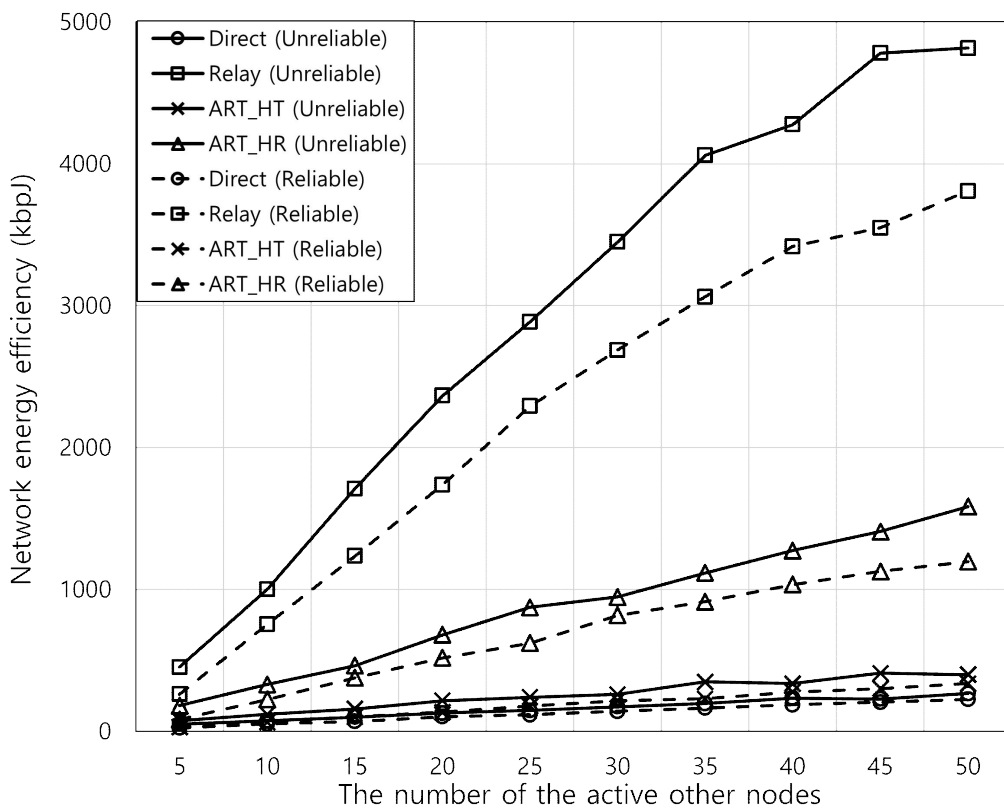


FIGURE 10. Network energy efficiency vs. the number of the active other nodes

Fig. 10은 활성화된 Other nodes의 수가 증가함에 따른 네트워크 에너지 효율을 측정하였으며, 점선 그래프는 신뢰 네트워크 에너지 효율을 나타내고,

실선 그래프는 비신뢰 네트워크 에너지 효율을 나타낸다. 활성화된 Other nodes의 수가 증가할수록 네트워크 내에서 트래픽 발생률은 증가한다. 네트워크 에너지 효율의 경우, 네트워크 내 모든 활성화 노드의 에너지 효율을 고려하기 때문에 활성화된 Other nodes의 수가 증가할수록 에너지 효율은 전반적으로 증가했다. 근거리 전송을 수행하는 relay 모델은 링크 내 STA nodes가 Other nodes에 미치는 간섭의 영향이 상대적으로 적으므로 가장 높은 에너지 효율을 보였다. 반면, direct 모델은 STA nodes가 Other nodes에 미치는 간섭의 영향이 크고, 패킷을 장거리 전송하기 때문에 가장 낮은 에너지 효율을 보였다. 또한, direct, relay, ART\_HT, ART\_HR 모델의 비신뢰 네트워크 에너지 효율을 계산할 때는 도청 여부를 고려하지 않았기 때문에 신뢰 네트워크 에너지 효율보다 높은 에너지 효율이 측정되었다.

