Anti In-Band Full-Duplex Interception For Wireless Tactical Networks

by

Van Huynh NGUYEN

THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT OF A MASTER'S DEGREE
WITH THESIS IN TELECOMMUNICATION NETWORKS
M.A.Sc.

MONTREAL, MAY 04, 2026

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

Prof. Kim Khoa Nguyen, Thesis supervisor
Department of Electrical Engineering, Ecole de technologie superieure

Prof. Wael Jaafar, Chair, Board of Examiners
Department of Software and IT Engineering, Ecole de technologie superieure

Prof. Richard Al Hadi, Member of the Jury
Department of Electrical Engineering, Ecole de technologie superieure

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND THE PUBLIC

ON APRIL 27, 2026

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, Professor Kim Khoa Nguyen, for giving me the opportunity to pursue my studies at ÉTS and for his invaluable guidance and support throughout my program. His direction in developing my academic thinking, problem-solving skills, and technical writing has been truly inspiring and will be greatly beneficial to my future work and studies.

I would also like to thank Mr. Van Hau Le, Mr. Minh Hai Dao, and my colleagues in the Synchromedia Lab for their support and for sharing valuable knowledge with me. During my research program, whenever I faced difficulties, they were always willing to help.

Last but not least, I sincerely thank my parents and my two little sisters for their love and encouragement over the years. Without them, none of what I have achieved would have been possible.

Anti-interception en bande, en duplex intégral, pour les réseaux tactiques sans fil

Van Huynh NGUYEN

RÉSUMÉ

Les réseaux véhiculaires tactiques ad hoc (TVAN) constituent un élément clé des communications militaires modernes, en permettant la coordination entre des entités très mobiles sur le champ de bataille telles que les véhicules de combat terrestres, les postes de commandement et les plateformes relais. Toutefois, la nature diffusée des transmissions sans fil rend les TVAN intrinsèquement vulnérables à l'interception et à l'écoute clandestine, en particulier face à des menaces avancées comme les intercepteurs en bande à duplex intégral (IBFD), capables de brouiller et d'intercepter simultanément les liaisons légitimes. En pratique, la protection anti-interception doit préserver une faible probabilité d'interception (LPI) tout en garantissant les exigences de qualité de service (QoS) des trafics critiques, sous des contraintes strictes de mobilité, de latence et d'énergie.

Cette thèse développe un cadre anti-interception inter-couches pour des TVAN basés sur le DS-CDMA en intégrant conjointement trois mécanismes de protection complémentaires : (i) une protection passive via l'adaptation des ressources de communication (p. ex., contrôle de puissance ou du facteur d'étalement), (ii) un brouillage coopératif actif visant à perturber les tentatives d'interception, et (iii) un brouillage/chiffrement de couche physique basé sur l'AES avec une longueur de clé adaptative afin d'équilibrer confidentialité, délai et consommation d'énergie.

Tout d'abord, une stratégie à double couche combinant l'adaptation passive des ressources et le brouillage coopératif est formulée comme un problème d'allocation conjointe des ressources impliquant la puissance d'émission, la puissance de brouillage et des paramètres liés à l'étalement, sous des contraintes de QoS et de LPI. Comme le problème résultant est non convexe et couplé par interférences, un référentiel d'optimisation efficace est établi à l'aide d'approximations tractables (dont une linéarisation de Taylor du premier ordre), d'une décomposition différence de convexes (DC) et d'une décomposition séquentielle/itérative, afin d'obtenir des solutions quasi optimales. Ensuite, le cadre est étendu à une conception à triple couche en intégrant le chiffrement adaptatif dans l'allocation des ressources. Pour quantifier l'impact conjoint des défenses de couche physique et du chiffrement, une métrique de performance de confidentialité tenant compte du chiffrement est utilisée, mettant en évidence les compromis entre résistance à l'interception, QoS, délai de chiffrement et coût énergétique. Bien que le référentiel d'optimisation fournisse des solutions de haute qualité, sa charge de calcul augmente avec la taille du réseau et la mobilité, ce qui limite son déploiement en temps réel.

Afin de permettre un fonctionnement quasi en temps réel, cette thèse propose également une solution assistée par apprentissage fondée sur l'apprentissage profond par renforcement multi-agents (MADRL) selon le paradigme d'entraînement centralisé et d'exécution décentralisée (CTDE). La formulation MADRL cible les dimensions de contrôle les plus coûteuses en calcul et apprend des politiques d'allocation des ressources qui approchent les performances

de l'optimisation avec un faible temps de calcul en ligne. Des simulations dans des conditions tactiques dynamiques montrent que les solutions proposées, basées sur l'optimisation et sur le MADRL, améliorent la protection LPI tout en maintenant la QoS plus efficacement que des références représentatives à une seule couche, tandis que l'approche MADRL permet une prise de décision rapide adaptée au fonctionnement des TVAN à forte mobilité.

Mots-clés: Réseaux véhiculaires tactiques ad hoc, faible probabilité d'interception, DS-CDMA, brouillage coopératif, chiffrement basé sur l'AES, optimisation inter-couches, programmation différence de convexes, apprentissage profond par renforcement multi-agents

Anti In-Band Full-Duplex Interception For Wireless Tactical Networks

Van Huynh NGUYEN

ABSTRACT

Tactical Vehicular Ad Hoc Networks (TVANs) are a key enabler of modern battlefield communications, supporting coordination among highly mobile entities such as ground combat vehicles, command posts, and relay platforms. However, the broadcast nature of wireless transmissions makes TVANs inherently vulnerable to interception and eavesdropping, especially under advanced threats such as in-band full-duplex (IBFD) interceptors that can simultaneously jam and intercept legitimate links. In practice, anti-interception protection must preserve low probability of interception (LPI) while still guaranteeing the quality-of-service (QoS) requirements of mission-critical traffic under stringent mobility, latency, and energy constraints.

This thesis develops a cross-layer anti-interception framework for DS-CDMA-based TVANs by jointly integrating three complementary protection mechanisms: (i) passive protection via communication resource adaptation (e.g., power or spreading control), (ii) active cooperative jamming to disrupt interception attempts, and (iii) AES-based physical-layer scrambling with adaptive key length to balance confidentiality, delay, and energy consumption.

First, a double-layer strategy combining passive resource adaptation and cooperative jamming is formulated as a joint resource allocation problem involving transmit power, jamming power, and spreading-related parameters under QoS and LPI constraints. Since the resulting problem is non-convex and interference-coupled, an efficient optimization-based benchmark is derived using tractable approximations, including first-order Taylor linearization, difference-of-convex (DC) decomposition, and sequential/iterative decomposition to obtain near-optimal solutions. Second, the framework is extended to a triple-layer design by incorporating adaptive encryption into the resource allocation. To quantify the joint impact of physical-layer defenses and encryption, an encryption-aware secrecy performance metric is employed, revealing the trade-offs among interception resistance, QoS, encryption delay, and energy cost. While the optimization benchmark provides high-quality solutions, its computational burden increases with network size and mobility, which limits real-time deployment.

To enable near real-time operation, this thesis further proposes a learning-assisted solution based on multi-agent deep reinforcement learning (MADRL) under a centralized training and decentralized execution (CTDE) paradigm. The MADRL formulation targets the most computationally intensive control dimensions and learns resource allocation policies that approximate optimization-quality performance with low online runtime. Simulations under dynamic tactical conditions demonstrate that the proposed optimization and MADRL solutions improve LPI protection and maintain QoS more effectively than representative single-layer baselines, while the MADRL approach achieves fast decision making suitable for high-mobility TVAN operation.

Keywords: Tactical vehicular ad hoc networks, low probability of interception, DS-CDMA, cooperative jamming, AES-based encryption, cross-layer optimization, difference-of-convex programming, multi-agent deep reinforcement learning

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

TVAN	Tactical Vehicular Ad Hoc Network
GCV	Ground Combat Vehicle
QoS	Quality of Service
LPI	Low Probability of Interception
IBFD	In-Band Full-Duplex
DS-CDMA	Direct-Sequence Code Division Multiple Access
PHY	Physical Layer
GPU	Graphics Processing Unit
FPGA	Field-Programmable Gate Array
TPU	Tensor Processing Unit
AES	Advanced Encryption Standard
DRL	Deep Reinforcement Learning
MADRL	Multi-Agent Deep Reinforcement Learning
CTDE	Centralized Training and Decentralized Execution
DC	Difference-of-Convex
MAC	Medium Access Control
RF	Radio Frequency
SINR	Signal-to-Interference-plus-Noise Ratio
UWAC	Underwater Acoustic Communication

UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network
IEEE	Institute of Electrical and Electronics Engineers
ICC	IEEE International Conference on Communications
WIN-T	Warfighter Information Network-Tactical
SU	Source User
DU	Defensive User
rBS	Relay Base Station
E2E	End-to-End
EVE	Eavesdropper
AWGN	Additive White Gaussian Noise
JA	Jamming Allocation
PA	Power Allocation
SA	Spreading Assignment
DDQN	Double Deep Q-Network
DF	Decode-and-Forward
MMSE	Minimum Mean Squared Error
AF	Amplify-and-Forward
NLOS	Non-Line-Of-Sight
LPD	Low Probability of Detection

CFAR	Constant False Alarm Rate
TTI	Transmission Time Interval
QPSK	Quadrature Phase Shift Keying
BPSK	Binary Phase Shift Keying
LFSR	Linear Feedback Shift Register
RAT	Radio Access Technology
LTE	Long Term Evolution
NR	New Radio
KA	Key-length Assignment
KKT	Karush–Kuhn–Tucker
MINLP	Mixed-Integer Nonlinear Programming

LIST OF SYMBOLS AND UNITS OF MEASUREMENTS

s	Second
ms	Millisecond
J	Joule
W	Watt
KHz	Kilohertz
Kbps	Kilobits per second
dB	Decibel
dBm	Decibel milliwatts
m	Meter
m^2	Meter Squared
km/m	Kilometer per meter
%	Percent

INTRODUCTION

Context and Motivation

Tactical Vehicular Ad Hoc Networks (TVANs) are a critical component of modern military communications, enabling reliable connectivity and information sharing among mobile battlefield entities such as ground combat vehicles (GCVs), command posts, and relay platforms. Unlike civilian cellular systems, TVANs must operate in contested spectrum with limited infrastructure, rapid topology changes, and strict mission-driven requirements. Due to the broadcast nature of wireless transmissions, any signal intended for legitimate users can also be observed by adversaries, which makes TVAN communications inherently vulnerable to interception and eavesdropping [Pirayesh & Zeng (2022)]. Therefore, practical TVAN deployments typically require self-defensive mechanisms that protect the network while still ensuring mission-critical quality-of-service (QoS) [Shi, Wang, Sellathurai, Zhou & Salous (2020)], [Le, Nguyen & Nguyen (2023a)], [Park, Wang & Alouini (2013)], [Zhong, Yao & Xu (2019)].

A key security requirement in such a strategy is Low Probability of Interception (LPI), which aims to reduce an adversary's ability to detect, identify, and intercept sensitive communications [Elmasry & Corwin (2021)]. To preserve LPI, existing approaches are commonly categorized into passive and active anti-interception techniques. Passive methods attempt to reduce exposure by controlling communication parameters such as transmit power [Shi *et al.* (2020)] or spreading factor [Le *et al.* (2023a)]. While effective for lowering detectability, these controls can directly degrade QoS because they reduce link reliability and throughput. Active methods introduce friendly jammers that transmit interference to confuse the interceptor and reduce its decoding capability [Park *et al.* (2013)], [Zhong *et al.* (2019)]; however, if not carefully coordinated, jamming may also harm legitimate receivers and lead to QoS degradation. As a result, prior single-layer designs based on only passive or only active protection may struggle to meet the stringent requirements of modern TVANs, especially against advanced threats such as in-band

full-duplex (IBFD) interception, where an eavesdropper can simultaneously jam legitimate links while intercepting confidential signals.

Beyond passive and active defenses, secure tactical communication also relies on long-term protection mechanisms from two complementary domains: physical-layer (PHY) security and cryptographic encryption. PHY security leverages wireless channel randomness and interference to limit an interceptor's decoding capability while maintaining reliable communication for legitimate users, whereas encryption protects information by transforming plaintext into ciphertext that can be recovered only with a secret key. However, conventional assumptions in these two domains are often misaligned in practice: PHY-security analysis frequently assumes plaintext transmission (i.e., no encryption), while encryption design often assumes error-free ciphertext reception (i.e., no PHY-layer impairments) [Sadig, Maleki, Tran & Bahrami (2020)]. In real systems, encryption can reduce the burden on PHY security because partial information leakage may be tolerable, and PHY-layer impairments can reduce cryptographic requirements by inducing errors in the interceptor's received ciphertext. This interdependence motivates a joint design in which encryption is treated as an adaptive layer rather than a fixed module. In particular, with modern hardware accelerators (e.g., Graphics Processing Units (GPUs), Field-Programmable Gate Arrays (FPGAs), TPUs (Tensor Processing Units)), dynamically selecting the encryption key length becomes feasible, enabling a practical trade-off among confidentiality, latency, and energy consumption. This motivates extending anti-interception strategies toward a triple-layer view that integrates passive LPI control, active cooperative defense, and Advanced Encryption Standard (AES)-based encryption in a unified design.

Although such triple-layer protection is promising, integrating these mechanisms creates a highly coupled resource allocation problem that is challenging for conventional control systems that rely heavily on traditional optimization approaches (e.g., solvers [Zhong *et al.* (2019)] or meta-heuristics [Conceição, Antunes, Gomes, Silva & Dinis (2022))]. In high-mobility scenarios,

the state and decision variables evolve quickly, and the time available for re-optimization becomes very limited; meanwhile, the computational complexity can grow sharply with the problem dimension. This motivates learning-assisted approaches, particularly deep reinforcement learning (DRL), which can provide near real-time decision making after offline training and can handle high-dimensional state and action spaces in dynamic wireless environments [Qi, Zhang, Qi & Peng (2024)], [Aref, Jayaweera & Machuzak (2017)], [Pourranjbar, Kaddoum, Ferdowsi & Saad (2021)]. Moreover, because TVAN protection is inherently multi-user and distributed, multi-agent DRL (MADRL) is attractive for scalability and coordination. Using the centralized training and decentralized execution (CTDE) paradigm, MADRL can learn cooperative policies that approximate optimization-quality solutions while enabling fast online execution in rapidly changing tactical conditions.

In summary, motivated by sophisticated interception threats, high mobility, and practical latency and energy constraints, this thesis develops a cross-layer anti-interception framework that jointly integrates passive LPI control, active cooperative defense, and adaptive AES-based encryption, supported by learning-assisted resource allocation for near real-time tactical operation.

Challenges

Designing anti-interception protection for TVANs is challenging because the system must simultaneously satisfy the QoS requirements of legitimate users while preserving LPI against sophisticated eavesdroppers, including advanced threats such as in-band full-duplex (IBFD) interception. In addition, high mobility, limited computation time, and encryption overhead further restrict feasible control decisions. The main challenges addressed in this thesis are:

- Trade-off: This thesis integrates three protection layers: passive LPI control, cooperative jamming, and AES-based encryption with adaptive key length. These mechanisms are strongly coupled. For example, stronger jamming can reduce interception but may degrade the SINR of legitimate users [Park *et al.* (2013); Zhong *et al.* (2019)]; reducing transmit power

or increasing spreading factors can improve LPI but may violate QoS constraints [Shi *et al.* (2020); Le *et al.* (2023a)]; and stronger encryption improves confidentiality but increases latency and energy consumption [Sadig *et al.* (2020)]. Therefore, designing each layer independently can be suboptimal and may lead to infeasible operation [Elmasry & Corwin (2021)].

- Reliability: Optimization-based methods can provide near-optimal QoS–LPI trade-offs, but they often require iterative updates and repeated sub-problem solving [Zhong *et al.* (2019); Conceição *et al.* (2022)]. In high-mobility TVANs, channel and interference conditions change quickly, so resource decisions must be updated within short time intervals. Many legacy LPI strategies were designed for lower-mobility cases and may not track these fast variations well, which can cause delayed or inaccurate updates and degrade defensive performance.
- Scalability: MADRL with CTDE can support fast online decisions in dynamic TVANs [Qi *et al.* (2024); Aref *et al.* (2017); Pourranjbar *et al.* (2021)], but scalability remains challenging. As the number of users grows, the state/action spaces and the coordination burden increase. Under high mobility, the available decision time becomes even shorter, making it harder to support many users when decisions must be updated frequently.

These challenges motivate the cross-layer optimization and the MADRL framework proposed in this thesis for practical anti-interception operation in modern tactical environments.

Research Question

Motivated by the above context and challenges, this thesis is guided by the following research question:

- **RQ.** Which cross-layer framework can jointly optimize passive LPI control, cooperative jamming, and adaptive AES-based encryption for DS-CDMA TVANs under QoS, latency, and

energy constraints, while enabling scalable near real-time decision making in high-mobility scenarios?

Objectives of the Thesis

The overall objective of this thesis is to develop a practical cross-layer anti-interception framework for tactical vehicular wireless networks that preserves LPI, guarantees QoS for legitimate users, and supports near real-time operation in highly dynamic and adversarial environments. To achieve this goal, the following sub-objectives (SOs) are defined:

- **SO1.** Design a unified architecture for DS-CDMA TVANs that integrates passive LPI control, cooperative jamming, and adaptive AES-based encryption to improve interception resistance while meeting QoS requirements.
- **SO2.** Formulate the joint resource allocation problem (transmit power, jamming power, and encryption key length) under QoS, LPI, and practical latency and energy constraints, and derive an efficient near-optimal solution using decomposition and tractable approximations (e.g., Taylor approximation and DC-based methods).
- **SO3.** Develop a MADRL solution under the CTDE paradigm to approximate the optimization benchmark with low online runtime, and evaluate its LPI and QoS performance under dynamic tactical conditions.

Thesis organization

This thesis is based on our publications. It is organized into an Introduction, three chapters, and a final chapter containing the Conclusion and Recommendations.

The Introduction establishes the research background and explains why new anti-interception strategies are needed for emerging tactical scenarios. It then presents the main challenges, research questions, and objectives that guide the thesis.

Chapter 1 provides a comprehensive literature review on anti-interception in tactical wireless networks. It summarizes passive LPI-oriented techniques, active cooperative-jamming defenses, and encryption-aware PHY security. The chapter then reviews optimization- and DRL-based methods for dynamic anti-interception, highlighting the scalability limitations of traditional optimization and motivating the MADRL framework adopted in this thesis.

Chapter 2 describes the overall thesis framework and presents the essential background that connects the literature review to the proposed methodologies.

Chapter 3 presents our proposed anti-interception framework in two parts. First, it develops a double-layered anti-interception strategy for ground combat vehicles. Second, it extends this study to a cross-layer design spanning the Medium Access Control (MAC), PHY, and Radio Frequency (RF) layers, resulting in a triple-layered anti-interception strategy for tactical wireless networks. The material in this chapter is adapted from our journal article published in *IEEE Transactions on Vehicular Technology (TVT)* in 2026 and from two conference papers published in the *IEEE International Conference on Communications (ICC)* in 2025 and 2026.

Chapter 4 summarizes the numerical results and provides detailed analyses for the scenarios studied in Chapters 3.

The Conclusion and Recommendation summarizes the main contributions of the thesis and outline potential improvements and directions for future research.

Journal and Conference Publications.

The main contributions of this thesis are reported in one journal paper, one submitted journal paper, and two conference papers:

- "Anti In-Band Full-Duplex Interception for Wireless Tactical Networks via Joint Passive Defense, Active Defense, and AES-Based Encryption," accepted for publication in *IEEE Transactions on Vehicular Technology (TVT)*, Apr. 2026.
- "Protecting Tactical Ground Combat Vehicles with Joint Active–Passive Anti-Interception Approach," submitted to *IEEE Transactions on Vehicular Technology (TVT)*, Mar. 2026.
- "Double-Layered Anti-Interception Strategy for Ground Combat Vehicles," published in the *IEEE International Conference on Communications (ICC)*, Jun. 2025 [Nguyen & Nguyen (2025)].
- "Triple-Layered Anti-Interception Security Framework for Ground Combat Vehicular Networks," accepted for publication in the *IEEE International Conference on Communications (ICC)*, May 2026.

CHAPTER 1

LITERATURE REVIEW

In this section, we review prior studies on anti-interception for tactical wireless networks from four complementary perspectives. First, we summarize passive LPI-oriented techniques (e.g., waveform, Signal-to-Interference-plus-Noise Ratio (SINR), power control) that aim to keep the transmitted energy below the eavesdropper's detection threshold. Second, we discuss active defenses based on cooperative jamming and artificial-noise transmission, highlighting both their secrecy benefits and their potential impact on legitimate links. Third, we survey encryption-aware PHY-security and AES-based scrambling approaches in DS-CDMA and related systems, which motivate our selectable key-length design to balance confidentiality, latency, and energy consumption. Fourth, we review optimization- and DRL-based methods for dynamic anti-interception problems, emphasizing the scalability limitations of traditional optimization in rapidly varying tactical environments and motivating our MADRL framework. Finally, we distinguish our work from existing literature and summarize the key differences in Table 1.1.

1.1 Passive anti-interception

Motivated by the comparison in Table 1.1, we begin with passive anti-interception techniques, which primarily focus on reducing the detectability of legitimate transmissions while maintaining reliable communication. Ensuring LPI is challenging because it is closely linked to other system factors such as waveform design, modulation type, and data rate, requiring careful design and technology integration. In a spread spectrum system, passive anti-interception techniques aim primarily to keep the signal's energy below a certain threshold. This can be achieved by controlling metrics such as the SINR or transmit power, which helps keep the signal's energy undetectable by eavesdroppers. By continuously monitoring channel conditions and adapting power levels, the system can maintain communication quality while reducing detectability. For example, in [Lu, Xu, Ren & Yi (2022)], LPI for moving airborne radar systems is ensured through a power consumption strategy that maintains the SINR of the suspicious link at a certain threshold

[Shi, Salous, Wang & Zhou (2016)] explore various waveform optimization criteria to minimize detectability by optimizing the multicarrier radar waveform with a set SINR constraint and a required minimum capacity for cellular communications. [Zhang, Chen, Jia & Wang (2024)] propose a power optimization method for frequency diverse array radar with a cooperative jammer, enhancing LPI capability while maintaining reliable performance. Similar approaches have been proposed for underwater acoustic communication (UWAC) systems, where a minimum SINR is determined to evade interception by energy detectors [Diamant, Lampe & Gamroth (2017)]. However, these methods often compromise communication performance, such as throughput or accuracy, when LPI performance is prioritized. Thus, tactical network administrators should strive to find effective solutions that balance the target LPI and QoS performance.

1.2 Active anti-interception

To further enhance the security of wireless communications, researchers have explored various active anti-interception mechanisms. Jamming is a proactive technique used to degrade the performance of eavesdroppers by adding interference to their channels. Cooperative jamming schemes, where legitimate users send jamming signals to confuse eavesdroppers, have been proven to improve both data security and transmission rates [Jameel, Wyne, Kaddoum & Duong (2019)]. In cooperative jamming, a collaborating node transmits a jamming signal to disrupt an eavesdropper's ability to intercept communications, directly targeting unauthorized listeners. As discussed in [Park *et al.* (2013)], the destination node can also act as a cooperating node by transmitting a jamming signal to deliver targeted interference. In [He, Ni, Chen, Yang & Lv (2019)], both the secrecy outage probability and the average secrecy rate are theoretically analyzed in a scenario where the destination transmits jamming noise to disrupt signal reception at an untrusted relay. In [Guo *et al.* (2019)], the authors focus on selecting the best intermediate node as the relay while utilizing the remaining nodes as friendly jammers to maximize the system's secrecy rate. The authors in [Bastami *et al.* (2021)] utilize unmanned aerial vehicle (UAV) cooperation to secure transmissions for legitimate users by simultaneously transmitting artificial noise to disrupt potential eavesdroppers while relaying confidential messages [Li, Zhang,

Rong & Han (2021)] investigate a relay-aided secure communication system that maximizes the expected secrecy rate by exploiting artificial noise transmitted by the source and relay nodes. One relay node forwards the intended message as a standard relay, while a second relay node serves as a helper to jam and disrupt the eavesdropper's ability to intercept the signal [Wang *et al.* (2017)]. However, transmitting jamming signals has certain disadvantages, such as interfering with legitimate receivers or degrading the main communication link. Therefore, tactical networks must carefully deploy active anti-interception mechanisms.

