Ultra-High Reliable Multi-AP Cooperation Utilizing Securely Compressed Channel Status Information for Next Generation Wireless LANs

So-Eun Jeon
Future convergence technology engineering
Sungshin Women's University
Seoul, South Korea
soeun727@naver.com

Il-Gu Lee
Future convergence technology engineering,
Convergence security engineering
Sungshin Women's University
Seoul, South Korea
iglee@sungshin.ac.kr

***Abstract*— As Wi-Fi 8 standardization aimed at ultra-high reliability (UHR) has progressed, advanced communication technologies are being actively studied. As hyper-connected intelligent network environments have become more common, ensuring high throughput and low latency in wireless communication networks, as well as seamless communication for real-time applications, has become increasingly important. Typically, in Wi-Fi 8, the multi-AP cooperation technique in which multiple APs work together to transmit data has been actively discussed. This has the advantage of improving communication coverage by performing coordinated transmission with an optimized transmission technique by exchanging control information by multiple APs. However, there is a limitation in that it can cause an overhead problem in the network and a security threat that exploits channel state information in that the control information transmitted and received between devices increases together. However, conventional technologies do not consider the problem of a malicious attacker manipulating channel state information to reduce communication efficiency or the problem of increasing overhead. Therefore, this study proposes a Bitmap Compression-based Secure Channel Management Mechanism (BC-SCMM), a hash-based bitmap compression method to minimize overhead due to control information in an intelligent communication environment. According to the experimental results, BC-SCMM reduced latency by 74.12% and energy consumption by 105.19% while ensuring the confidentiality of channel status information compared to the non-channel management mechanism (NCMM).**

Keywords*— *Wi-Fi 8, 802.11bn, Dense network, Multi-AP cooperation, Channel management.

I. Introduction

As real-time applications for industrial automation are applied to many industries, ensuring high throughput and low latency in Wi-Fi networks has become critical [1,2]. If these requirements are not met, communication delays will occur in mission-critical systems, significantly compromising vast network systems' reliability. Accordingly, intelligent wireless network technology has become common, and machine learning-based network optimization technology is actively studied [3,4]. In particular, the Wi-Fi 8 (802.11bn) study group (SG), which is currently discussing standardization, is conducting research and development with the goal of Ultra-High Reliable (UHR), and a representative example is multi-AP coordination technology to improve spectrum efficiency. AP coordination technology was introduced, starting with Wi-Fi 7 (802.11be). Multi-AP coordination technology is a technique that optimizes network performance by collaborating with multiple access points (APs). It has the advantage of improving coverage as the number of APs participating in the cooperative network increases. The multi-AP coordination techniques of 802.11be include joint transmission [5], coordinated beamforming (co-BF) [6], coordinated uplink (UL) multiple user multiple input multiple output (MU-MIMO) [7], coordinated spatial reuse (co-SR) [8], coordinated Orthogonal Frequency Division Multiplexing (co-OFDMA) [9], and coordinated Time-Division Multiplexing Access (TDMA) [10] technologies were introduced. In Wi-Fi 8, real-time Multi-AP cooperation technology, which exchanges control information and performs cooperative transmission, began to be discussed in earnest [11,12,13,14,15].

To improve network performance and efficiency by utilizing such advanced cooperative communication technologies, there is a problem that traffic for information exchange between wireless communication devices increases, causing interference. Increasing interference and overhead compromises the network's quality of service (QoS) by reducing the communication availability of real-time applications, leading to a large damage impact on mission-critical smart systems. However, the existing focus has been on improving network performance, failing to consider increasing overhead and security threats [11,12,13]. Previously, techniques for communicating through a clean sub-channel by specifying the channel state experienced by each STA as a bitmap and techniques for displaying punctured channel information as a bitmap are being studied [16,17]. However, the existing multi-AP cooperation technique is limited because it does not address the interference problems arising from communication among multiple APs; it primarily focuses on communication methods in small BSS environments with minimal ambient interference. In other words, the current multi-AP cooperation is expected to experience substantial overhead in a realistic dense AP environment where interference is significant. In addition, even if the channel state is expressed in a simple bitmap form, this has the limitation of acting as a significant overhead in a high-bandwidth dense network environment, and header information is vulnerable to frame injection attacks because it is unencrypted public information.

