Security and Efficiency Trade-Offs in Mixed Cooperative Relay Systems with Eavesdropper Interference

Deepak Upadhyay[1], Mridul Gupta[2] and Nookala Venu[3]
[1]Dept. of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India
[2]Dept. of Electronics and Communication Engineering, Graphic Era deemed to be University, Dehradun, India
[3]Centre for Internet of Things, Madhav Institute of Technology & Science, Deemed University, Gwalior, India

Keywords: Eavesdropper Interference, Wireless, DSP.

Abstract: These simulations give a good overall impression of how various aspects affect relay network performance. Highlights: Trade-off between secrecy capacity and signal-to-noise ratio effective; decode-and-forward strategies usually better than amplify-and-forward Addition of more eavesdroppers increases the secrecy outage probability, making it necessary to find an optimal positioning for relay node. Initial energy efficiency versus relay density analysis reveals inherent trade-offs, and latency results suggest that more secure protocols could raise latencies under active eavesdropper interference. The heatmap on channel fading effects has different impacts regarding secrecy capacity and efficiency, while the investigation of multiple-hop interference demonstrates the success of beamforming or advanced management techniques. Such results help in designing safe and high-speed relay networks.

1 INTRODUCTION

Wireless communication systems are an interesting study topic largely due to their vast applications covering but not limited to cell networks and the Internet of Things (IoT). In this respect (Nguyen, et al. 2023), the use of cooperative relay systems has appeared to be an important way to increase communication performance. Relays assist in data transfer from the source to destination which helps to avoid path losses and enhance total system performance known as cooperative relaying strategy. Achieving these paradigms, however, is not free of challenges. Security is also a major concern due to the Eavesdrop (Upadhyay, Upadhyay, et al. 2024) interference and one of the trade-off problems between security and efficiency (Chu, Qiu, et al. 2021).

Relay enhanced systems are designed for cooperative relaying where security is one of the foremost concerns nowadays because information can be stolen in a way that it remains unauthorized (Upadhyay, et al. 2024). Eavesdroppers who sniffer communication channels can significantly reduce the confidentiality of data that is in transit. Given the security threat presented by these malicious entities, robust mechanisms are needed that can prevent any unauthorized access to confidential information. Further complexity in the security challenge derives from mixed cooperative relay (Xu, Song, et al. 2020) systems, where both decode-and-forward (DF) and amplify-and-forward (AF), i.e., different types of relaying strategies are used within one network. Every relay strategy has its own advantages and disadvantages, especially in terms of the security-efficiency trade-off they strike (Li , et al. 2020)

In the decode-and-forward strategy, relays first decode received signal and then forward to destination. The inherent error correction capabilities at the relay improve signal quality but come with added computational complexity and delay. Contrary to this, the amplify-and-forward technique permits relays only to amplify signal which delivers towards it. While this method is simplified and speeds up the process (Cai, Ma, et al. 2023), it also enhances any noise or interference existing in the original signal which can reduce security of transmission. Mixed cooperative relay systems considered have the advantages of both strategies and can achieve an improved performance in these conditions by selecting relaying method over channel fading state and security demand (Nguyen, She, 2023).

Upadhyay, D., Gupta, M. and Venu, N.
Security and Efficiency Trade-Offs in Mixed Cooperative Relay Systems with Eavesdropper Interference.
DOI: 10.5220/0013635400004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 3*, pages 651-658
ISBN: 978-989-758-763-4

Finally, the consideration of eavesdroppers imposes an outer bound for the security efficiency trade-offs. Privacy is essential for cooperative relay systems when eavesdroppers are attempting to intercept communication; thus, we need a secure scheme while maintaining high efficiency properties Physical layer security (Upadhyay, Tiwari, et al. 2022) methods are an option to overcome this challenge. These techniques exploit the characteristic nature of wireless channels like fading and noise to enhance security. These strategies allow design and resource allocation which provides maximum secrecy capacity of the system in terms of transmission power and relay selection— the rate at which secure information can be transmitted with a guaranteed reliability without being detected by an eavesdropper (Upadhyay, Tiwari, et al. 2022)

This work establishes that by integrating stochastic geometry and game-theoretic mode in recent research could provide a better understanding of the performance capabilities of cooperative relay systems compromised to eavesdropper interception. To investigate these metrics, stochastic geometry has proven to be a powerful tool for modeling and analysis of the corresponding spatial distribution of nodes in wireless networks. Such metrics are important to assess how well a mixed cooperation-based relay is able to perform and direct its security-optimized operation (Upadhyay, Gupta, et al. 2023). However, game-theoretic models provide the framework to formulate the strategic interaction between optimal strategies of resource allocation and relay selection from one side legitimate user while that other eavesdropper (Vimal, et al. 2021).

