

Presented by:

Engr. Rida Ashfaq

- BS Electronics Engineering, IIUI, Pakistan
- MS Information Security, NUST, Pakistan
- Member of NetMission.Asia

- **Certification:**
 - Accredited Professional Certification in ISO/IEC 27001:2022 Information Security Associate from SkillFront
 - Certification Course of Cybersecurity Essentials, CISCO Networking Academy
 - Certification Course of Cyber Security, Security Experts, Islamabad (Pakistan)
 - Certification Course of Internet of Things (IoT) System Development and Application, NuTech University, Islamabad (Pakistan)

- **Publication:**
 - "Smart Pillow: Sleep Apnea Monitoring & Minimization Device," 2019 7th International Conference on Robot Intelligence Technology and Applications (RiTA), 2019, pp. 215-219, doi: 10.1109/RITAPP.2019.8932822
<https://ieeexplore.ieee.org/document/8932822>



➤ **Work Experience:**

- Management Trainee Officer, One Network in FWO, Pakistan
- Management Trainee Officer, Pakistan Telecommunication Authority, Pakistan
- Internee at Siemens, Selected by GIZ (German Internationale Zusammenarbeit) through NAVTTC
- Intern in Rohde & Schwarz, Islamabad (Pakistan)
- Trainee on Radio Frequency Spectrum Management, Frequency Allocation Board

➤ **Email ID:** ridaashfaq2409@gmail.com

➤ **Linkdin:** www.linkedin.com/in/ridaashfaq/

➤ **Contact:** +92 3065261597

Agenda



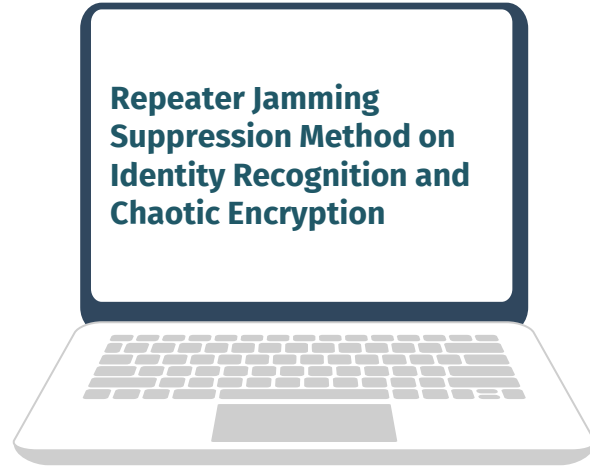
Introduction



Motivation



Literature Review



Repeater Jamming
Suppression Method on
Identity Recognition and
Chaotic Encryption

Proposed Solution



Relevance with
ICANN

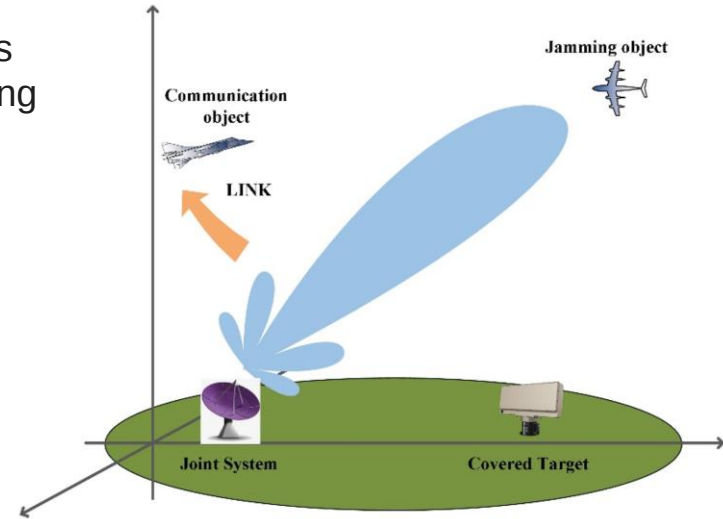
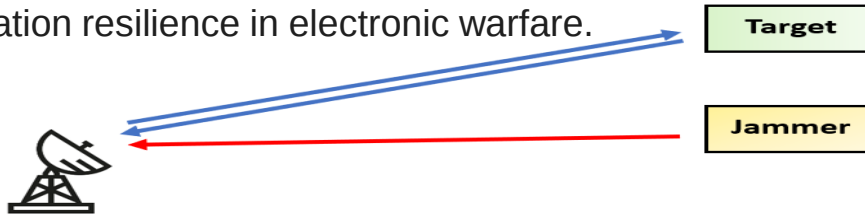


