Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Enhancing Security and Privacy in 5G Device-to-Device Communication: A Grey Wolf Optimization Algorithm Approach

Dr. K. Nagi Reddy[1], G. Mounika[2], K. Deepika[3], M. Sasitha[4], A. Charisma[5],
[1]Assistant Professor, [2,3,4,5]UG Scholars, Department of ECE
[1,2,3,4,5]N.B.K.R Institute of Science and Technology, Vidyanagar, Tirupati District, Andhra Pradesh, India

***Abstract*—Device-to-Device (D2D) communication has emerged as a key technology in 5G networks, enabling direct data exchange between devices with reduced latency and improved spectral efficiency. However, the decentralized nature of D2D communication introduces significant security and privacy challenges, including interference, jamming, and unauthorized access. Conventional approaches, such as the Gale–Shapley algorithm, primarily focus on stable pairing and fail to optimize overall system performance in dynamic and adversarial environments.**

To overcome these limitations, this paper proposes a secure and efficient framework based on Grey Wolf Optimization (GWO) for optimal transmitter–receiver association in 5G D2D networks. The proposed approach formulates the pairing problem as a multi-objective optimization task, incorporating key parameters such as Signal-to-Interference-plus-Noise Ratio (SINR), transmission distance, energy efficiency, and jamming effects. Furthermore, an AI-based threat detection mechanism is integrated to enable real-time identification and mitigation of potential security threats.

Simulation results demonstrate that the proposed GWO-based framework significantly improves throughput, energy efficiency, and overall network security compared to conventional methods. Additionally, the inclusion of privacy-preserving key generation enhances secure data transmission, making the proposed system suitable for next-generation wireless communication environments.

***Index Terms*—5G networks, Device-to-Device communication, Grey Wolf Optimization, Security, Privacy, Multi-objective optimization, AI-based threat detection**

I. Introduction

The rapid evolution of wireless communication technologies has led to the widespread deployment of fifth-generation (5G) networks, which aim to provide ultra-low latency, high data rates, and massive device connectivity. One of the key enabling technologies in 5G is Device-to-Device (D2D) communication, which allows direct communication between nearby devices without relying on centralized infrastructure. This approach enhances spectral efficiency, reduces communication delay, and improves overall network performance, making it suitable for applications such as the Internet of Things (IoT), smart cities, and real-time services.

Despite its advantages, D2D communication introduces significant challenges, particularly in terms of security and interference management. The decentralized nature of D2D networks makes them vulnerable to various threats, including jamming, eavesdropping, and unauthorized access. Additionally, the presence of multiple transmitter–receiver pairs operating in close proximity leads to severe interference, which degrades signal quality and reduces system efficiency. Therefore, developing efficient and secure resource allocation mechanisms is essential for reliable D2D communication.

Traditional approaches for transmitter–receiver pairing, such as the Gale–Shapley algorithm, focus on achieving stable matching between devices. Although these methods ensure pairing stability, they do not consider multiple performance metrics simultaneously and are not well-suited for dynamic and adversarial environments. As a result, they fail to achieve optimal performance in terms of throughput, energy efficiency, and security.

To address these limitations, optimization-based approaches have gained significant attention. Among them, metaheuristic algorithms provide an effective way to solve complex optimization problems by exploring large search spaces. Grey Wolf Optimization (GWO), inspired by the social hierarchy and hunting behavior of grey wolves, is particularly suitable for multi-objective optimization tasks due to its balance between exploration and exploitation.

In this paper, a secure and efficient framework based on Grey Wolf Optimization is proposed for optimal transmit- ter–receiver pairing in 5G D2D networks. The proposed approach formulates the pairing process as a multi-objective optimization problem, considering parameters such as Signal-to-Interference-plus-Noise Ratio (SINR), transmission distance, energy efficiency, and jamming effects. Furthermore, an AI-based threat detection mechanism is integrated to identify potential security threats in real time and enhance system robustness.

Simulation results demonstrate that the proposed method significantly improves throughput, energy efficiency, and security compared to conventional approaches. The integration of optimization and artificial intelligence provides a scalable and reliable solution for secure D2D communication in next-generation wireless networks.

II. Literature Review

The rapid development of 5G wireless communication systems has significantly increased the demand for efficient and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

secure Device-to-Device (D2D) communication. D2D communication enables direct interaction between nearby devices, improving spectral efficiency, reducing latency, and offloading traffic from base stations. However, achieving efficient resource allocation and ensuring security in such decentralized environments remains a major challenge.