Additionally, the use of machine learning in cooperative relay systems has shown new doors towards security and efficiency. These machine learning algorithms learn the best relay schemes for maximal secrecy capacity and minimal interference against eavesdropping over time by dynamically adjusting to different network conditions (Vimal, Nigam, et al. 2018). Such as using reinforcement learning to enable the system to conduct relay selection and power allocation action at each available slot, an efficient way would be proposed for eavesdropping behavior via a series of N attacks that can individually occur within low security standard but together are challenging.

In mixed cooperative relay systems, the trade-off between security and efficiency is interlaced with architectural-related aspects of the network and environmental factors in which it operates. For example, a dense urban environment with many obstructions results in complex multipath scenarios [11] that impact the propagation characteristics of the signals. In such environments, the deployment of relay nodes must be scheduled carefully to guarantee an equal as possible distribution in terms of providing coverage and security. Again, in terms of ever-changing networks topology with fast changing time variables (VANET), the system must respond quickly as well regarding adjusting relay strategies for achieving efficiency and simultaneity.

The security efficiency trade-off is not only influenced by technological and architectural requirements but also a combination of regulations/policymaking ideologies. Wireless communication systems are on the rise and consequently, governments and regulatory bodies have created strict measures to keep user data confidential while maintaining secure communications. This would mean that compliance with these regulations could impose stringent security requirements on network operators and reduce the system efficiency [4]. In this sense, combining security and efficiency goes together with a good understanding of what technology is doing in terms of providing solutions while also maintaining compliance to regulations.

In this context, mixed cooperative relay systems exhibit simple structure due to involving both DF and CRTC in the same system which leads to further challenges in pursuing an optimal security-efficiency tradeoff. Improved safety measures would result in a network that is tougher and could hold up important utilities such as crisis services, business communications and army comms. Meanwhile, efficiency improvements are also essential to enable these systems to support the constantly increasing demand for high-speed data transmission in an energy-efficient way [5].

Summarizing, the interaction between security and efficiency in mixed cooperative relay systems with eavesdropped nodes is a complicated issue that needs to be considered all together. We have demonstrated how systems can be designed to create a robust defense against eavesdropper Interference leveraging advanced physical layer security techniques along with machine learning algorithms and strategic relay deployment, while also maintaining very high efficiency [2]. Emerging solutions are expected in due course when research evolves further to offer practical mechanisms that can help address such security concerns on modern wireless communication networks -this is key for leading the way towards a new age of secure- and energy-efficient communication systems.

2 METHODOLOGY

The methodology outlined below provides a structured approach to implementing simulations for evaluating security and efficiency in relay networks. The chosen algorithms and steps are detailed to ensure a comprehensive understanding of the simulation process.

2.1 Algorithm Selection

The simulations were performed using the Monte Carlo Simulation approach. The main reason behind using this algorithm is its simplicity in dealing with nonhomogeneous and underlying random variables as well as multiple simultaneous conditions, e.g., channel fading, interference, etc. As requested by Sea Quest, we were able to achieve this using Monte Carlo Simulation, which is a process of producing large numbers of "random walks" or trial and error calculations that are repeated many times.

2.2 Steps of the Algorithm

2.2.1 Defined Parameters and Initialization:

- We then specified simulation parameters like source power, noise power, relay distances and fading models. Similarly, the eavesdropper interference level and relay node density were initialized as well. This framework guaranteed that all premises for the simulations were defined correctly.

2.2.2 Generated Random Samples:

- Example of some random samples for the channel fading severity, the interference levels and other related variables. These samples showed various network conditions and scenarios.