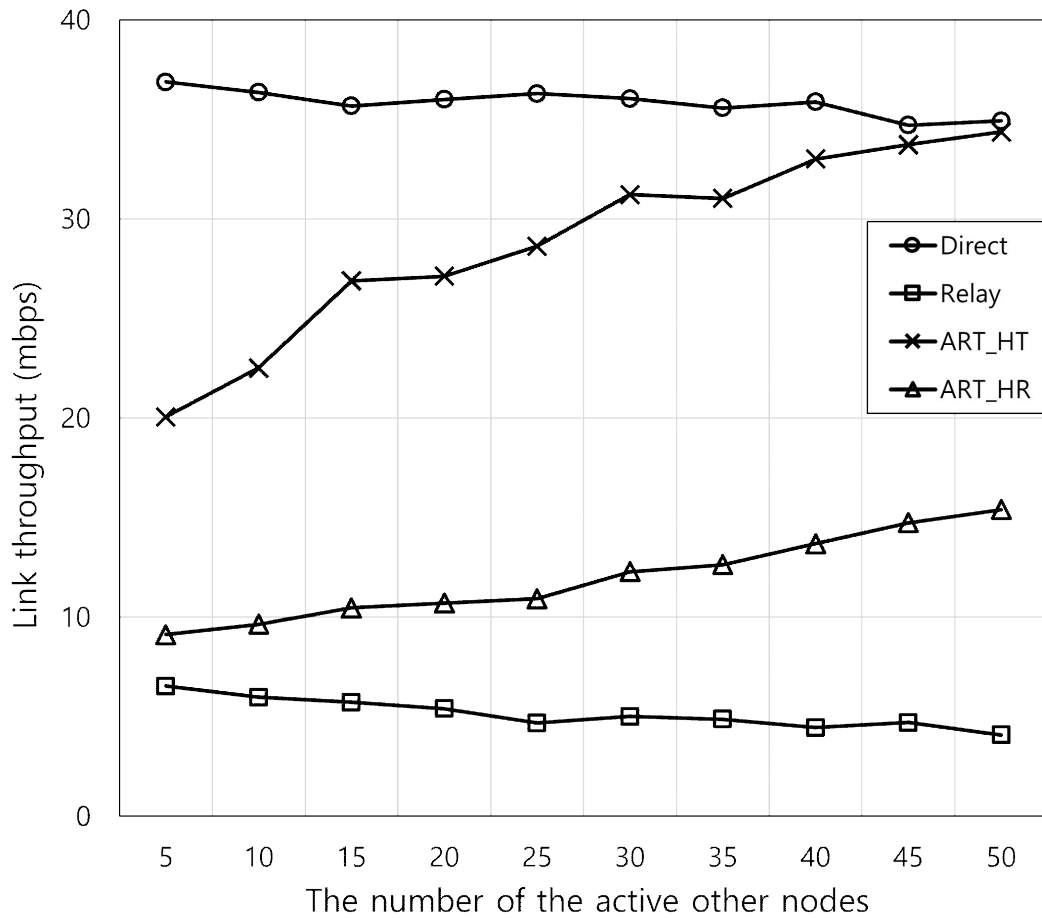


FIGURE 11. Link throughput vs. the number of the active other nodes

Fig. 11은 활성화된 Other nodes의 수가 증가함에 따른 링크 처리율을 측정 한 그래프이다. 큰 파워를 사용하여 단일 홉 전송하는 direct 모델이 가장 높은 링크 처리율을 보였고, 작은 파워를 사용하여 다중 홉 전송하는 relay 모델이 가장 낮은 링크 처리율을 보였다. 통신 링크에 간섭원이 되는 Other nodes의 수가 증가할수록 STA nodes의 수신 에러율은 증가하고, 전송 지연은 감소한다. ART\_HT, ART\_HR 모델의 경우, 수신 에러율 대비 전송 지연 감소율이 크기 때문에 링크 처리율은 점차 증가했다. 또한, 처리율을 우선적으로

로 고려하는 ART\_HT 모델이 ART\_HR 모델보다 direct 전송 횟수가 많아서 링크 처리율이 더 높았다.