1.3 Encryption anti-interception

In standard DS-CDMA, the PHY is employed to counter eavesdroppers by leveraging the random nature of communication channels. This approach ensures that an eavesdropper cannot successfully decipher confidential messages while maintaining reliable transmission. On the other hand, encryption schemes are designed to remain secure even if eavesdroppers have full access to the ciphertext. Consequently, the joint design of encryption and PHY security schemes provides a flexible strategy for balancing system resources such as throughput, latency, and energy consumption while potentially enhancing the system's overall security. Toward this practical approach, [Zhang, Wang & Li (2013)] introduce an anti-jamming scheme based on the spread spectrum technique, using AES-generated secure ID sequences to combat disguised jamming, enhance signal extraction, and improve system efficiency with a multi-carrier extension. Similarly, [Song, Zhou & Li (2016)] analyze the impact of disguised jamming on CDMA systems and proposes AES-based secure scrambling to break signal-jammer symmetry and ensure positive channel capacity. In satellite networks, [Jeon, Kwak & Choi (2022)] propose CFB-AES-TURBO, a joint encryption and channel coding scheme that integrates AES and turbo coding to enhance both data security and error correction. Additionally, the anti-eavesdropping framework in [Sadig *et al.* (2020)] explore encryption-aware PHY security and employs the bisection method to optimize transmit power, aiming to maximize the secure transmission rate based on encryption strength. Building on these encryption-based anti-interception techniques, our study introduces the concept of a selectable key length for AES-based scrambling. This ensures that eavesdroppers

cannot successfully decipher confidential messages while also improving latency and reducing energy consumption at the PHY. Additionally, at the same time, we incorporate the passive anti-interception strategy designed to reduce the detection capabilities of eavesdroppers by optimizing the transmit power of users, while the active anti-interception strategy proactively counters potential interception attempts by emitting jamming signals. However, traditional optimization algorithms often struggle due to high complexity, rendering them impractical for real-world scenarios. Tactical environments are dynamic and require near real-time resource allocation. To address these limitations, we propose a learning-based approach in our work.

1.4 MADRL framework

Recently, MADRL has increasingly been applied in anti-interception scenarios where collaboration is key to achieving goals. In spread spectrum systems, agents must work together to optimize the overall anti-interception objective rather than individual aims. The design of the anti-interception strategy dictates how agents and their corresponding actions align with the system's components. For example, in [Qi *et al.* (2024)], the authors address probabilistic multi-channel jamming by proposing a deep Q-learning-assisted frequency-hopping strategy for wideband communication systems, achieving superior anti-jamming performance in dynamic environments without prior knowledge of jamming patterns. However, this study focuses solely on a single-user scenario, limiting its applicability to wireless sensor networks (WSNs) with multiple sensor nodes. The authors in [Aref *et al.* (2017)] expand the anti-jamming problem to include a multi-user scenario where each user employs an independent Q-learning algorithm to determine the optimal strategy for channel switching. A multi-user collaborative reinforcement learning-based anti-jamming strategy is proposed in [Pourranjbar *et al.* (2021)] to deceive jammers while optimizing channel selection and power allocation. Unlike previous studies that typically assign an agent to a single system element, such as a mobile user or a UAV, our research assigns multiple system elements, specifically a source, a destination, and a base station, to represent an agent. While this design may necessitate more collaboration between agents, it has the potential to align the actions taken by agents more closely with the optimal solution.

1.5 Proposed strategy versus prior works

Based on the above review, we compare our proposed anti-interception strategy with representative prior works in Table 1.1. Existing studies typically focus on one aspect of defense, such as passive LPI-oriented power/waveform control, active cooperative jamming, or encryption-aware PHY security, and they often treat the remaining mechanisms as fixed parameters. In contrast, our framework requires joint decision-making over three complementary types of control variables across layers: (i) passive LPI-oriented transmit controls (e.g., transmit power), (ii) active defense controls (e.g., jamming allocation), and (iii) adaptive AES-based encryption control via a selectable key length, which couples confidentiality with practical latency and energy constraints.

Moreover, while traditional optimization can achieve strong performance, its computational burden can be prohibitive in rapidly varying tactical environments. To address this, our approach integrates optimization and DRL in a complementary manner: the optimization model establishes a principled baseline and performance targets, whereas the MADRL framework enables fast, near real-time decision making once trained. As summarized in Table 1.1, this joint cross-layer design differentiates our work from prior literature and provides a practical balance between anti-interception performance and computational scalability.

Table 1.1 Literature review on anti-interception strategies

Literature	**Category**	**Technique**	**Approach**	**Military Scenario**
Lu *et al.* (2022)	Passive	Energy control	Optimization	Less-variant environment
Shi *et al.* (2016)	Passive	Waveform modulation	Optimization	Less-variant environment
Zhang *et al.* (2024)	Passive	Energy control	Optimization	Less-variant environment
Park *et al.* (2013) He *et al.* (2019) Guo *et al.* (2019)	Active	Power jamming	Optimization	Less-variant environment
Zhang *et al.* (2013)	Encryption	AES-generated ID sequences	Optimization	Less-variant environment
Song *et al.* (2016)	Encryption	AES-based secure scrambling	Optimization	Less-variant environment
Jeon *et al.* (2022)	Encryption	CFB-AES-TURBO	Optimization	Less-variant environment
Qi *et al.* (2024)	Passive	Hopping decision	DRL	Time-sensitive decision-making
Aref *et al.* (2017)	Passive	Channel switching	DRL	Time-sensitive decision-making
Pourranjbar *et al.* (2021)	Passive	Channel selection and power allocation	DRL	Time-sensitive decision-making
Our proposed strategy	Passive, Active and Encryption	Joint power, jamming and key length	Optimization and DRL	Time-sensitive decision-making

CHAPTER 2

METHODOLOGY

This chapter presents the methodology of our work, including (i) a double-layered anti-interception strategy for ground combat vehicles, adapted from our paper published in the *IEEE International Conference on Communications (ICC)* (2025), and (ii) a triple-layered anti-interception strategy for tactical wireless networks, adapted from our paper published in the *IEEE International Conference on Communications (ICC)* (2026) and an extended journal article published in *IEEE Transactions on Vehicular Technology (TVT)* (2026).

2.1 Double-Layered Anti-Interception Strategy for Ground Combat Vehicles

2.1.1 System Model

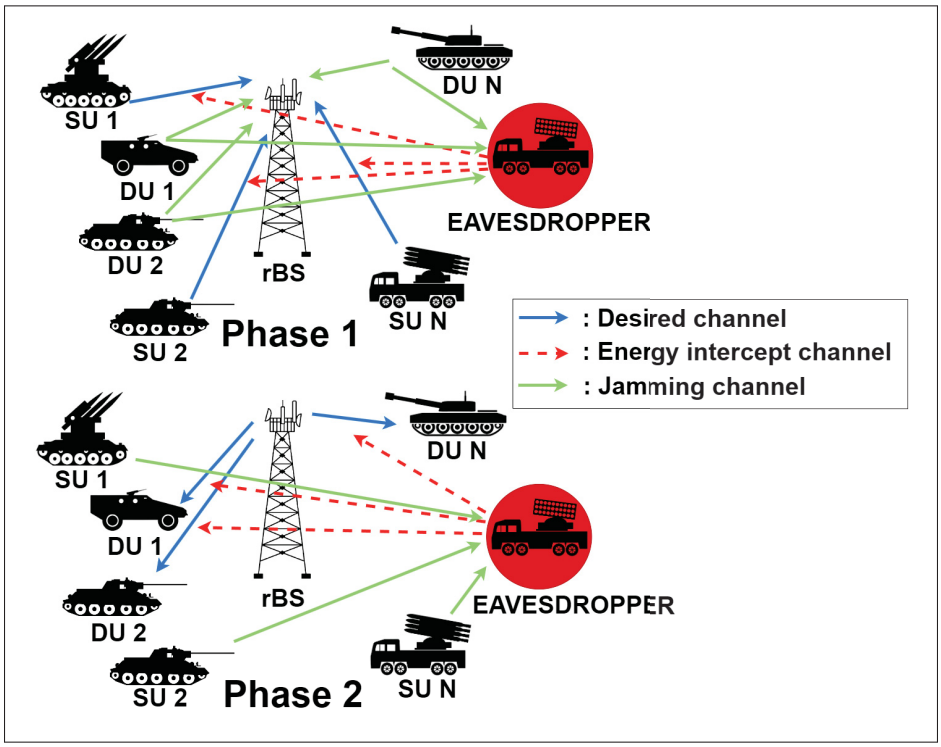

Figure 2.1 System model

Fig. 2.1 depicts a Warfighter Information Network-Tactical (WIN-T) configuration that employs DS-CDMA technology. The system consists of two transmission stages, including a set of source users (SUs) $\mathcal{S} = \{1, 2, ..., S\}$, a set of destination users (DUs) $\mathcal{J} = \{1, 2, ..., J\}$, and a relay base station (rBS). In this scenario, the users are GCVs, specifically designed for mobility, including tanks and missile-carrying trucks. Each GCV is equipped with a communication module and a jamming module, capable of broadcasting signals at maximum power levels denoted $P_{s,\max}$ and $PZ_{s,\max}$, respectively. Each SU is paired with a corresponding DU, creating a group of End-to-End (E2E) communication links $C = \{1, 2, \ldots, C\}$. These communication links are established only via rBS. The rBS has multiple communication interfaces, represented by the set $\mathcal{B} = \{1, 2, \ldots, B\}$. Each interface $b \in \mathcal{B}$ serves a dual purpose: it receives data from a specific SU s and transmits data to a corresponding DU j.

We propose a double-layered anti-interception mechanism for a dual-stage relay network, where both SUs and DUs transmit jamming signals in two distinct phases to disrupt the eavesdropper (EVE). In phase 1, SU s transmits a data signal with transmit power $p_{c,s}^{(t)}$, while DU j transmits a jamming signal with jamming transmit power $pz_{c,j}^{(t)}$. The channel is modeled as an Additive White Gaussian Noise (AWGN) distribution with a free-space path loss factor of $\alpha = 2$. According to [Suard, Naguib, Xu & Paulraj (1993)], at time slot t, the received SINR of the standard CDMA system for channels between SU s and rBS b, and SU s and EVE u belonging to E2E connection c, can be determined by

$$\gamma_{c,s,b}^{(t)} = \frac{m_{c,s}^{(t)}.G_{c,s,b}^{(t)}.p_{c,s}^{(t)}}{\sigma^2 + \sum_{k\neq s} G_{c,k,b}^{(t)}.p_{c,k}^{(t)} + \sum_{j\in\mathcal{J}} G_{c,j,b}^{(t)}.pz_{c,j}^{(t)}}, \tag{2.1}$$

$$\gamma_{c,s,u}^{(t)} = \frac{m_{c,s}^{(t)}.G_{c,s,u}^{(t)}.p_{c,s}^{(t)}}{\sigma^2 + \sum_{k\neq s} G_{c,k,u}^{(t)}.p_{c,k}^{(t)} + \sum_{j\in\mathcal{J}} G_{c,j,u}^{(t)}.pz_{c,j}^{(t)}}, \tag{2.2}$$

where $G_{c,x,y}^{(t)} = \left(d_{c,x,y}^{(t)}\right)^{-\alpha}$, with $d_{c,x,y}^{(t)}$ representing the channel gain and the distance between transmitter x and receiver y, respectively, $m_{c,s}^{(t)}$ is the spreading factor of the SU s, $p_{c,s}^{(t)}$ is the transmit power of the SU s, $p_{c,k}^{(t)}$ is the transmit power of interfering transmitter k, $pz_{c,l}^{(t)}$ is the

jamming transmit power of the DU j, all belonging to E2E connection c at time slot t, and σ^2 is the noise power. In phase 2, rBS b amplifies and forwards its received signal to DU j with transmit power $p_{c,b}^{(t)}$ while SU s transmits a jamming signal with jamming transmit power $pz_{c,s}^{(t)}$. In this article, we assume that DUs, knowing SUs' jamming signals, perfectly cancel the jamming signals from SUs. Therefore, the received SINR at DU j belonging to E2E connection c at time slot t is given by

$$\gamma_{c,b,j}^{(t)} = \frac{m_{c,b}^{(t)}.G_{c,b,j}^{(t)}.p_{c,b}^{(t)}}{\sigma^2 + \sum_{k\neq b} G_{c,k,j}^{(t)}.p_{c,k}^{(t)}}. \tag{2.3}$$

Meanwhile, EVE u combines the two signals: the desired signal from rBS b and the jamming signal from SU s. After selection combining, the received SINR at EVE u belonging to E2E connection c at time slot t can be formulated as

$$\gamma_{c,b,u}^{(t)} = \frac{m_{c,b}^{(t)}.G_{c,b,u}^{(t)}.p_{c,b}^{(t)}}{\sigma^2 + \sum_{k\neq b} G_{c,k,u}^{(t)}.p_{c,k}^{(t)} + \sum_{s\in\mathcal{S}} G_{c,s,u}^{(t)}.pz_{c,s}^{(t)}}, \tag{2.4}$$

where $m_{c,b}^{(t)}$ is the spreading factor of the rBS b, $p_{c,b}^{(t)}$ is the transmit power of the rBS b, $pz_{c,s}^{(t)}$ is the jamming transmit power of SU s, all belonging to E2E connection c at time slot t. The radar system assumes that the users know the eavesdropper's location, allowing them to estimate the signal strength received by the eavesdropper. In this scenario, the eavesdropper can use an energy-based detection technique, which allows it to detect intercepted signals from SUs and the rBS based on the amplitude of the SINR value.

In our WIN-T system, the SUs, rBS, and DUs must cooperate to transmit jamming and desired signals that meet two key requirements. First, the EVE must receive SINR values in both transmission phases that are below the detection threshold μ, and second, the SINR at the desired receivers (DUs and rBS) must exceed the decoding threshold $\gamma_{\min}$ to maintain an acceptable outage probability. The constraints for our system during the two transmission phases can be

represented as

$$\gamma_{c,s,u}^{(t)} \leq \mu, \quad \gamma_{c,b,u}^{(t)} \leq \mu, \quad \gamma_{c,s,b}^{(t)} \geq \gamma_{\min}, \quad \gamma_{c,b,j}^{(t)} \geq \gamma_{\min}. \tag{2.5}$$

For example, the LPI capacity of many state-of-the-art systems is considered secure when the intercept SINR remains below -8dB, while the desired SINR stays above -14 dB [Diamant & Lampe (2018)].

2.1.2 Problem Formulation

Given the mobility of GCV users, balancing LPI capability with QoS becomes a significant challenge. To address this, we formulate an optimization problem that focuses on conserving LPI while maximizing transmission rates through jamming allocation, power control, and spreading factor assignment schemes. This problem is mathematically expressed as

$$\begin{aligned}
(\mathcal{P}_1) \quad & \max_{pz_s, pz_j, p_s, p_b, m_s, m_b} \sum_{c \in C} \min\left(\tau_{c,s,b}^{(t)}, \tau_{c,b,j}^{(t)}\right) \\
\text{s.t.} \quad & (\text{C1}) : \gamma_{c,s,u}^{(t)} \leq \mu, \qquad (\text{C2}) : \gamma_{c,b,u}^{(t)} \leq \mu, \\
& (\text{C3}) : \gamma_{c,s,b}^{(t)} \geq \gamma_{\min}, \qquad (\text{C4}) : \gamma_{c,b,j}^{(t)} \geq \gamma_{\min}, \\
& (\text{C5}) : p_{c,s}^{(t)} \leq P_{s,\max}, \qquad (\text{C6}) : \sum_{c \in C} p_{c,b}^{(t)} \leq P_{b,\max}, \\
& (\text{C7}) : pz_{c,s}^{(t)} \leq PZ_{s,\max}, \qquad (\text{C8}) : pz_{c,j}^{(t)} \leq PZ_{j,\max}, \\
& (\text{C9}) : m_{c,s}^{(t)} \leq M_{s,\max}, \qquad (\text{C10}) : m_{c,b}^{(t)} \leq M_{b,\max}.
\end{aligned} \tag{2.6}$$

where $pz_s = \{pz_{c,s}\}$, $pz_j = \{pz_{c,j}\}$, $p_s = \{p_{c,s}\}$, $p_b = \{p_{c,b}\}$, $m_s = \{m_{c,s}\}$, $m_b = \{m_{c,b}\}$, $\forall c \in C$.

The objective function is to maximize the total transmission rate of all E2E connections at each time slot t. The transmission rate of each link from transmitter x and receiver y belonging to E2E connection c at time slot t is defined as $\tau_{c,x,y}^{(t)} = W_0 \log_2\left(1 + \gamma_{c,x,y}^{(t)}\right)$. W_0 is the original signal bandwidth. Constraint (C1) ensures that the SINR at the eavesdropper, denoted by $\gamma_{c,s,u}^{(t)}$

Algorithm 2.1 The iterative algorithm for problem $\mathcal{P}_1$

1: **initialize:** Init values for $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, $m_{c,s}^{(i)}$, $m_{c,b}^{(i)}$;
   Set counter $i = 0$, $i_{\max} = 10^6$, coverage tolerance $\omega = 10^{-3}$
2: **repeat**
3: Solve $(\mathcal{JA})$ with fixed $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, $m_{c,s}^{(i)}$, $m_{c,b}^{(i)}$, obtain $pz_{c,s}^{*}$ and $pz_{c,j}^{*}$, update $pz_{c,s}^{(i)} = pz_{c,s}^{*}$ and $pz_{c,j}^{(i)} = pz_{c,j}^{*}$
4: Solve $(\mathcal{PA})$ with fixed $m_{c,s}^{(i)}$, $m_{c,b}^{(i)}$, $pz_{c,s}^{(i)}$, $pz_{c,j}^{(i)}$, obtain $p_{c,s}^{*}$ and $p_{c,b}^{*}$, update $p_{c,s}^{(i)} = p_{c,s}^{*}$ and $p_{c,b}^{(i)} = p_{c,b}^{*}$
5: Solve $(\mathcal{SA})$ with fixed $pz_{c,s}^{(i)}$, $pz_{c,j}^{(i)}$, $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, obtain $m_{c,s}^{*}$ and $m_{c,b}^{*}$, update $m_{c,s}^{(i)} = m_{c,s}^{*}$ and $m_{c,b}^{(i)} = m_{c,b}^{*}$
6: $i = i + 1$
7: **until** $\sum_{c} \left(\left| pz_{c,s}^{(i)} - pz_{c,s}^{(i+1)} \right| + \left| pz_{c,j}^{(i)} - pz_{c,j}^{(i+1)} \right| \right) \leq \omega$ or $i \geq i_{\max}$
8: **return** $pz_{c,s}^{*}$, $pz_{c,j}^{*}$, $p_{c,s}^{*}$, $p_{c,b}^{*}$, $m_{c,s}^{*}$, $m_{c,b}^{*}$.

is lower than an energy detection threshold μ during phase 1. The same constraint (C2) applies in phase 2. For the rBS and DU to accurately detect the desired signals, the measured SINR values at these receivers must be above a certain threshold. The requirements are enforced by constraints (C3) and (C4). Constraints (C5), (C6), (C9), and (C10) specify the maximum transmit power and spreading factor levels for each SU and the rBS, while constraints (C7) and (C8) limit the maximum jamming transmit power levels for each SU and DU.

Problem $(\mathcal{P}_1)$ is a non-convex optimization problem due to the presence of a logarithm of a fractional function in the objective function. To address this, the objective function is first decomposed into three sub-problems, Jamming Allocation $(\mathcal{JA})$, Power Allocation $(\mathcal{PA})$, and Spreading Assignment $(\mathcal{SA})$. These sub-problems are then solved sequentially. As outlined in Algorithm 2.1, $\mathcal{JA}$ is solved with fixed transmit power and spreading factors. The optimal jamming power levels, pz_s^{*} and pz_j^{*}, are used to solve the power allocation sub-problem $\mathcal{PA}$, while keeping spreading factors fixed. The optimal jamming and transmit power values from $\mathcal{JA}$ and $\mathcal{PA}$ are then used to solve the spreading assignment sub-problem $\mathcal{SA}$. The algorithm iterates until consecutive $\mathcal{JA}$ solutions converge within a tolerance ω or the maximum number

of iterations $i_{\max}$ is reached. It outputs optimal jamming power, transmit power, and spreading factors for each time slot t.

2.1.2.1 Active Anti-Interception: Jamming Power Allocation

We consider $pz_{c,s}$ and $pz_{c,j}$ as variables while holding $p_{c,s}$, $p_{c,b}$, $m_{c,s}$, and $m_{c,b}$ constant in problem $\mathcal{P}_1$. Consequently, the sub-problem $\mathcal{JA}$ is expressed as

$$\begin{aligned} (\mathcal{JA}) \quad & \max_{pz_s,\, pz_j} \sum_{c\in C} \min\left(\tau^{(t)}_{c,s,b}, \tau^{(t)}_{c,b,j}\right) \\ \text{s.t.} \quad & \text{(C1), (C2), (C3), (C7), (C8).} \end{aligned} \tag{2.7}$$

The transformed problem $\mathcal{JA}$ is a non-convex optimization problem due to the inclusion of the logarithm of a fractional function in the objective function. To address this, the function $\tau^{(t)}_{c,s,b}(pz)$ is first rewritten in a DC function form as follows

$$\tau^{(t)}_{s,b}(pz) = W_0 \log_2(1+\gamma^{(t)}_{s,b}(pz)) = -[U(pz) - V(pz)], \quad \text{where} \tag{2.8}$$

$$U(pz) = -W_0 \log_2(\sigma^2 + \sum_{k\neq s} G^{(t)}_{k,b}.p^{(t)}_k + \sum_{j\in\mathcal{J}} G^{(t)}_{j,b}.pz^{(t)}_j + m^{(t)}_s.G^{(t)}_{s,b}.p^{(t)}_s), \tag{2.9}$$

$$V(pz) = -W_0 \log_2(\sigma^2 + \sum_{k\neq s} G^{(t)}_{k,b}.p^{(t)}_k + \sum_{j\in\mathcal{J}} G^{(t)}_{j,b}.pz^{(t)}_j). \tag{2.10}$$

Although both functions $U(pz)$ and $V(pz)$ are convex, (2.8) remains non-convex because of the negative sign before $V(pz)$. Next, we use the first-order Taylor expansion to linearize the terms $V(pz)$. Linearizing will convexify the objective function. As a result, $\tau^{(t)}_{s,b}(pz)$ is approximated as

$$\tau^{(t)}_{s,b}(pz) \triangleq -[U(pz) - V(pz') - \nabla V(pz')^T(pz - pz')], \tag{2.11}$$

where $\nabla V(pz')^T$ is the gradient of $V(.)$ at pz'. The same transformations in (2.8) and (2.11) are applied similarly to the $\tau^{(t)}_{b,j}$ term, with $pz^{(t)}_s$ as the variable. Thus, the original problem is

approximated by a convex problem. Finally, the optimal solution can then be found using an iterative algorithm, as described in [Kuang, Speidel & Droste (2012)].

2.1.2.2 Passive Anti-Interception: Power Allocation

With fixed $m_{c,s}$ and $m_{c,b}$, and the optimal $pz^*_{c,s}$ and $pz^*_{c,j}$ obtained from solving $\mathcal{JA}$, we derive the power allocation problem $\mathcal{PA}$. This is done by removing constraints (C7), (C8), (C9), and (C10) from problem $\mathcal{P}_1$ as follows

$$\begin{aligned} (\mathcal{PA}) \quad & \max_{p_s,\, p_b} \sum_{c \in C} \min\left(\tau^{(t)}_{c,s,b}, \tau^{(t)}_{c,b,j}\right) \\ \text{s.t.} \quad & \text{(C1)–(C6).} \end{aligned} \tag{2.12}$$

The proof of non-convexity of problem $\mathcal{PA}$ is straightforward. To solve $\mathcal{PA}$, the terms $\tau^{(t)}_{s,b}$ and $\tau^{(t)}_{b,j}$ within the objective function are transformed as described in (2.8) and (2.11), using $p^{(t)}_s$ and $p^{(t)}_b$ as respective variables. These linearizations result in two convex functions. Consequently, we reuse the algorithm in [Kuang *et al.* (2012)] to solve these.

2.1.2.3 Passive Anti-Interception: Spreading Assignment

By removing constraints from (C5) to (C8) from problem $\mathcal{P}_1$, we formulate the spreading factor assignment problem $\mathcal{SA}$ using the optimal values $pz^*_{c,s}$, $pz^*_{c,j}$, $p^*_{c,s}$, and $p^*_{c,b}$ obtained from solving $\mathcal{JA}$ and $\mathcal{PA}$ as parameters. The sub-problem $\mathcal{SA}$ is given by

$$\begin{aligned} (\mathcal{SA}) \quad & \max_{m_s,\, m_b} \sum_{c \in C} \min\left(\tau^{(t)}_{c,s,b}, \tau^{(t)}_{c,b,j}\right) \\ \text{s.t.} \quad & \text{(C1)–(C4), (C9)–(C10).} \end{aligned} \tag{2.13}$$

Due to the convex form of the sub-problem $\mathcal{SA}$, it can be efficiently solved using conventional optimization solvers.

2.1.3 Complexity Analysis

Let N_{iter}^{0} represent the number of iterations in the outer loop of Algorithm 2.1, while N_{iter}^{1} and N_{iter}^{2} correspond to the iterations for solving the $\mathcal{JA}$ and $\mathcal{PA}$ sub-problems, respectively. The complexity to solve a convex problem with m_1 constraints and m_2 variables using the interior-point method is $O(m_1^{1/2}(m_1 + m_2)m_2^2)$ [Hoang, Le & Le-Ngoc (2016)]. For $\mathcal{JA}$, with $5S$ constraints and $2S$ variables, the complexity is $O(N_{iter}^{1}S^{3.5})$, and for $\mathcal{PA}$, with $6S$ constraints and $2S$ variables, it is $O(N_{iter}^{2}S^{3.5})$. The complexity of solving the $\mathcal{SA}$ sub-problem by the closed-form expression is considered insignificant compared to $\mathcal{JA}$ and $\mathcal{PA}$. Therefore, the overall complexity of Algorithm 2.1 is $O(N_{iter}^{0}(N_{iter}^{1} + N_{iter}^{2})S^{3.5})$.