Boccardi *et al.* [1] explored key technological advancements shaping 5G networks, including massive multiple-input multiple-output (mMIMO), millimeter-wave (mmWave) communication, ultra-dense networks (UDN), and D2D communication. Their work highlights the importance of D2D communication in enhancing network capacity and reducing latency. Additionally, they emphasized the role of advanced interference management techniques in maintaining reliable communication in dense wireless environments. Despite these advancements, the study does not focus on security challenges associated with direct device communication.

Ding *et al.* [2] provided a comprehensive survey on non-orthogonal multiple access (NOMA), which is considered a promising technique for improving spectral efficiency in 5G systems. The authors discussed various NOMA schemes, including power-domain and code-domain approaches, and analyzed their advantages over traditional orthogonal multiple access techniques. While NOMA improves spectrum utilization and supports massive connectivity, it introduces challenges such as interference management, power allocation complexity, and security vulnerabilities. These challenges indicate the need for intelligent and adaptive resource allocation strategies.

Iqbal *et al.* [3] proposed a cognitive D2D-enabled relay selection algorithm (CDERSA) to address coverage issues and mitigate blind spots in 5G networks. The algorithm utilizes D2D-enabled devices as relays to improve connectivity and enhance network performance. The study demonstrated improvements in coverage probability, spectral efficiency, and energy efficiency. However, the proposed approach primarily focuses on performance enhancement and does not incorporate advanced security mechanisms to protect against potential cyber threats.

In another study, Iqbal *et al.* [4] investigated various spectral efficiency techniques for D2D communication in 5G networks. The authors analyzed different resource allocation strategies, power control mechanisms, and interference mitigation techniques. Their results showed that hybrid approaches combining multiple techniques can significantly improve network performance. However, the study also highlighted challenges related to scalability, dynamic adaptation, and computational complexity, particularly in dense network environments.

Seok *et al.* [5] introduced a lightweight cryptographic framework for securing D2D communication in 5G Internet of Things (IoT) networks. The proposed approach focuses on reducing computational overhead while maintaining strong security through efficient encryption mechanisms. The study demonstrated that lightweight cryptography can provide secure communication for resource-constrained devices. Nevertheless, the approach lacks adaptability to dynamic network conditions and does not consider multi-objective optimization involving performance and security parameters.

Overall, existing research primarily addresses individual aspects of D2D communication, such as spectral efficiency, resource allocation, or security, rather than providing a unified solution. Traditional approaches, including stable matching algorithms like Gale–Shapley, ensure pairing stability but fail to optimize system performance in dynamic and adversarial environments. Moreover, most existing methods do not incorporate real-time threat detection or adaptive optimization techniques.

To overcome these limitations, there is a need for an integrated framework that simultaneously considers performance optimization, interference management, and security enhancement. In this context, metaheuristic optimization algorithms have gained significant attention due to their ability to handle complex and multi-objective problems. This motivates the use of Grey Wolf Optimization (GWO), which provides an effective balance between exploration and exploitation, enabling efficient global optimization.

The proposed work builds upon these insights by integrating Grey Wolf Optimization with AI-based threat detection to develop a secure and efficient D2D communication framework. Unlike conventional methods, the proposed approach considers multiple parameters such as signal quality, interference, energy efficiency, and security simultaneously, thereby addressing the key limitations identified in existing literature.

III. Existing System

The existing system for resource allocation in 5G Device-to-Device (D2D) communication primarily relies on the Gale–Shapley (GS) algorithm, which is widely used for solv- ing stable matching problems. The algorithm ensures that transmitter–receiver pairs are formed in a stable manner, such that no two participants prefer each other over their assigned partners. This property of stability makes the algorithm suitable for applications in communication systems where consistent pairing is required.

In the context of D2D communication, transmitters and receivers are treated as two distinct sets of participants. Each transmitter maintains a preference list of receivers based on parameters such as signal strength, distance, and channel conditions, while receivers also rank transmitters according to their preferences. The algorithm operates iteratively, where transmitters propose to receivers in order of their preference, and receivers accept or reject proposals based on their own ranking criteria. This process continues until all devices are matched, resulting in a stable pairing configuration.

The existing system follows a structured workflow, as shown in Fig. 1. Initially, network parameters such as Signal-to-Noise Ratio (SNR) and transmission power are collected to evaluate communication conditions. Based on these parameters, the Gale–Shapley algorithm is applied to perform transmitter–receiver pairing. Subsequently, basic security mechanisms such as AI-based key generation and threat detection are incorporated to enhance communication security. Finally, the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

system performance is evaluated in terms of metrics such as throughput, energy efficiency, and reliability.