Reference



Introduction

- **Pulse Doppler fuzes** are essential in radar-guided systems due to their high resolution in detecting targets by measuring range and velocity.
- **Repeater jamming** is a technique where the enemy attempts to deceive the radar by retransmitting delayed signals, creating false targets.
- Repeater jamming exploits DRFM technologies to disrupt signals, posing severe challenges to PD fuze effectiveness.
- **Jamming Vulnerability:** The increasing sophistication of DRFM technology exacerbates the challenges posed by repeater jamming on PD fuzes.
- **Need for Anti-Jamming Strategies:** Modern conflicts necessitate effective anti-jamming strategies to ensure communication resilience in electronic warfare.



Comparison with Previous Work and Methods

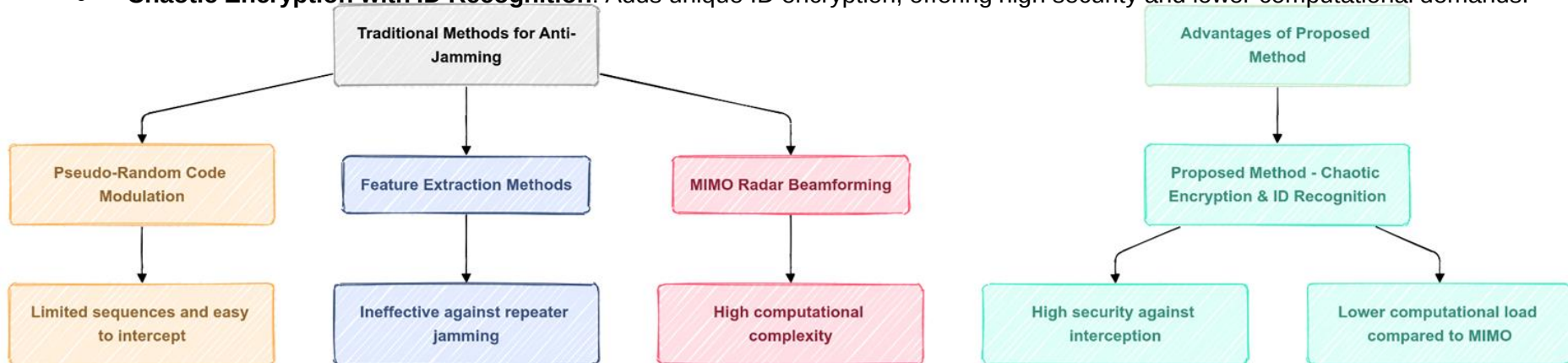
Traditional Methods:

- **Pseudo-Random Codes:** Limited in variety; easily intercepted by jammers.
- **Feature Extraction:** Struggles with repeater jamming.
- **MIMO Beamforming:** Effective but computationally heavy.

Challenges: These methods either lack effectiveness against repeater jamming or are too complex for real-time use.

Proposed Method:

- **Chaotic Encryption with ID Recognition:** Adds unique ID encryption, offering high security and lower computational demands.



Proposed Solution Overview

- **Novel Anti-Jamming Methodology:** This approach combines unique identity recognition and chaotic encryption to enhance PD fuze resilience.
- **Unique Fuze ID System:** Each fuze incorporates a unique ID encrypted through chaotic sequences, improving target signal differentiation.
- **Improved Signal Distinction:** Enhanced capability to distinguish genuine echoes from jamming attempts ensures better operational reliability.
- **Key Findings of Study:** Simulations demonstrate substantial improvements in jamming resistance, affirming the proposed method's effectiveness against threats.