Therefore, in this study, we propose a Bitmap Compression-based Secure Channel Management Mechanism (BC-SCMM) that converts the channel state experienced by each STA into a bitmap and compresses it based on the hash. BC-SCMM expresses the channel state experienced by each STA in a simple bitmap form and can effectively respond to overhead and header frame injection threats by hash-based compression and encryption. The AP can effectively estimate the channel state by transmitting the hash-based compressed channel bitmap to the AP and decrypting it through the channel codebook. Furthermore, a malicious attacker can maliciously manipulate the channel bitmap by hash-based encryption of the channel state information. There is an advantage in that it reduces the possibility of occurrence. BC-SCMM is a technique designed to mitigate interference within a BSS. In this study, performance evaluation was conducted on a simplified BSS, demonstrating its potential for extension to a multi-AP environment.

The main contributions of this paper are as follows.

- We proposed BC-SCMM, which can effectively manage interference and overhead within the network by compressing and expressing the channel state with a hash using a simple bitmap-based mechanism. It is also scalable while maintaining compatibility with existing standards.
- An evaluation framework was proposed to evaluate the effectiveness of the channel state management mechanism.
- By evaluating the latency, throughput, and energy consumption of BC-SCMM, we demonstrated that performance, efficiency, and security can be significantly improved compared to conventional channel measurement models.

This paper is structured as follows. Section 2 analyzes previous research, and Section 3 describes the operating mechanism of the proposed BC-SCMM model. Section 4 analyzes the performance evaluation results of the BC-SCMM model, and Chapter 5 concludes the study.

II. Related Work

This chapter analyzes previous studies related to efficient channel measurement methods. Recently, machine learning (ML)-based channel management techniques have been actively researched, and ML-based and non ML-based methods were analyzed separately. Table 1 analyzes related prior research from the perspective of techniques and limitations. Security enhancement was evaluated based on whether the technique proposed in the previous study included a mechanism to respond to attacks, such as header frame injection attack detection, which may occur during the channel management process. Efficiency improvement was assessed by determining whether interference could be managed efficiently to enhance overall system performance.

H. Sun et al. [18] studied the ML-based channel management mechanism, considered the input/output of the signal processing algorithm as unknown non-linear mapping, and proposed a technique to approximate it as a deep neural network (DNN). At this time, the interference was managed using the weighted minimum mean square error (WMMSE) algorithm, designed for efficient interference management and performance optimization, but its computational complexity was high. Therefore, in this preceding study, a mechanism capable of real-time processing was proposed to approximate the WMMSE algorithm using DNN. However, there is still a large overhead limitation due to the complexity of the DNN model itself, and there was no performance comparison analysis with the non-ML model, so it was impossible to prove the performance improvement value compared to the conventional model. The study of N. Naderializadeh et al. [19] proposed a Multi-Agent Deep Reinforcement Learning (RL)-based interference management mechanism for resource management and interference mitigation in wireless networks. This works by mounting an RL agent on each transmitter to learn and make decisions. However, the distributed learning mechanism in which all transmitters learn and make decisions has a limitation in that complexity is very high.