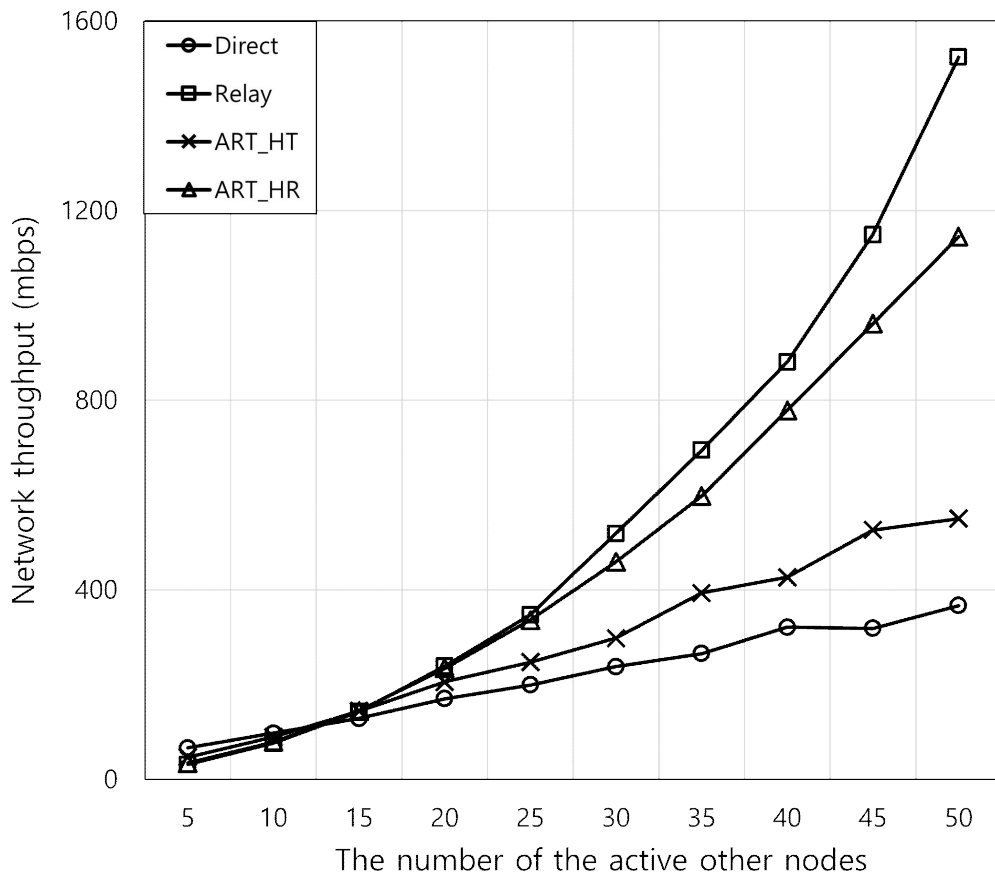


FIGURE 12. Network throughput vs. the number of the active other nodes

Fig. 12는 활성화된 Other nodes의 수가 증가함에 따른 네트워크 처리율을 측정된 결과이다. Other nodes의 수가 증가할수록 네트워크 내에서 발생하는 트래픽의 수도 증가하므로, 네 가지 모델 모두 네트워크 처리율이 증가한다. 또한, 활성화된 Other nodes의 수가 증가할수록 Other nodes의 처리율이 전체

네트워크 처리율에 미치는 영향이 커진다. 따라서, Other nodes에 큰 간섭을 주는 direct 모델이 가장 낮은 네트워크 처리율을 보였다. 반면 relay 모델은 STA nodes가 Other nodes에 미치는 간섭의 영향이 상대적으로 적어서 가장 높은 네트워크 처리율을 보였다. 또한, 신뢰성을 향상시키기 위해 보안, 에너지 효율, 처리율을 종합적으로 고려하는 ART\_HR 모델은 relay 전송 횟수가 상대적으로 많으므로, ART\_HT 모델과 direct 모델보다 평균적으로 108.2%, 212.4% 개선된 네트워크 처리율을 보였다. 활성화된 Other nodes의 수가 많을수록 네트워크 내 노드 밀집도는 증가한다. 노드 밀집도가 큰 네트워크 환경에서 ART\_HT 모델을 적용하여 링크 처리율을 크게 개선할 수 있었고, ART\_HR 모델을 적용하여 네트워크 처리율을 크게 개선할 수 있었다.

