FAST-FORWARD FULL-DUPLEX STRATEGIES TO MITIGATE REACTIVE JAMMING ATTACKS ON LOW-LATENCY COMMUNICATION

VIVEK CHAUDHARY

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI

JANUARY 2023

© Indian Institute of Technology Delhi (IITD), New Delhi, 2023

Fast-Forward Full-Duplex Strategies to Mitigate Reactive Jamming Attacks on Low-Latency Communication

by

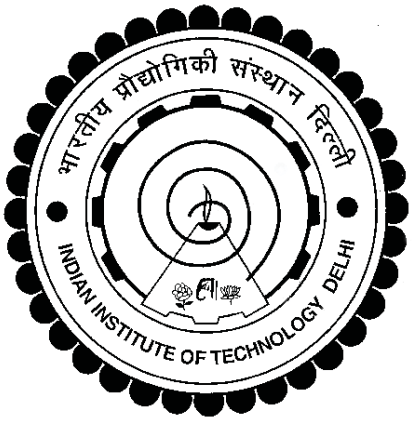
VIVEK CHAUDHARY

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

In fulfilment of the requirements of the degree of Doctor of Philosophy

to the



INDIAN INSTITUTE OF TECHNOLOGY DELHI

January 2023

CERTIFICATE

This is to certify that the thesis titled **Fast-Forward Full-Duplex Strategies to Mitigate Reactive Jamming Attacks on Low-Latency Communication**, submitted by **Vivek Chaudhary**, to the Indian Institute of Technology, Delhi, for the award of the degree of **Doctor of Philosophy**, is a bona fide record of the research work done by him under my supervision.

The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Harshan Jagadeesh
Thesis Supervisor
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Hauz Khas New Delhi 110016

Place: New Delhi

ACKNOWLEDGEMENTS

I take this opportunity to thank them for making my stay at IIT Delhi memorable and enjoyable.

First, I would like to thank my advisor, Prof. Harshan Jagadeesh, for his tremendous patience, timely advice and support throughout my spell as a graduate student. He has given me invaluable insights into our research work, taught me the art of problem-solving, along with helping me to strive for an excellent work-life balance. His inspiring thoughts and the constant pursuit of excellence and perfection have made me a better person and a researcher.

I thank my student research committee members, Prof. Shiv Dutt Joshi, Prof. Saif Khan Mohammed, and Prof. Prabhu Babu, for their valuable comments and suggestions. Their invaluable comments and suggestions have helped me substantially streamline my work and progress.

Life as a PhD student is incomplete without a technically interactive and intellectually vibrant lab. I would like to thank my colleagues, Kamal Agrawal, Anand Jee, Amit Patel, Deebakshi Dey, Amar Mishra, Manish Bansal, and Rohit Joshi, who have always motivated me during the course of my journey at IIT Delhi. Moreover, the PhD duration is long and tends to have so many highs and lows. I thank my friends, Anuj Jain, Ritij Chaudhary, Vishal Patel, Aakar Srivastav, Shashank Shekshar, Rahul Neema, Chetan Singh, Abhinay Pardeshi, Anuj Srivastav, Anand Jee, Abhishek Shukla, and Himanshu Rai for being with me in my lows and celebrate my high times. I would also like to thank my cycling mates, Anand Jee, Himanshu Rai, Kamal Agrawal, Kalyan Dash, and Dr Amit Prasad, for memorable cycling rides on weekends exploring the capital city.

Last but not least, I am genuinely indebted to my parents, Smt. Sudha Singh and Dr Vijay Singh, and my brother, Abhishek, for believing in me and helping me through my PhD program. I sincerely thank my friend Preeti for always being by my side and supporting me during difficult times. Thanks for always being there for me.

Vivek Chaudhary

ABSTRACT

In the context of 5G/5G+, securing wireless links becomes crucial due to the services offered by the applications running on these networks. Since some of these applications have mission-critical data with low-latency constraints, a slight delay in the reception could have undesirable effects—for instance, autonomous vehicles, unmanned aerial vehicles, and the industrial internet of things. The low-latency constraints of these applications attract a plethora of attacks, mainly jamming attacks since these attacks are easy to execute. Moreover, radio architecture advancements have also created a new class of jammers, known as reactive jammers. Unlike a traditional jammer, a reactive jammer may monitor the network for possible countermeasures and change its attacking strategies based on its observations. While countermeasures like frequency hopping are known to provide reliable communication amidst traditional jamming attacks, using them against reactive jammers might not offer the anticipated outcome. Thus, this thesis aims to provide new mitigation strategies against reactive jammers to facilitate reliable, low-latency communication to the victim with the help of a nearby full-duplex helper. Under the framework of fast-forward full-duplex strategies, we design constellations for the victim and the helper that minimize the error rates at the destination. In particular, we solve optimal constellations at the victim and the helper, subject to average energy constraints at the victim and the helper, under various channel conditions and radio architectures at the full-duplex helper. In addition to minimizing the error rates, we also analyze the covertness of our proposed schemes in deceiving a family of countermeasure detectors deployed by the reactive jammer.