As such, conventional ML-based mechanisms still have inefficient limitations in terms of complexity, and in recent standards, non-ML mechanisms have been actively discussed for efficient channel management. R. J. Yu et al. [20] proposed a mechanism to manage channel interference simply by specifying and sharing punctured channel information as a bitmap. This reduced the complexity compared to the existing ML-based method in that it proposed simply expressing the channel state as a bitmap. However, in the high-bandwidth environment, the overhead problem caused by the lengthening of the bitmap remains, and the possibility of a malicious attacker manipulating channel state information was not taken into account. A. Rahmati et al. [21] proposed utilizing unmanned aerial vehicles (UAV) to reduce interference in the communication process. It aimed to keep the interference below a certain level by designing the three-dimensional path and power allocation mechanism of UAVs. It proposed an alternating maximization approach that optimizes UAVs' three-dimensional path and transmission power together. However, there is a limitation because it is a mechanism that can only use mobile devices such as UAVs. A. Tölli et al. [22] proposed combining multiple antenna systems and coded caching (CC) techniques to reduce interference. CC is a method in which the user terminals cache content in advance and increases transmission efficiency by utilizing cached data when the base station transmits data, thereby reducing interference through CC. However, the complexity of multiple antenna systems remains, and there are limitations in the performance degradation of preconfigured caching methods in dynamically changing interference environments.

As such, conventional channel interference management techniques still have high complexity issues, and it did not consider a frame injection attack that allows a malicious attacker to manipulate the channel state. Therefore, in this study, we propose a channel state management method that minimizes hash-based overhead and BC-SCMM, which can respond to a malicious attacker's frame injection attack by encrypting the original channel information based on the hash.

III. Bitmap Compression-based Secure Channel Management Mechanism

This chapter describes the operating mechanism of the BC-SCMM model, which is a channel measurement method to efficiently manage interference in the network. Fig. 1 shows the proposed operating mechanism of BC-SCMM.

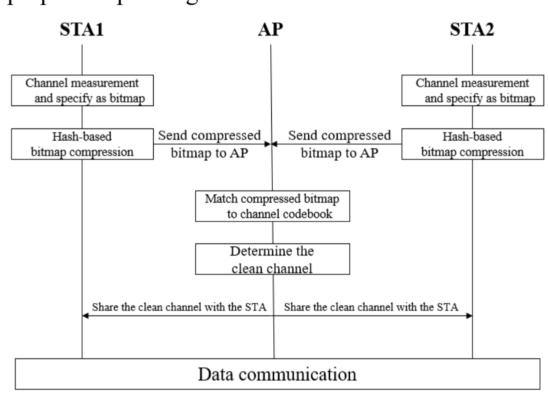

Fig. 1. Flowchart of BC-SCMM

Table 1. Previous studies of channel management mechanisms

Category	Ref.	Techniques	Limitation	Security Enhancement	Efficiency Improvement
Machine learning-based method	[18]	• Propose a method to approximate the weighted minimum mean square error (WMMSE) interference management algorithm to a deep neural network (DNN)	• The complexity of the DNN model itself is high • Need to compare complexity performance with Non-ML model	X	O
	[19]	• Multi-Agent Deep Reinforcement Learning (RL) based resource management techniques for resource management and interference mitigation in wireless networks • The mechanism by which each transmitter's reinforcement learning agent learns the signal	• Increasing complexity and overhead as each transmitter performs RL-based distributed learning	X	X
Non-machine learning-based method	[20]	• Suggestion on how to inform the punctured channel information by bitmap	• No consideration of overhead due to the longer bitmap length • Possibility of malicious attackers manipulating channel state information	X	X
	[21]	• Proposed mechanisms to keep interference below a certain level by designing the three-dimensional path and power allocation of unmanned aerial vehicles (UAVs)	• Only considered for mobile devices such as UAVs	X	X
	[22]	• Combine multiple antenna systems and Coded Caching (CC) techniques to reduce interference • Reduce data transfer with CC to minimize interference	• The complexity of the multi-antenna system itself • Challenging to achieve optimal performance in dynamically changing interference environments	X	O
Our Work		• Proposed communication method with a clean channel by expressing the bitmap-based channel state • Compress and encrypt hash-based channel state fields	• Attackers can also be decrypted if codebooks are leaked	O	O

BC-SCMM is a technique of transmitting and receiving channel states between STAs and APs in each basic service set (BSS) to communicate with an optimal clean channel. First, each STA goes through a process of measuring the channel state of each subchannel and converting the same into a bitmap. The channel is measured using a signal-to-interference plus noise ratio (SINR).