5) 간섭이 큰 네트워크 환경에서의 성능 비교

본 장에서는 Other nodes의 간섭 반경이 변화함에 따른 direct, relay, ART\_HT, ART\_HR 모델의 비신뢰 네트워크 에너지 효율, 신뢰 네트워크 에너지 효율, 링크 처리율, 네트워크 처리율을 측정하였다. 활성화된 Other nodes의 수는 20, 링크 내 발생하는 지연에 민감한 패킷과 지연이 허용되는 패킷은 1:1로 고정하였다.

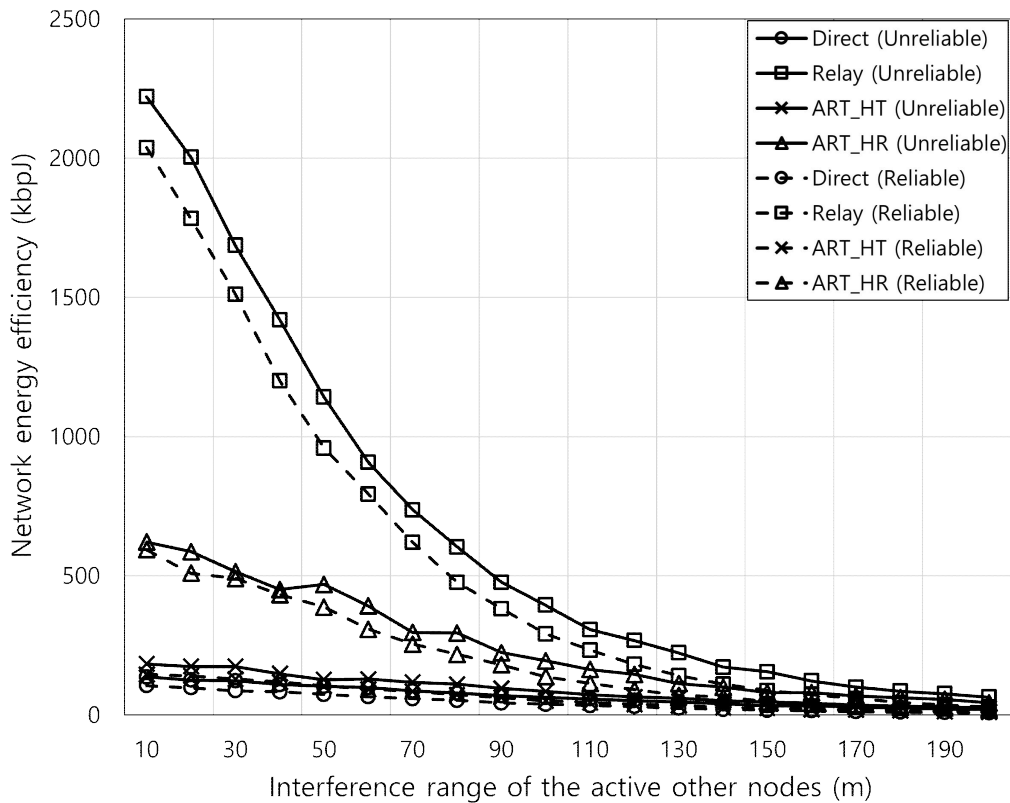


FIGURE 13. Network energy efficiency vs. interference range of the active other nodes

Fig. 13은 Other nodes의 간섭 반경에 따른 비신뢰 네트워크 에너지 효율

과 신뢰 네트워크 에너지 효율을 측정 한 결과이다. Other nodes의 간섭 반경이 증가하면 간섭 파워도 증가하므로, Other nodes의 에너지 소모량이 증가한다. 또한, Other nodes의 간섭 반경이 증가하면, STA nodes의 전송 반경과 접칠 확률이 증가하므로, 네트워크의 패킷 수신 에러율이 증가한다. 따라서, STA nodes와 Other nodes의 에너지 효율이 감소하며, 네트워크 에너지 효율도 점차 감소하였다. 간섭 반경이 작을 때는 relay 모델이 나머지 모델보다 에너지 효율이 월등히 높았지만, 간섭 반경이 커짐에 따라 ART\_HR 모델의 에너지 효율과 비슷해지는 결과를 보였다. 에너지 효율은 relay, ART\_HR, ART\_HT, direct 모델 순으로 높았으며, 간섭 환경에서의 신뢰 네트워크 에너지 효율은 비신뢰 네트워크 에너지 효율보다 더 낮은 성능을 보였다.