Although the Gale–Shapley algorithm provides stable matching, it has several limitations in practical D2D communication scenarios. The algorithm focuses only on stability and does not consider multiple performance metrics simultaneously. It assumes static preference lists and lacks adaptability to dynamic network conditions. Furthermore, it does not effectively handle interference, energy optimization, or advanced security threats, which are critical in modern 5G environments.

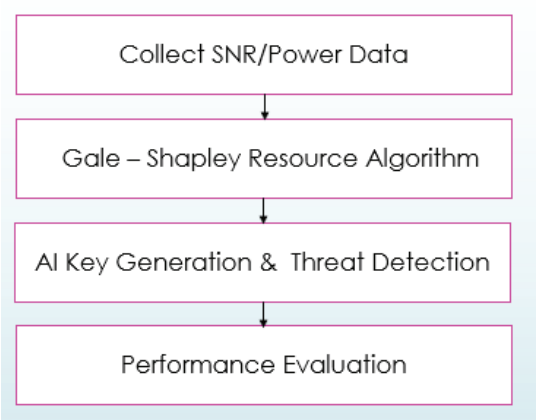

Fig. 1. Flow of Existing Method

A. Limitations of Existing System

- Limited to stability without achieving global optimality
- Inability to handle multi-objective optimization
- Poor adaptability to dynamic and adversarial environments
- Lack of integrated security and interference-aware mechanisms

IV. Proposed System

To overcome the limitations of traditional matching-based approaches, this paper proposes a secure and efficient framework based on Grey Wolf Optimization (GWO) for optimal transmitter–receiver pairing in 5G Device-to-Device (D2D) communication. Unlike conventional algorithms that focus only on stability, the proposed method aims to achieve global optimization by considering multiple performance and security parameters simultaneously.

The proposed system integrates optimization techniques, artificial intelligence, and security mechanisms to improve overall network performance. The workflow of the proposed method is illustrated in Fig. 2. Initially, the network is initialized by randomly distributing multiple transmitter–receiver pairs within a defined communication area. Key parameters such as Signal-to-Interference-plus-Noise Ratio (SINR), transmission power, distance between devices, path loss, and interference levels are calculated to model the communication environment accurately.

To enhance system security, an AI-based threat detection module is incorporated into the framework. This module analyzes network behavior and identifies potential threats in real time. Machine learning techniques are employed to process features such as SINR fluctuations, jamming patterns, transmission power variations, and channel conditions. Based on these features, the model classifies communication links as secure or compromised. The identified threats are then integrated into the optimization process, ensuring that insecure links are avoided during transmitter–receiver pairing.

The core component of the proposed system is the Grey Wolf Optimization algorithm, which is used to determine optimal transmitter–receiver associations. GWO is a nature-inspired metaheuristic algorithm based on the social hierarchy and cooperative hunting behavior of grey wolves. In this algorithm, candidate solutions are categorized into alpha, beta, delta, and omega wolves. The alpha wolf represents the best solution, followed by beta and delta wolves, which guide the search process, while the remaining wolves update their positions accordingly.

In the context of D2D communication, each wolf represents a possible transmitter–receiver pairing configuration. A multi-objective fitness function is designed to evaluate the quality of each solution. The fitness function incorporates multiple parameters, including SINR, transmission distance, energy efficiency, interference levels, and security constraints derived from threat detection. By combining these factors, the proposed approach ensures a balanced optimization of performance and security.

During each iteration, the positions of wolves are updated based on the influence of the alpha, beta, and delta wolves. This update mechanism enables the algorithm to explore the solution space efficiently while gradually converging toward optimal or near-optimal solutions. The balance between exploration and exploitation is controlled through adaptive parameters, which allow the algorithm to avoid premature convergence and local optima.

Furthermore, the proposed framework incorporates interference-aware and security-aware optimization strategies. By considering jamming effects and malicious activities within the fitness function, the system can dynamically avoid unreliable communication links. This significantly enhances the robustness of the network, particularly in adversarial environments where security threats are prevalent.

Another important aspect of the proposed system is its adaptability to dynamic network conditions. In real-world scenarios, network parameters such as user mobility, channel conditions, and interference levels change frequently. The optimization-based approach allows continuous updating of pairing decisions, ensuring consistent performance under varying conditions.