2.1.4 Deep Reinforcement Learning Approach

To reduce the complexity of Algorithm 2.1 in solving $\mathcal{P}_1$, we use a deep reinforcement learning (DRL) strategy. This transforms the $\mathcal{JA}$ and $\mathcal{PA}$ problems into a DRL framework, while the simple $\mathcal{SA}$ is solved conventionally. In this multi-agent system, each E2E link from an SU to a DU through rBS acts as an agent using an individual Double Deep Q-Network (DDQN). During each time slot t, an agent i receives a state input $s_i^{(t)}$ and selects the optimal action $a_i^{(t)}$. The optimal action is determined by identifying the highest Q-value among output values of the DDQN.

2.1.4.1 State Space, Action Space, and Reward Design

The state space of the MADRL problem is formed by the combination of channel gain variations across different channel segments. This state space exists within a continuous domain, with the upper and lower bounds of the channel gain corresponding to the values at the closest and farthest distances between users. The state space is mathematically represented as

$$\bar{S} = \left[G_{s,b}^{(t)}, G_{s,u}^{(t)}, G_{j,u}^{(t)}, G_{b,j}^{(t)}, G_{b,u}^{(t)}\right], \tag{2.14}$$

where $G_{s,b}^{(t)}$, $G_{s,u}^{(t)}$, $G_{j,u}^{(t)}$, $G_{b,j}^{(t)}$, $G_{b,u}^{(t)}$ are channel gain measured in the channels among SU s, rBS interface b, DU j, and eavesdropper's interface u.

The action taken by each agent involves allocating optimally both jamming power levels to SU s and DU j, and transmit power to SU s and rBS b for each E2E connection c at time slot t. Defining a discrete action space that spans all possible power levels would be inefficient, as agents typically use a limited number of actions. To reduce the computational burden, we define a restricted action space. Let n_1 and n_2 be the selected jamming power actions for SU $(X_1, X_2, \ldots, X_{n_1})$ and DU $(Y_1, Y_2, \ldots, Y_{n_2})$, respectively. Let n_3 and n_4 be the power actions for SU $(U_1, U_2, \ldots, U_{n_3})$ and rBS $(V_1, V_2, \ldots, V_{n_4})$. The combined action space $\bar{\mathcal{A}}$ can be represented as

$$\bar{\mathcal{A}} = \{X_{m_1} Y_{m_2} U_{m_3} V_{m_4} \mid m_1 \in [1, n_1],\ m_2 \in [1, n_2], m_3 \in [1, n_3],\ m_4 \in [1, n_4]\}. \tag{2.15}$$

The reward function is crucial for transforming an optimization problem into a MADRL problem. When designing a reward function, it's essential to incorporate terms related to both the objective function and the constraints of the optimization problem. This approach ensures that the agents' actions adhere to the problem constraints. Our reward function is formulated to provide a mutual reward value to all agents at each time slot t as follows

$$r^{(t+1)} = \lambda_0 K_0^{(t)} - \lambda_1 K_1^{(t)} - \lambda_2 K_2^{(t)} + \lambda_3 K_3^{(t)} + \lambda_4 K_4^{(t)} + \lambda_5 K_5^{(t)}, \tag{2.16}$$

where $\lambda_i, i = 0, \ldots, 5$ are coefficients tuned to achieve optimal solutions while satisfying constraints, and $K_i^{(t)}, i = 0, \ldots, 5$ are functions that are defined as

$$\begin{aligned} K_0^{(t)} &= (\mathcal{P}_1)_{\text{Objective}},\ \ K_1^{(t)} = \sum_{c \in C} \left(\gamma_{c,s,u}^{(t)} - \mu\right), \\ K_2^{(t)} &= \sum_{c \in C} \left(\gamma_{c,b,u}^{(t)} - \mu\right),\ \ K_3^{(t)} = \sum_{c \in C} \left(\gamma_{c,s,b}^{(t)} - \gamma_{\min}\right), \\ K_4^{(t)} &= \sum_{c \in C} \left(\gamma_{c,b,j}^{(t)} - \gamma_{\min}\right),\ \ K_5^{(t)} = P_{b_{\max}} - \sum_{c \in C} p_{c,b}^{(t)}. \end{aligned} \tag{2.17}$$

Specifically, $K_0^{(t)}$ represents the total transmission rate of all E2E connections at timeslot t. The term $\lambda_0 K_0^{(t)}$ corresponds to the objective function. Terms $\lambda_1 K_1^{(t)}$ and $\lambda_2 K_2^{(t)}$ are designed to protect the system from energy-based detectors, derived from constraints (C1) and (C2). The negative signs before these terms indicate penalties, encouraging reduced SINR to achieve higher LPI performance. Terms $\lambda_3 K_3^{(t)}$ and $\lambda_4 K_4^{(t)}$ aim to satisfy constraints (C3) and (C4), respectively. The term $\lambda_5 K_5^{(t)}$ regulates the transmit power of the rBS within the allowable range specified in constraint (C6). Constraints (C5), (C7), (C8), (C9), and (C10) are not included in the reward function design as they can be satisfied through the action space design.

2.1.4.2 Proposed MADRL Algorithm

We employ a central training and distributed implementation approach to implement our proposed MADRL strategy. This paradigm enables efficient training while allowing agents to act independently during execution. The detailed training process is outlined in Algorithm 2.2.

2.2 Triple-Layered Anti-Interception Security Framework for Ground Combat Vehicular Networks

2.2.1 System Model

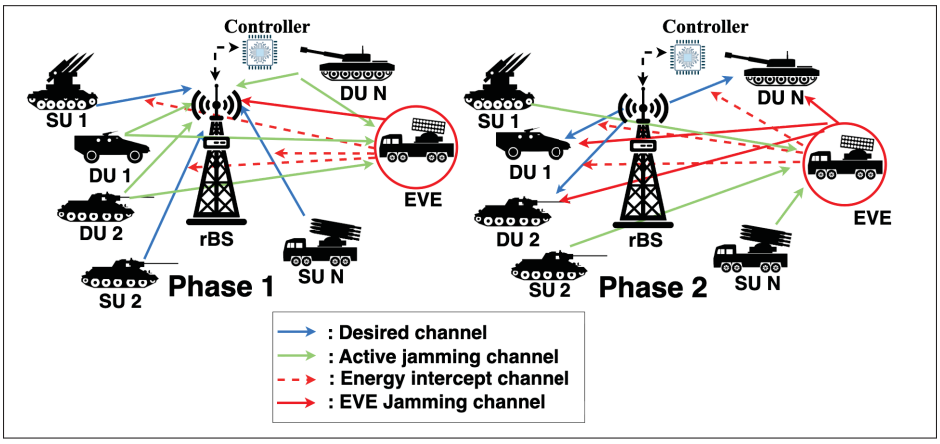

Figure 2.2 System model

Algorithm 2.2 MADRL Algorithm for solving problem $\mathcal{P}_1$

initialize:
The main Q-network $Q\left(s^{(t)}, a^{(t)}; \theta^{(t)}\right)$
The target Q-network $\hat{Q}\left(s^{(t)}, a^{(t)}; \theta'^{(t)}\right)$
The replay memory $\mathcal{D}$ with capacity C
repeat
  Observe the whole network state $s^{(t)}$
  for each agent i **do**
    if $\epsilon < \epsilon_{\text{greedy}}$ **then**
      Solve $\mathcal{JA}$ and $\mathcal{PA}$ by using random action $a_i^{(t)} \in \bar{\mathcal{A}}$
    else
      Solve $\mathcal{JA}$ and $\mathcal{PA}$ by selecting DRL model

$$a_i^{(t)} = \arg\max_{a \in \bar{\mathcal{A}}} Q\left(s_i^{(t+1)}, a; \theta_i^{(t)}\right)$$

    end if
  end for
  Solve problem $(\mathcal{SA})$ with $a_i^{(t)}$, obtain $m_s^{(t)*}$ and $m_b^{(t)*}$
  Observe next state $s^{(t+1)}$ and calculate mutual reward
  Store transition $\left(s^{(t)}, a^{(t)}, r^{(t)}, s^{(t+1)}\right)$ in $\mathcal{D}$
  if the replay memory $\mathcal{D}$ is full **then**
    Sample a mini-batch of K transitions from $\mathcal{D}$
    Update $\theta^{(t+1)}$ using Adam optimizer
    After Z timesteps, update $\theta'^{(t+1)} = \theta^{(t)}$
  end if
  $t \leftarrow t + 1$
until Done all tasks or maximum time slots is reached.

Fig. 2.2 depicts two transmission stages of a DS-CDMA TVAN system, including a set of source users (SUs) $\mathcal{S} = \{1, 2, ..., S\}$, a set of destination users (DUs) $\mathcal{J} = \{1, 2, ..., J\}$, and a decode-and-forward (DF) relay base station (rBS). The DF relay plays a critical role by decoding the signal received from the SUs using the encryption key, applying filtering techniques (e.g., matched filter or Minimum Mean Squared Error (MMSE)) to filter out noise and multiuser interference, reconstructing a clean version of the signal, and forwarding it to the DUs. This process mitigates signal degradation during the first transmission phase (i.e., SU-to-rBS),

which would otherwise occur in amplify-and-forward (AF) schemes. In this scenario, the users are Ground Combat Vehicles (GCVs), specifically designed for mobility, including tanks and missile-carrying trucks. Each GCV is equipped with a communication module and a jamming module, capable of broadcasting signals at maximum power levels denoted by $P_{s,max}$ and $PZ_{s,max}$, respectively. Each SU is paired with a corresponding DU, creating a group of E2E communication links. This group is represented by the set $C = \{1, 2, \ldots, C\}$ of E2E connections. These communication links are established via the rBS. The rBS supports multiple simultaneous connections by assigning distinct spreading codes to each user pair, represented by the set $\mathcal{B} = \{1, 2, \ldots, B\}$. Each logical connection $b \in \mathcal{B}$ serves a dual purpose: it receives and decodes data from a specific SU s and transmits data to a corresponding DU j. Each communication link from transmitter x to receiver y (i.e., from SU s to rBS or from rBS to DU j) belonging to E2E connection c at time slot t is characterized by the following channel coefficient

$$g_{c,x,y}^{(t)} = d_{c,x,y}^{(t)} f_{c,x,y}^{(t)}, \tag{2.18}$$

where $d_{c,x,y}^{(t)}$ denotes the large-scale fading (including distance loss and shadowing), and $f_{c,x,y}^{(t)}$ represents the small-scale fading coefficient following a Rayleigh distribution. This model accurately captures the non-line-of-sight (NLOS) propagation and dynamic mobility conditions typically encountered in battlefield or tactical vehicular environments, where obstacles and multipath propagation dominate.

For decision variables, $pz_{c,s}^{(t)}$ and $pz_{c,j}^{(t)}$ denote the jamming transmit power of SU s and DU j respectively, for connection c at time slot t. The transmit power of SU s and rBS for connection c at time slot t are represented by $p_{c,s}^{(t)}$ and $p_{c,b}^{(t)}$ respectively. The communication system is attacked by an in-band full-duplex (IBFD) eavesdropper (EVE), which can simultaneously eavesdrop on signals from the SUs and rBS while jamming these receivers.

In our proposed triple-layered anti-interception strategy for a dual-stage relay network, each time slot is divided into two synchronized phases. This synchronization is managed by the rBS via control channels [Liu, Shen, Guo & Win (2018)], which broadcast timing signals to ensure that

all users are aligned and know exactly when to transmit or jam. In phase 1, SU s transmits a data signal with transmit power $p_{c,s}^{(t)}$, while DU j transmits a jamming signal with jamming transmit power $pz_{c,j}^{(t)}$. To secure the transmitted data, AES encryption is applied with a key of length $l_c^{(t)}$, where $l_c^{(t)}$ denotes the key length at time slot t, belonging to E2E connection c. The encryption key at this time is given by $k_c^{(t)} \in \mathcal{K}$, where $\mathcal{K} = \{1, 2, \ldots, K\}$ represents the set of possible encryption key values. According to [Garnaev, Petropulu, Trappe & Poor (2022)], at time slot t, the received SINR of the standard CDMA system for a channel between SU s and rBS b, as well as a channel between SU s and EVE u belonging to E2E connection c, can be determined by

$$\gamma_{c,s,b}^{(t)} = \frac{m_{c,s}^{(t)} |g_{c,s,b}^{(t)}|^2 p_{c,s}^{(t)}}{\sigma^2 + P_E^{(t)} |g_{c,u,b}^{(t)}|^2 + \sum_{k \neq s} |g_{c,k,b}^{(t)}|^2 p_{c,k}^{(t)} + \sum_{j \in \mathcal{J}} |g_{c,j,b}^{(t)}|^2 pz_{c,j}^{(t)}} \tag{2.19}$$

$$\gamma_{c,s,u}^{(t)} = \frac{m_{c,s}^{(t)} |g_{c,s,u}^{(t)}|^2 p_{c,s}^{(t)}}{\sigma^2 + \sum_{k \neq s} |g_{c,k,u}^{(t)}|^2 p_{c,k}^{(t)} + \sum_{j \in \mathcal{J}} |g_{c,j,u}^{(t)}|^2 pz_{c,j}^{(t)}}, \tag{2.20}$$

where $g_{c,x,y}^{(t)}$ is the coefficient of channel between transmitter x and receiver y belonging to E2E connection c at time slot t, $m_{c,s}^{(t)}$ is the spreading factor of the SU s belonging to E2E connection c at time slot t, $p_{c,s}^{(t)}$ is the transmit power of the SU s belonging to E2E connection c at time slot t, $p_{c,k}^{(t)}$ is the transmit power of interfering transmitter k belonging to E2E connection c at time slot t, $pz_{c,j}^{(t)}$ and $P_E^{(t)}$ are the jamming transmit power of the DU j and EVE, respectively, belonging to E2E connection c at time slot t, and σ^2 is the noise power. As shown in (2.19), the signal received at the rBS includes the interference generated by the DUs. In this work, no interference cancellation scheme is assumed at the rBS. The DU-to-rBS interference is treated as part of the total interference term, representing a conservative and realistic assumption for tactical environments where advanced cancellation techniques may not be available. The proposed joint jamming allocation, power control, and key-length optimization ensure that the resulting SINR at the rBS satisfies all system constraints (e.g., reliable decoding, EVE detection threshold) even in the presence of this interference.

In phase 2, rBS b decodes and forwards its received signal to DU j with transmit power $p_{c,b}^{(t)}$ while SU s transmits a jamming signal with jamming transmit power $pz_{c,s}^{(t)}$. Therefore, the received SINR at DU j and EVE u, which belong to the E2E connection c at time slot t are given by

$$\gamma_{c,b,j}^{(t)} = \frac{m_{c,b}^{(t)} |g_{c,b,j}^{(t)}|^2 p_{c,b}^{(t)}}{\sigma^2 + P_E^{(t)} |g_{c,u,j}^{(t)}|^2 + \sum_{k \neq s} |g_{c,k,j}^{(t)}|^2 p_{c,k}^{(t)} + \sum_{s \in \mathcal{S}} |g_{c,s,u}^{(t)}|^2 pz_{c,s}^{(t)}}. \tag{2.21}$$

$$\gamma_{c,b,u}^{(t)} = \frac{m_{c,b}^{(t)} |g_{c,b,u}^{(t)}|^2 p_{c,b}^{(t)}}{\sigma^2 + \sum_{k \neq s} |g_{c,k,u}^{(t)}|^2 p_{c,k}^{(t)} + \sum_{s \in \mathcal{S}} |g_{c,s,u}^{(t)}|^2 pz_{c,s}^{(t)}}, \tag{2.22}$$

where $m_{c,b}^{(t)}$ is the spreading factor of the rBS b belonging to E2E connection c at time slot t, $p_{c,b}^{(t)}$ is the transmit power of the rBS b belonging to E2E connection c at time slot t, $p_{c,k}^{(t)}$ is the transmit power of interfering transmitter k belonging to E2E connection c at time slot t, $pz_{c,s}^{(t)}$ is the jamming transmit power of SU s belonging to E2E connection c at time slot t.

The location of the EVE is assumed to be known to the users through prior sensing, surveillance intelligence, or radar-assisted detection in tactical environments [Su, Liu & Masouros (2024)], allowing them to estimate the signal strength received by the EVE. This information is processed by a centralized controller, which is integrated at the rBS, to either solve the optimization problem directly or coordinate the centralized training phase in the MADRL framework. In this scenario, the IBFD EVE can use an energy-based detection technique, which allows it to detect transmitted signals from SUs and the rBS based on the amplitude of the SINR values.

2.2.2 Enegy-Based Interception

Energy detection, also known as radiometry, is the most common method for intercepting unknown signals when no information about the signal format or modulation is available. This technique is particularly useful in TVAN scenarios where a low probability of detection (LPD) is desired. The energy detection process involves multiple crucial stages. Initially, the received

signal is processed through a whitening filter to address the colored ambient noise commonly encountered in tactical environments. Then, the energy of the filtered signal is measured over a specific interval of time that corresponds to the expected signal duration. Finally, the measured energy is compared to a predetermined threshold to determine whether a signal is present or absent. A common approach in energy detection is to use a Constant False Alarm Rate (CFAR) system [Raghavan (2019)], where the detection threshold is dynamically calculated based on the desired false alarm probability and the statistical characteristics of the measured noise. This adaptive threshold helps maintain a consistent false alarm rate across varying noise conditions. Eavesdroppers are typically equipped with energy receivers that measure the SINR values to intercept signals.

In spread spectrum networks, the selection of the decoding threshold is particularly critical. Desired receivers must distinguish between the desired spread spectrum signal and background noise or interference. The decoding decision is typically based on an outage probability, $\Pr(\gamma_{c,x,y}^{(t)} \geq \gamma_{\min})$, where $\gamma_{\min}$ is the decoding threshold of the receivers.

In this context, the SUs, rBS, and DUs must cooperate to transmit jamming and desired signals that meet two key requirements. First, the EVE must receive SINR values in both transmission phases that are below the detection threshold μ, and second, the SINR at the desired receivers (DUs and rBS) must exceed the decoding threshold $\gamma_{\min}$ to maintain an acceptable outage probability. The constraints for our system during the two transmission phases can be represented as

$$\gamma_{c,s,u}^{(t)} \leq \mu, \;\; \gamma_{c,b,u}^{(t)} \leq \mu, \tag{2.23}$$

$$\gamma_{c,s,b}^{(t)} \geq \gamma_{\min}, \;\; \gamma_{c,b,j}^{(t)} \geq \gamma_{\min}. \tag{2.24}$$

where μ is an SINR detection threshold for the eavesdropper, and $\gamma_{\min}$ is the decoding threshold for the receivers of the rBS and DUs. For example, the LPI capacity of many state-of-the-art systems is considered secure when the intercept SINR value remains below -8 dB and the desired SINR value stays above -14 dB [Liu, Khan, Bilal & Zuberi (2025)].

2.2.3 AES-based Encryption Anti-Interception

2.2.3.1 Physical Layer Security Evaluation Of DS-CDMA

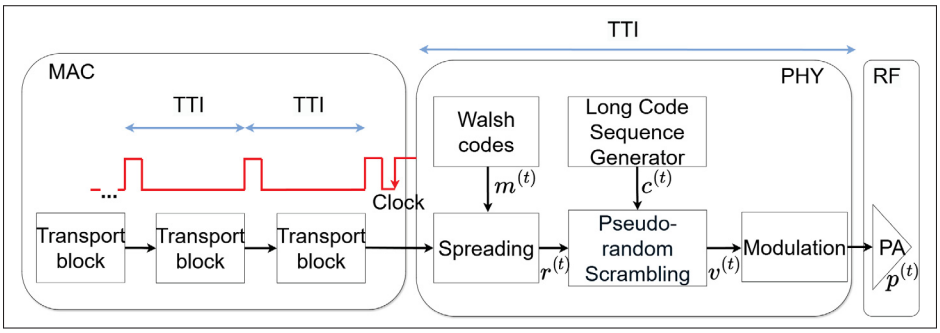

Figure 2.3 Block diagram of a DS-CDMA System

Fig. 2.3 illustrates the operational flow of a DS-CDMA system, including the MAC, PHY, and RF stages. The DS-CDMA process begins at the MAC layer, which forms transport blocks containing user data or control information. These transport blocks are generated periodically based on the Transmission Time Interval (TTI). To ensure synchronization, the PHY layer generates clock signals that are sent to the MAC layer. These clock signals serve as a reference, ensuring that the data prepared by the MAC layer, such as transport blocks, are handed off to the PHY layer with precise timing. This synchronization guarantees that the TTI boundaries align between the two layers, preventing data buffering issues or misalignment.

In the PHY layer, the first step is spreading, where each user's signal is spread using a code sequence $m^{(t)}$, known as a channelization code or Walsh code. The output of this spreading process is then scrambled with a Long Code Sequence Generator, which produces a unique pseudo-random sequence $c^{(t)}$ for each user. This scrambling operation further separates users during demodulation and makes it difficult for eavesdroppers to intercept or detect the transmitted signal. The resulting scrambled signal is denoted as $v^{(t)}$. Without knowledge of both the user's channelization code $m^{(t)}$ and the scrambling code $c^{(t)}$, it is impossible to retrieve the intended user's signal. This characteristic serves as a built-in security feature of DS-CDMA systems.

Next, the scrambled signal $r^{(t)}$ is modulated onto a carrier frequency using standard techniques, such as Quadrature Phase Shift Keying (QPSK) or Binary Phase Shift Keying (BPSK), to produce the modulated signal. In the RF stage, this modulated signal is amplified by the Power Amplifier to ensure it has sufficient power for transmission. The transmit power, denoted as $p^{(t)}$, represents the power level of the signal as it is transmitted over the air interface to the base station or mobile receiver.

Since the channelization code or Walsh code is known to the public, a correlation-based eavesdropper can estimate the code sequence $m^{(t)}$ by performing cross-correlation analysis on the received signal [Wei *et al.* (2022)]. Therefore, the PHY security of DS-CDMA systems primarily relies on the long pseudo-random scrambling sequence, commonly referred to as the long code $c^{(t)}$. The long code sequence $c^{(t)}$ is generated using a long code generator, as depicted in Fig. 2.4. This generator consists of a 42-bit number, known as the long code mask $q^{(t)}$, and a 42-bit Linear Feedback Shift Register (LFSR) $s^{(t)}$ defined by the following characteristic polynomial:

$$\begin{aligned} &s^{42} + s^{35} + s^{33} + s^{31} + s^{27} + s^{26} + s^{25} + s^{22} + s^{21} + s^{19} \\ &+s^{18} + s^{17} + s^{16} + s^{10} + s^{7} + s^{6} + s^{5} + s^{3} + s^{2} + s + 1. \end{aligned} \tag{2.25}$$

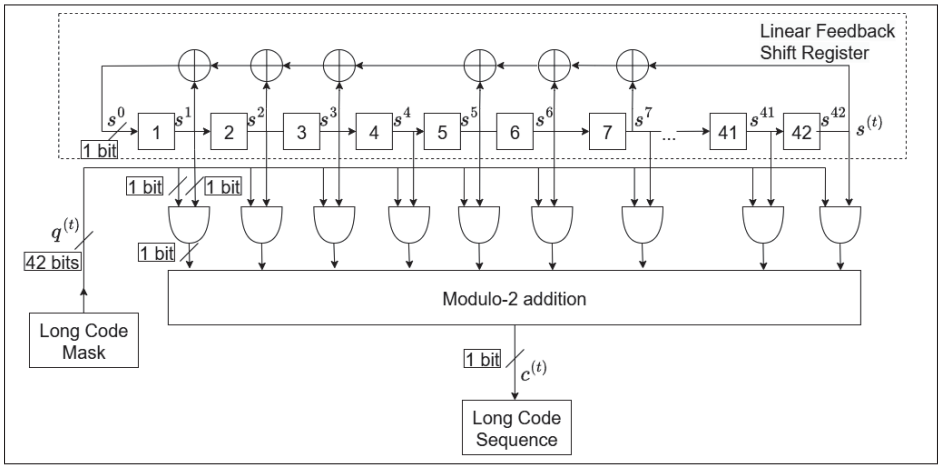

Figure 2.4 The long code generator

The long code sequence $c^{(t)}$ is generated by calculating the inner product of the LFSR state $s^{(t)}$ and the long code mask $q^{(t)}$. The long code mask $q^{(t)}$ is not transmitted through any channel; it is independently constructed by both the base station and the mobile user. Since the LFSR $s^{(t)}$ used to generate the long code sequence is publicly known, it is accessible to the eavesdropper. To recover the long code sequence, the eavesdropper could perform an exhaustive search of the 42-bit long code mask $q^{(t)}$, which has a time complexity of $O(2^{42})$. Moreover, it can be shown that the long code sequence $c^{(t)}$ can also be recovered if the eavesdropper obtains 42 bits of the sequence within approximately one second [Li, Song & Liang (2018)].