Transmitted Signal Design

Fuze ID

Fuze ID:

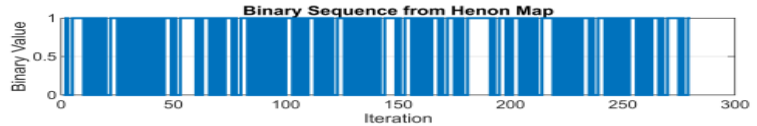
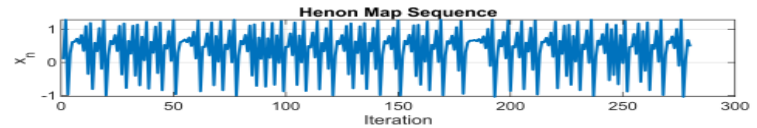
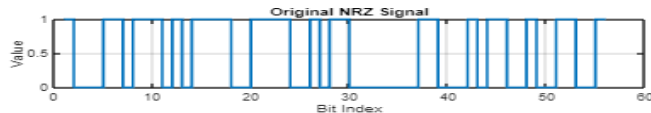
Fuze@123

Binary Representation:

1 0 0 0 1 1 0 1 1 1 0 1 0 1 1

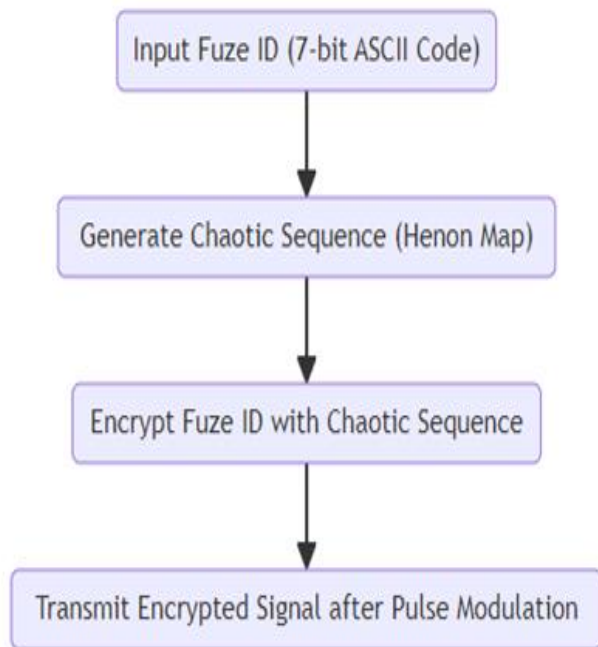
Convolution and Summation:

$$Y(t) = \sum_{m=0}^{7L-1} P_{EM}(t - m\tau_M) y_m \otimes \sum_{k=-\infty}^{\infty} \delta(t - 7KL\tau_M)$$