Finally, the optimized transmitter–receiver pairs are evaluated using performance metrics such as throughput, energy efficiency, latency, and security robustness. The results demonstrate that the proposed GWO-based framework significantly outperforms conventional Gale–Shapley-based approaches by

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

achieving better resource utilization, improved communication quality, and enhanced security.

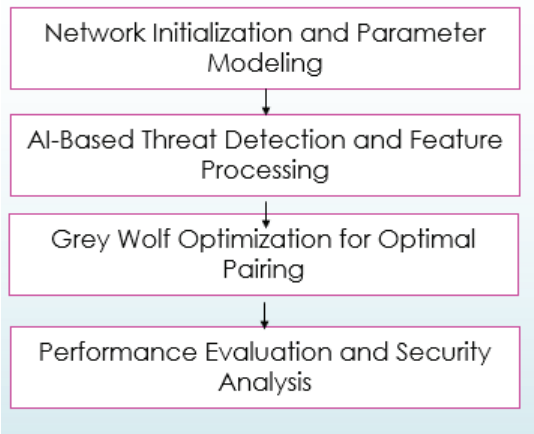

Fig. 2. Flow of Proposed Method

V. Advantages and Applications

A. Advantages

The proposed Grey Wolf Optimization (GWO)-based framework provides several significant advantages over traditional matching-based approaches in 5G Device-to-Device (D2D) communication systems. Unlike conventional methods that focus only on stable pairing, the proposed system enhances both performance and security through intelligent optimization.

One of the major advantages of the proposed system is enhanced security and threat resilience. By integrating AI-based threat detection, the system can identify malicious activities such as jamming, spoofing, and unauthorized access in real time. This enables the system to avoid compromised communication links, thereby improving overall network security and reliability.

Another key advantage is improved throughput and network efficiency. The optimization-based approach ensures effective resource allocation by selecting optimal transmitter–receiver pairs. This reduces interference and enhances signal quality, resulting in higher data transmission rates and better utilization of available network resources.

The proposed framework also supports multi-objective optimization, which is a significant improvement over traditional algorithms. In real-world communication systems, multiple factors such as Signal-to-Interference-plus-Noise Ratio (SINR), transmission distance, energy efficiency, and security must be considered simultaneously. The GWO algorithm effectively balances these parameters, leading to globally optimized solutions.

Furthermore, the system demonstrates strong adaptability to dynamic network conditions. In practical scenarios, factors such as user mobility, interference levels, and channel conditions continuously change. The proposed approach dynamically updates pairing decisions based on real-time conditions, ensuring consistent performance in highly dynamic environments.

In addition, the system exhibits robust performance under interference and jamming conditions. By incorporating interference and security parameters into the optimization process, the framework can effectively mitigate the impact of malicious attacks and maintain stable communication links.

Another important advantage is scalability. The proposed framework can efficiently handle a large number of devices without significant performance degradation. This makes it suitable for dense 5G and future 6G networks, where massive connectivity is required.

Overall, the proposed system provides a balanced combination of performance optimization, security enhancement, adaptability, and scalability, making it a reliable solution for next-generation wireless communication systems.

B. Applications

The proposed framework can be applied in various real-world 5G and next-generation communication scenarios:

- **5G and Beyond Wireless Networks:** Enables secure and efficient D2D communication for enhanced network performance and reduced latency.
- **Internet of Things (IoT):** Supports secure communication among connected devices in smart environments such as smart homes and smart cities.
- **Public Safety and Emergency Communication:** Provides reliable and secure communication in disaster scenarios where centralized infrastructure may not be available.
- **Industrial Automation:** Facilitates low-latency and secure communication in Industry 4.0 applications such as robotics and automated manufacturing.
- **Vehicular Communication Systems:** Enables secure and efficient communication between vehicles in intelligent transportation systems.

VI. Hardware and Software Requirements

A. Software Requirements

The implementation and evaluation of the proposed Grey Wolf Optimization (GWO)-based D2D communication framework are carried out using MATLAB R2022b. MATLAB provides a flexible and efficient environment for developing simulation models, implementing optimization algorithms, and visualizing system performance.

The software is utilized for modeling the D2D communication network, generating transmitter–receiver pairs, and simulating various network parameters such as Signal-to-Interference-plus-Noise Ratio (SINR), transmission power, and interference levels. Additionally, MATLAB is used to implement the Grey Wolf Optimization algorithm, where iterative updates are performed to obtain optimal pairing configurations.