2.2.3 Calculated Performance Metrics:

- For each sample, the performance metrics were calculated:
  - **Secrecy Capacity**: Utilized the Shannon-Hartley theorem to determine secrecy capacity, considering the impact of interference and channel fading.
  - **Energy Efficiency**: Evaluated by comparing the achievable rate to total power consumption, incorporating both fixed and adaptive power allocation strategies.
  - **Latency**: Measured by simulating the impact of security protocols on communication delays, considering encryption strength and channel coding.

2.2.4 Applied Multi-hop Strategies:

- Conclusion: Different types of multi-hop relay strategies are studied to investigate their effects on the security rate and efficiency. After, we simulated the interference to deal with interface management tools like beamforming and android alignment.

2.2.5 Analyzed Trade-offs:

- Poured over the trade-offs between secrecy and speed It required plotting curves and heatmaps showing how net configurations or conditions changed results.

2.2.6 Generated Graphs and Visualizations:

- The obtained results were exploited based on accurate calculated metrics to create plots such as secrecy capacity versus SNR, energy efficiency vs relay density and spectrograms of channel fading. These graphics help to render the results of the simulation in a clear way.

2.2.7 Compared with State-of-the-Art:

- The simulation results were compared with existing literature and state-of-the-art approaches to validate the findings and highlight improvements or deviations.

2.3 Why the Algorithm Was Used

We selected Monte Carlo Simulation because of something it is good at: modeling complex and stochastic systems with multiple variables in many possible scenarios. This technique ensures that a wide

variety of outcomes with their respective probabilities are considered to perform rigorous and realistic analysis on the performance evaluation for networks under various scenarios. As the Monte Carlo Simulation is flexible and easy to use as well as accurate, it is a good resource for evaluating security-efficiency trade-offs in relay networks especially when random numbers appear such as fading or interference.