When the SINR of each sub-channel exceeds the SINR threshold, the channel state with low interference is identified as 1, and when the signal state below the SINR threshold is measured, the bitmap is generated by identifying it as a subchannel with high interference and specifying it as 0. When the bitmap is generated, each STA hashes the bitmap generated for compression and encryption and transmits the same to the AP. The AP receiving this decrypts the bitmap received from each STA by comparing it with a codebook in which the hashed channel bitmap and the original bitmap are matched and reshare the clean subchannel identified in common by the STAs in the BSS to thereby communicate with the channel with minimal interference.

Fig. 2 shows the conceptual diagram of BC-SCMM. Each STA measures the SINR of eight subchannels, specifies 0 or 1, and generates a channel status bitmap, and measures the channel states of adjacent nodes together to hash the SSID of the device and the channel state information. The length of the compressed bitmap may be flexibly adjusted within the range of reserved bits of the frame header specified in the standard. Upon receiving the compressed bitmap, the AP may decode the channel by comparing it with the previously generated channel bitmap codebook, and the channel bitmap codebook may be generated in the form in which the hash bitmap and the original bitmap are matched, as shown in Fig. 2.

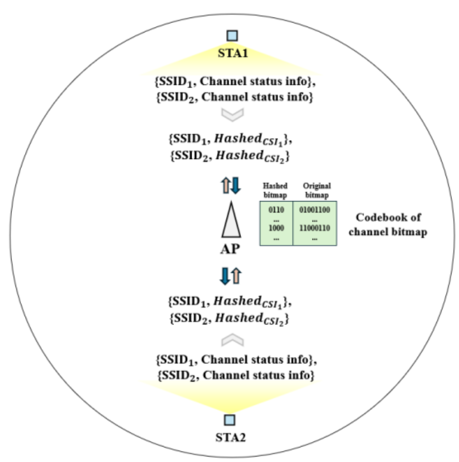

Fig. 2. Conceptual diagram of BC-SCMM in 160MHz bandwidth environment

Table 2. New encoding rule of Duration/ID field.

Existing Standard modes	Bits 0-13	Bit 14	Bit 15	Usage
	0-32767		0	Duration value applies to all frames except PS-Poll frames during the Contention Period (CP) and to frames transmitted during the Contention Free Period (CFP) under the Hybrid Coordination Function (HCF).
	0	0	1	Fixed value under point coordination function (PCF)
	1-16383	0	1	Reserved
	0	1	1	Reserved
	1-2007	1	1	AID in PS-Poll frames
	2008-16383	1	1	Reserved

Newly added mode	Bits 0-13		Bit 14	Bit 15	Usage
	Bits 0-12	Bit 13			
	1-8191	1	1	1	Hashed channel status information

BC-SCMM proposes a method of using the reserved bit as a hashed channel status information by newly defining the encoding rule of the duration/ID field of the existing MAC frame. The encoding rule of the duration/ID field was defined as shown in Table 2.

In the existing standard, the usage when bits 14 and 15 of the duration/ID field are each 1, or all 1 is defined as shown in Table 2. In the new encoding rule proposed in this paper, when 13,14,15 bits of duration/ID are all 1, we propose a method that can be expanded while maintaining the compatibility of existing standards by using bits 0-12 as hashed channel status information. It is compatible with existing standards in that it is possible to use the hashed channel status information only by specifying bit 13 as 1 without changing the indication for each value of bits 14 and 15, and it is scalable in that it can be used as a channel management field.

IV. Performance Evaluation and Analysis

A. Evaluation environment

This chapter describes the experimental environment used to verify the performance of the proposed BC-SCMM. Figure 3 shows the node configuration of this experiment. In this study, a single BSS environment was implemented to evaluate the performance of BC-SCMM and demonstrate the effectiveness of the proposed methodology in a simplified experimental setup.