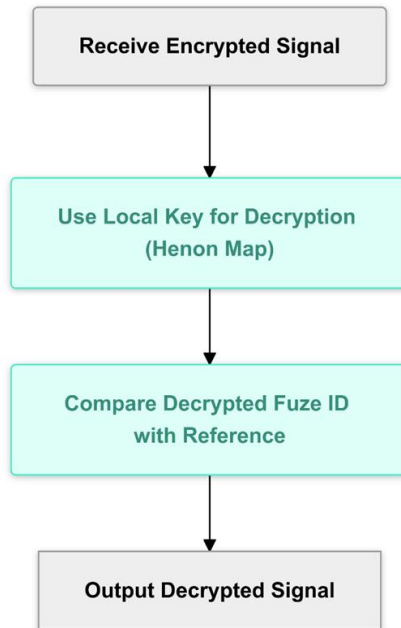


Solution Architecture

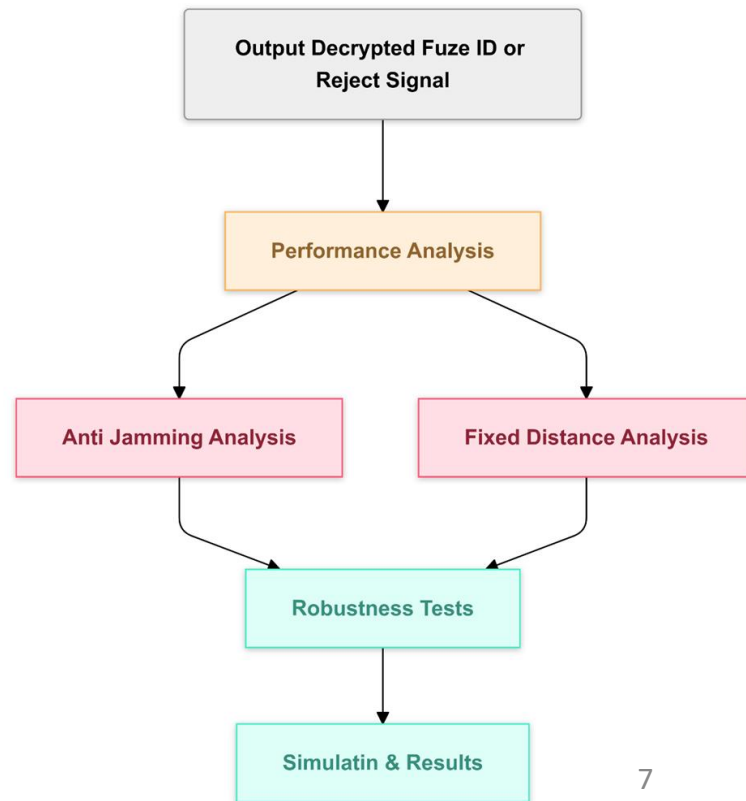
For Encryption



For Decryption

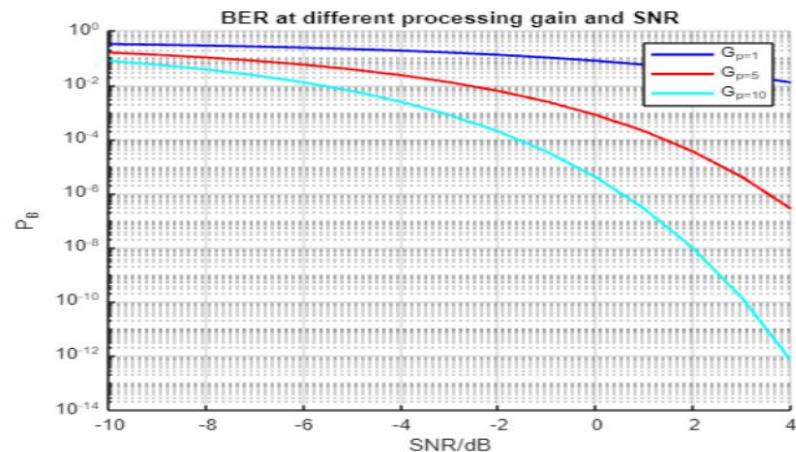
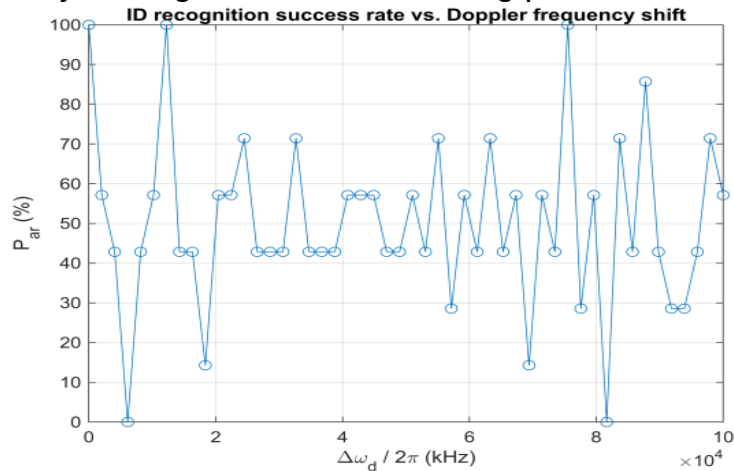