The platform also supports data visualization tools that enable graphical representation of performance metrics such as throughput, latency, energy efficiency, and jamming effects. These capabilities make MATLAB a suitable choice for analyzing the effectiveness of the proposed system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

B. Hardware Requirements

The proposed system is implemented on a standard computing platform with moderate hardware specifications sufficient for simulation and data processing. The following hardware configuration is recommended to ensure smooth execution of the MATLAB environment and efficient simulation performance:

- **Processor:** Intel or AMD x86-64 processor with at least dual-core architecture (quad-core recommended for faster computation).
- **RAM:** Minimum 4 GB, with 8 GB or higher recommended for handling large datasets and multiple simulation iterations.
- **Storage:** Minimum 5 GB of available disk space for MATLAB installation and simulation files; SSD storage is preferred for improved performance.
- **Operating System:** Windows-based operating system compatible with MATLAB R2022b.

The above configuration ensures efficient execution of optimization algorithms, faster convergence during iterative processes, and smooth visualization of simulation results. The system is scalable and can be executed on higher-performance machines for large-scale network simulations.

VII. Results and Discussion

The performance of the proposed Grey Wolf Optimization (GWO)-based framework is evaluated using MATLAB simulations. The system is analyzed using key performance metrics such as Signal-to-Interference-plus-Noise Ratio (SNR), transmission power, distance, utility, jamming power, throughput, and latency. The results are compared with the conventional Gale–Shapley-based approach to demonstrate the effectiveness of the proposed method.

A. Threat Detection Analysis

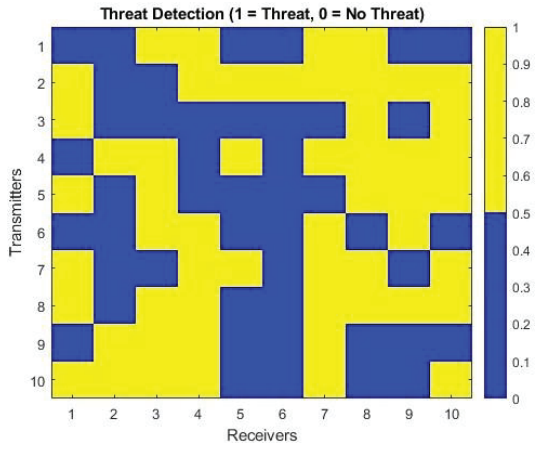

Fig. 3. Threat Detection Between Transmitters and Receivers

Fig. 3 shows the binary heatmap representation of threat detection. A value of '1' indicates the presence of a threat, while '0' represents a secure communication link. The results demonstrate that the system effectively identifies malicious links, allowing the optimization algorithm to avoid insecure connections.

B. Device and Attacker Distribution

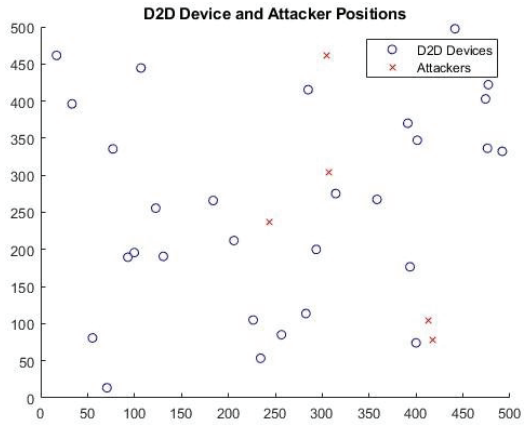

Fig. 4. D2D Device and Attacker Positions

Fig. 4 illustrates the spatial distribution of D2D devices and attackers. The presence of attackers introduces interference and security challenges, which are effectively handled by the proposed system through adaptive optimization and threat detection.

C. Threat Response Over Time

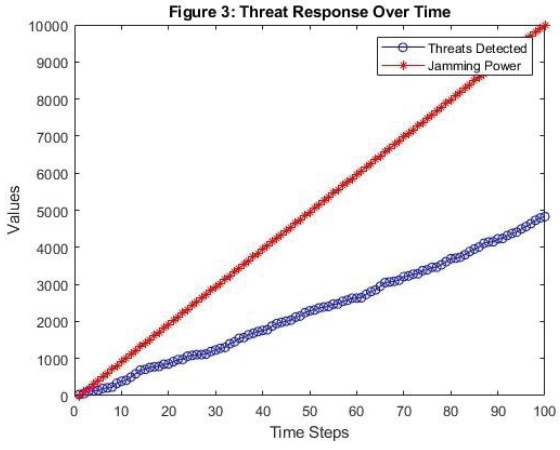

Fig. 5. Threat Response Over Time

Fig. 5 shows the variation of detected threats and jamming power over time. The system demonstrates consistent threat detection capability and adapts to increasing jamming conditions, ensuring stable network performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