The conventional model for performance verification of BC-SCMM was selected as the non-channel management mechanism (NCMM) [23], which communicates in a fixed subchannel without measuring channel status, and the simplified channel management mechanism (SCMM) [16], which specifies channels with bitmaps but does not perform hash-based compression and encryption.

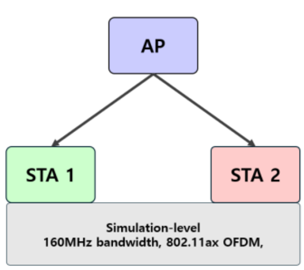

Fig. 3. Node configuration of evaluation environment

In this experiment, each model was implemented with Matlab to verify its performance. As an orthogonal frequency division multiplexing (OFDM) environment with a bandwidth of 160 MHz, it was implemented as a network environment composed of eight subchannels. It is assumed that two STAs and APs in one BSS communicate, and an environment in which each STA transmits four 10,000byte data per 1 ns is implemented. Latency, throughput, and energy consumption were used as evaluation metrics. Latency was calculated according to Eq. (1).

$$\mathrm{Latency(sec)} = \mathrm{T_{Header}} + \mathrm{T_{Data}} + \mathrm{T_{SIFS}} + \mathrm{T_{ACK}} + \mathrm{T_{DIFS}} \quad (1)$$

Each notation in Eq. (1) is summarized in Table 3.

Table 3. Notation of latency formula.

Notation	Description	Value
T_{Header}	Time duration of header frame	$\mathrm{T_{frame\ control}} + \mathrm{T_{reserved\ bit}} + \mathrm{T_d} + \mathrm{T_{address}} + \mathrm{T_{sequence\ control}}$
T_{Data}	Time duration of data frame	80,000ms
T_{SIFS}	Time duration of SIFS frame	16ms
T_{ACK}	Time duration of ACK frame	0.1ms
T_{DIFS}	Time duration of DIFS frame	34ms

T_{Header} was implemented to vary the time duration based on each model's reserved bits size. Throughput was calculated according to Eq. (2).

$$Throughput = \frac{Amount\ of\ data\ received\ successfully}{Transmission\ time} \quad (2)$$

Each STA environment takes 1ns to transmit 1 bit and transmits data of four 10,000 byte sizes. In this case, the total network throughput, the sum of each STA's throughput, was calculated. In addition, it is implemented as an environment in which the channel state changes randomly each time data is transmitted, and the transmission fails when the data is transmitted to a subchannel with an SINR threshold or less and retransmits up to 8 times. Energy consumption was calculated by defining the energy consumption by state based on the finite state machine (FSM) of Fig. 4 [24].

The state of this model was defined as TX, RX, IDLE, and Collision. In the case of the TX state, it was assumed that 0.0001 mW of energy was consumed per 1 bit, and the RX state was implemented to consume 250.5 mW, the IDLE state

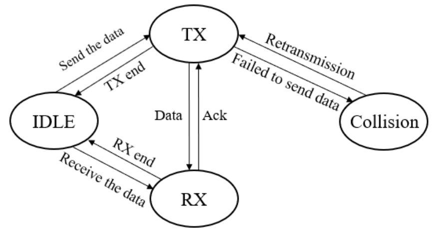

Fig. 4. FSM in this study.

0.5 mW, and the collision state, which fails to transmit data due to channel interference, consumes 1,000 mW.

B. Evaluation results and analysis

Fig. 5 shows the latency performance of the proposed BC-SCMM compared to the conventional models SCMM and NCMM. According to Fig. 5, the latency increased linearly in proportion as the channel interference rate increased. NCMM communicating with a fixed channel without measuring the channel state increases the probability of data transmission failure, so increasing the number of retransmissions showed inefficient results in increasing the latency. On the other hand, the SCMM measures the channel state experienced by each STA and communicates with the optimal clean subchannel, and the proposed BC-SCMM showed more efficient latency results than NCMM. Less latency was required compared to SCMM because BC-SCMM compresses the hash-based bitmap channel measurement field and reduces channel overhead.