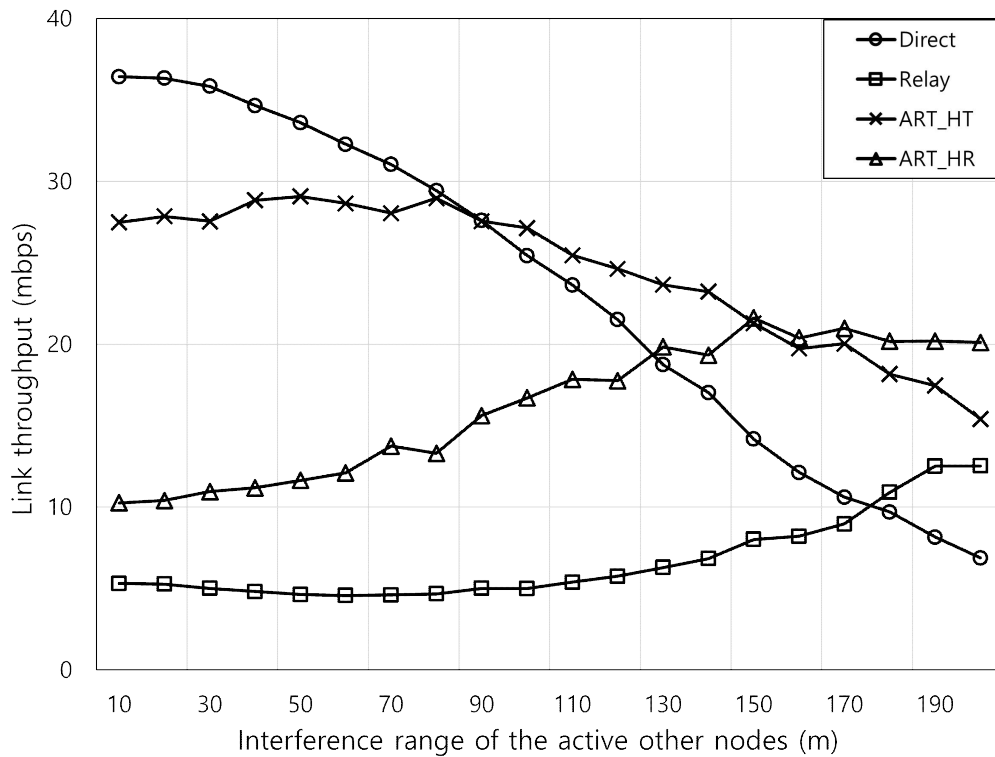


FIGURE 14. Link throughput vs. interference range of the active other nodes

Fig. 14는 Other nodes의 간섭 반경이 변화함에 따른 링크 처리율의 변화를 나타낸 그래프이다. 링크 처리율의 경우, direct 모델과 ART\_HT 모델은 Other nodes의 간섭 반경이 증가하면, 링크 내 패킷 수신 에러율이 증가하기 때문에 링크 처리율이 감소하였다. 반면, 전송 홉의 수에 비례하여 지연이 증가하는 relay 모델은 패킷 전송에 실패할 때 전송 홉의 개수가 감소하며, 이에 따른 지연이 크게 감소한다. 이에 따라 relay 모델은 Other nodes의 간섭이 증가할수록 패킷 수신 에러의 증가율 대비 전송 지연이 크게 감소하여 링크 처리율이 개선되는 결과를 보였다. 또한, ART\_HR 모델은 신뢰성을 향상시키기 위해 relay 전송 횟수가 상대적으로 많으므로 relay 모델과 유사한 결과를 보였다. ART\_HT 모델은 링크 처리율이 점차 감소하지만, ART\_HR 모델은 링크 처리율이 개선되기 때문에 두 모델은 간섭 반경이 약 150m일 때 교차한다. 이를 통해 채널 상황에 따라 HT 모드와 HR 모드를 동적으로 선택하여 동작하는 ART 모델은 간섭 반경이 매우 큰 상황에서도 15.4 Mbps의 링크 처리율 성능 유지가 가능함을 입증하였다.