2.2.3.2 Proposed AES-Based Scrambling

To enhance the security of the PHY in DS-CDMA systems, which primarily relies on the scrambling process, and address the inadequacy of information-theoretic privacy provided by the current system, we propose the scrambling process using the AES. The proposed secure scrambling scheme aims to strengthen the PHY security of DS-CDMA systems, prevent exhaustive key search attacks, and minimize modifications to the existing DS-CDMA standard.

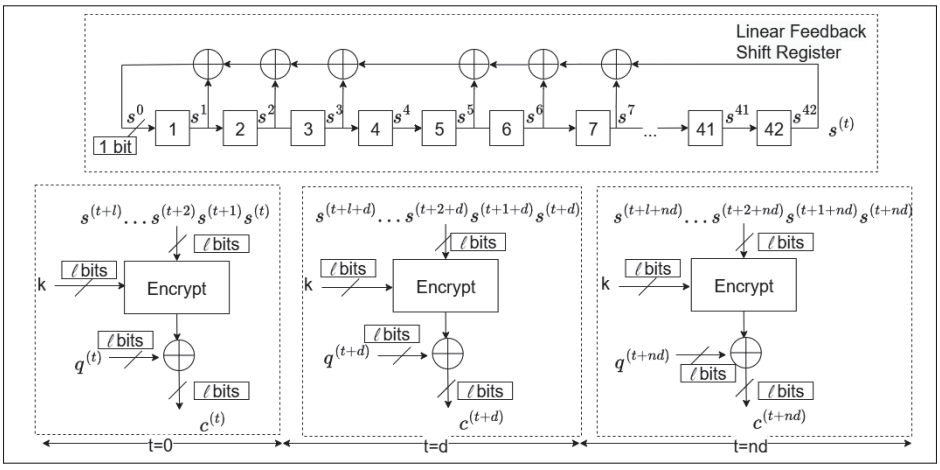

Figure 2.5 Proposed AES-Based Scrambling

In Fig. 2.5, at $t = 0$, $s^{(t+l)}, \ldots, s^{(t+2)}, s^{(t+1)}, s^{(t)}$ represent the l-bit output of the LFSR defined by (2.25), where k is the l-bit common secret encryption key shared between the base station

and the mobile station (which may be 128, 192, or 256 bits, depending on the selection of l), $q^{(t)}$ denotes the long code mask of the same size as k, and d represents the shift between successive inputs to the AES engine. The secure scrambling process can be summarized as follows:

- The base station and the users share a common initial state for the LFSR $s^{(t)}$ and an l-bit ($l = 128, 192,$ or 256) common secret encryption key k.
- The long scrambling sequence $c^{(t)}$ is generated by encrypting a specific segment of the sequence produced by the LFSR $s^{(t)}$ using the shared secret key k.

The shared secret data between the users and the base station can be periodically updated for each connection.

2.2.3.3 Encryption-Aware Secrecy Capacity

In general, the achievable secrecy rate for E2E connection c at time slot t in two transmission phases can be written as

$$r_{c,s,b}^{(t)} = \tau_{c,s,b}^{(t)} - \tau_{c,s,u}^{(t)}, \quad r_{c,b,j}^{(t)} = \tau_{c,b,j}^{(t)} - \tau_{c,b,u}^{(t)}, \tag{2.26}$$

where the transmission rate of each link from transmitter x to receiver y belonging to E2E connection c at time slot t is defined as $\tau_{c,x,y}^{(t)} = W_0 \log_2 \left(1 + \gamma_{c,x,y}^{(t)}\right)$. Here, W_0 is the original signal bandwidth.

The results presented in (2.26) concerning the secrecy capacity $r_{c,x,y}^{(t)}$ are valid only under the assumption that encryption is employed and EVE can perfectly recover the entire ciphertext without errors. However, in scenarios involving error-prone ciphertexts, the interception and decoding of messages become significantly more challenging for EVE. In such cases, EVE would require greater computational resources or more advanced attack strategies to compromise the encryption successfully. Consequently, in this paper, we do not utilize the results in (2.26) as part of our objective function. As discussed in [Sadig *et al.* (2020)], the error threshold P_{cipher} represents the minimum error level needed in the ciphertext to prevent an EVE from successfully decoding a message. If EVE has high computational power, P_{cipher} needs to be

close to 1. Conversely, when EVE's computational power is low, a smaller P_{cipher} suffices. The secrecy condition is thus defined by $P_{\text{EVE}} \geq P_{\text{cipher}}$, where P_{EVE} is the probability of error at EVE. The encryption strength parameter θ is used to establish a link between PHY security and encryption. With stronger encryption, a lower P_{cipher} can achieve security, whereas weaker encryption demands a higher P_{cipher} for adequate protection.

According to [Sun *et al.* (2019)], we can further define encryption strength as

$$\theta_c^{(t)} = \log_2(l_c^{(t)}), \tag{2.27}$$

where $l_c^{(t)}$ is the key length for connection c at time t. A higher encryption strength, represented by a larger θ, implies a smaller required P_{cipher}, thereby enhancing security. This inverse relationship between θ and P_{cipher} suggests that as encryption strength increases, the required error threshold decreases, further improving confidentiality.

The choice of the encryption-strength model $\theta_c^{(t)} = \log_2(l_c^{(t)})$ follows the opportunistic encryption framework in [Sun *et al.* (2019)], where a logarithmic function of the block or key length is used to characterize practical cryptographic strength. This formulation presents that brute-force attacks against a cipher of key length $l_c^{(t)}$ require $O(2^{l_c^{(t)}})$ operations, i.e., the search space grows exponentially, while the achievable security gains in real-time wireless systems increase more slowly due to latency and energy constraints. As a result, $\log_2(l_c^{(t)})$ provides a realistic and tractable security metric that captures the diminishing returns of longer keys while remaining compatible with PHY-layer optimization. The parameter $\theta_c^{(t)}$ scales the information-theoretic secrecy rate but is bounded by the transmission rate, ensuring physical consistency. Thus, increasing the AES key length enhances the effective secrecy capacity while still satisfying the latency and energy requirements of tactical vehicular networks.

Consequently, we define the encryption-aware secrecy rates $\hat{r}_{c,s,b}^{(t)}$ and $\hat{r}_{c,b,j}^{(t)}$, which depend on the encryption strength $\theta_c^{(t)}$, the secrecy capacities $r_{c,s,b}^{(t)}$ and $r_{c,b,j}^{(t)}$, and the transmission rates

$\tau_{c,s,b}^{(t)}$ and $\tau_{c,b,j}^{(t)}$, given by [Sadig *et al.* (2020)] as

$$\hat{r}_{c,s,b}^{(t)} = \min(\theta_c^{(t)} r_{c,s,b}^{(t)}, \tau_{c,s,b}^{(t)}), \quad \hat{r}_{c,b,j}^{(t)} = \min(\theta_c^{(t)} r_{c,b,j}^{(t)}, \tau_{c,b,j}^{(t)}), \tag{2.28}$$

which ensures that the effective secrecy rate is not overestimated beyond the physical transmission limit.

2.2.3.4 Latency Requirement

As described in Fig. 2.3, the TTI is the duration during which a set of transport blocks is transferred from the MAC layer to the PHY layer and serves as the fundamental time unit for scheduling in the MAC and resource mapping in the PHY. The TTI length varies depending on the Radio Access Technology (RAT) to meet different transmission delay requirements in various service scenarios. For example, in DS-CDMA, the minimum TTI, as defined in 3GPP TS 25.201, is a radio frame of 10 ms, which can also be configured to 20 ms, 40 ms, or 80 ms. In Long Term Evolution (LTE), the conventional TTI length corresponds to one subframe, which is 1 ms. In New Radio (NR), the basic unit of scheduling is a slot, so the duration of one TTI equals the duration of one slot. In an NR network, the duration of one frame is 10 ms, comprising 10 subframes, with the number of slots in each subframe calculated as $10 \times \mu$, where μ depends on the subcarrier spacing. For instance, when $\mu = 1$, the minimum TTI is 1 ms. In the context of our TVAN, the total processing latency of the PHY layer includes the processing time for spreading, pseudo-random scrambling, and modulation. However, the complexity of processing pseudo-random scrambling is considered significantly greater compared to the spreading and modulation blocks.

According to [Xiao, Hong, Xu, Yang & Ji (2022)], for an E2E connection c at time slot t, the transmitter requires time to handle the key setup, and the encryption process can be formulated as

$$t_{c,\text{phy}}^{(t)} = t_{0,\text{phy}} + \rho l_c^{(t)}, \tag{2.29}$$

where $t_{0,\text{phy}}$ (s) represents the offset time for the key setup and encryption process, and ρ (s/bit) is the encryption latency coefficient. Therefore, the key length selected for the E2E connection c at time slot t must ensure that the processing time for AES-based scrambling is less than a TTI. The constraint for the PHY layer in our system can be expressed as

$$t_{c,\text{phy}}^{(t)} \leq T_{\text{TTI}}. \tag{2.30}$$

2.2.3.5 Energy Consumption Requirement

According to [Xiao *et al.* (2022)], the energy consumption for encrypting a transport block during T_{TTI} is mathematically written as

$$e_{c,\text{phy}}^{(t)} = e_{0,\text{phy}} + \vartheta l_c^{(t)}, \tag{2.31}$$

where $e_{0,\text{phy}}$ (J) represents the offset energy consumption for the key setup and encryption process, and ϑ (J/bit) denotes the energy required to process one bit of the key length $l_c^{(t)}$.

In phase 1, the SU s transmits encrypted data to DU j during $T_{c,s,1}^{(t)}$. In phase 2, the SU s transmits jamming data during $T_{c,s,2}^{(t)}$. Consequently, the total energy consumption of SU s for an E2E connection c at time slot t can be described as

$$e_{c,s}^{(t)} = \frac{T_{c,s,1}^{(t)}}{T_{\text{TTI}}}(e_{0,\text{phy}} + \vartheta l_c^{(t)}) + T_{c,s,1}^{(t)} p_{c,s}^{(t)} + T_{c,s,2}^{(t)} p z_{c,s}^{(t)}, \tag{2.32}$$

where $T_{c,s,1}^{(t)}$ is the transmission time of SU s in phase 1 for connection c at time slot t, and $T_{c,s,2}^{(t)}$ is the jamming transmission time of SU s in phase 2 for connection c at time slot t. Given that each GVC has a limited power budget for communication, an energy consumption constraint is imposed. This constraint can be represented as

$$e_{c,s}^{(t)} \leq E_{c,s,\max}^{(t)}, \tag{2.33}$$

where $E^{(t)}_{c,s,\max}$ represents the maximum allowable energy consumption of SU s for connection c at time slot t.

2.2.4 Problem Formulation

Our triple-layered anti-eavesdropping in a dual-stage relay network problem aims at maximizing the transmission rate for high-mobility users. The problem is formulated as follows.

$$
\begin{aligned}
(\mathcal{P}_1) \quad & \max_{pz_s, pz_j, p_s, p_b, l} \sum_{c\in C} \min(\hat{r}^{(t)}_{c,s,b}, \hat{r}^{(t)}_{c,b,j}) \overset{(*)}{=} \\
& -\min \sum_{c\in C} \max(-\hat{r}^{(t)}_{c,s,b}, -\hat{r}^{(t)}_{c,b,j}) = \\
& -\min \sum_{c\in C} \max(-\min(\theta^{(t)}_c r^{(t)}_{s,b}, \tau^{(t)}_{s,b}), -\min(\theta^{(t)}_c r^{(t)}_{s,b}, \tau^{(t)}_{s,b})) = \\
& -\min \sum_{c\in C} \max(\max(-\theta^{(t)}_c r^{(t)}_{s,b}, -\tau^{(t)}_{s,b}), \max(-\theta^{(t)}_c r^{(t)}_{s,b}, -\tau^{(t)}_{s,b})) \\
\text{s.t.} \quad & (\text{C1}) : \gamma^{(t)}_{c,s,u} \le \mu, \ \ (\text{C2}) : \gamma^{(t)}_{c,b,u} \le \mu, \\
& (\text{C3}) : \gamma^{(t)}_{c,s,b} \ge \gamma_{\min}, \ \ (\text{C4}) : \gamma^{(t)}_{c,b,j} \ge \gamma_{\min}, \\
& (\text{C5}) : p^{(t)}_{c,s} \le P_{s,\max}, \ \ (\text{C6}) : \sum_{c\in C} p^{(t)}_{c,b} \le P_{b,\max}, \\
& (\text{C7}) : pz^{(t)}_{c,s} \le PZ_{s,\max}, \ \ (\text{C8}) : pz^{(t)}_{c,j} \le PZ_{j,\max}, \\
& (\text{C9}) : L_{\min} \le l^{(t)}_c \le L_{\max}, \ \ (\text{C10}) : t^{(t)}_{c,\text{phy}} \le T_{\text{TTI}}, \\
& (\text{C11}) : e^{(t)}_{c,s} \le E^{(t)}_{c,s,\max},
\end{aligned}
\tag{2.34}
$$

where $l = \{l_c\}$, $pz_s = \{pz_{c,s}\}$, $pz_j = \{pz_{c,j}\}$, $p_s = \{p_{c,s}\}$, $p_b = \{p_{c,b}\}$, $\forall c \in C$. $L_{\max}$ and $L_{\min}$ are the maximum and minimum key lengths, respectively. The equality marked by $\overset{(*)}{=}$ is rewritten in a minimization form instead of a maximization form for the convenience of proving the convexity and convergence of the objective function.

Constraint (C1) ensures that the SINR at EVE, denoted by $\gamma^{(t)}_{c,s,u}$ is lower than an energy detection threshold μ during phase 1. The same constraint (C2) applies in phase 2. For the rBS and DU to detect the desired signals accurately, the measured SINR values at these receivers must be above a certain threshold. The requirements are enforced by constraints (C3) and (C4). Constraints (C5), (C6) specify the maximum transmit power levels for each SU and the rBS, while constraints (C7) and (C8) limit the maximum jamming transmit power levels for each SU

Algorithm 2.3 The iterative algorithm for problem $\mathcal{P}_1$

1: **initialize:** Init values for $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, $l_c^{(i)}$;
Set counter $i = 0$, $i_{\max} = 10^6$, coverage tolerance $\omega = 10^{-3}$
2: **repeat**
3: Solve $(\mathcal{JA})$ with fixed $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, $l_c^{(i)}$, find $pz_{c,s}^*$ and $pz_{c,j}^*$
Update $pz_{c,s}^{(i)} = pz_{c,s}^*$ and $pz_{c,j}^{(i)} = pz_{c,j}^*$
4: Solve $(\mathcal{PA})$ with fixed $l_c^{(i)}$, $pz_{c,s}^{(i)}$, $pz_{c,j}^{(i)}$, find $p_{c,s}^*$ and $p_{c,b}^*$
Update $p_{c,s}^{(i)} = p_{c,s}^*$ and $p_{c,b}^{(i)} = p_{c,b}^*$
5: Solve $(\mathcal{KA})$ with fixed $pz_{c,s}^{(i)}$, $pz_{c,j}^{(i)}$, $p_{c,s}^{(i)}$, $p_{c,b}^{(i)}$, find l_c^*
Update $l_c^{(i)} = l_c^*$
6: $i = i + 1$
7: **until** $\sum_c \left(\left| pz_{c,s}^{(i)} - pz_{c,s}^{(i+1)} \right| + \left| pz_{c,j}^{(i)} - pz_{c,j}^{(i+1)} \right| \right) \leq \omega$ **or** $i \geq i_{\max}$
8: **return** $pz_{c,s}^*$, $pz_{c,j}^*$, $p_{c,s}^*$, $p_{c,b}^*$, l_c^*.

and DU. Constraint (C9) expresses the lower and upper bounds on the number of key lengths applied for the encryption process. Constraint (C10) ensures that the time for key setup and the encryption process needs to be less than a TTI. Constraint (C11) limits the energy consumption of each user.

Problem $(\mathcal{P}_1)$ is a non-convex optimization problem due to the presence of a logarithm of a fractional function in the objective function, as well as the inclusion of both continuous and discrete variables. To address this, the objective function is first decomposed into three sub-problems, $\mathcal{JA}$, $\mathcal{PA}$, and Key-length Assignment $(\mathcal{KA})$. These sub-problems are then solved sequentially. As presented in Algorithm 2.3, $\mathcal{JA}$ can be solved with the fixed transmit power levels and key length. The optimal jamming power levels pz_s^* and pz_j^* obtained from solving $\mathcal{PZ}$ are then used to solve the power allocation sub-problem $\mathcal{PA}$ while keeping the key length fixed. Finally, the optimal jamming transmit power values pz_s^* and pz_j^* and the optimal transmit power values p_s^* and p_b^* obtained from solving $\mathcal{JA}$ and $\mathcal{PA}$, respectively, are used as parameters to solve the key length assignment sub-problem $\mathcal{KA}$. This iterative process continues with an increasing iteration counter i. The algorithm terminates when the difference

between two consecutive $\mathcal{JA}$ solutions falls below a convergence tolerance ω, or when the maximum number of iterations $i_{\max}$ is reached. The algorithm outputs the optimal jamming power, transmit power, and key length values, which are allocated to the system at each time slot t.

2.2.4.1 Active Anti-Interception: Jamming Allocation

Allocation We consider the jamming power allocation factors $pz_{c,s}$ and $pz_{c,j}$ as variables while holding the power allocation and key length constant in problem $\mathcal{P}_1$. Consequently, the sub-problem $\mathcal{JA}$ is expressed as

$$\begin{aligned} (\mathcal{JA}) \quad & -\min_{pz_s, pz_j} \sum_{c \in C} \max(-\hat{r}^{(t)}_{c,s,b}, -\hat{r}^{(t)}_{c,b,j}) \\ \text{s.t.} \quad & \text{(C1), (C2), (C3), (C7), (C8), (C11).} \end{aligned} \tag{2.35}$$

The transformed problem $\mathcal{JA}$ is a non-convex optimization problem due to the inclusion of the logarithm of a fractional function in the objective function. To address this, the functions $-\theta^{(t)}_c r^{(t)}_{s,b}$ and $-\tau^{(t)}_{s,b}$ in $-\hat{r}^{(t)}_{s,b} = -\min(\theta^{(t)}_c r^{(t)}_{s,b}, \tau^{(t)}_{s,b}) = \max(-\theta^{(t)}_c r^{(t)}_{s,b}, -\tau^{(t)}_{s,b})$ are first rewritten in a DC function form as follows

$$\begin{aligned} f^{(t)}_1(pz) = -\theta^{(t)}_c r^{(t)}_{s,b} &= -\log_2(l^{(t)}) r^{(t)}_{s,b} = -\log_2(l^{(t)})(\tau^{(t)}_{s,b} - \tau^{(t)}_{s,u}) \\ &= -\log_2(l^{(t)}) W_0[\log_2(1+\gamma^{(t)}_{s,b}) - \log_2(1+\gamma^{(t)}_{s,u})] \\ &= \log_2(l^{(t)}) W_0[U_1(pz) + U_4(pz) - ((U_2(pz) + U_3(pz))], \end{aligned} \tag{2.36}$$

$$f^{(t)}_2(pz) = -\tau^{(t)}_{s,b} = -W_0 \log_2(1+\gamma^{(t)}_{s,b}) = W_0[U_1(pz) - U_2(pz)], \tag{2.37}$$

where

$$U_1(pz) = -\log_2(\sigma^2 + P^{(t)}_E . |g^{(t)}_{u,b}|^2 + \sum_{k \neq s} |g^{(t)}_{k,b}|^2 . p^{(t)}_k + \sum_{j \in \mathcal{J}} |g^{(t)}_{j,b}|^2 . pz^{(t)}_j + m^{(t)}_s . |g^{(t)}_{s,b}|^2 . p^{(t)}_s), \tag{2.38}$$

$$U_2(pz) = -\log_2(\sigma^2 + P_E^{(t)}.|g_{u,b}^{(t)}|^2 + \sum_{k\neq s}|g_{k,b}^{(t)}|^2.p_k^{(t)} + \sum_{j\in\mathcal{J}}|g_{j,b}^{(t)}|^2.pz_j^{(t)}), \tag{2.39}$$

$$U_3(pz) = -\log_2(\sigma^2 + \sum_{k\neq s}|g_{k,u}^{(t)}|^2.p_k^{(t)} + \sum_{j\in\mathcal{J}}|g_{j,u}^{(t)}|^2.pz_j^{(t)} + m_s^{(t)}.|g_{s,u}^{(t)}|^2.p_s^{(t)}), \tag{2.40}$$

$$U_4(pz) = -\log_2(\sigma^2 + \sum_{k\neq s}|g_{k,u}^{(t)}|^2.p_k^{(t)} + \sum_{j\in\mathcal{J}}|g_{j,u}^{(t)}|^2.pz_j^{(t)}). \tag{2.41}$$

Although all functions $U_1(pz), U_2(pz), U_3(pz)$ and $U_4(pz)$ are convex, (2.36) and (2.37) remains non-convex because of the negative sign before $(U_2(pz) + U_3(pz))$ and $U_2(pz)$, respectively. However, we resort to solving two sequences of convex problems given as (2.42) and (2.43).

$$\begin{aligned}\hat{f}_1^{(t)}(pz) = \log_2(l_c^{(t)})W_0[U_1(pz) + U_4(pz) - \left(U_2(pz^{(n)}) + U_3(pz^{(n)})\right) \\ -\nabla\left(U_2(pz^{(n)}) + U_3(pz^{(n)})\right)^T(pz - pz^{(n)})],\end{aligned} \tag{2.42}$$

$$\hat{f}_2^{(t)}(pz) = W_0[U_1(pz) - U_2(pz^{(n)}) - \nabla U_2(pz^{(n)})^T(pz - pz^{(n)})], \tag{2.43}$$

where $\nabla\left(U_2(pz^{(n)}) + U_3(pz^{(n)})\right)^T$ and $\nabla U_2(pz^{(n)})^T$ are the gradient of $(U_2 + U_3)(.)$ and $U_2(.)$ at $pz^{(n)}$, respectively. The convexity of (2.42) and (2.43) is straightforward because $-(U_2(pz) + U_3(pz))$ and $-U_2(pz)$ are now linear functions at $pz^{(n)}$. The transformations in (2.36) and (2.42) are applied to the $-\log_2(l_c^{(t)})r_{b,j}^{(t)}$ term, and similarly, the transformations in (2.37) and (2.43) are applied to the $-\tau_{b,j}^{(t)}$ term, with $pz_s^{(t)}$ as the variable. Finally, the optimal solutions can then be found using an iterative algorithm, e.g, (2.43) can be solved as described in Algorithm 2.4.

As shown in (2.43), the first-order Taylor expansion is used to linearize the nonconvex part $-U_2(pz)$ of the objective function is replaced by its convex majorant $-U_2(pz^{(n)}) - \nabla U_2(pz^{(n)})^T(pz - pz^{(n)})]$.

Proof. For any convex function, the first-order Taylor expansion provides a global lower bound.

Algorithm 2.4 The iterative algorithm for DC problems

1: **initialize:** : $n = 0$, $pz^{(n)} = pz^0$
2: **repeat**
3: Solve min $\hat{f}_2(pz)$ with $pz^{(n)}$ to obtain the optimal solution pz^*
4: $pz^{(n+1)} = pz^*$
5: $n = n + 1$
6: **until** $\|pz^{(n+1)} - pz^{(n)}\| \leq \varepsilon$ with a given tolerance $\varepsilon > 0$
7: **return** pz^*.

Since $U_2(pz)$ is convex, we have

$$U_2(pz) \geq U_2(pz^{(n)}) + \nabla U_2(pz^{(n)})^T (pz - pz^{(n)}). \tag{2.44}$$

Therefore,

$$f_2(pz) \leq \hat{f}_2(pz), \ \forall \, pz. \tag{2.45}$$

Thus, the solution to (2.43) is always feasible for (2.37). We solve (2.43) sequentially with the updated variable $pz^{(n)}$, as described in Algorithm 2.4. In fact, Algorithm 2.4 is a decent method that produces a non-increasing sequence of objective values for (2.37), because

$$f_2(pz^{(n)}) \overset{(a)}{=} \hat{f}_2(pz^{(n)}) \overset{(b)}{\geq} \hat{f}_2(pz^{(n+1)}) \overset{(c)}{\geq} f_2(pz^{(n+1)}). \tag{2.46}$$

The convergence of the algorithm then follows directly. Equality (a) holds because, at the nth iteration step, both functions $\hat{f}_2(pz)$, given by (2.43), and $f_2(pz)$ have the same value at $pz^{(n)}$. Inequality (b) follows from the fact that $pz^{(n+1)}$ is the optimal solution to the problem min $\hat{f}_2(pz)$. Inequality (c) follows from (2.45), i.e., $\hat{f}_2(pz) \geq f_2(pz)$ for all pz. Therefore, the sequence $\{f_2(pz^{(n)})\}$ is monotonically decreasing as n increases. It can be shown that Algorithm 2.4 converges to a local minimum solution of the original non-convex problem (2.37),

i.e., a point that satisfies the Karush–Kuhn–Tucker (KKT) conditions [Vucic, Shi & Schubert (2010)].