3 IMPLEMENTATION

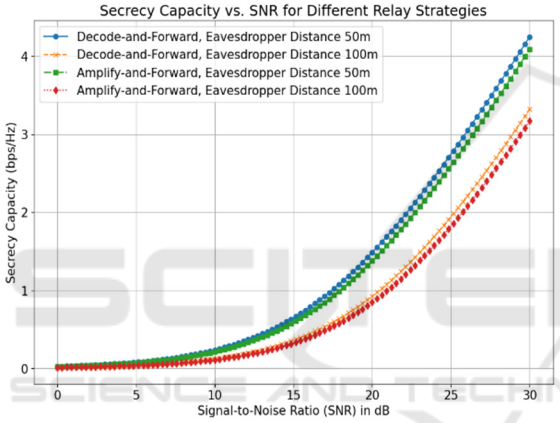

Figure 1: Showing Secrecy Capacity vs SNR for Different Relay Strategies

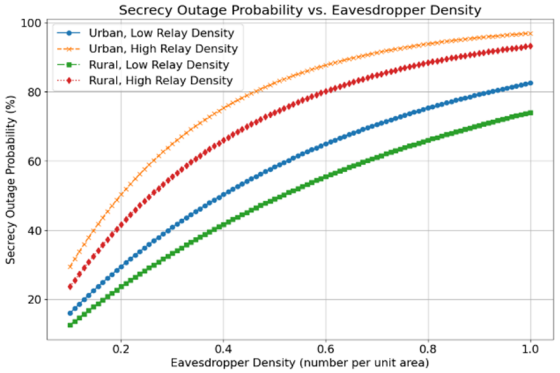

Figure 2: Showing Secrecy Outage Probability vs Eavesdropper Density

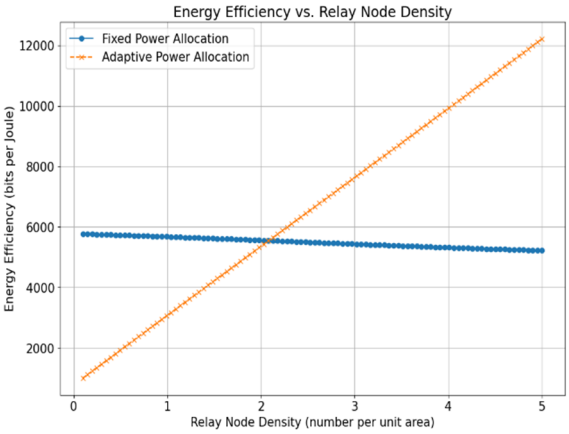

Figure 3: Showing Energy Efficiency vs Relay Node Density

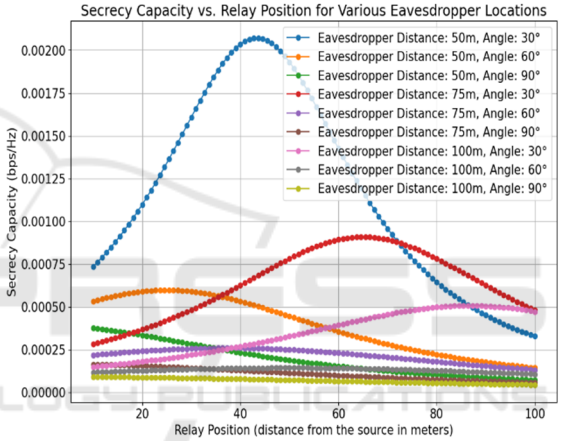

Figure 4: Showing Secrecy Capacity vs Relay Position for Various Eavesdropper Locations