Fig. 6 shows the throughput performance comparison between the proposed BC-SCMM and the conventional models SCMM and NCMM. According to Fig. 6, overall, the throughput decreased in inverse proportion as the channel interference rate increased. Since NCMM, which communicates with a fixed channel without measuring the channel state, is highly likely to communicate with a subchannel containing interference, the throughput decreased in increasing the number of retransmissions. On the other hand, the SCMM communicating with the optimal clean subchannel and the proposed BC-SCMM showed higher throughput results than NCMM, and the BC-SCMM, which compresses the hash-based channel measurement field, took less latency to transmit data. Hence, the throughput also showed more efficient results.

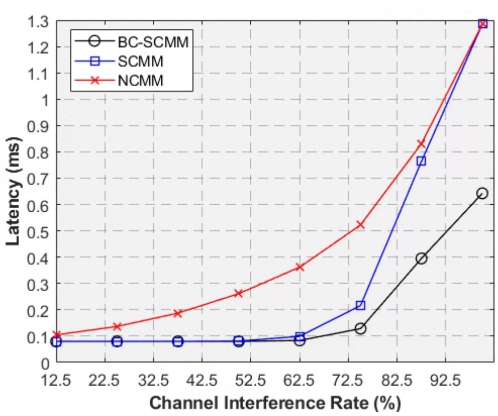

Fig. 5. Latency performance of the channel interference rate

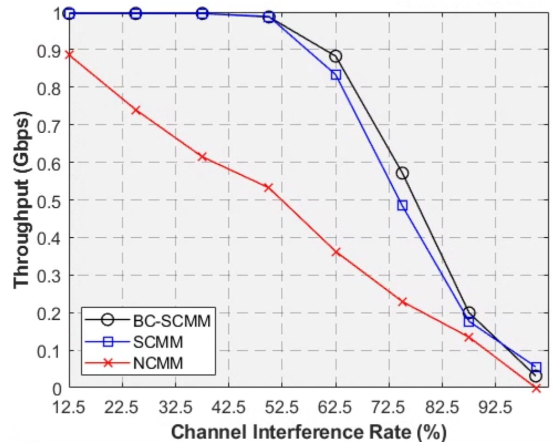

Fig. 6. Throughput performance of the channel interference rate

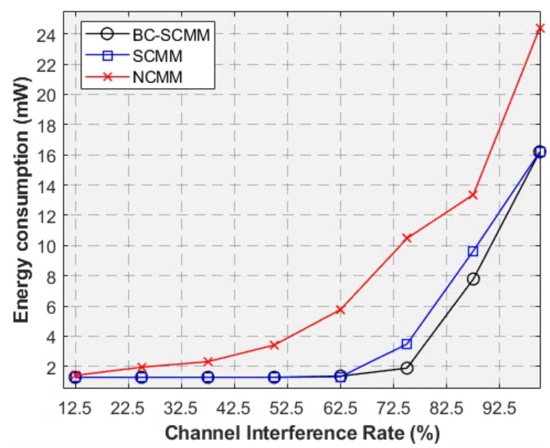

Fig. 7. Energy consumption performance of the channel interference rate

Fig. 7 shows the energy conversion performance of the proposed BC-SCMM compared to the conventional models SCMM and NCMM. According to Fig. 7, as the channel interference rate increased, the energy conversion increased proportionally. Due to retransmission, NCMM with many TXs showed the most inefficient results, while SCMM and BC-SCMM communicating through a clean channel showed relatively energy-efficient results. In particular, the least energy was consumed because the size of the header field transmitted by BC-SCMM, which compresses the hash-based channel measurement field, was smaller.

C. Security analysis

Table 4 analyzes the security of BC-SCMM and SCMM, which operate as channel measurement information targeted by an attacker.

Table 4. Security analysis of each model.