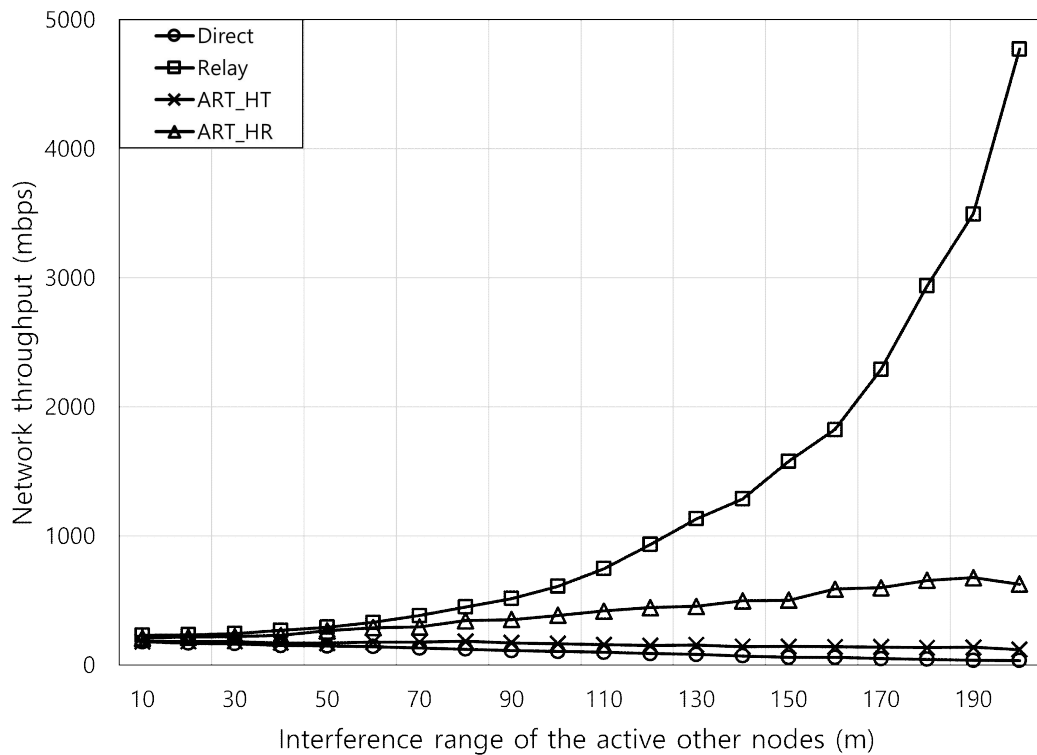


FIGURE 15. Network throughput vs. interference range of the active other nodes

Fig. 15는 Other nodes의 간섭 반경이 증가함에 따른 네트워크 처리율 성능을 나타낸다. 네트워크 처리율의 경우, Other nodes의 간섭 반경이 증가할수록 relay 모델은 direct 모델보다 Other nodes와 STA nodes가 서로에게 미치는 간섭의 영향이 적다. 또한, relay 모델은 Other nodes의 간섭 파워가 증가하면, 패킷 수신 에러율이 증가하지만, 전송 지연이 크게 감소하여 네트워크 처리율이 개선되었다. relay 전송 횟수가 상대적으로 많은 ART\_HR 모델도 점차 개선된 네트워크 처리율을 보였다. 반면, 간섭 반경이 증가할수록 direct 모델의 전송 반경과 Other nodes의 간섭 반경이 겹칠 확률이 증가하며, 이에 따른 네트워크 내에서 모든 노드의 간섭 영향이 커지기 때문에 네트워크 처리

율이 점차 감소했다. ART\_HT 모델은 ART\_HR 모델보다 direct 전송 횟수가 많으며, direct 모델과 유사한 네트워크 처리율을 보였다. 그뿐만 아니라, 간접이 큰 네트워크 환경에서는 ART\_HR 모델이 ART\_HT 모델보다 링크 처리율과 네트워크 처리율을 크게 개선하였다.