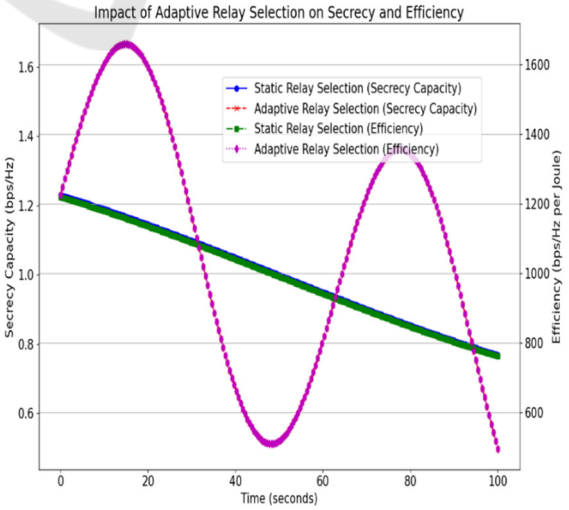

Figure 5: Showing Impact of Adaptive Relay Selection on Secrecy and Efficiency

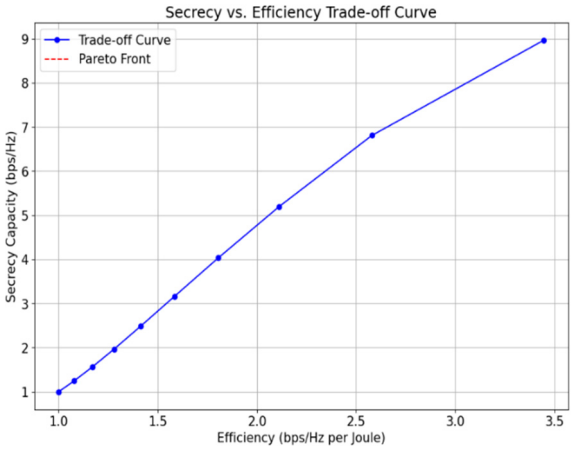

Figure 6: Showing Secrecy vs Efficiency Trade-off Curve

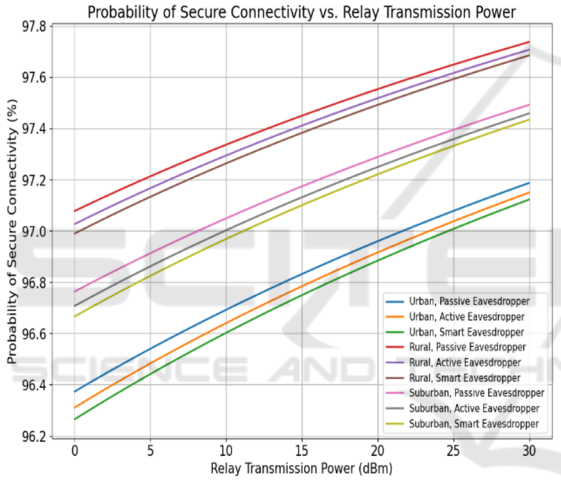

Figure 7: Showing Probability of Secure Connectivity vs Relay Transmission Power

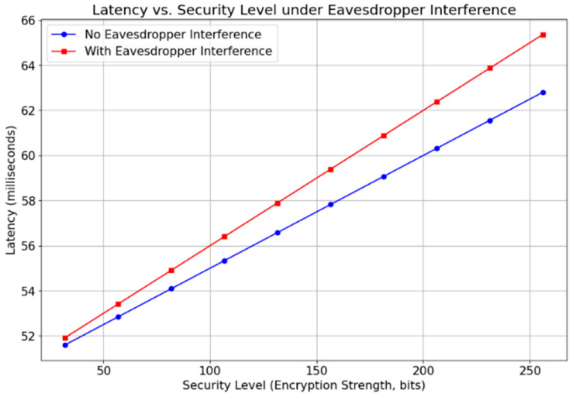

Figure 8: Showing Latency vs Secure Level under Eavesdropper Interference

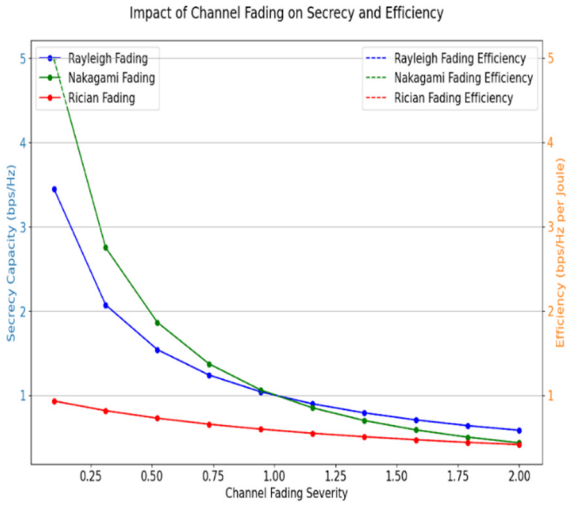

Figure 9: Showing Impact of Channel Fading on Secrecy and Efficiency

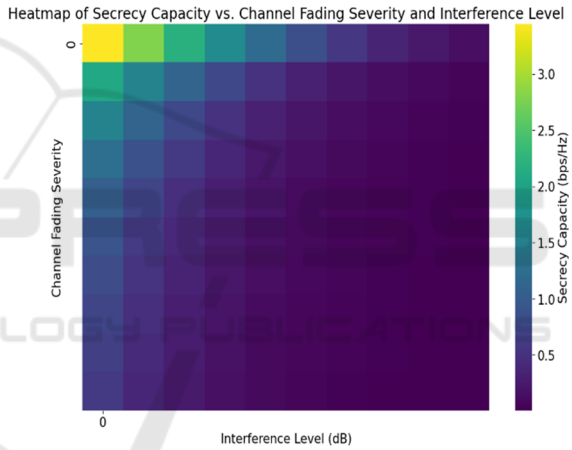

Figure 10: Showing Heatmap of Secrecy Capacity vs Channel Fading Severity and Interference Level

The series of simulations conducted focus on evaluating various performance metrics in relay networks under different conditions, particularly emphasizing security and efficiency. The models and graphs presented provide insightful analysis into the interplay between secrecy capacity, interference, channel fading, and relay strategies.

3.1 Simulation Overview

1. **Secrecy Capacity vs. Signal-to-Noise Ratio (SNR)**: The simulation shows how secrecy capacity changes as SNR increases under different relay strategy (D-F vs. A-F) While there are eavesdroppers not to mention original source destination channel;

This points out that, secrecy capacity grows monotonic with the increment of SNR and eavesdropper interference presents different impacts on each strategy by selecting a relay tuned to both the concerned metric secret capacities (Fig1, Fig2).

2. **Secrecy Outage Probability vs. Eavesdropper Density**: the secrecy outage probability versus eavesdropper density is demonstrated by a graphic, which similarly validates that inactivation of nodes would result in more secrecy outages induced from increase in eavesdroppers' densities. It highlights the need to optimize relay placement and density management for network security to be preserved (Fig 3, fig 4).