2.2.4.2 Passive Anti-Interception: Power Allocation

With fixed key length l_c and the optimal jamming transmit powers $pz^*_{c,s}$ and $pz^*_{c,j}$ obtained from solving $\mathcal{JA}$, we derive the power allocation problem $\mathcal{PA}$. This is done by removing constraints (C7), (C8), (C9), and (C10) from problem $\mathcal{P}_1$ as follows

$$\begin{aligned} (\mathcal{PA}) \quad & \max_{p_s, p_b} \sum_{c \in C} \min(\hat{r}^{(t)}_{c,s,b}, \hat{r}^{(t)}_{c,b,j}) \\ \text{s.t.} \quad & \text{(C1)-(C6), (C11).} \end{aligned} \tag{2.47}$$

The proof of non-convexity of the problem $\mathcal{PA}$ is straightforward. To solve $\mathcal{PA}$, the terms $\log_2(l^{(t)}_c) r^{(t)}_{s,b}$ and $\log_2(l^{(t)}_c) r^{(t)}_{b,j}$ in the objective function will use the transformations described in equations (2.36) and (2.42), with $p^{(t)}_s$ and $p^{(t)}_b$ as the respective variables. Similarly, the transformations described in equations (2.37) and (2.43) will apply to $\tau^{(t)}_{s,b}$ and $\tau^{(t)}_{b,j}$, with $p^{(t)}_s$ and $p^{(t)}_b$ as the respective variables. These linearizations result in four convex functions. Consequently, we reuse the Algorithm 2.4 to solve these.

2.2.4.3 AES-based Encryption Anti-Interception

By removing constraints from (C1) to (C8) from problem $\mathcal{P}_1$, we formulate the key length assignment problem $\mathcal{KA}$ using the optimal values $pz^*_{c,s}$, $pz^*_{c,j}$, $p^*_{c,s}$, and $p^*_{c,b}$ obtained from solving $\mathcal{JA}$ and $\mathcal{PA}$ as parameters. The sub-problem $\mathcal{KA}$ is given by

$$\begin{aligned} (\mathcal{KA}) \quad & \max_{l} \sum_{c \in C} \min(\hat{r}^{(t)}_{c,s,b}, \hat{r}^{(t)}_{c,b,j}) \\ \text{s.t.} \quad & \text{(C9)-(C11).} \end{aligned} \tag{2.48}$$

In $\mathcal{KA}$, constraints (C9), (C10), and (C11) are equivalently reformulated as

$$L_{\min} \leq l^{(t)}_c \leq \min\left\{\delta^{\max}_{c,1}, \delta^{\max}_{c,2}\right\}, \text{where} \tag{2.49}$$

$$\delta_{c,1}^{\max} = \min\left\{L_{\max}, \frac{T_{TTI} - t_{0,\text{phy}}}{\rho}\right\}, \tag{2.50}$$

$$\delta_{c,2}^{\max} = \max\left\{L_{\min}, \frac{T_{\text{TTI}}(E_{c,s,\max}^{(t)} - T_{c,s,2}^{(t)} p z_{c,s}^{(t)}) - e_{0,\text{phy}} T_{c,s,1}^{(t)}}{T_{c,s,1}^{(t)} \vartheta}\right\} \tag{2.51}$$

The two objective terms $l_c^{(t)} r_{c,s,b}^{(t)}$ and $l_c^{(t)} r_{c,b,j}^{(t)}$ are increasing and concave functions because $r_{c,s,b}^{(t)} > 0$ and $r_{c,b,j}^{(t)} > 0$. Therefore, to maximize the objective subject to box constraint (2.49), the optimal l_c^* is given by $\left\lfloor \min\left\{\delta_{c,1}^{\max}, \delta_{c,2}^{\max}\right\}\right\rfloor$, where $\lfloor\cdot\rfloor$ denotes the floor function, which returns the largest integer less than or equal to the given value.

2.2.5 Complexity Analysis

Let N_{iter}^0 be the number of iterations of the outer loop of Algorithm 2.3, and let N_{iter}^1 and N_{iter}^2 represent the number of iterations for solving the $\mathcal{JA}$ and $\mathcal{PA}$ sub-problems, respectively. According to [Hoang *et al.* (2016)], the computational complexity of solving a convex problem with m_1 inequality constraints and m_2 variables using the interior-point method is $O(m_1^{1/2}(m_1 + m_2)m_2^2)$. For the $\mathcal{JA}$ sub-problem, where S is the number of E2E connections, there are $5S$ constraints and $2S$ variables, resulting in a complexity of $O(N_{iter}^1 S^{3.5})$. Similarly, for the $\mathcal{PA}$ sub-problem, with $6S$ constraints and $2S$ variables, the complexity is $O(N_{iter}^2 S^{3.5})$. The complexity of solving the $\mathcal{KA}$ sub-problem via its closed-form expression is negligible compared to $\mathcal{JA}$ and $\mathcal{PA}$. Therefore, the overall complexity of Algorithm 2.3 is $O(N_{iter}^0(N_{iter}^1 + N_{iter}^2)S^{3.5})$.

It is worth noting that the original problem $(\mathcal{P}_1)$ is a mixed-integer nonlinear program (MINLP) because it jointly optimizes continuous power and jamming variables together with discrete integer key-length decisions. Such MINLP formulations are known to be NP–hard, and their worst-case complexity grows exponentially with the size of the integer decision space. In contrast, the proposed DC-based decomposition and convexification produce a sequence of convex subproblems whose complexity scales polynomially with S, as characterized above. This

demonstrates that our approach provides a tractable approximation to ($\mathcal{P}_1$) while maintaining convergence to a stationary (KKT) point.

2.2.6 MADRL Approach

To address the computational complexity associated with Algorithm 2.3 in solving problem $\mathcal{P}_1$, particularly due to its iterative nature and the increasing number of variables as the number of user equipment increases, we propose a reinforcement learning strategy. This strategy also accounts for the need to adapt to reduced execution time under high UE mobility. Our approach focuses on transforming the $\mathcal{JA}$ and $\mathcal{PA}$ problems into a deep reinforcement learning (DRL) framework to reduce execution time, while the simpler $\mathcal{KA}$ problem is solved directly. In this RL framework, multiple E2E connections collaborate to jointly optimize the overall transmission rate. This scenario is modeled as a multi-agent system, where each E2E link from an SU to a DU through rBS functions as an independent agent. Each agent employs a Double Deep Q-Network (DDQN) for operation. In this work, DDQN is selected because the jamming and power decisions are modeled as discrete actions to reflect practical implementations, such as those defined in the 3GPP standard. DDQN is well-suited for discrete action spaces and improves training stability by mitigating Q-value overestimation through its double-network structure. In contrast, policy-gradient methods such as Proximal Policy Optimization (PPO) or other Actor–Critic algorithms are primarily designed for continuous action spaces and generally require more complex tuning while exhibiting higher variance when applied to discrete combinatorial decision problems. Therefore, DDQN provides a more stable and computationally efficient solution for our discrete tactical decision environment.

During each time slot t, an agent i receives a state input $s_i^{(t)}$ and selects the optimal action $a_i^{(t)}$. The optimal action is determined by identifying the highest Q-value output by the DDQN. The agents are expected to cooperate to maximize the cumulative transmission rate across all E2E connections. This cooperative MADRL approach is schematically represented in Fig. 2.6.

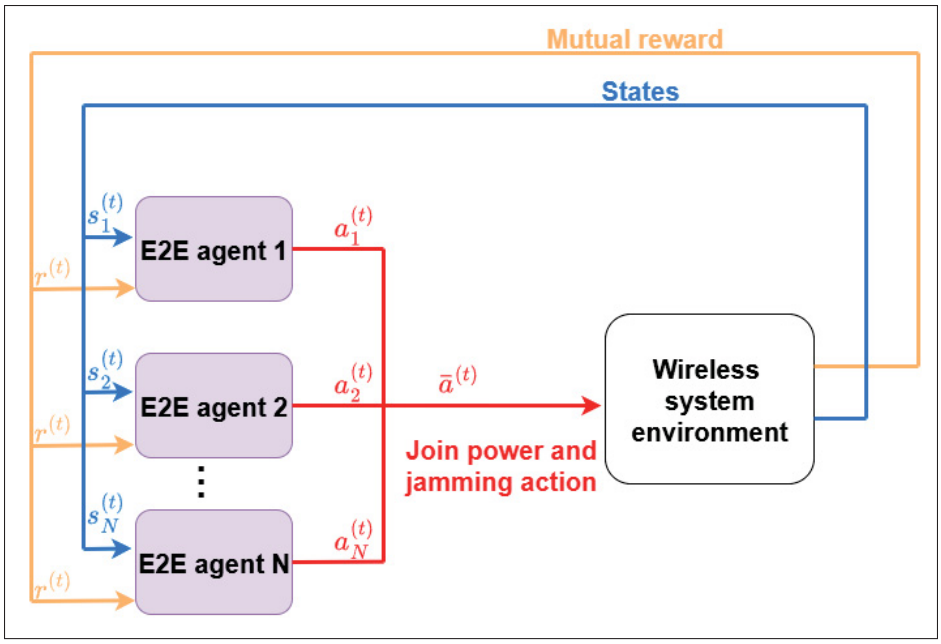

Figure 2.6 Proposed MADRL System

2.2.6.1 State Space

The state space of the MADRL problem is formed by the combination of the estimated channel gains across different channel segments. This state space exists within a continuous domain, with the upper and lower bounds of the estimated channel gains corresponding to the values at the closest and farthest distances between users. The state space is mathematically represented as

$$\bar{S} = \left[|g_{s,b}^{(t)}|^2, |g_{s,u}^{(t)}|^2, |g_{j,u}^{(t)}|^2, |g_{b,j}^{(t)}|^2, |g_{b,u}^{(t)}|^2\right], \tag{2.52}$$

where $|g_{s,b}^{(t)}|^2$, $|g_{s,u}^{(t)}|^2$, $|g_{j,u}^{(t)}|^2$, $|g_{b,j}^{(t)}|^2$, $|g_{b,u}^{(t)}|^2$ are the estimated channel gains for the channels among SU s, rBS interface b, DU j, and eavesdropper's interface u.

This formulation allows for a comprehensive understanding of the network's state, enabling the development of strategies to optimize communication performance in the presence of varying channel conditions.

2.2.6.2 Action Space

The action taken by each agent involves allocating the optimal jamming power levels to SU s and DU j, as well as transmit power to SU s and rBS b for each E2E connection c at time slot t. A discrete action space can be defined based on the minimum and maximum jamming transmit power and transmit power levels. However, defining a discrete action space that spans from minimum to maximum power levels is not advisable, as it can lead to computational inefficiencies. This is because agents typically utilize a limited number of actions. Including unnecessary options in the action space can increase the computational burden on the system.

To address this, we can define an action space with a limited set of actions. Let n_1 and n_2 be the selected jamming power actions for SU $(X_1, X_2, \ldots, X_{n_1})$ and DU $(Y_1, Y_2, \ldots, Y_{n_2})$, respectively. Let n_3 and n_4 be the selected transmit power actions for SU $(U_1, U_2, \ldots, U_{n_3})$ and rBS $(V_1, V_2, \ldots, V_{n_4})$. The combined action space $\bar{\mathcal{A}}$ can be represented as

$$\bar{\mathcal{A}} = \{X_{m_1} Y_{m_2} U_{m_3} V_{m_4} \mid m_1 \in [1, n_1],\ m_2 \in [1, n_2], m_3 \in [1, n_3],\ m_4 \in [1, n_4]\}. \tag{2.53}$$

This representation indicates the possible combinations of actions for the SU, DU, and rBS, allowing for efficient management of power levels while minimizing computational complexity. By selecting specific actions, the system can maintain the necessary E2E connections without unnecessary processing overhead.

2.2.6.3 Reward Design

The reward function is crucial for transforming an optimization problem into a MADRL problem. When designing a reward function, it's essential to incorporate terms related to both the objective function and the constraints of the optimization problem. This approach ensures that the agents' actions adhere to the problem constraints. Notably, some constraints can be omitted from the reward function because they are inherently satisfied by the design of the state and action spaces. Our reward function is formulated to provide a mutual reward value to all agents at each time

slot t as follows

$$r^{(t+1)} = \lambda_0 K_0^{(t)} - \lambda_1 K_1^{(t)} - \lambda_2 K_2^{(t)} + \lambda_3 K_3^{(t)} + \lambda_4 K_4^{(t)} + \lambda_5 K_5^{(t)} + \lambda_6 K_6^{(t)}, \tag{2.54}$$

where $\lambda_i, i = 0, \ldots, 6$ are coefficients tuned to achieve optimal solutions while satisfying constraints, and $K_i^{(t)}, i = 0, \ldots, 6$ are functions that are defined as

$$K_0^{(t)} = (\mathcal{P}_1)_{\text{Objective}}, K_1^{(t)} = \sum_{c \in C} \left(\gamma_{c,s,u}^{(t)} - \mu \right), K_2^{(t)} = \sum_{c \in C} \left(\gamma_{c,b,u}^{(t)} - \mu \right), K_3^{(t)} = \sum_{c \in C} \left(\gamma_{c,s,b}^{(t)} - \gamma_{\min} \right),$$
$$K_4^{(t)} = \sum_{c \in C} \left(\gamma_{c,b,j}^{(t)} - \gamma_{\min} \right), \quad K_5^{(t)} = P_{b,\max} - \sum_{c \in C} p_{c,b}^{(t)}, K_6^{(t)} = \sum_{c \in C} \left(E_{c,s,\max}^{(t)} - e_{c,s}^{(t)} \right). \tag{2.55}$$

Specifically, $K_0^{(t)}$ represents the total transmission rate of all E2E connections at timeslot t. The term $\lambda_0 K_0^{(t)}$ corresponds to the objective function. Terms $\lambda_1 K_1^{(t)}$ and $\lambda_2 K_2^{(t)}$ are designed to protect the system from energy-based detectors, derived from constraints (C1) and (C2). The negative signs before these terms indicate penalties, encouraging reduced SINR to achieve higher LPI performance. Terms $\lambda_3 K_3^{(t)}$ and $\lambda_4 K_4^{(t)}$ aim to satisfy constraints (C3) and (C4), respectively. The term $\lambda_5 K_5^{(t)}$ controls the transmit power of the rBS, ensuring it remains within the allowable range defined by constraint (C6). The term $\lambda_6 K_6^{(t)}$ regulates the energy consumption, satisfying constraint (C11). Constraints (C5), (C7), (C8), (C9), and (C10) are not included in the reward function design as they can be satisfied through the action space design. This formulation provides a comprehensive reward function that balances the optimization objective with the necessary constraints, guiding the MADRL agents toward optimal solutions within the problem's constraints.

2.2.7 Proposed MADRL Algorithm

We employ a CTDE approach to implement our proposed MADRL strategy. This paradigm allows for efficient training while maintaining the ability for agents to act independently during execution.

2.2.7.1 Training Phase

A centralized controller at the rBS collects the entire network environment states $s^{(t)}$ of all agents. The centralized critic uses this global information to select actions based on an ϵ-greedy algorithm. The output action is selected randomly or based on the highest Q-value. These selected actions are then used to determine the optimal key length by solving problem $\mathcal{KA}$ for the next state $s^{(t+1)}$. Subsequently, a mutual reward is distributed to all agents in the system. Finally, the weight sets of the DDQN model are updated accordingly. Algorithm 2.5 provides detailed training procedures

2.2.7.2 Execution Phase

The trained DRL models are then distributed from the centralized controller to the local agents. This decentralized approach allows each agent to download and utilize the trained DRL models locally. Agents can make independent decisions on jamming and power transmission at each timeslot t, and adapt to local conditions without constant communication with a central entity. The achieved power values are then used as input to solve problem $\mathcal{KA}$, yielding an optimal key length value. This decentralized execution ensures both the scalability and robustness of the system, as agents can operate autonomously based on their learned policies.

2.2.8 MADRL Computational Complexity

The feed-forward pass of each agent's DDQN network consists of $\sum_{i=0}^{L} N_i N_{i+1}$ multiplications, $\sum_{i=1}^{L+1} N_i$ activations, and $\sum_{i=0}^{L} N_i N_{i+1}$ additions, where N_0 is the input size, N_i $(i = 1, \ldots, L)$ are the hidden-layer sizes, and N_{L+1} is the output size. Since multiplications dominate the computational cost, the operations to run the feed-forward pass algorithm are estimated $S \cdot N^m \cdot \sum_{i=0}^{L} N_i N_{i+1}$ multiplications, where N^m is the number of operations to realize a 1-digit multiplication. Generally, multiplying two n-digit numbers requires approximately n^2 1-digit multiplications. In our implementation, we have 3 hidden layers with sizes as specified in Table II, $S = 5$ agents, and $N^m = 64^2$ for 64-bit floating-point operations. Substituting the values from our

Algorithm 2.5 MADRL Algorithm for solving problem $\mathcal{P}_1$

initialize:
  for each agent i **do**
    Initialize the main Q-network $Q\left(s^{(t)}, a^{(t)}; \theta^{(t)}\right)$
    Initialize the target Q-network $\hat{Q}\left(s^{(t)}, a^{(t)}; \theta'^{(t)}\right)$
    Initialize the replay memory $\mathcal{D}$ with capacity C
  end for
repeat
  Observe the whole network state $s^{(t)}$
  for each agent i **do**
    ε = random.randrange(0, 1)
    if $\varepsilon < \varepsilon_{\text{greedy}}$ **then**
      Solve $\mathcal{JA}$ and $\mathcal{PA}$ by using random action $a_i^{(t)} \in \bar{\mathcal{A}}$
    else
      Solve $\mathcal{JA}$ and $\mathcal{PA}$ by selecting DRL model $a_i^{(t)} = \arg\max_{a \in \bar{\mathcal{A}}} Q\left(s_i^{(t+1)}, a; \theta_i^{(t)}\right)$
    end if
  end for
  Solve problem ($\mathcal{KA}$) with $a_i^{(t)}$, obtain $l^{(t)*}$
  Observe next state $s^{(t+1)}$ and calculate mutual reward
  Store transition $\left(s^{(t)}, a^{(t)}, r^{(t)}, s^{(t+1)}\right)$ in $\mathcal{D}$
  if the replay memory $\mathcal{D}$ is full **then**
    Sample a mini-batch of K transitions from $\mathcal{D}$
    Update $\theta^{(t+1)}$ using Adam optimizer
    After Z timesteps, update $\theta'^{(t+1)} = \theta^{(t)}$
  end if
  $t \leftarrow t + 1$
until Done all tasks or maximum time slots is reached.

implementation: $5 \cdot 64^2 \cdot (5 \cdot 250 + 250 \cdot 120 + 120 \cdot 60 + 60 \cdot 1000) \approx 2.016 \times 10^9$ operations. For a CPU chipset with a processing capacity of 20 TOPS, the time to calculate the output of the learner can be estimated as $(2.016 \times 10^9$ operations$)/(20 \times 10^{12}$ operations/second$) \approx 0.1$ milliseconds.

To obtain the jamming-power, power-allocation, and key-length decisions in Algorithm 2.5, we need to run the feed-forward pass algorithm. Therefore, the total number of operations per timestep during the execution phase is approximately $S \cdot N^m \cdot \sum_{i=0}^{L} N_i N_{i+1}$.

CHAPTER 3

RESULTS AND ANALYSIS

In this chapter, we report numerical results and analyze the proposed anti-interception strategies presented in Section 2 (Subsections 2.1 and 2.2). For each scenario, we detail the simulation setup and the corresponding parameter values.

3.1 Numerical Results for the Double-Layered Anti-Interception Strategy

3.1.1 Simulation Setup

In this section, we evaluate the performance of our proposed MADRL strategy through a series of simulations. We compare our MADRL with four baselines: i) our proposed optimization strategy (Proposed OPT), ii) the PASA optimization strategy from [Le, Nguyen & Nguyen (2023b)], which optimizes both the transmit power and spreading factor of SUs and rBS, iii) the power allocation (PA) strategy from [Shi, Wang, Salous & Zhou (2017)], which optimizes user transmit power, iv) a fully random method where the transmit power and spreading factor for both SUs and rBS are allocated randomly. The simulations are conducted in a DS-CDMA-based WIN-T network with 10 GCV users in a 100x100m^2 area covered by the base station. The enemy eavesdropper is located 200m from the rBS. Other parameters are shown in Table 3.1.

To achieve prompt action computation and prevent over-parameterization, we design a simple neural network architecture comprising one input layer, three hidden layers, and one output layer. The hidden layers are structured with N1=1000, N2=500, and N3=250 neurons, respectively. The input dimension is configured as 5, corresponding to the number of state dimensions. The output dimension is 1000, covering both jamming and transmit power actions. This parameter is intentionally kept slightly large to ensure that the actions generated by the MADRL model closely approximate those of the optimization results. We show time-series results starting from the 25th timeslot to avoid initial parameter influence, maintaining consistent simulation parameters across all baselines.

Table 3.1 Parameters used in the network simulation.

Parameter	**Value**
Number of users	10
SU max transmit power ($P_{s,\max}$)	0.25 W
rBS max transmit power ($P_{b,\max}$)	19.95 W
SU max jamming power ($PZ_{s,\max}$)	2 W
DU max jamming power ($PZ_{j,\max}$)	2 W
SU max spreading factor ($M_{s,\max}$)	255
rBS max spreading factor ($M_{b,\max}$)	255
Original bandwidth (W_0)	38.4 kHz
Path-loss exponent (α)	2
Noise power (σ^2)	0.01 W
Decoding threshold ($\gamma_{\min}$)	-14 dB
EVE detection threshold (μ)	-8 dB
User velocity range	[50, 100] km/h

3.1.2 Simulation Results

3.1.2.1 Reward Convergence

In Fig. 3.1, we present the mutual reward per training episode, illustrating the convergence behavior of the proposed MADRL method. During the first 1400 episodes, the cumulative reward per episode increases significantly due to the exploration-exploitation process. After approximately 1400 episodes, the performance gradually converges to a stable value, though some fluctuations remain due to the mobility of the GCV users. As the ϵ-greedy algorithm is employed, the actions taken during the final 2600 episodes are mostly based on the current DRL model instead of the random process. This demonstrates the efficiency of our training process.

3.1.2.2 Energy-based Interception Avoidance

With μ = -8dB, we use the measured average SINR at EVE to assess the system's defense against energy-based interception. Fig. 3.2 compares SINR values for the random, PA, PASA, and our proposed optimization and MADRL strategies. The random strategy shows the weakest

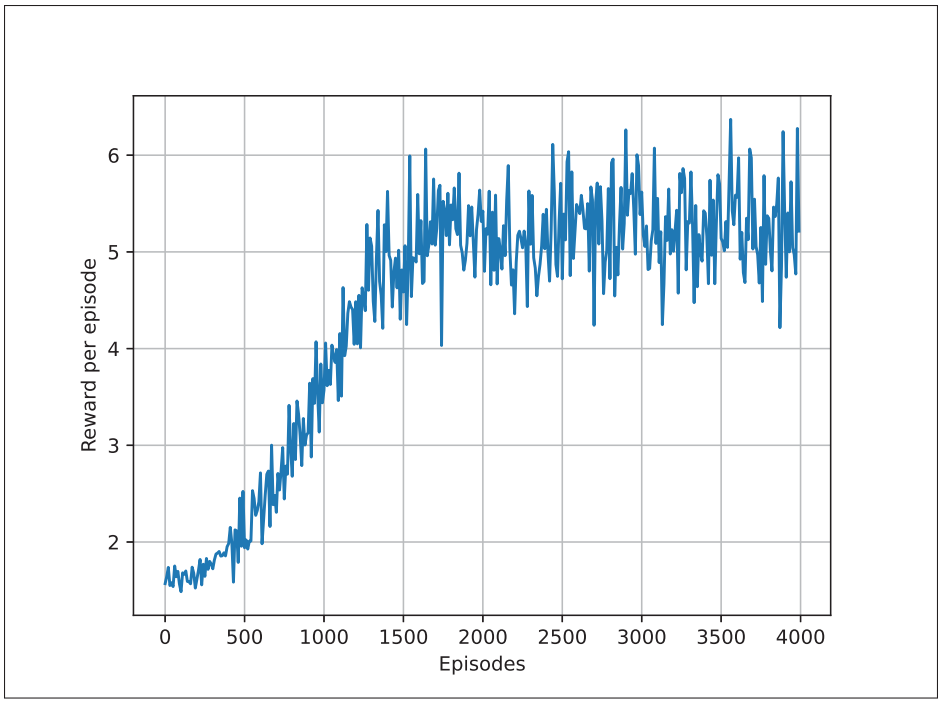

Figure 3.1 Training reward convergence

performance, with most values around -7.7dB, making the system vulnerable to interception. This result is expected, as users transmit at high power without considering eavesdropping risks. The PA and PASA solutions offer the best and second-best protection against energy-based interception, with SINR levels around -12dB for PA and -10dB for PASA. However, this requires reducing signal energy to very low levels, indicating a poor trade-off between LPI performance and the QoS objective. In contrast, our proposed solutions can maintain LPI at a level close to -8dB, achieving a better balance between security and performance. The LPI performance of the proposed MADRL method closely matches that of the proposed optimization method, with SINR values around -8.5dB for both.