D. Latency Analysis

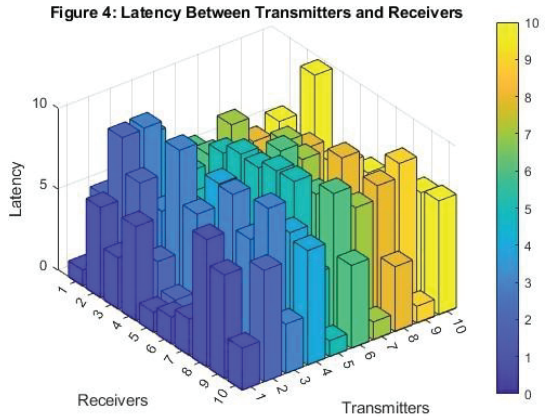

Fig. 6. Latency Between Transmitters and Receivers

Fig. 6 presents the latency between transmitters and receivers. The optimized pairing achieved through GWO reduces communication delays, resulting in improved responsiveness and efficiency.

E. Transmitter–Receiver Matching

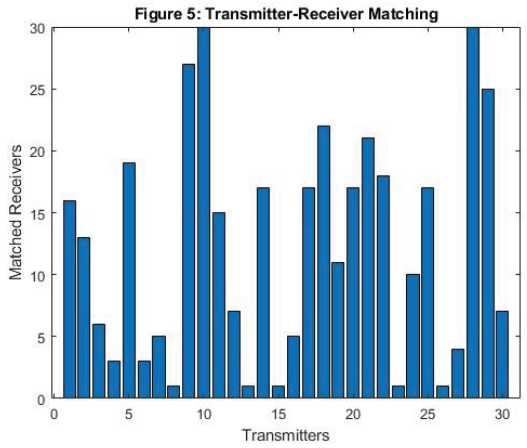

Fig. 7. Transmitter-Receiver Matching

Fig. 7 illustrates the optimized transmitter–receiver pairing. The proposed method ensures efficient allocation of communication links, improving network utilization compared to traditional approaches.

F. Energy Efficiency Analysis

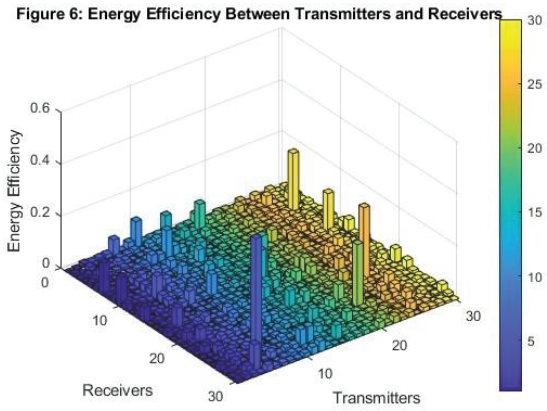

Fig. 8. Energy Efficiency Between Transmitters and Receivers

Fig. 8 shows the energy efficiency achieved by the proposed system. The optimization-based approach minimizes energy consumption while maintaining communication quality, making it suitable for large-scale networks.

G. Throughput Analysis

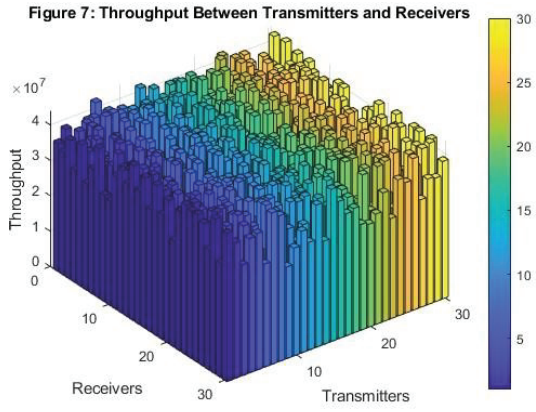

Fig. 9. Throughput Between Transmitters and Receivers

Fig. 9 illustrates the throughput performance of the system. The proposed method achieves higher data transmission rates due to efficient resource allocation and reduced interference.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