Model	Access feasibility of an attacker	Exposure of channel state for an attacker
BC-SCMM	O	X
SCMM	O	O

Since both BC-SCMM and SCMM operate with channel information stored in the bitmap channel measurement field of the unencrypted header, attackers can always access this channel state information. However, BC-SCMM performs hash-based de-identification and compression processing only on the corresponding field section, so even if the attacker can access the channel state information, the original channel state information cannot be known, so it cannot be manipulated with the channel information intended by the attacker. On the other hand, SCMM is vulnerable in terms of security in that the channel state is marked with a bitmap for each subchannel, so when the attacker approaches the field, the channel can be manipulated as intended by the attacker.

V. CONCLUSION

As intelligent network environments become ubiquitous, network performance is rapidly advancing. However, the proliferation of control information exchanged between devices with sophisticated mechanisms escalates network overhead issues and security threats. While technologies for measuring channel states are under research, existing interference mitigation techniques still suffer from significant overhead, especially in wider bandwidth environments where the overhead of measuring each subchannel state increases sharply. Moreover, the security threat of malicious attackers manipulating channel state information to degrade user communication efficiency is not adequately addressed. Therefore, this study proposes a hash-based bitmap compression method, BC-SCMM, to minimize overhead and security threats in intelligent communication environments. Experimental results demonstrate that BC-SCMM improves efficiency in terms of latency, throughput, and energy consumption compared to conventional models.

In this study, the experimental environment was simplified by verifying the performance of BC-SCMM in a single BSS environment, while demonstrating its extended applicability in a multi-AP environment. Furthermore, the network performance evaluation was conducted at the simulation level without modeling the attack environment. In future work, the performance of BC-SCMM will be verified by implementing a multi-AP environment, where interference is intensified due to control information. Furthermore, we plan to demonstrate that security performance metrics can be improved by designing realistic attack scenarios.

ACKNOWLEDGMENT

This work is supported by the Ministry of Trade, Industry and Energy (MOTIE) under Training Industrial Security Specialist for High-Tech Industry (RS-2024-00415520) supervised by the Korea Institute for Advancement of Technology (KIAT), and the Ministry of Science and ICT (MSIT) under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310) supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP), and the 2024 Real Challenge program grant funded by Korea Institute of Human Resources Development in Science and Technology(KIRD).

REFERENCES

[1] Y. Jeon, J. Ryu, and I. Lee, "ART: Adaptive relay transmission for highly reliable communications in next-generation wireless LANs," in Computer Networks, vol. 254 (2024).

[2] S. Kim, S. Park, J. Lee, and I. Lee. "Secure Triggering Frame-Based Dynamic Power Saving Mechanism against Battery Draining Attack in Wi-Fi-Enabled Sensor Networks" Sensors 24, no. 16 (2024).

[3] R. Amin, E. Rojas, A. Aqdus, S. Ramzan, D. Casillas-Perez and J. M. Arco, "A Survey on Machine Learning Techniques for Routing Optimization in SDN," in IEEE Access, vol. 9, 104582-104611, (2021).

[4] M. Wang, Y. Cui, X. Wang, S. Xiao and J. Jiang, "Machine Learning for Networking: Work-flow, Advances and Opportunities," in IEEE Network, vol. 32, no. 2, 92-99 (2018)

[5] A. Titus, R. Bansal, T. V. Sreejith, A. A. Kherani and N. Akhtar, "Decision Problems for Joint Transmission in Multi-AP Coordination Framework of IEEE 802.11be," 2021 International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 326-333 (2021).

[6] O. Mutgan, P. Varshney, L. G. Giordano, M. Kasslin, F. Wilhelmi, G. Fontanesi, "Coordinated Beamforming for 802.11bn," in 802.11 TGbn (Nokia) (2024).

[7] M. Ge and D. M. Blough, "High Throughput and Fair Scheduling for Multi-AP Multiuser MIMO in Dense Wireless Networks," in IEEE/ACM Transactions on Networking, vol. 26, no. 5, 2414-2427 (2018).