3.1.2.3 Transmission Rate Performance

Fig. 3.3 illustrates the achievable total rate across different time slots. We can see that the PA method achieves the lowest transmission rate, while the PASA method demonstrates moderate performance. This can be attributed to the trade-off these methods face between throughput

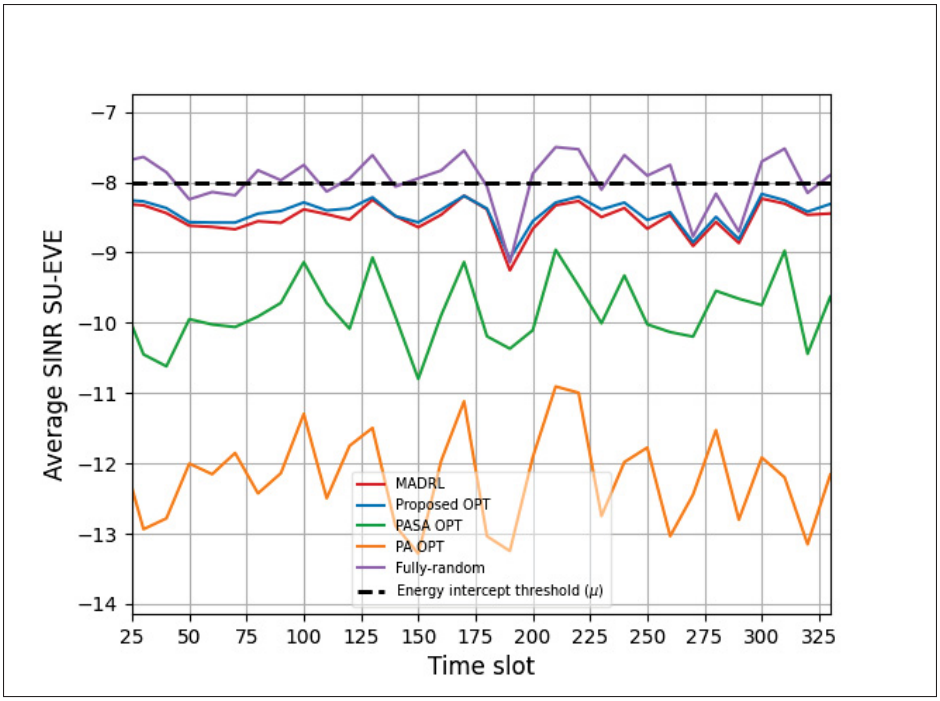

Figure 3.2 Average measured SINR value

performance and energy interception avoidance. On the other hand, the two proposed methods maintain the SINR at the eavesdropper near -8dB (refer to Fig. 3), indicating that the system is in a secure state without sacrificing the total transmission rate objective. Specifically, the proposed optimization method significantly enhances throughput performance, exceeding 60Kbps. Additionally, the rate achieved by the MADRL method is relatively close to that of the optimization method, with less than a 6% difference across all simulation scenarios. In practice, the transmission rate of the MADRL method can be effectively enhanced by adjusting the coefficients λ_i. This adjustment enables a balance between LPI performance and the QoS objective.

3.1.2.4 Complexity Comparison

Fig. 3.4 compares the computational complexity, represented by the time required for the system to find an optimal solution at each time slot t. The result highlights the main advantage of applying the proposed MADRL method over traditional optimization solvers. Overall, the

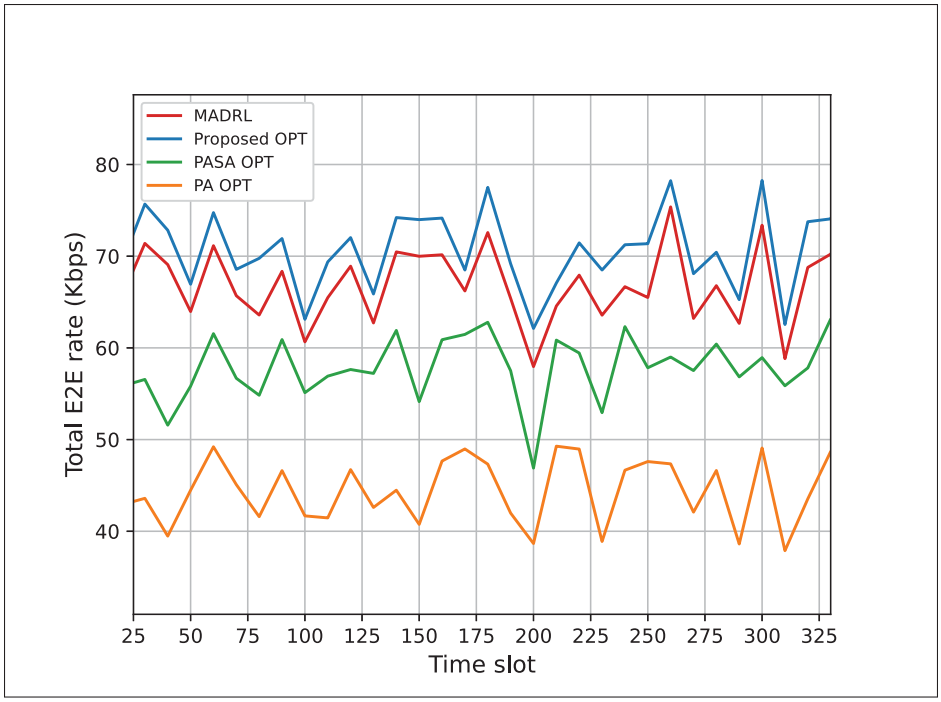

Figure 3.3 E2E total transmission rate

proposed MADRL solution requires significantly less time than the proposed optimization method. The MADRL approach consistently requires less than 0.2s to find a solution in each time slot t, while the proposed optimization method needs more than 0.75s when the coverage tolerance ω = 1e-3. The complexity of the proposed OPT method increases rapidly as the convergence tolerance ω decreases from 1e-3 to 1e-5, which affects the accuracy of the optimization solution. This comparison suggests that the MADRL method can be applied to systems with high mobility-induced channel variation. In contrast, the optimization method is more appropriate for systems with low-mobility users and relatively low accuracy requirements for solutions.

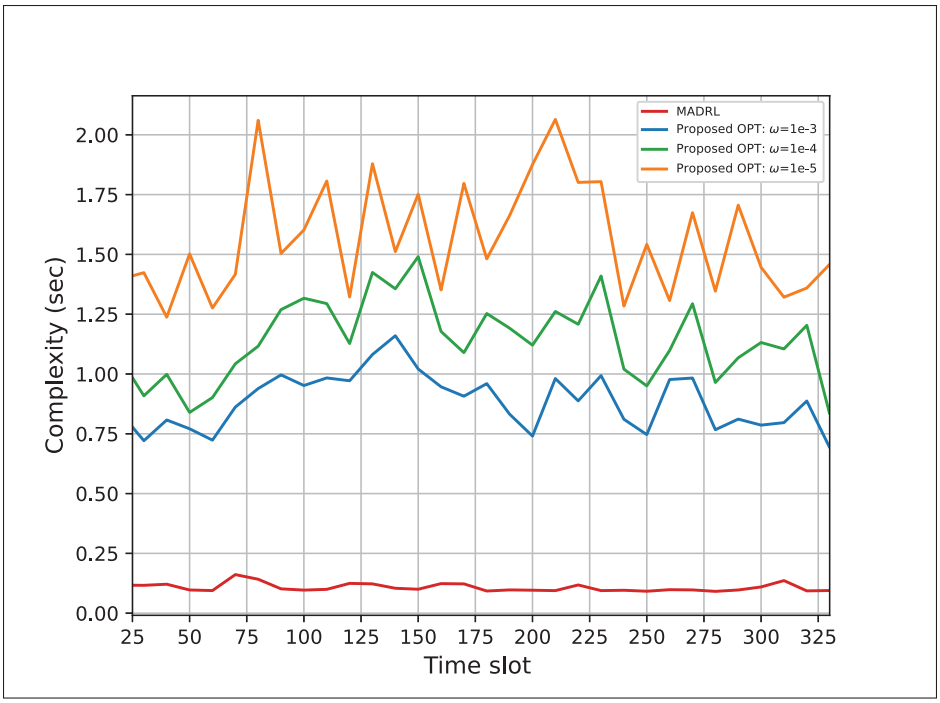

Figure 3.4 Time execution comparison

3.2 Numerical Results for the Triple-Layered Anti-Interception Strategy

3.2.1 Simulation Setup

We compare our MADRL strategy with four baselines: i) our proposed optimization strategy (Proposed OPT), ii) the Passive OPT optimization strategy from [Shi *et al.* (2020)], which optimizes the transmit power of SUs and rBS, iii) the Active OPT from [Park *et al.* (2013)], which optimizes jamming transmit power of SUs and DUs, iv) a fully random method where the transmit power for both SUs and rBS is allocated randomly. Our proposed strategies utilize AES encryption with key lengths of 128, 192, or 256 bits, whereas the baselines (i) to (iii) employ a fixed key length of $l_c = 42$, as used in basic DS-CDMA. The selected baselines serve four main purposes. First, they demonstrate the energy-based interception avoidance capability of our proposed MADRL method compared to either optimization methods or the absence of optimization. Second, they evaluate the efficiency of throughput performance in the combined triple-layered anti-interception framework, which includes jamming strategies,

power allocation, and encryption, relative to other methods. Third, they highlight the reduced energy consumption of our methods while achieving the same targeted rate as non-encrypted systems. Finally, they compare the execution time of our proposed MADRL method with that of traditional optimization strategies. A tactical network topology is simulated over relatively flat terrain, where the communication channel characteristics of SUs, rBS, DUs, and EVE are similar. The small-scale fading coefficients follow an exponential distribution with a unit mean. The large-scale path loss is modeled as $128.1 + 37.6 \log_{10}(d)$, where d (in kilometers) represents the distance between the transmitter and receiver. The noise power, σ^2, is set at -73 dBm. We conduct a simulation in a DS-CDMA-based TVAN with 10 GCV users located within an area of 100x100 m^2 covered by the base station. The enemy eavesdropper is positioned at a distance of 200 m from the rBS. The other simulation parameters are provided in Table 3.2.

Table 3.2 Parameters for network simulation.

Parameter	**Value**
Number of users	10
Transmission time interval (TTI)	10 ms
SU maximum energy consumption ($E_{c,s,\max}^{(t)}$)	0.1 J
SU max transmit power ($P_{s,\max}$)	0.25 W
rBS max transmit power ($P_{b,\max}$)	19.95 W
SU max jamming power ($PZ_{s,\max}$)	2 W
DU max jamming power ($PZ_{j,\max}$)	2 W
SU spreading factor ($M_{s,\max}$)	255
rBS spreading factor ($M_{b,\max}$)	255
Original bandwidth (W_0)	38.4 kHz
Decoding threshold ($\gamma_{\min}$)	-14 dB
EVE detection threshold (μ)	-8 dB
User velocity range	[50, 100] km/h

To achieve prompt action computation and prevent over-parameterization, we design a simple neural network architecture comprising one input layer, three hidden layers, and one output layer. The hidden layers are structured with N1 = 250, N2 = 120, and N3 = 60 neurons, respectively. The input dimension is configured as 5, corresponding to the number of state dimensions. The output dimension is 1000, covering both jamming and transmit power actions. This parameter is

intentionally kept relatively large to ensure that the actions generated by the MADRL model closely approximate those of the optimization results. The detailed parameter setup for DRL is summarized in Table 3.3. We display time-series results from the 25th time slot onwards due to scale and resolution constraints, ensuring that the initial parameters do not significantly influence the outcome. The simulation parameters are consistently applied across all baselines.

Table 3.3 DRL parameters summary.

Hyperparameter	**Value**
Neural network input dimension	5
Neural network hidden layers (1,2,3)	250, 120, 60
Neural network output dimension	1000
Learning rate	0.001
Discount factor	0.95
ϵ decay stop threshold	0.02
Replay memory batch size	2000
Reward coefficient $\lambda_i,\ i = 0, \ldots, 6$	0.000005, 1.8, 0.35, 0.0000375, 0.0003, 0.005, 0.25

3.2.2 Simulation Results

3.2.2.1 Reward Convergence

In Fig. 3.5, we present the mutual reward per training episode, illustrating the convergence behavior of the proposed MADRL method. During the first 1850 episodes, the cumulative reward per episode increases significantly due to the exploration-exploitation process. After approximately 1850 episodes, the performance gradually converges to a stable value, though some fluctuations remain due to the dynamic mobility of the GCV users. As the ϵ-greedy algorithm is employed, the actions taken during the final 3150 episodes are mostly based on the current DRL model instead of the random process. This demonstrates the efficiency of our training process.

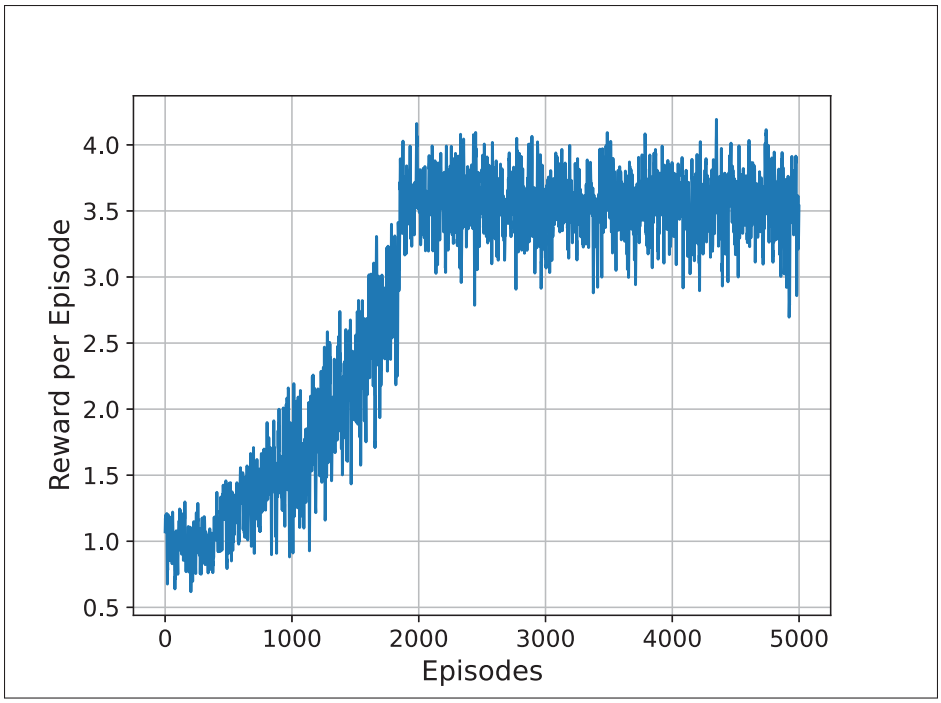

Figure 3.5 Mutual reward obtained at each episode

3.2.2.2 Energy-based Interception Avoidance

With energy intercept threshold μ = -8 dB, we base the measured average SINR at EVE to evaluate the system's defense against energy-based interception. Fig. 3.6 compares the SINR values among the fully random strategy, Passive OPT strategy, Active OPT strategy, and our Proposed OPT and MADRL strategies. The SINR value in the fully random strategy demonstrates the worst performance, with most values remaining around -7.5 dB above the energy intercept threshold μ = -8 dB. This indicates that the system is vulnerable to interception during user communication. This result is expected, as all users in the system attempt to transmit information at high power levels without considering potential eavesdropping.

The Passive OPT and Active OPT solutions achieve the highest and second-highest performance in protecting the system against energy-based interception. The SINR fluctuates around -9.8 dB for Passive OPT and -11.2 dB for Active OPT. These results suggest that signal energy must be reduced to a significantly low level, which reflects a poor trade-off between LPI performance

and the QoS objective. In contrast, our proposed solutions can maintain the network's LPI at a level close to -8 dB, ensuring an acceptable balance between security and performance. The LPI performance of the proposed MADRL method closely matches that of the Proposed OPT method, with SINR values around -8.4 dB for both. In scenarios with high user mobility, MADRL is preferred over the proposed optimization approach due to its comparable LPI performance and significantly lower execution time (see Fig.3.12, 3.13).

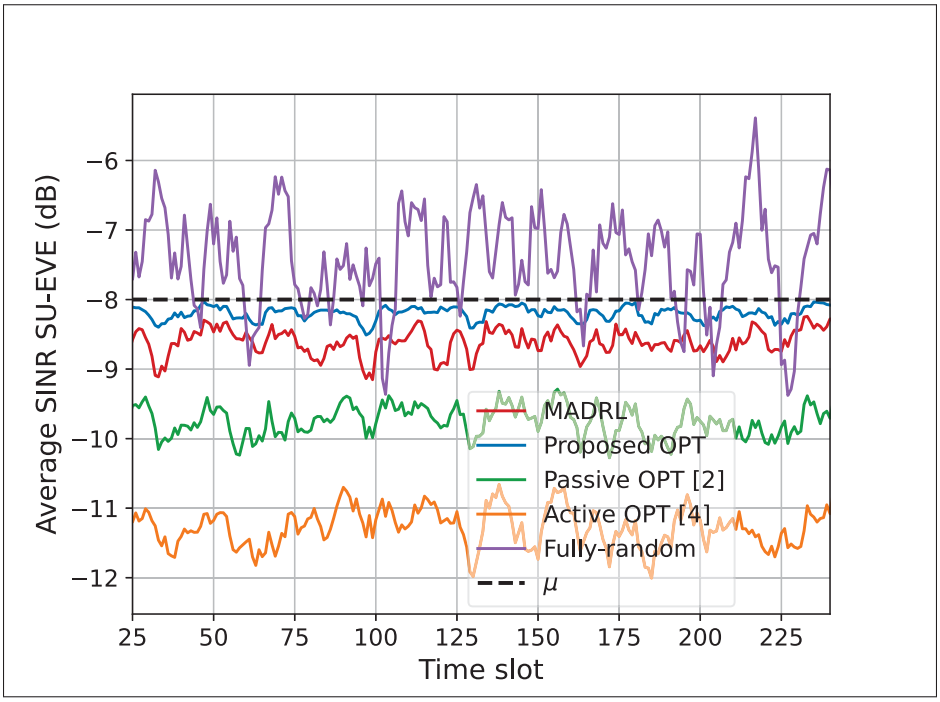

Figure 3.6 Average measured SINR in channel SU-EVE

In Fig. 3.7, we investigate the secrecy throughput performance when the system must satisfy lower energy interception thresholds μ. This reflects scenarios where EVE uses more sensitive receivers that can detect weaker signals. In general, when $\mu = -8$ dB, EVE employs the least sensitive receiver, meaning the system does not need to significantly compromise QoS to maintain LPI. As a result, the secrecy throughput of all methods is highest. By contrast, when $\mu = -12$ dB, EVE is assumed to use the most sensitive detection capability, which forces all approaches to reduce their secrecy throughput to enhance LPI performance. We observe that both the MADRL and Proposed OPT methods consistently achieve higher secrecy throughput

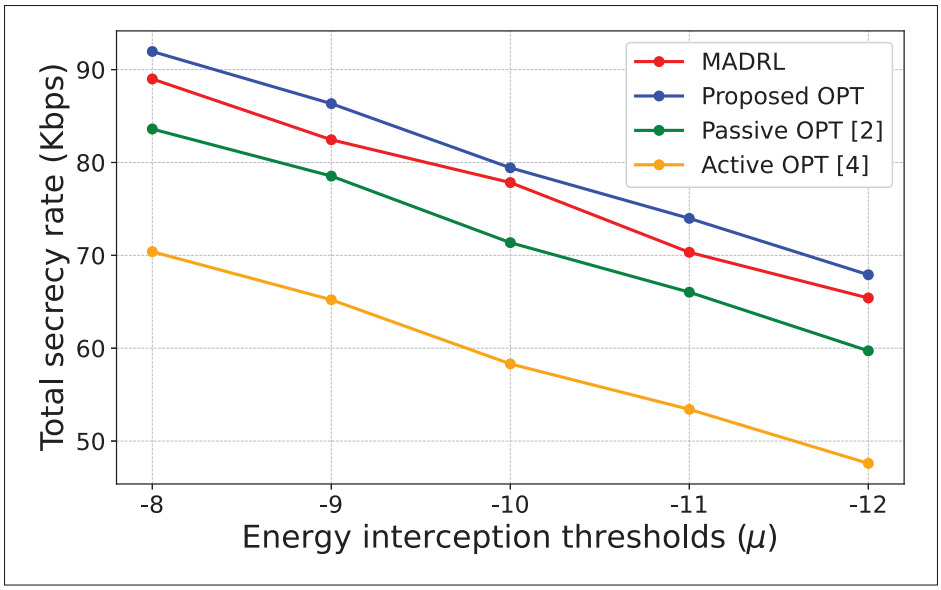

Figure 3.7 Total encryption-aware secrecy rate under different energy interception thresholds (μ)

than the Passive OPT and Active OPT baselines, thus better preserving system QoS. Additionally, the MADRL method closely follows the performance of the Proposed OPT method across all threshold values μ. For instance, at $\mu = -9$ dB, the MADRL method attains 95.56% of the throughput achieved by the Proposed OPT method.

3.2.2.3 Encryption-Aware Secrecy Rate Performance

Fig. 3.8 illustrates the achievable total encryption-aware secrecy rate across different time slots. We can see that the Active OPT method achieves the lowest transmission rate, approximately 70 Kbps, while the Passive OPT method demonstrates moderate performance at around 83 Kbps. This can be attributed to the trade-off between throughput performance and energy interception avoidance faced by these methods. On the other hand, the two proposed methods maintain the SINR at the eavesdropper near -8 dB (see Fig. 3.6), indicating that the system is in a secure state without sacrificing the total transmission rate objective. Specifically, the Proposed OPT method significantly enhances throughput performance, exceeding 87 Kbps. Additionally, the rate achieved by the MADRL method is relatively close to that of the optimization method, with

less than a 5% difference across all simulation scenarios. In practice, the rate of the MADRL can be effectively enhanced by adjusting the coefficients λ_i. This adjustment enables a balance between LPI performance and the QoS objective.

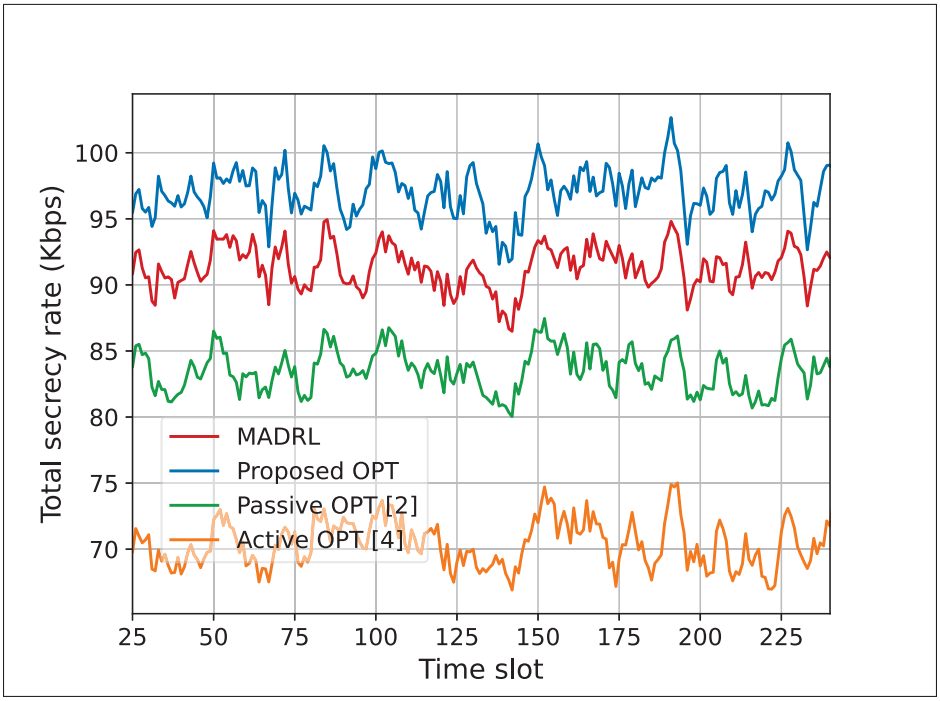

Figure 3.8 Total encryption-aware secrecy rate of E2E connections over time

Fig. 3.9 illustrates the total E2E encryption-aware secrecy rate across varying TTI durations. It can be observed that both the MADRL and Proposed OPT methods achieve significantly higher secrecy rates than the Passive OPT and Active OPT approaches across all TTI durations. For example, at a short TTI of 8 ms, the Proposed OPT and MADRL methods attain secrecy rates of 91.9 Kbps and 88.3 Kbps, respectively, compared to only 85.0 Kbps and 70.9 Kbps for Passive and Active OPT. This demonstrates that even under constrained conditions, the learning-based and optimization-based strategies outperform the fixed-key-length baselines (e.g., 42 bits for Passive and Active OPT). Furthermore, as the TTI increases, the secrecy rates of MADRL and Proposed OPT continue to improve, reaching 99.3 Kbps and 103.3 Kbps at 12 ms, respectively. This improvement is due to the use of adaptive key lengths in these methods, enabling them to leverage longer TTIs for more secure transmission. In contrast, the Passive

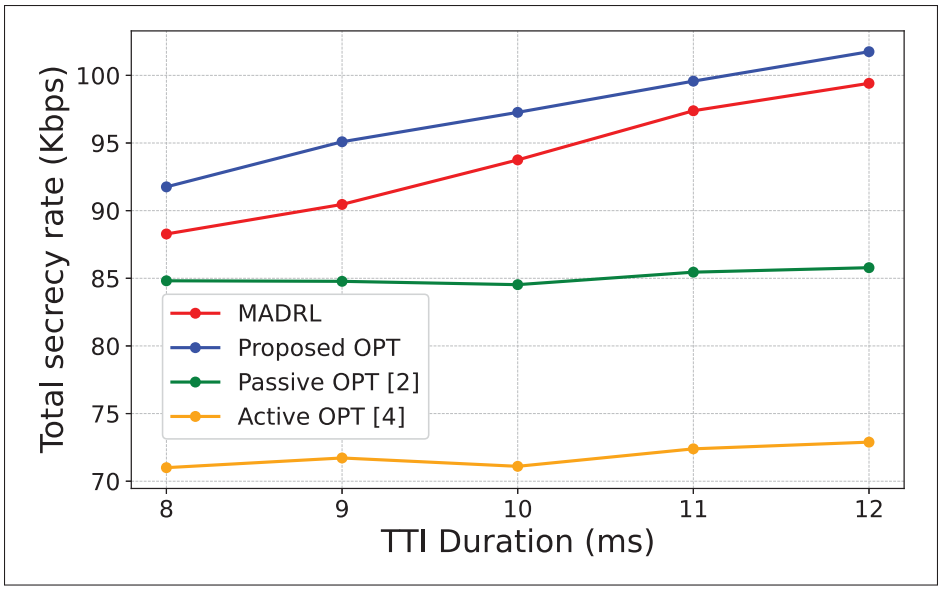

Figure 3.9 Total E2E encryption-aware secrecy rate across different transmission time intervals (TTIs)

and Active OPT methods exhibit nearly constant performance across all TTIs, as they rely on fixed-length encryption keys that do not benefit from longer transmission durations.