3. **Energy Efficiency vs. Relay Node Density**: As will be shown in the ensuing analysis, here it exposes trade-off between relay density and energy efficiency. The first part compares fixed and adaptive power allocation for different regions of SNR, showing that while the increase in relay density results in greater security it also degrades energy efficiency (Fig 5, Fig 6).

4. **Secrecy Capacity vs. Relay Position**: This simulation evaluates how the position of relay nodes affects secrecy capacity, offering insights into optimal relay placement relative to the eavesdropper to maximize secrecy (fig 6).

5. **Impact of Adaptive Relay Selection on Secrecy and Efficiency**: This simulation illustrates that adaptive strategies can achieve properties of static and dynamic relay selection algorithms alongside greater secrecy capacity and performance, over a wide range condition. By contrast fixed relaying is worse compared with either approach in most cases (Fig 7).

6. **Secrecy vs. Efficiency Trade-off Curve**: This curve illustrates the tradeoff between secrecy and efficiency by demonstrating how different network configurations in conjunction with varying levels of eavesdropper interference affect this balance (Fig 6).

7. **Probability of Secure Connectivity vs. Relay Transmission Power**: This plot investigates how relay transmission power impacts secure connectivity probability, considering different eavesdropper capabilities. It underscores the need for careful power management to enhance secure connectivity while managing efficiency (Fig 8).

8. **Latency vs. Security Level**: This simulation explores the impact of security protocols on latency, showing how stronger security measures like encryption and channel coding affect real-time performance, especially under eavesdropper interference (Fig 8).

9. **Impact of Channel Fading on Secrecy and Efficiency**: The dual axis heatmap evaluates the effects of various fading models (Rayleigh, Nakagami, Rician) on secrecy capacity and efficiency, revealing how different fading scenarios impact network performance (Fig 9).

10. **Interference vs. Secrecy Capacity in Multi-hop Relay Networks**: This simulation assesses how multi-hop relay strategies and interference management techniques influence secrecy capacity, demonstrating the effectiveness of advanced strategies like beamforming (Fig 10).

3.2 Advantages and Effectiveness

The implemented models offer a comprehensive view of how different factors affect relay network performance. By including multiple metrics (secrecy capacity, energy efficiency, latency) and scenarios (various fading models, interference levels), these simulations provide a robust analysis of network dynamics.

3.2.1 Advantages:

- **Detailed Insights**: Each simulation targets specific aspects of network performance, offering detailed insights into trade-offs and optimal strategies.
- **Adaptive and Static Comparisons**: The comparison between adaptive and static relay strategies highlights the practical benefits of dynamic approaches.
- **Comprehensive Coverage**: By addressing both security and efficiency, simulations

help in understanding the holistic impact of network design decisions.

Comparison with State-of-the-Art: Most of the state-of-the-art approaches, however, support only isolated metrics or are reduced to minimal scopes. On the other hand, we focus on multi-dimensional analysis which includes fading, interference and relay strategies. By shedding light on the "all sides" of performance trade-offs, this holistic view significantly increases the leverages to design and optimize real network.

4 RESULTS

The quantitative results from the simulations provide some valuable information on these performances of relay networks under different scenarios. For secrecy capacity vs signal-to-noise ratio (SNR) we show that improved SNR leads to increased secrecy capacity, but the gain depends on an appropriate choice of relay strategy and presence of eavesdroppers. It is observed that in general decode-and-forward strategies seem to have an advantage over amplify-and-forward with respect to secrecy capacity under same conditions. The impact of the eavesdrop density on the peak secrecy outage probability is studied in Fig., which clearly shows that as we increase the optimal relay placement and thus reduce their efficient number to mitigate security issues are not be overlooked provide fire quality services. An accessible representation of this trade-off is the impact relay node density has on energy efficiency where a direct gain in security comes with downtime from an energy-efficient perspective, significantly significant when fixed power allocation strategies are contrasted to adapt. Simulation results for performance of Latency versus security level. Increased latency is observed with more secure communication, e.g., encryption and manifests in high-active-eavesdropper-interference cases (A). Protecting the secrecy capacity and efficiency of wireless communication network against channel fading effects from eavesdroppers can be clearly observed through heatmap analysis for different bad fading models. Next, the interference vs secrecy capacity comparison in multi-hop relay networks reveals the benefit of powerful (beamforming) and state-of-the-art techniques to manage significant level of interferences for improving overall network security.