[8] D. Nunez, F. Wilhelmi, S. Avallone, M. Smith and B. Bellalta, "TXOP sharing with Coordinated Spatial Reuse in Multi-AP Cooperative IEEE 802.11be WLANs," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 864-870 (2022)

[9] Z. Yan, M. Yang, and X. Zhang, "Co-NOMA: AP Coordination Based NOMA Protocol for the Next-Generation WLANs," in Mobile Networks and Applications, 1059–1075 (2023).

[10] D. Das, C. Chen, L. Cariou, D. Akhmetov, "C-TDMA Follow-up," in 802.11 TGbn (Intel) (2024).

[11] L. Lanante, J.i Kim, S. Erkucuk, J. Zhang, T. Baykas, “Cross Interference During Coordinated Spatial Reuse,” IEEE 802.11 UHR SG (Ofinno) (2023).

[12] Abdel Karim Ajami, Alfred Asterjadhi, Abhishek Patil, Duncan Ho, George Cherian, Gau-rang Naik, Yanjun Sun (Qualcomm), "Considerations for AP coordination in UHR: Coordinated Medium Access", IEEE 802.11 UHR SG (2023).

[13] J. Y. Guo, Y. Li, G. Huang, M. Gan, R. J. Yu., “Coordinated Spatial Reuse for UHR”, IEEE 802.11 UHR SG (Huawei) (2023).

[14] K. Aio, Y. Tanaka, R. Hirata, K. Tanaka, T. Handte., "Overhead Analysis of Coordinated Spatial Reuse", IEEE 802.11 UHR SG (Sony) (2023).

[15] L. Lu, C. Luo, P. Zhou. “MultiAP Coordination for Low Latency Traffic Delivery”, IEEE 802.11 (OPPO) (2022).

[16] S. Jeon, I. Lee, "Simplified Channel Management Mechanism for Multi-AP Cooperation in Dense Networks," Annual Symposium of KIPS 2024, Pyeongchang, Korea (2024).

[17] R. J. Yu, M. Hu, M. Gan, W. Jiang, “Preamble Puncture Bitmap Indication for 20 and 40 MHz OFDMA Transmission,” in 802.11 TGbe (Huawei) (2020).

[18] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu and N. D. Sidiropoulos, "Learning to Optimize: Training Deep Neural Networks for Interference Management," in IEEE Transactions on Signal Processing, vol. 66, no. 20, 5438-5453 (2018).

[19] N. Naderializadeh, J. J. Sydir, M. Simsek and H. Nikopour, "Resource Management in Wireless Networks via Multi-Agent Deep Reinforcement Learning," in IEEE Transactions on Wireless Communications, vol. 20, no. 6, 3507-3523 (2021).

[20] R. J. Yu, M. Hu, M. Gan, W. Jiang, “Preamble Puncture Bitmap Indication for 20 and 40 MHz OFDMA Transmission,” in 802.11 TGbe (Huawei) (2020).

[21] A. Rahmati et al., "Dynamic Interference Management for UAV-Assisted Wireless Networks," in IEEE Transactions on Wireless Communications, vol. 21, no. 4, 2637-2653 (2022).

[22] A. Tölli, S. P. Shariatpanahi, J. Kaleva and B. H. Khalaj, "Multi-Antenna Interference Management for Coded Caching," in IEEE Transactions on Wireless Communications, vol. 19, no. 3, 2091-2106 (2020)

[23] D. Nunez, M. Smith, B. Bellalta., "Multi-AP Coordinated Spatial Reuse for Wi-Fi 8: Group Creation and Scheduling", 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), 203-208 (2023).

[24] F. Wu, W. Yang, J. Ren, F. Lyu, P. Yang, Y. Zhang, and X. Shen, “Named data networking enabled power saving mode design for WLAN,” IEEE Trans. Veh. Technol., vol. 69, no. 1, 901–913 (2020).