Security Enhancement

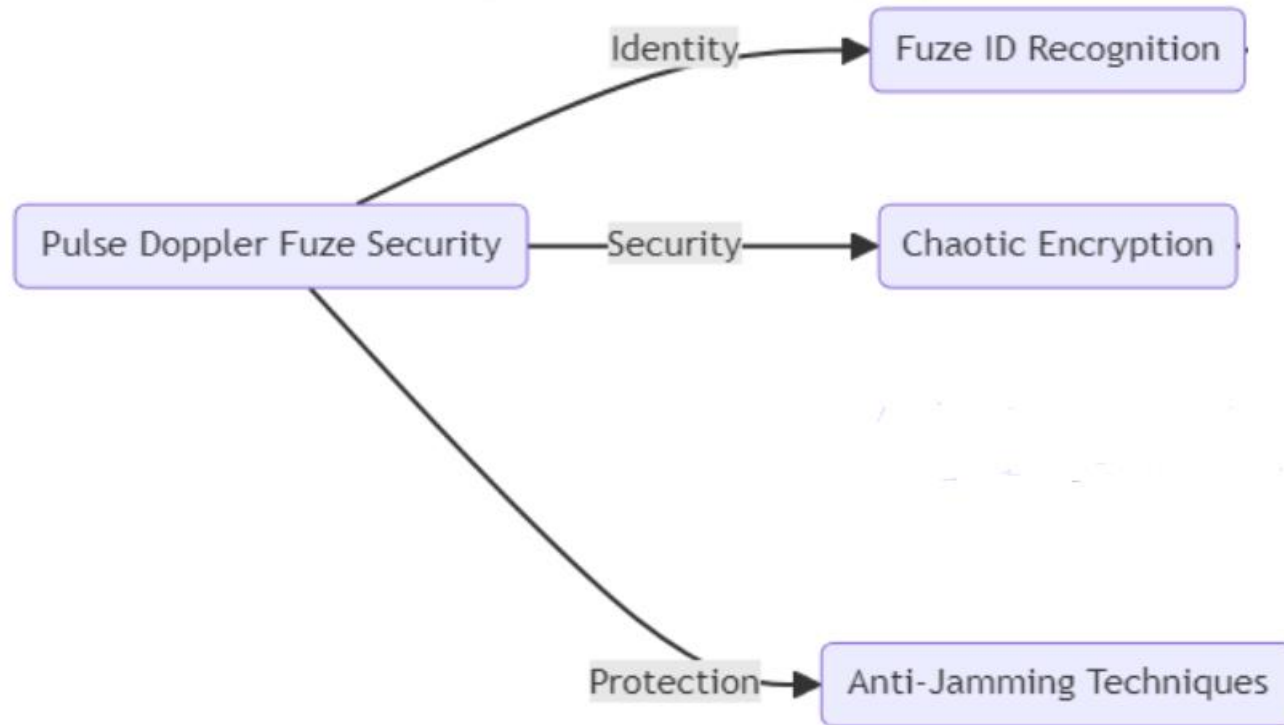


Robustness Testing & Simulation Results

- **Simulation Success Rates:** Results demonstrate over 90% anti-jamming performance across various SNR conditions, validating effectiveness.
- **Adaptive Response Mechanism:** The system adapts to changing jamming techniques, maintaining robustness even under low SNR scenarios.
- **Implications for Defense Applications:** Improved jamming resistance supports critical defense operations where reliable radar clarity is essential.
- **Simulation Performance Overview:** Simulation results indicate notable enhancements under varying jamming conditions, including power levels and Doppler frequency.