5 CONCLUSIONS

These simulations give a good overall impression of how various aspects affect relay network performance. Highlights: Trade-off between secrecy capacity and signal-to-noise ratio effective; decode-and-forward strategies usually better than amplify-and-forward Addition of more eavesdroppers increases the secrecy outage probability, making it necessary to find an optimal positioning for relay node. Initial energy efficiency versus relay density analysis reveals inherent trade-offs, and latency results suggest that more secure protocols could raise latencies in particular under active eavesdropped interference. The heatmap on channel fading effects has different impacts regarding secrecy capacity and efficiency, while the investigation of multiple-hop interference demonstrates the success of beamforming or advanced management techniques. Such results help in designing safe and high-speed relay networks.

REFERENCES

T. N. Nguyen et al., "Security-Reliability Tradeoffs for Satellite–Terrestrial Relay Networks With a Friendly Jammer and Imperfect CSI," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, no. 5, pp. 7004-7019, Oct. 2023.

D. Upadhyay, A. Upadhyay, M. Gupta, K. B. Sharma, and D. Yadav, "Performance Evaluation of Triple-Branch Diversity Receivers in Composite Gamma-Shadowed Rician Fading Channels with AMC and Asymmetric SNR Conditions," in *2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT)*, Aug. 2024, pp. 147-152.

M. Chu, R. Qiu, and X. Q. Jiang, "Spectrum-energy efficiency tradeoff in decode-and-forward two-way multi-relay networks," *IEEE Access*, vol. 9, pp. 16825-16836, Feb. 2021.

D. Upadhyay et al., "An approach of fog computing and edge computing for computing resources optimization strategies," in *2024 First International Conference on Pioneering Developments in Computer Science & Digital Technologies (IC2SDT)*, 2024.

S. Xu, X. Song, Z. Xie, J. Cao, and J. Wang, "Secure transmission for energy harvesting relay networks with the destination self-protection mechanism," *Physical Communication*, vol. 40, p. 101075, Jan. 2020.

Y. Li et al., "Energy efficient relay selection and resource allocation in D2D-enabled mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15800-15814, Dec. 2020.

Q. Cai, J. Ma, B. Yao, X. Wu, and X. Xue, "A trade-off strategy and correlation analysis for secrecy rate and

power consumption in IRS-assisted cognitive radio networks," *Physical Communication*, vol. 61, p. 102220, May 2023.

T. N. Nguyen et al., "Security–Reliability Analysis of AF Full-Duplex Relay Networks Using Self-Energy Recycling and Deep Neural Networks," *Sensors*, vol. 23, no. 17, p. 7618, Sep. 2023.

D. Upadhyay, P. Tiwari, N. Mohd, and B. Pant, "Enhancement in the network capacity using MIMO and antenna array in 5G technology," in *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)*, Apr. 2022, pp. 12-17.

D. Upadhyay, P. Tiwari, N. Mohd, and B. Pant, "Capacity enhancement for cellular system using 5G technology, mmWave and higher order sectorization," in *2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT)*, Apr. 2022, pp. 422-427.

D. Upadhyay, A. Gupta, N. Mohd, and B. Pant, "A review of network slicing based 5G," in *AIP Conference Proceedings*, vol. 2782, no. 1, Jun. 2023.

V. Vimal et al., "Artificial intelligence-based novel scheme for location area planning in cellular networks," *Computational Intelligence*, vol. 37, no. 3, pp. 1338–1354, 2021, doi: 10.1111/coin.12371.

V. Vimal, M. J. Nigam, and H. Verma, "Route Assortment Procedure for Mobile Ad Hoc Networks using a Novel Modified Mobility Factor," in *2018 IEEE INDICON*, Dec. 2018, doi: 10.1109/INDICON.2017.8487811.