H. Detailed Threat Detection Analysis

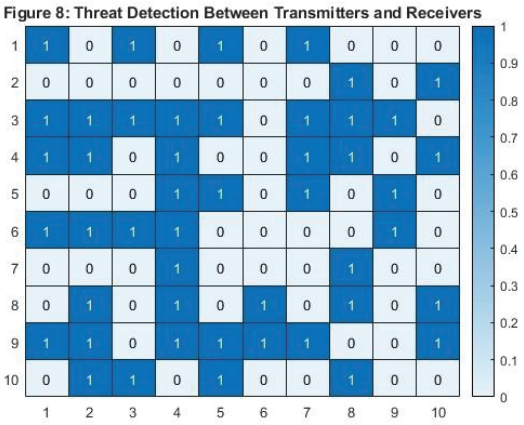

Fig. 10. Detailed Threat Detection Between Transmitters and Receivers

Fig. 10 provides a detailed matrix representation of threat detection across transmitter–receiver pairs. Each cell indicates whether a communication link is secure or compromised. The distribution of threats highlights the presence of potential vulnerabilities in the network. The proposed system effectively identifies these threats and incorporates this information into the optimization process, ensuring that secure communication links are prioritized during pairing. This enhances overall system reliability and security.

I. Jamming Power Analysis

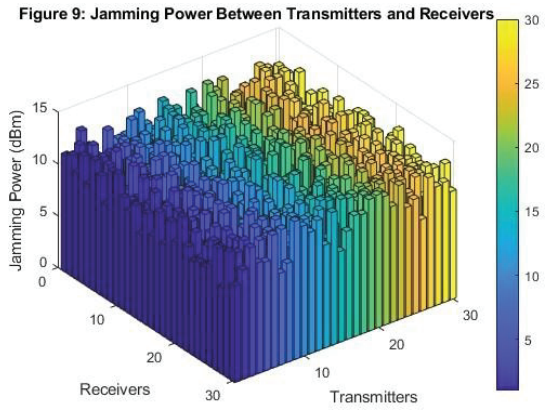

Fig. 11. Jamming Power Between Transmitters and Receivers

Fig. 11 represents the distribution of jamming power in the network. The proposed system effectively mitigates jamming effects by avoiding compromised communication links.

J. Performance Comparison

The comparison results indicate that the proposed GWO-based framework significantly improves network performance. The SNR increases from 12.3911 dB to 19.9969 dB, indicating better signal quality. Transmission power is reduced, leading to improved energy efficiency. The utility value is significantly enhanced, demonstrating better overall system performance. Additionally, jamming power is reduced, indicating improved resistance to interference. The throughput also shows a slight improvement, confirming efficient data transmission.

TABLE I
PERFORMANCE COMPARISON OF EXISTING AND PROPOSED SYSTEMS

Metric	Existing	Proposed
SNR (dB)	12.3911	19.9969
Transmission Power (dBm)	2.9814	1.0042
Distance (m)	252.1126	238.58
Utility	0.3644	0.75628
Jamming Power (dBm)	10.8696	8.3344
Throughput (Mbps)	3.65	3.68

Overall, the results demonstrate that the proposed system outperforms the traditional Gale–Shapley-based approach in terms of performance, efficiency, and security, making it a suitable solution for next-generation 5G D2D communication systems.

K. Discussion on Existing vs Proposed System

The comparison between the existing Gale–Shapley-based approach and the proposed Grey Wolf Optimization-based framework clearly demonstrates the superiority of the optimization-driven method. The existing system primarily focuses on achieving stable matching without considering multiple performance parameters, which limits its effectiveness in dynamic and interference-prone environments.

In contrast, the proposed system incorporates multi-objective optimization by simultaneously considering SINR, energy efficiency, distance, and security constraints. This results in a significant improvement in signal quality, as observed by the increase in SNR from 12.3911 dB to 19.9969 dB. Furthermore, the reduction in transmission power indicates improved energy efficiency, which is essential for large-scale communication systems.

The decrease in jamming power highlights the enhanced robustness of the proposed system against interference and malicious attacks. This improvement is achieved through the integration of AI-based threat detection and security-aware optimization. Additionally, the substantial increase in utility value reflects the overall enhancement in system performance. Although the throughput improvement is marginal, it confirms that the proposed approach maintains efficient data transmission while optimizing other critical parameters. Overall, the proposed Grey Wolf Optimization-based framework provides a more reliable, adaptive, and secure solution compared to the traditional Gale–Shapley algorithm.