## VI. 결론

최근 WiFi 기술을 활용하여 대량의 트래픽을 실시간으로 처리하고 있으며, 이를 통한 안정적인 저지연 통신의 중요성은 더욱 커지고 있다. 또한, 무선랜의 보안 위협이 증가함에 따라 보안성을 향상시키는 기술이 필수적으로 요구된다. 즉, 성능과 보안을 모두 고려한 표준 기술 개발이 필수적이다. WiFi 8에서 활발하게 논의되는 relay 전송 기술은 성능과 보안을 최적화하기 위한 핵심 기술로서 높은 보안을 유지함과 동시에 높은 처리율과 에너지 효율을 달성할 수 있다. 그러나, relay 전송 기술은 여전히 지연이 큰 문제가 존재하며, 이를 개선하는 기술이 개발되어야 한다. 이에 본 연구에서는 relay 전송을 통해 도청의 확률을 줄여 보안성을 향상시키며, direct 전송을 통해 저지연성을 보장하는 ART 모델을 제안했다. 실험 결과에 따르면, ART\_HR 모델은 DTN에서 direct 모델 대비 13.1배 개선된 신뢰 네트워크 에너지 효율을 보였고, 보안 취약 네트워크에서 relay 모델과 동일한 수준의 정보유출량을 보였다. 또한, DTN 환경, 보안 위협이 큰 환경, 간섭 환경에서의 데이터 처리율을 측정했을 때, ART\_HT 모델은 relay 모델보다 개선된 링크 처리율을 보였으며, ART\_HR 모델은 direct 모델보다 네트워크 처리율을 향상시켜 처리율 성능 또한 개선하였다. 본 연구에서 ART 모델은 패킷의 요구사항을 고려하여 전송 방식을 결정하는 동적 전송 모델을 적용했다. 향후 연구에서는 패킷의 요구사항뿐만 아니라 네트워크 상황을 실시간으로 인지하여 최적의 전송 방식을 결정하는 동적 전송 모델을 연구할 계획이다.

## 참고문헌

- [1] Sachan, Smriti, Rohit Sharma, and Amit Sehgal. "Energy efficient scheme for better connectivity in sustainable mobile wireless sensor networks." *Sustainable Computing: Informatics and Systems* 30 (2021): 100504.
- [2] Giordano, Lorenzo Galati, et al. "What Will Wi-Fi 8 Be? A Primer on IEEE 802.11 bn Ultra High Reliability." *arXiv preprint arXiv:2303.10442* (2023).
- [3] Reshef, Ehud, and Carlos Cordeiro. "Future directions for Wi-Fi 8 and beyond." *IEEE Communications Magazine* 60.10 (2022): 50-55.
- [4] "IEEE 802.11-22/1908r1: UHR Rate-vs-Range Enhancement with Relay,"<https://mentor.ieee.org/802.11/dcn/22/11-22-1908-01-0uhr-uhr-rate-vs-range-enhancement-with-relay.pptx>, 2022, accessed Dec 15, 2023.
- [5] "IEEE 802.11-23/1146r1: Relaying for Low Latency Traffic in UHR,"<https://mentor.ieee.org/802.11/dcn/23/11-23-1146-01-0uhr-relaying-for-low-latency-traffic-in-uhr.pptx>, 2023, accessed Dec 15, 2023.
- [6] "IEEE 802.11-23/1146r1: Relay transmission in uhr,"<https://mentor.ieee.org/802.11/dcn/23/11-23-1139-00-0uhr-relay-transmission-in-uhr.pptx>, 2023, accessed Dec 15, 2023.
- [7] Lee, Sun-Jin, et al. "Machine learning-based jamming attack classification and effective defense technique." *Computers & Security* 128 (2023): 103169.
- [8] Raza, Muhammad Ahmad, et al. "Statistical Learning-based Adaptive Network Access for the Industrial Internet-of-Things." *IEEE*

Internet of Things Journal (2023).