3.2.2.4 Reduced energy consumption

With the advantage of AES-based encryption approach, we can reduce energy consumption while still achieving the same targeted encryption-aware secrecy rate as non-encrypted systems. This benefit is demonstrated in Fig. 3.10, which shows the energy consumption for the Passive OPT strategy, Active OPT strategy, and our proposed optimization and MADRL strategies, using a targeted rate such as the voice rate of 9.6 kbps. Overall, the proposed optimization and MADRL strategies require significantly less energy than the Passive and Active OPT strategies. Specifically, our approaches consistently require less than 0.058 J to achieve a voice rate of 9.6 kbps in each time slot t, whereas the baseline optimization methods require more than 0.06 J. Furthermore, the energy consumption performance of the optimization method is slightly better than that of the MADRL method. Specifically, the energy consumption of the optimization method reaches around 0.0054 J, while the MADRL method fluctuates around 0.0056 J. This

difference can be logically explained by the fact that the encryption-aware secrecy rate of MADRL is higher than that of the optimization method (refer to Fig. 3.8), leading to slightly higher energy consumption.

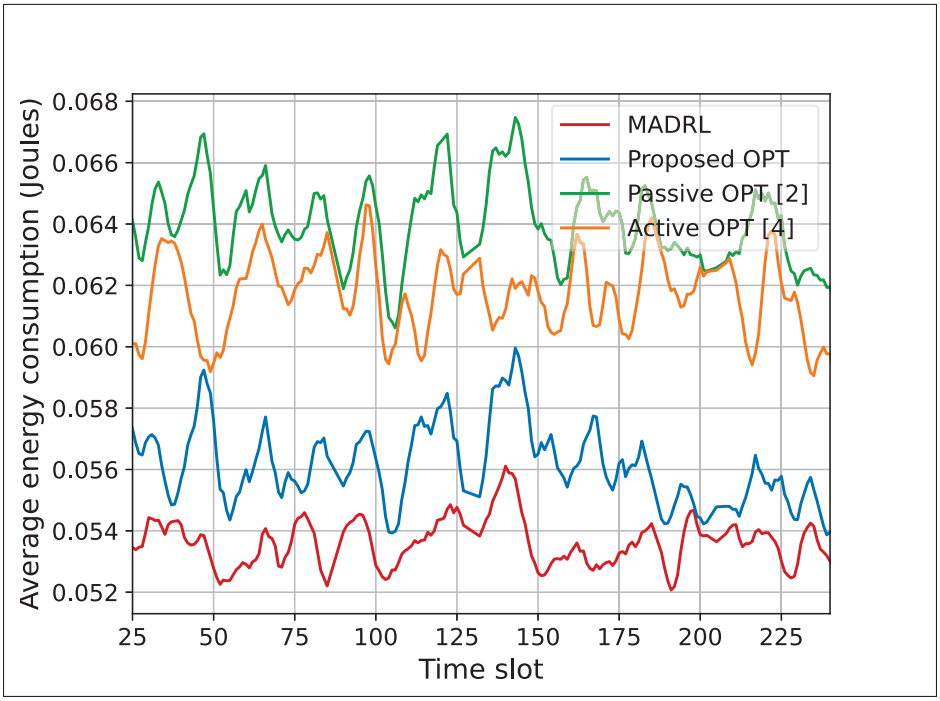

Figure 3.10 Average energy consumption per connection over time

Fig. 3.11 illustrates the total E2E encryption-aware secrecy rate achieved by different methods under varying maximum energy consumption constraints per UE. As observed, the secrecy rate of all approaches increases with higher energy budgets. This is in alignment with our expectation, as more available energy allows UEs to transmit with higher power and generate longer encryption keys, resulting in improved secure throughput. Furthermore, the Proposed OPT and MADRL methods consistently outperform the Passive OPT and Active OPT baselines across all energy levels. For instance, at the maximum energy consumption of 0.12 J, the Proposed OPT and MADRL methods achieve 97.7 Kbps and 96.2 Kbps, respectively, while Passive and Active OPT only reach 88.7 Kbps and 75.8 Kbps. These results highlight the

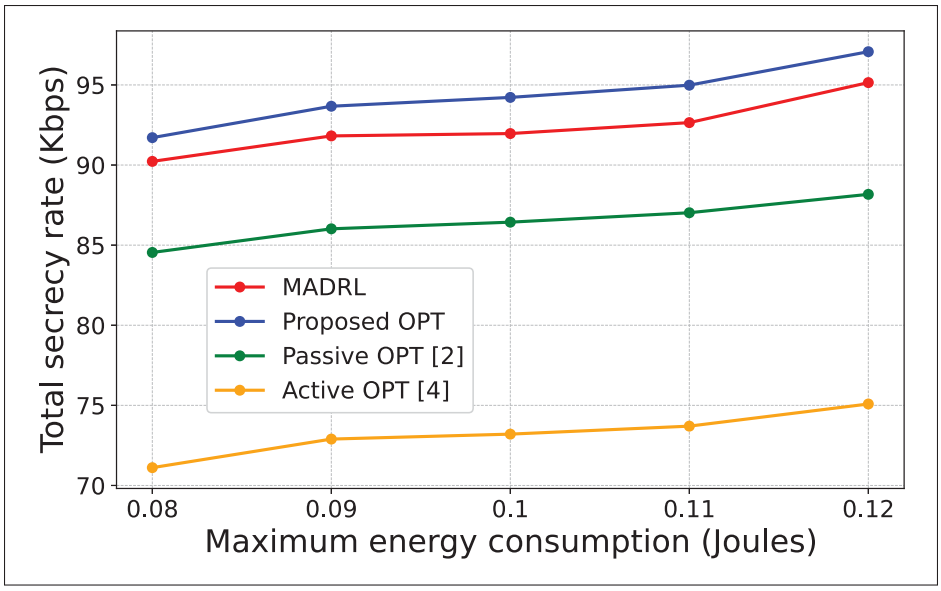

Figure 3.11 Total E2E encryption-aware secrecy rate across different maximum energy consumption levels of UEs

superior performance of the proposed learning-based and optimization-based approaches in energy-constrained environments.

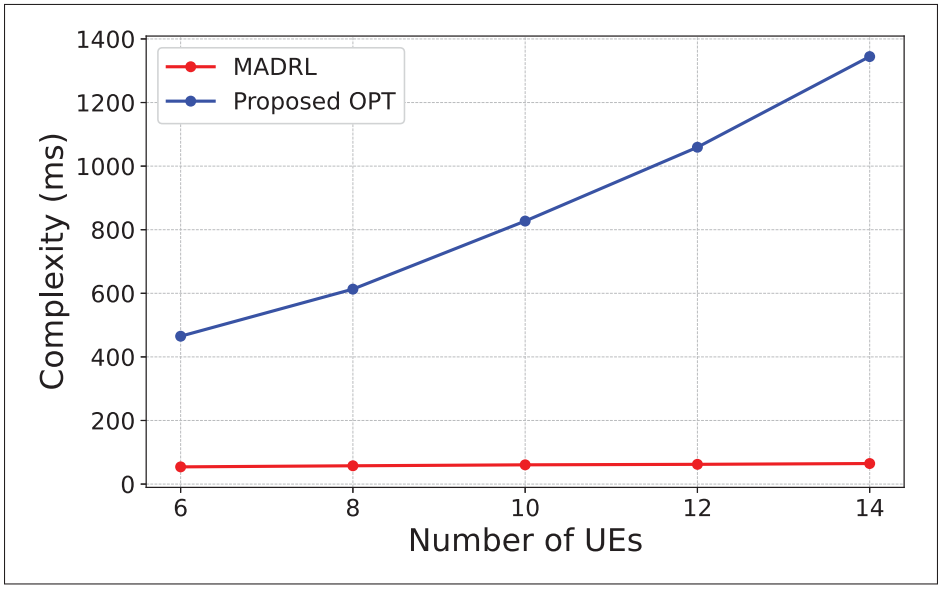

Figure 3.12 Complexity comparison over different numbers of users

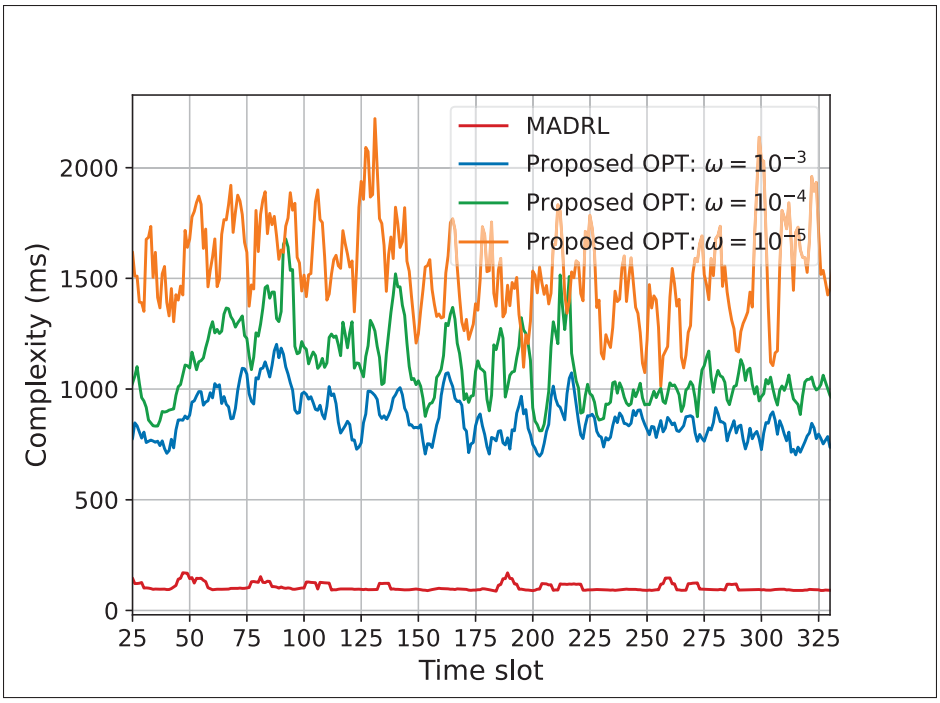

Figure 3.13 Complexity comparison over time slots

3.2.2.5 Complexity Comparison

Fig. 3.12 shows the computational complexity of the proposed optimization and MADRL methods, measured in milliseconds, for different numbers of UEs. The complexity reflects the average time required to compute resource allocation solutions at each time slot t. As observed, the complexity of the proposed OPT method increases sharply with the number of users, reaching nearly 1400 ms for 14 UEs. In contrast, the MADRL method demonstrates remarkable scalability, maintaining a nearly constant computation time below 70 ms regardless of the number of UEs. Specifically, at 6 UEs, the OPT method is approximately 7 times more computationally demanding than the MADRL approach. These results highlight the significant efficiency advantage of the learning-based MADRL method in dynamic multi-user environments, particularly as the network scales.

Fig. 3.13 compares the computational complexity, represented by the time required for the system to find optimal solutions at each time slot t. The result highlights the main advantage

of applying the proposed MADRL method over traditional optimization solvers. Overall, the proposed MADRL solution requires significantly less time than the optimization method. The MADRL approach consistently takes less than 70 ms to find a solution in each time slot t, while the proposed optimization method needs more than 730 ms when the coverage tolerance ω is set at 1e-3. In addition, the complexity of the proposed OPT method increases rapidly as the convergence tolerance ω decreases from 1e-3 to 1e-5, which affects the accuracy of the optimization solution. This comparison suggests that the MADRL method can be applied to systems with high mobility-induced channel variation. In contrast, the optimization method is more appropriate for systems with low-mobility users and relatively low accuracy requirements for solutions.

3.2.2.6 Performance Under Eavesdropper Location Uncertainty

To capture this uncertainty without imposing heavy distributional assumptions, we adopt a channel-gain uncertainty model for the EVE links and derive a Markov-inequality-based safe approximation for the LPI chance constraints. Specifically, the actual channel power gain between any transmitter x and EVE u on carrier c at time slot t is modeled as

$$|g_{c,x,u}^{(t)}|^2 = X_c^{(t)} \left|\hat{g}_{c,x,u}^{(t)}\right|^2, \tag{3.1}$$

where $\hat{g}_{c,x,u}^{(t)}$ is the estimated gain from the path-loss model, and $X_c^{(t)} \geq 0$ captures residual mismatch due to EVE location uncertainty. Under (3.1), the instantaneous EVE SINRs in the two transmission phases, corresponding to (2.20) and (2.22), become

$$\gamma_{c,s,u}^{X,(t)} = \frac{X_c^{(t)} m_{c,s}^{(t)} \left|\hat{g}_{c,s,u}^{(t)}\right|^2 p_{c,s}^{(t)}}{\sigma^2 + X_c^{(t)} \sum_{k \neq s} \left|\hat{g}_{c,k,u}^{(t)}\right|^2 p_{c,k}^{(t)} + X_c^{(t)} \sum_{j \in \mathcal{J}} \left|\hat{g}_{c,j,u}^{(t)}\right|^2 p z_{c,j}^{(t)}} \tag{3.2}$$

$$\gamma_{c,b,u}^{X,(t)} = \frac{X_c^{(t)} m_{c,b}^{(t)} \left|\hat{g}_{c,b,u}^{(t)}\right|^2 p_{c,b}^{(t)}}{\sigma^2 + X_c^{(t)} \sum_{k \neq b} \left|\hat{g}_{c,k,u}^{(t)}\right|^2 p_{c,k}^{(t)} + X_c^{(t)} \sum_{s \in \mathcal{S}} \left|\hat{g}_{c,s,u}^{(t)}\right|^2 p z_{c,s}^{(t)}}. \tag{3.3}$$

Accordingly, $\mathcal{P}_1$ can be rewritten with the probabilistic channel-gain uncertainty constraints as

$$\begin{aligned}(\mathcal{P}_X) \quad & \max_{pz_s,\, pz_j,\, p_s,\, p_b,\, l} \sum_{c\in C} \min\Big(\hat{r}^{(t)}_{c,s,b},\ \hat{r}^{(t)}_{c,b,j}\Big) \\ \text{s.t.} \quad & (\text{C1X}):\ \mathbb{P}\Big(\gamma^{X,(t)}_{c,s,u} \geq \mu\Big) \leq \epsilon, \\ & (\text{C2X}):\ \mathbb{P}\Big(\gamma^{X,(t)}_{c,b,u} \geq \mu\Big) \leq \epsilon, \\ & (\text{C3})\text{–}(\text{C11}).\end{aligned} \tag{3.4}$$

where constraints (C1) and (C2) are replaced by the probabilistic constraints (C1X) and (C2X), which guarantee that the probability of the EVE SINR exceeding the energy-detection threshold μ in phases 1 and 2 does not exceed ϵ.

To obtain a tractable formulation of $\mathcal{P}_X$, we apply Markov's inequality to derive sufficient linear surrogates for the chance constraints (C1X) and (C2X) [Alsenwi *et al.* (2021)]. Consider the generic form $\gamma^X = \frac{XU}{\sigma^2+XV}$, where $U \geq 0$ and $V \geq 0$ collect the desired-signal and interference-plus-jamming terms, respectively, and $X \geq 0$ denotes the random channel-gain uncertainty factor. Define the margin $D \triangleq U - \mu V$. Then

$$\gamma^X \geq \mu \iff X(U-\mu V) \geq \mu\sigma^2 \iff X \geq \frac{\mu\sigma^2}{D}, \tag{3.5}$$

where the last step holds for $D > 0$ (if $D \leq 0$, then $\mathbb{P}(\gamma^X \geq \mu) = 0$ and the chance constraint is trivially satisfied). Applying Markov's inequality to the nonnegative random variable X, $\mathbb{P}(X \geq a) \leq \mathbb{E}[X]/a$ for $a > 0$, and setting $a = \mu\sigma^2/D$ yields

$$\mathbb{P}\Big(\gamma^X \geq \mu\Big) \leq \frac{\mathbb{E}[X]\, D}{\mu\sigma^2}. \tag{3.6}$$

Therefore, sufficient Markov-safe replacements of (C1X) and (C2X) are

$$U^{(t)}_{c,s,u} - \mu V^{(t)}_{c,s,u} \leq \frac{\epsilon\, \mu\, \sigma^2}{\mathbb{E}[X^{(t)}_c]}, \tag{3.7}$$

$$U^{(t)}_{c,b,u} - \mu V^{(t)}_{c,b,u} \leq \frac{\epsilon\, \mu\, \sigma^2}{\mathbb{E}[X^{(t)}_c]}, \tag{3.8}$$

where

$$U_{c,s,u}^{(t)} = m_{c,s}^{(t)} \left|\hat{g}_{c,s,u}^{(t)}\right|^2 p_{c,s}^{(t)}, \tag{3.9}$$

$$V_{c,s,u}^{(t)} = \sum_{k \neq s} \left|\hat{g}_{c,k,u}^{(t)}\right|^2 p_{c,k}^{(t)} + \sum_{j \in \mathcal{J}} \left|\hat{g}_{c,j,u}^{(t)}\right|^2 p z_{c,j}^{(t)}, \tag{3.10}$$

$$U_{c,b,u}^{(t)} = m_{c,b}^{(t)} \left|\hat{g}_{c,b,u}^{(t)}\right|^2 p_{c,b}^{(t)}, \tag{3.11}$$

$$V_{c,b,u}^{(t)} = \sum_{k \neq b} \left|\hat{g}_{c,k,u}^{(t)}\right|^2 p_{c,k}^{(t)} + \sum_{s \in \mathcal{S}} \left|\hat{g}_{c,s,u}^{(t)}\right|^2 p z_{c,s}^{(t)}. \tag{3.12}$$

Finally, $\mathcal{P}_X$ can be solved by decomposing it into three subproblems, as presented in Algorithm 2.3.

With a bounded localization error Δ, the worst case occurs when EVE is closest to transmitter x, i.e., at distance $\hat{r}_{c,x,u}^{(t)} - \Delta$. Since $|g|^2 \propto r^{-\alpha}$, this implies the gain-inflation factor $X_c^{(t)} \triangleq |g_{c,x,u}^{(t)}|^2 / |\hat{g}_{c,x,u}^{(t)}|^2 \leq \left(\frac{\hat{r}_{c,x,u}^{(t)}}{\hat{r}_{c,x,u}^{(t)} - \Delta}\right)^{\alpha}$. Hence, in a distribution-free manner, $\mathbb{E}[X_c^{(t)}] \leq \max_{x \in \mathcal{S}/\mathcal{B}} \left(\frac{\hat{r}_{c,x,u}^{(t)}}{\hat{r}_{c,x,u}^{(t)} - \Delta}\right)^{\alpha}$, and we use this worst-case upper bound to set the Markov parameter $\mathbb{E}[X_c^{(t)}]$.

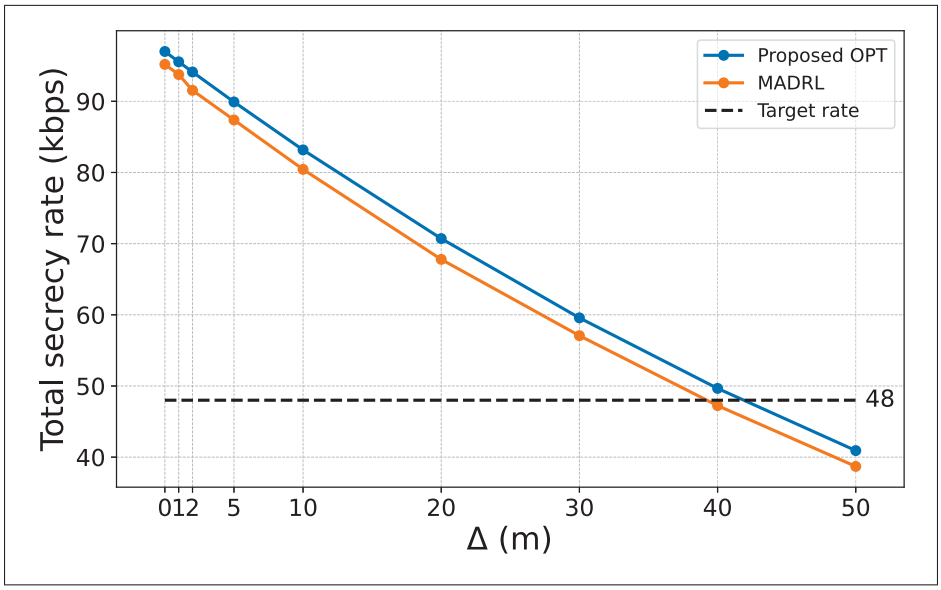

Figure 3.14 Total encryption-aware secrecy rate versus Δ under probabilistic constraints

Fig. 3.14 depicts the total encryption-aware secrecy rate achieved by the proposed OPT and MADRL schemes versus the bounded EVE localization uncertainty radius Δ, which captures the practical case where the EVE position is imperfectly estimated in tactical environments. As Δ increases, the achievable secrecy rate decreases monotonically for both schemes because a larger uncertainty region yields a more conservative gain-inflation bound (i.e., a larger upper bound on $\mathbb{E}[X_c^{(t)}]$), which tightens the Markov-safe LPI constraints and forces more conservative power/jamming/key-length decisions. To assess mission-level feasibility, we also plot the target rate required to support voice traffic, i.e., 9.6 kbps $\times$5 connections = 48 kbps. At $\Delta = 0$ (idealized perfect EVE location knowledge), OPT achieves about 97 kbps, while MADRL achieves about 95 kbps. For moderate uncertainty (e.g., Δ = 10–20 m), the secrecy rate reduces to approximately 83–71 kbps for OPT and 80–68 kbps for MADRL, which remains well above the 48 kbps target. Importantly, even under a large localization error of $\Delta = 40$ m, OPT still maintains a secrecy rate of about 50 kbps, satisfying the target voice requirement, while MADRL remains very close to the target (about 47 kbps), indicating strong robustness and good policy generalization under bounded EVE uncertainty. Under severe uncertainty $\Delta = 50$ m, the secrecy rate drops to roughly 41 kbps for OPT and 39 kbps for MADRL. This uncertainty level is consistent with the spatial scale of the simulated 100 m$\times$100 m tactical field and corresponds to an EVE location error of roughly 25% relative to the nominal 200 m EVE–rBS separation. Overall, the results confirm that the proposed framework remains effective and exhibits a graceful robustness–performance tradeoff when the EVE position is not perfectly known.

CONCLUSION AND RECOMMENDATIONS

This thesis studied anti-interception protection for tactical wireless networks operating in highly dynamic and adversarial environments. The main contributions of this thesis are summarized as follows.

First, a double-layered anti-interception strategy was developed for DS-CDMA WIN-T ground combat vehicular networks. The joint allocation of transmit power, jamming power, and spreading factors was formulated as a non-convex optimization problem under QoS and LPI constraints. Using first-order Taylor approximation, DC decomposition, and a sequential JA–PA–SA solution structure, an iterative algorithm was derived to obtain near-optimal solutions. The results also showed that the optimization approach becomes computationally expensive as the system size increases.