VIII. CONCLUSION

This paper presents a secure and efficient framework for enhancing 5G Device-to-Device (D2D) communication by transitioning from traditional matching-based approaches to an optimization-driven model using Grey Wolf Optimization (GWO). Unlike the conventional Gale–Shapley algorithm,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

which focuses primarily on stable pairing, the proposed approach formulates the transmitter–receiver association problem as a multi-objective optimization task that simultaneously considers communication quality, interference, energy efficiency, and security.

The integration of AI-based threat detection enables the system to identify and mitigate potential security threats such as jamming and unauthorized access in real time. By incorporating security constraints into the optimization process, the proposed method ensures that only reliable communication links are selected. In addition, the inclusion of privacy-preserving mechanisms further enhances data security and confidentiality.

Simulation results demonstrate that the proposed GWO-based framework significantly improves key performance metrics, including Signal-to-Interference-plus-Noise Ratio (SNR), energy efficiency, utility, and resistance to jamming, while maintaining efficient throughput. The results confirm that the proposed system outperforms traditional Gale–Shapley-based approaches in both performance and security aspects.

Overall, the proposed framework provides a scalable, adaptive, and intelligent solution for next-generation wireless communication systems. It is well-suited for dynamic 5G environments and can be extended to future 6G networks and advanced communication scenarios.

REFERENCES

[1] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, Feb. 2014.

[2] Z. Ding *et al.*, "A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, Oct. 2017.

[3] A. Iqbal *et al.*, "CDERSA: Cognitive D2D enabled relay selection algorithm to mitigate blind-spots in 5G cellular networks," *IEEE Access*, vol. 9, pp. 89972–89988, 2021.

[4] J. Iqbal *et al.*, "Comparison of spectral efficiency techniques in device-to-device communication for 5G," *IEEE Access*, vol. 7, pp. 57440–57449, 2019.

[5] B. Seok *et al.*, "Secure D2D communication for 5G IoT network based on lightweight cryptography," *Applied Sciences*, vol. 10, no. 1, p. 217, 2019.

[6] R. Zhang *et al.*, "Resource allocation in D2D enabled cellular networks with fractional frequency reuse," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 8933–8946, 2016.

[7] T. Taleb *et al.*, "On multi-access edge computing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.

[8] C. Wang *et al.*, "Trustworthy health monitoring based on distributed wearable electronics with edge intelligence," *IEEE Transactions on Consumer Electronics*, 2024.

[9] L. Liu *et al.*, "Reputation management for consensus mechanism in vehicular edge metaverse," *IEEE JSAC*, 2023.

[10] J. G. Panicker *et al.*, "Authentication and access control in 5G D2D communication," in *Proc. IEEE TrustCom*, 2021.

[11] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6727–6740, 2014.

[12] D. Feng *et al.*, "Device-to-device communications underlaying cellular networks," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3541–3551, 2013.

[13] M. Hasan and E. Hossain, "Distributed resource allocation for relay-aided D2D communication," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2632–2646, 2014.

[14] Y. Sun, D. W. K. Ng, and R. Schober, "Optimal resource allocation for secure communication in D2D networks," *IEEE Transactions on Communications*, vol. 65, no. 12, pp. 5596–5610, 2017.

[15] S. Mumtaz *et al.*, "Cognitive D2D communication in 5G," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 22–28, 2014.

[16] M. Dorigo and T. Stutzle, "Ant colony optimization," *MIT Press*, 2004.

[17] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf Optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014.

[18] H. ElSawy *et al.*, "Modeling and analysis of cellular networks using stochastic geometry," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 167–203, 2017.

[19] Q. Wang *et al.*, "Machine learning for wireless networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3039–3071, 2018.

[20] Y. Li, M. Chen, and W. Saad, "Security in 5G and beyond networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 74–80, 2019.

[21] J. Wang *et al.*, "Deep learning for wireless communications," *IEEE Network*, vol. 32, no. 5, pp. 10–17, 2018.

[22] L. Xiao *et al.*, "Reinforcement learning for security in 5G networks," *IEEE Communications Magazine*, vol. 57, no. 4, pp. 76–81, 2019.

1. Dr. K.Nagi Reddy,M.Tech.,Ph.D
Professor & Head,Department of ECE(H0D)
N.B.K.R Institute of Science and Technology
Vidyanagar ,Andhra Pradesh ,India