Flow Diagram of Pulse Doppler Fuze Security

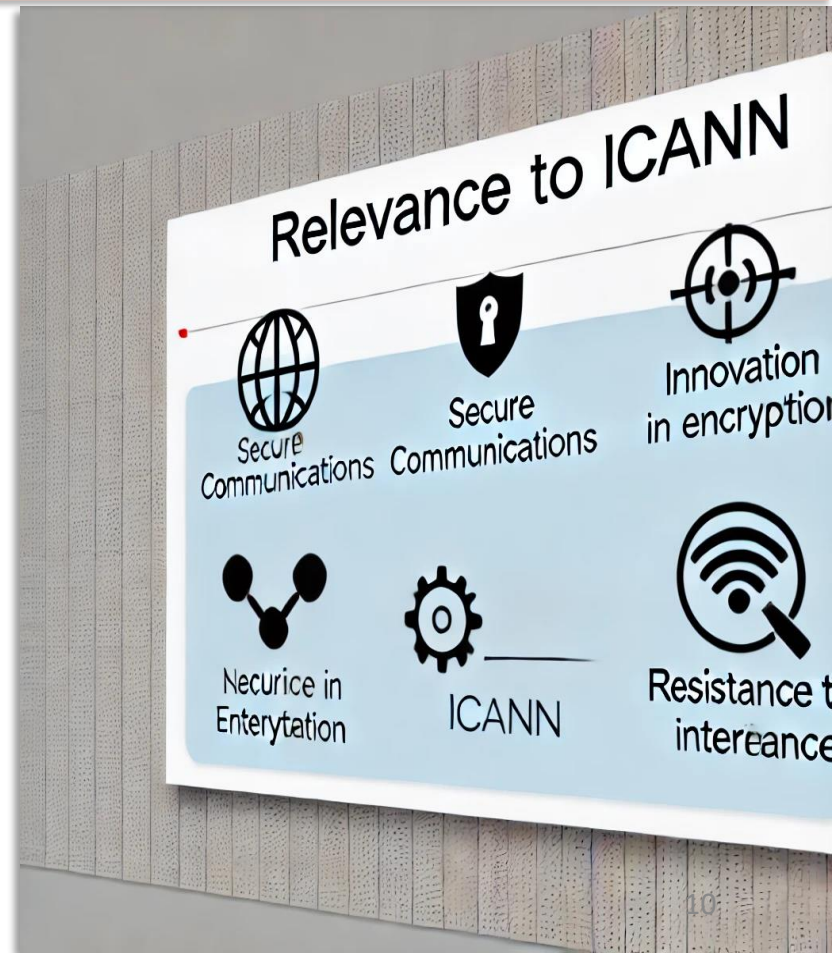


Relevance to ICANN

Potential Contributions to ICANN:

- a. **Strengthening Security Protocols:** Applying my expertise to enhance the security measures ICANN uses to protect DNS infrastructure.
- b. **Contributing to Policy on Internet Security:** Partnering with ICANN's security team to explore robust methods that mitigate threats against critical Internet infrastructures.
- c. Assisting in the creation of policies that emphasize the importance of **signal protection** and **encryption** in maintaining the security and stability of the Internet.
- d. **Promoting Encryption Standards:** Assisting in the development of robust encryption best practices to secure global digital communication

By integrating my background in **Information Security** with ICANN's mission to maintain a secure, stable, and interoperable Internet, I aim to contribute to safeguarding critical Internet resources and supporting secure global communication frameworks.



Acknowledgement and Way forward

Acknowledgement:

- Grateful to mentors, supervisor, and my institution for their support in advancing my encryption research.

Way Forward with ICANN:

- **DNS and Root Server Expertise:** Eager to expand my technical knowledge of DNS and root server operations.
- **DNSSEC Contribution:** Utilize my encryption background to enhance DNSSEC for greater DNS security and integrity.
- **IRI and APAC Initiatives:** Support ICANN's resilience initiatives, focusing on anti-jamming strategies for APAC root servers.
- **DNS Security Issues:** Work on identifying and mitigating DNS threats, contributing to ICANN's efforts in cyber defense.
- **Policy and Process Development:** Engage in ICANN's policy-making to advocate for robust DNS security protocols.

Reference

- Ali, S. Z. -e. -Z., Ashfaq, R., Afzal, R., Mehr-UN-Nisa, Sultan, B., & Jalil, A. (2019). *Smart Pillow: Sleep Apnea Monitoring & Minimization Device*. In 2019 7th International Conference on Robot Intelligence Technology and Applications (RiTA) (pp. 215-219). IEEE. <https://doi.org/10.1109/RITAPP.2019.8932822>
- NetMission.Asia. (n.d.). *Our team*. NetMission. <https://netmission.asia/our-team/>
- International Telecommunication Union (ITU). (2024). *Public consultation for the ITU 2024*. ITU. https://www.itu.int/en/SiteAssets/Lists/consultationFeb2024/AllItems/NMA_ITU%20public%20consultation%202024.pdf
- Youth Internet Governance Forum (YIGF). (n.d.). *YIGF 2024 fellows*. YIGF. <https://www.yigf.asia/yigf-2024-fellows.html>
- NetMission.Asia. (n.d.). *NetMission Ambassadors 2023-24*. NetMission. <https://netmission.asia/netmission-ambassadors-2023-24/>
- NetMission.Asia. (2023, December 1). *NetMission Academy 2024 result announcement*. NetMission. <https://netmission.asia/2023/12/01/netmission-academy-2024-result-announcement/>
- Germany in Pakistan [@GermanyinPAK]. (2020, December 9). *We're hiring! Please share this post and help us spread the word!* [Tweet]. X (formerly Twitter). <https://twitter.com/GermanyinPAK/status/1336715345760047106>



Thank you



Contact : +92 3065261597



Email : ridaashfaq2409@gmail.com



Linkdin : # <https://www.linkedin.com/in/ridaashfaq>