Second, to enable near real-time operation, a MADRL-based solution was proposed. A hybrid design was adopted: the most computationally intensive parts (jamming and power allocation) were handled by learning, while spreading assignment was solved using a simpler conventional step. By embedding the constraints into the reward design, the agents learned feasible and high-quality policies. The MADRL solution reduced runtime significantly while maintaining performance close to the optimization baseline.

Third, the framework was extended to a triple-layered strategy by adding AES-based scrambling with adaptive key length. This introduced a practical trade-off among confidentiality, latency, and energy consumption. To capture this trade-off, an encryption-aware secrecy rate metric was introduced. The results showed that adaptive key-length selection, when jointly optimized with passive and active defenses, can improve secrecy while satisfying latency and energy constraints.

Recommendations and Future Work

- **More realistic tactical channels and scenarios:** Future work should evaluate the framework under more complex propagation conditions (e.g., strong shadowing, urban/forest environments, maritime reflections, or underwater links). The strategy can also be extended to other tactical systems such as UAV ad-hoc networks and satellite communications.
- **Multiple and smarter interceptors:** This thesis mainly considered a single interceptor with dual interception capability. Future studies should model multiple coordinated interceptors with heterogeneous and more advanced interception techniques, and develop robust defenses against such threats.
- **Cooperation with additional defense modules:** The framework can be strengthened by integrating additional modules such as adaptive jamming and intelligent reflecting surfaces (IRS) to further reduce leakage toward interceptors while improving desired links.
- **Experimental and hardware validation:** Implementing the proposed strategy on SDR/FPGA testbeds or tactical radio prototypes would provide practical validation and highlight implementation issues such as synchronization, latency, and hardware constraints.

BIBLIOGRAPHY

Alsenwi, M., Tran, N. H., Bennis, M., Pandey, S. R., Bairagi, A. K. & Hong, C. S. (2021). Intelligent Resource Slicing for eMBB and URLLC Coexistence in 5G and Beyond: A Deep Reinforcement Learning Based Approach. *IEEE Transactions on Wireless Communications*, 20(7), 4585-4600. doi: 10.1109/TWC.2021.3060514.

Aref, M. A., Jayaweera, S. K. & Machuzak, S. (2017). Multi-Agent Reinforcement Learning Based Cognitive Anti-Jamming. *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-6. doi: 10.1109/WCNC.2017.7925694.

Axell, E. & Larsson, E. G. (2011). Optimal and Sub-Optimal Spectrum Sensing of OFDM Signals in Known and Unknown Noise Variance. *IEEE Journal on Selected Areas in Communications*, 29(2), 290-304. doi: 10.1109/JSAC.2011.110203.

Bark, G. (1997). Power control in an LPI adaptive frequency-hopping system for HF communications. *Seventh International Conference on HF Radio Systems and Techniques*, pp. 301-305. doi: 10.1049/cp:19970809.

Bastami, H., Letafati, M., Moradikia, M., Abdelhadi, A., Behroozi, H. & Hanzo, L. (2021). On the Physical Layer Security of the Cooperative Rate-Splitting-Aided Downlink in UAV Networks. *IEEE Transactions on Information Forensics and Security*, 16, 5018-5033. doi: 10.1109/TIFS.2021.3122989.

Benincasa, G., Bunch, L., Casini, E., Lenzi, R., Morelli, A., Paulini, M. S., Suri, N. & Uszok, A. (2018). Bridging the gap between enterprise and tactical networks via mission- and network-sensitive adaptation. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1-8. doi: 10.1109/ICMCIS.2018.8398699.

Conceição, F., Antunes, C. H., Gomes, M., Silva, V. & Dinis, R. (2022). Max-Min Fairness Optimization in Uplink Cell-Free Massive MIMO Using Meta-Heuristics. *IEEE Transactions on Communications*, 70(3), 1792-1807. doi: 10.1109/TCOMM.2022.3144989.

Diamant, R. & Lampe, L. (2018). Low Probability of Detection for Underwater Acoustic Communication: A Review. *IEEE Access*, 6, 19099-19112. doi: 10.1109/ACCESS.2018.2818110.

Diamant, R., Lampe, L. & Gamroth, E. (2014). Low probability of detection for underwater acoustic communication. *2014 Oceans - St. John's*, pp. 1-6. doi: 10.1109/OCEANS.2014.7003005.

Diamant, R., Lampe, L. & Gamroth, E. (2017). Bounds for Low Probability of Detection for Underwater Acoustic Communication. *IEEE Journal of Oceanic Engineering*, 42(1), 143-155. doi: 10.1109/JOE.2016.2550278.

Dong, L., Han, Z., Petropulu, A. P. & Poor, H. V. (2010). Improving Wireless Physical Layer Security via Cooperating Relays. *IEEE Transactions on Signal Processing*, 58(3), 1875-1888. doi: 10.1109/TSP.2009.2038412.

Elmasry, G. & Corwin, P. (2021). Hiding the RF Signal Signature in Tactical 5G. *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, pp. 733-738. doi: 10.1109/MILCOM52596.2021.9652968.

Garnaev, A., Petropulu, A., Trappe, W. & Poor, H. V. (2022). An Anti-Jamming Multiple Access Channel Game Using Latency as Metric. *IEEE Wireless Communications Letters*, 11(9), 1800-1804. doi: 10.1109/LWC.2022.3181301.

Goeckel, D., Vasudevan, S., Towsley, D., Adams, S., Ding, Z. & Leung, K. (2011). Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks. *IEEE Journal on Selected Areas in Communications*, 29(10), 2067-2076. doi: 10.1109/JSAC.2011.111216.

Gong, P., Zhang, Z., Wu, Y. & Wang, W.-Q. (2022). Joint Design of Transmit Waveform and Receive Beamforming for LPI FDA-MIMO Radar. *IEEE Signal Processing Letters*, 29, 1938-1942. doi: 10.1109/LSP.2022.3205206.

Gu, X., Zhao, Z. & Shen, L. (2016). Blind estimation of pseudo-random codes in periodic long code direct sequence spread spectrum signals. *IET Communications*, 10(11), 1273-1281. doi: https://doi.org/10.1049/iet-com.2015.0374.

Guo, H., Yang, Z., Zou, Y., Qian, M., Zhu, J. & Hanzo, L. (2019). Joint Optimization of Power Splitting and Beamforming in Energy Harvesting Cooperative Networks. *IEEE Transactions on Communications*, 67(12), 8247-8257. doi: 10.1109/TCOMM.2019.2945324.

Gutman, L. & Prescott, G. (1989). System quality factors for LPI communications. *IEEE Aerospace and Electronic Systems Magazine*, 4(12), 25-28. doi: 10.1109/62.46987.

Haleem, M., Mathur, C., Chandramouli, R. & Subbalakshmi, K. (2007). Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks. *IEEE Transactions on Dependable and Secure Computing*, 4(4), 313-324. doi: 10.1109/TDSC.2007.70214.

He, B., Ni, Q., Chen, J., Yang, L. & Lv, L. (2019). User-Pair Selection in Multiuser Cooperative Networks With an Untrusted Relay. *IEEE Transactions on Vehicular Technology*, 68(1), 869-882. doi: 10.1109/TVT.2018.2882178.

He, X. & Yener, A. (2010). Cooperation With an Untrusted Relay: A Secrecy Perspective. *IEEE Transactions on Information Theory*, 56(8), 3807-3827. doi: 10.1109/TIT.2010.2050958.

Hoang, T. D., Le, L. B. & Le-Ngoc, T. (2016). Energy-Efficient Resource Allocation for D2D Communications in Cellular Networks. *IEEE Transactions on Vehicular Technology*, 65(9), 6972-6986. doi: 10.1109/TVT.2015.2482388.

Huang, J. & Swindlehurst, A. L. (2011). Cooperative Jamming for Secure Communications in MIMO Relay Networks. *IEEE Transactions on Signal Processing*, 59(10), 4871-4884. doi: 10.1109/TSP.2011.2161295.

Hui, H., Swindlehurst, A. L., Li, G. & Liang, J. (2015). Secure Relay and Jammer Selection for Physical Layer Security. *IEEE Signal Processing Letters*, 22(8), 1147-1151. doi: 10.1109/LSP.2014.2387860.

HWANG, Y. M., JUNG, J. H., KIM, K. Y., KIM, Y. S., LEE, J. S., SHIN, Y. & KIM, J. Y. (2017). Energy-Efficient Resource Allocation Strategy for Low Probability of Intercept and Anti-Jamming Systems. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E100.A(11), 2498-2502. doi: 10.1587/transfun.E100.A.2498.

Jameel, F., Wyne, S., Kaddoum, G. & Duong, T. Q. (2019). A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Communications Surveys & Tutorials*, 21(3), 2734-2771. doi: 10.1109/COMST.2018.2865607.

Jans, W., Nissen, I., Gerdes, F., Sangfelt, E., Solberg, C.-e. & Walree, P. (2006, 01). UUV covert acoustic communications – preliminary results of the first sea experiment.

Jeon, S., Kwak, J. & Choi, J. P. (2022). Cross-Layer Encryption of CFB-AES-TURBO for Advanced Satellite Data Transmission Security. *IEEE Transactions on Aerospace and Electronic Systems*, 58(3), 2192-2205. doi: 10.1109/TAES.2021.3134988.

Krikidis, I., Thompson, J. S. & Mclaughlin, S. (2009). Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, 8(10), 5003-5011. doi: 10.1109/TWC.2009.090323.

Kuang, Q., Speidel, J. & Droste, H. (2012). Joint Base-Station Association, Channel Assignment, Beamforming and Power Control in Heterogeneous Networks. *IEEE Veh. Technol. Conf.*

Kumar, A. & Zhu, Y. (2021). Extending Direct Sequence Spread-Spectrum for Secure Communication. *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1-5. doi: 10.1109/ISNCC52172.2021.9615783.

Le, V. H., Nguyen, T. T. & Nguyen, K. K. (2023a). Dual Wireless Anti-Interception for Ground Combat Vehicles. *IEEE Transactions on Vehicular Technology*, 72(12), 16236-16248. doi: 10.1109/TVT.2023.3298514.

Le, V. H., Nguyen, T. T. & Nguyen, K. K. (2023b). Protecting Tactical Ground Combat Vehicle Networks Against Dual Wireless Interceptions. *ICC 2023 - IEEE International Conference on Communications*, pp. 2400-2405. doi: 10.1109/ICC45041.2023.10278656.

Le, V. H., Nguyen, T. T. & Nguyen, K. K. (2025). Dual Anti-Jamming Alleviation for Radio Frequency/Free-Space Optical (RF/FSO) Tactical Systems. *IEEE Transactions on Vehicular Technology*, 74(1), 1092-1103. doi: 10.1109/TVT.2024.3464128.

Lee, H., Eom, S., Park, J. & Lee, I. (2018). UAV-Aided Secure Communications With Cooperative Jamming. *IEEE Transactions on Vehicular Technology*, 67(10), 9385-9392. doi: 10.1109/TVT.2018.2853723.

Lee, J., Kapitanova, K. & Son, S. H. (2010). The price of security in wireless sensor networks. *Computer Networks*, 54(17), 2967-2978. doi: https://doi.org/10.1016/j.comnet.2010.05.011.

Li, B., Zhang, M., Rong, Y. & Han, Z. (2021). Artificial Noise-Aided Secure Relay Communication With Unknown Channel Knowledge of Eavesdropper. *IEEE Transactions on Wireless Communications*, 20(5), 3168-3179. doi: 10.1109/TWC.2020.3047926.

Li, T., Song, T. & Liang, Y. (2018). Enhanced CDMA System with Secure Scrambling. In *Wireless Communications under Hostile Jamming: Security and Efficiency* (pp. 15–44). Singapore: Springer Singapore.

Li, T., Ren, J., Ling, Q. & Jain, A. (2005). Physical layer built-in security analysis and enhancement of CDMA systems. *MILCOM*. doi: 10.1109/MILCOM.2005.1605803.

Ling, Q., Li, T. & Ren, J. (2005). Physical layer built-in security enhancement of DS-CDMA systems using secure block interleaving. *GLOBECOM '05. IEEE Global Telecommunications Conference, 2005.*, 3, 5 pp.-. doi: 10.1109/GLOCOM.2005.1577965.

Liu, S., Khan, M. A., Bilal, M. & Zuberi, H. H. (2025). Low Probability Detection Constrained Underwater Acoustic Communication: A Comprehensive Review. *IEEE Communications Magazine*, 63(2), 21-30. doi: 10.1109/MCOM.001.2400008.

Liu, X., Yuan, Y., Zhang, T., Cui, G. & Tay, W. P. (2024). Integrated Transmit Waveform and RIS Phase Shift Design for LPI Detection and Communication. *IEEE Transactions on Wireless Communications*, 23(6), 5663-5679. doi: 10.1109/TWC.2023.3327685.

Liu, Y., Shen, Y., Guo, D. & Win, M. Z. (2018). Network Localization and Synchronization Using Full-Duplex Radios. *IEEE Transactions on Signal Processing*, 66(3), 714-728. doi: 10.1109/TSP.2017.2770090.

Lu, X., Xu, Z., Ren, H. & Yi, W. (2022). LPI-based Resource Allocation Strategy for Target Tracking in the Moving Airborne Radar Network. *2022 IEEE Radar Conference (RadarConf22)*, pp. 1-6. doi: 10.1109/RadarConf2248738.2022.9764195.

Ma, X., Ballal, T., Chen, H., Aldayel, O. & Al-Naffouri, T. Y. (2021). A Maximum-Likelihood TDOA Localization Algorithm Using Difference-of-Convex Programming. *IEEE Signal Processing Letters*, 28, 309-313. doi: 10.1109/LSP.2021.3051836.

Mills, R. & Prescott, G. (1994). Detection of multiple access low-probability-of-intercept networks. *Proceedings of TCC'94 - Tactical Communications Conference*, pp. 497-504. doi: 10.1109/TCC.1994.472094.

Mobasseri, B. G. & Pham, K. D. (2018). Chirp Spread Spectrum Performance in Low Probability of Intercept Theater. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pp. 329-335. doi: 10.1109/MILCOM.2018.8599777.

Nguyen, V. H. & Nguyen, K. K. (2025). Double-Layered Anti-Interception Strategy for Ground Combat Vehicles. *ICC 2025 - IEEE International Conference on Communications*, pp. 1845-1850. doi: 10.1109/ICC52391.2025.11161286.

Nikjah, R. & Beaulieu, N. C. (2008). On antijamming in general CDMA systems-part I: multiuser capacity analysis. *IEEE Transactions on Wireless Communications*, 7(5), 1646-1655. doi: 10.1109/TWC.2008.060626.

Park, C., Kim, G. S., Park, S., Jung, S. & Kim, J. (2023). Multi-Agent Reinforcement Learning for Cooperative Air Transportation Services in City-Wide Autonomous Urban Air Mobility. *IEEE Transactions on Intelligent Vehicles*, 8(8), 4016-4030. doi: 10.1109/TIV.2023.3283235.

Park, K.-H., Wang, T. & Alouini, M.-S. (2013). On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming. *IEEE Journal on Selected Areas in Communications*, 31(9), 1741-1750. doi: 10.1109/JSAC.2013.130908.

Pirayesh, H. & Zeng, H. (2022). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 24(2), 767-809. doi: 10.1109/COMST.2022.3159185.

Pourranjbar, A., Kaddoum, G., Ferdowsi, A. & Saad, W. (2021). Reinforcement Learning for Deceiving Reactive Jammers in Wireless Networks. *IEEE Transactions on Communications*, 69(6), 3682-3697. doi: 10.1109/TCOMM.2021.3062854.

Qi, J., Zhang, H., Qi, X. & Peng, M. (2024). Deep Reinforcement Learning Based Hopping Strategy for Wideband Anti-Jamming Wireless Communications. *IEEE Transactions on Vehicular Technology*, 73(3), 3568-3579. doi: 10.1109/TVT.2023.3324387.

Raghavan, R. S. (2019). A CFAR Detector for Mismatched Eigenvalues of Training Sample Covariance Matrix. *IEEE Transactions on Signal Processing*, 67(17), 4624-4635. doi: 10.1109/TSP.2019.2929942.

Sadig, T., Maleki, M., Tran, N. H. & Bahrami, H. R. (2020). An Encryption-Aware PHY Security Framework for 4-Node Gaussian Wiretap Channels With Joint Power Constraint. *IEEE Transactions on Communications*, 68(12), 7837-7850. doi: 10.1109/TCOMM.2020.3024825.

Shi, C., Salous, S., Wang, F. & Zhou, J. (2016). Low probability of intercept-based adaptive radar waveform optimization in signal-dependent clutter for joint radar and cellular communication systems. *EURASIP Journal on Advances in Signal Processing*, 2016(1), 111.

Shi, C., Wang, F., Salous, S. & Zhou, J. (2017). Optimal Power Allocation Strategy in a Joint Bistatic Radar and Communication System Based on Low Probability of Intercept. *Sensors*, 17(12), 2731. doi: 10.3390/s17122731.

Shi, C., Wang, F., Sellathurai, M., Zhou, J. & Salous, S. (2020). Low Probability of Intercept-Based Optimal Power Allocation Scheme for an Integrated Multistatic Radar and Communication System. *IEEE Systems Journal*, 14(1), 983-994. doi: 10.1109/JSYST.2019.2931754.

Shojaeezand, T., Azmi, P. & Yadegari, A. (2010). Performance Analysis of a LDPC Coded CDMA System with Physical Layer Security Enhancement. *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, pp. 1-4. doi: 10.1109/WICOM.2010.5601271.

Slimeni, F., Scheers, B., Chtourou, Z. & Le Nir, V. (2015). Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm. *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1-7. doi: 10.1109/ICMCIS.2015.7158697.

Song, H., Roux, P., Hodgkiss, W., Kuperman, W., Akal, T. & Stevenson, M. (2006). Multiple-input-multiple-output coherent time reversal communications in a shallow-water acoustic channel. *IEEE Journal of Oceanic Engineering*, 31(1), 170-178. doi: 10.1109/JOE.2005.850911.

Song, T., Zhou, K. & Li, T. (2016). CDMA System Design and Capacity Analysis Under Disguised Jamming. *IEEE Transactions on Information Forensics and Security*, 11(11), 2487-2498. doi: 10.1109/TIFS.2016.2585089.

Su, N., Liu, F. & Masouros, C. (2024). Sensing-Assisted Eavesdropper Estimation: An ISAC Breakthrough in Physical Layer Security. *IEEE Transactions on Wireless Communications*, 23(4), 3162-3174. doi: 10.1109/TWC.2023.3306029.

Suard, B., Naguib, A., Xu, G. & Paulraj, A. (1993). Performance of CDMA mobile communication systems using antenna arrays. *1993 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 4, 153-156 vol.4. doi: 10.1109/ICASSP.1993.319617.

Sun, Z., Liu, Y., Wang, J., Mei, F., Deng, W. & Ge, Y. (2019). Non-Cooperative Game of Throughput and Hash Length for Adaptive Merkle Tree in Mobile Wireless Networks. *IEEE Transactions on Vehicular Technology*, 68(5), 4625-4650. doi: 10.1109/TVT.2019.2899647.

Tian, W., Jiang, X. & Zhang, C. (2021). High Anti-Interception Orbital Angular Momentum Spread Spectrum Communications Systems. *ICC 2021 - IEEE International Conference on Communications*, pp. 1-6. doi: 10.1109/ICC42927.2021.9500492.

Vucic, N., Shi, S. & Schubert, M. (2010). DC programming approach for resource allocation in wireless networks. *8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 380-386.

Wang, K., Yuan, L., Miyazaki, T., Zeng, D., Guo, S. & Sun, Y. (2017). Strategic Antieavesdropping Game for Physical Layer Security in Wireless Cooperative Networks. *IEEE Transactions on Vehicular Technology*, 66(10), 9448-9457. doi: 10.1109/TVT.2017.2703305.

Wang, W., Hempel, M., Peng, D., Wang, H., Sharif, H. & Chen, H.-H. (2010). On Energy Efficient Encryption for Video Streaming in Wireless Sensor Networks. *IEEE Transactions on Multimedia*, 12(5), 417-426. doi: 10.1109/TMM.2010.2050653.

Wei, F., Zheng, S., Zhou, X., Zhang, L., Lou, C., Zhao, Z. & Yang, X. (2022). Detection of Direct Sequence Spread Spectrum Signals Based on Deep Learning. *IEEE Transactions on Cognitive Communications and Networking*, 8(3), 1399-1410. doi: 10.1109/TCCN.2022.3174609.

Xiao, L., Hong, S., Xu, S., Yang, H. & Ji, X. (2022). IRS-Aided Energy-Efficient Secure WBAN Transmission Based on Deep Reinforcement Learning. *IEEE Transactions on Communications*, 70(6), 4162-4174. doi: 10.1109/TCOMM.2022.3169813.

Xie, D. G., Wu, N., Wang, C. & Liu, Q. F. (2012). Performance analysis and simulation of DSSS in tactical data link communication system. *2012 6th Asia-Pacific Conference on Environmental Electromagnetics (CEEM)*, pp. 194-197. doi: 10.1109/CEEM.2012.6410599.

Xu, J., Lou, H., Zhang, W. & Sang, G. (2020). An Intelligent Anti-Jamming Scheme for Cognitive Radio Based on Deep Reinforcement Learning. *IEEE Access*, 8, 202563-202572. doi: 10.1109/ACCESS.2020.3036027.

Yang, T. C. & Yang, W.-B. (2008). Performance analysis of direct-sequence spread-spectrum underwater acoustic communications with low signal-to-noise-ratio input signals. *The Journal of the Acoustical Society of America*, 123(2), 842-855. doi: 10.1121/1.2828053.

Yao, F. & Jia, L. (2019). A Collaborative Multi-Agent Reinforcement Learning Anti-Jamming Algorithm in Wireless Networks. *IEEE Wireless Communications Letters*, 8(4), 1024-1027. doi: 10.1109/LWC.2019.2904486.

Ye, Z., Memik, G. & Grosspietsch, J. (2008). Energy Detection Using Estimated Noise Variance for Spectrum Sensing in Cognitive Radio Networks. *2008 IEEE Wireless Communications and Networking Conference*, pp. 711-716. doi: 10.1109/WCNC.2008.131.

Yeh, C.-Y. & Knightly, E. W. (2021). Eavesdropping in Massive MIMO: New Vulnerabilities and Countermeasures. *IEEE Transactions on Wireless Communications*, 20(10), 6536-6550. doi: 10.1109/TWC.2021.3074941.

Yu, J. & Yao, Y.-D. (2005). Detection performance of chaotic spreading LPI waveforms. *IEEE Transactions on Wireless Communications*, 4(2), 390-396. doi: 10.1109/TWC.2004.842948.

Yuan, C., Tao, X., Li, N., Ni, W., Liu, R. P. & Zhang, P. (2019). Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming. *IEEE Transactions on Vehicular Technology*, 68(3), 2682-2696. doi: 10.1109/TVT.2019.2895911.

Zhang, L., Wang, H. & Li, T. (2013). Anti-Jamming Message-Driven Frequency Hopping—Part I: System Design. *IEEE Transactions on Wireless Communications*, 12(1), 70-79. doi: 10.1109/TWC.2012.120312.111706.

Zhang, M., Carroll, C. & Chan, A. (2001a). Analysis of IS-95 CDMA Voice Privacy. *Selected Areas in Cryptography*, pp. 1–13.

Zhang, M., Carroll, C. & Chan, A. (2001b). Analysis of IS-95 CDMA Voice Privacy. *Selected Areas in Cryptography*.

Zhang, S., Chen, H., Jia, W. & Wang, W. (2024). A Low Probability of Intercept Method Based on Power Optimization for Frequency Diverse Array and Cooperative Jammer. *IEEE Transactions on Aerospace and Electronic Systems*, 1-6. doi: 10.1109/TAES.2024.3451458.

Zhang, Y., Mou, Z., Gao, F., Jiang, J., Ding, R. & Han, Z. (2020). UAV-Enabled Secure Communications by Multi-Agent Deep Reinforcement Learning. *IEEE Transactions on Vehicular Technology*, 69(10), 11599-11611. doi: 10.1109/TVT.2020.3014788.

Zhang, Z. & Lei, J. (2017). A detecting algorithm of DSSS signal based on auto — Correlation estimation. *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 137-141. doi: 10.1109/IAEAC.2017.8053993.

Zheng, G., Choo, L.-C. & Wong, K.-K. (2011). Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays. *IEEE Transactions on Signal Processing*, 59(3), 1317-1322. doi: 10.1109/TSP.2010.2092774.

Zhong, C., Yao, J. & Xu, J. (2019). Secure UAV Communication With Cooperative Jamming and Trajectory Control. *IEEE Communications Letters*, 23(2), 286-289. doi: 10.1109/LCOMM.2018.2889062.

Zhou, Q., Li, Y. & Niu, Y. (2021). Intelligent Anti-Jamming Communication for Wireless Sensor Networks: A Multi-Agent Reinforcement Learning Approach. *IEEE Open Journal of the Communications Society*, 2, 775-784. doi: 10.1109/OJCOMS.2021.3056113.

Zou, Y., Zhu, J., Wang, X. & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, 104(9), 1727-1765. doi: 10.1109/JPROC.2016.2558521.