[9] Palmieri, Francesco. "A reliability and latency-aware routing framework for 5G transport infrastructures." *Computer Networks* 179 (2020): 107365.

[10] Robinson, Y. Harold, et al. "DRP: Dynamic routing protocol in wireless sensor networks." *Wireless Personal Communications* 111 (2020): 313-329.

[11] Tang, Liangrui, Zhilin Lu, and Bing Fan. "Energy efficient and reliable routing algorithm for wireless sensors networks." *Applied Sciences* 10.5 (2020): 1885.

[12] Prakash, P. Suman, D. Kavitha, and P. Chenna Reddy. "Delay-aware relay node selection for cluster-based wireless sensor networks." *Measurement: Sensors* 24 (2022): 100403.

[13] Abdul-Qawy, Antar Shaddad Hamed, et al. "TEMSEP: Threshold-oriented and energy-harvesting enabled multilevel SEP protocol for improving energy-efficiency of heterogeneous WSNs." *IEEE Access* 9 (2021): 154975-155002.

[14] Shi, Qiong, et al. "Information-aware secure routing in wireless sensor networks." *Sensors* 20.1 (2019): 165.

[15] Al-Kaseem, Bilal R., et al. "Optimized energy - efficient path planning strategy in WSN with multiple Mobile sinks." *IEEE Access* 9 (2021): 82833-82847.

[16] Devulapalli, Praveen Kumar, Pardha Saradhi Pokkunuri, and Maganti Sushanth Babu. "Delay aware hybrid routing for large scale cooperative D2D networks." *International Journal of Intelligent Engineering*

and Systems 14.2 (2021): 547-55.

[17] Hung, L-L., et al. "Energy-efficient cooperative routing scheme for heterogeneous wireless sensor networks." *IEEE Access* 8 (2020): 56321-56332.

[18] Khan, AB Feroz, and G. Anandharaj. "Ahkm: an improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in iot." *Egyptian Informatics Journal* 22.2 (2021): 119-124.

[19] Heinzelman, Wendi Rabiner, Anantha Chandrakasan, and Hari Balakrishnan. "Energy-efficient communication protocol for wireless microsensor networks." *Proceedings of the 33rd annual Hawaii international conference on system sciences*. IEEE, 2000.

[20] Alliance, Wi-Fi. "Wi-Fi CERTIFIED™ for WMM™-Support for multimedia applications with quality of service in Wi-Fi® networks." Austin, Wi-Fi Alliance (2004).

[21] Zhao, Jinjing, et al. "A Safety-Enhanced Dijkstra Routing Algorithm via SDN Framework." *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*. IEEE, 2020.

# ABSTRACT

## Adaptive Relay Transmission for Highly Reliable and Efficient Network

Yu-ran Jeon

Department of Future Convergence  
Technology Engineering  
Graduate School of  
Sungshin University

WiFi technology is evolving from generation to generation to realize high-performance, high-efficiency wireless networks, and in the recently started IEEE(Institute of Electrical and Electronics Engineers) 802.11bn standardization process, it is aiming to dramatically improve throughput, delay, and power consumption to ensure UHR(Ultra High Reliability). However, despite the recent growth in the market size of IT(Information Technology) products equipped with WiFi and the increasing security threats of WLAN(Wireless Local Area Network), standardization to improve security is insufficient. In this study, we propose a routing protocol that performs ART(Adaptive Relay Transmission) by recognizing the security and latency requirements of packets. When low-latency transmission is required, ART uses a direct transmission method using single-hop transmission, and when highly secured transmission is required, it uses a relay transmission method that reduces the probability of eavesdropping attack by transmitting short hops. In addition, in situations where low latency and strong security are simultaneously required, ART determines an optimal transmission method considering throughput, energy

efficiency, and security to increase network reliability. According to the experimental results, in DTN(Delay Tolerant Network) environments, the proposed ART showed 13.1 times improved reliable network energy efficiency compared to the direct model which always applies direct transmission method and in a security-vulnerable network, the same amount of information leakage as the relay model which always applies relay transmission method. Additionally, ART improved network throughput by 212.4% over the direct model in networks with high node density, and achieved a maximum link throughput of 15.4 Mbps even in network with strong interference.