सार

5जी/5जी+ के संदर्भ में, इन नेटवर्क पर चलने वाले अनुप्रयोगों द्वारा दी जाने वाली सेवाओं के कारण वायरलेस लिंक को सुरक्षित करना महत्वपूर्ण हो जाता है। चूंकि इनमें से कुछ अनुप्रयोगों में कम-विलंब बाधाओं के साथ मिशन-महत्वपूर्ण डेटा है, इसलिए रिसेप्शन में थोड़ी देरी से अवांछनीय प्रभाव हो सकते हैं - उदाहरण के लिए, स्वायत्त वाहन, मानव रहित हवाई वाहन और चीजों के औद्योगिक इंटरनेट। इन अनुप्रयोगों की कम-विलंबता की कमी हमलों की अधिकता को आकर्षित करती है, मुख्य रूप से इन हमलों को निष्पादित करना आसान है। इसके अलावा, रेडियो वास्तुकला प्रगति ने जैमर की एक नई कक्षा भी बनाई है, जिसे प्रतिक्रियाशील जैमर के रूप में जाना जाता है। एक पारंपरिक जैमर के विपरीत, एक प्रतिक्रियाशील जैमर संभावित प्रत्यूपायो के लिए नेटवर्क की निगरानी कर सकता है और अपने अवलोकन के आधार पर हमला करने की रणनीतियों को बदल सकता है। जबकि आवृत्ति हॉपिंग जैसे प्रत्युपाय को पारंपरिक जैमिंग हमलों के बीच विश्वसनीय संचार प्रदान करने के लिए जाना जाता है, प्रतिक्रियाशील जैमर के खिलाफ उनका उपयोग अनुमानित परिणाम प्रदान नहीं कर सकता है। इस प्रकार, इस शोध प्रबंध का उद्देश्य पास के फुल-डुप्लेक्स सहायक की मदद से पीड़ित को विश्वसनीय, कम-विलंब संचार की सुविधा के लिए प्रतिक्रियाशील जैमर के खिलाफ नई शमन रणनीति प्रदान करना है। फास्ट-फॉरवर्ड फुल-डुप्लेक्स रणनीतियों के ढांचे के तहत, हम पीड़ित और सहायक के लिए कॉन्स्टलेशन्स को डिजाइन करते हैं जो गंतव्य पर त्रुटि दरों को कम करते हैं। विशेष रूप से, हम पीड़ित और सहायक पर इष्टतम कॉन्स्टलेशन्स को हल करते हैं, पीड़ित और सहायक पर औसत ऊर्जा बाधाओं के अधीन, विभिन्न चैनल स्थितियों और फुल-डुप्लेक्स सहायक पर रेडियो आर्किटेक्चर के तहत। त्रुटि दरों को कम करने के अलावा, हम प्रतिक्रियाशील जैमर द्वारा तैनात प्रत्युपाय डिटेक्टरों को धोखा देने में हमारी प्रस्तावित योजनाओं की गुप्तता का भी विश्लेषण करते हैं।

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

DoS	Denial of Service
SNR	Signal-to-Noise Ratio
MIMO	Multiple-Input Multiple-Output
WLAN	Wireless Large Area Network
FH	Frequency Hopping
DSSS	Direct Sequence Spread Spectrum
FDD	Frequency Division Duplex
FD	Full-Duplex
HD	Half-Duplex
CR	Cognitive Radio
CRN	Cognitive Radio Network
FDCA	Full-Duplex Cognitive Adversary
SI	Self-Interference
SIC	Self-Interference Cancellation
RSS	Received Signal Strength
CST	Carrier Sensing Time
PER	Packet Error Rate
RTS	Request to Send
CTS	Clear to Send
ACK	Acknowledgement
LoS	Line of Sight
ADC	Analogue to Digital Converter
DAC	Digital to Analogue Converter
LNA	Low Noise Amplifier
DSP	Digital Signal Processing
OFDM	Orthogonal Frequency Division Multiplexing
MAP	Maximum A Posteriori
FFFD	Fast-Forward Full-Duplex

OOK	On-Off Keying
ASK	Amplitude Shift Keying
PSK	Phase Shift Keying
CSI	Channel State Information
JDD	Joint Dominant Decoder
AWGN	Additive White Gaussian Noise
MAC	Multiple Access Channel
SC-F2HD	Semi-Coherent Fast-Forward Half-Duplex
SC-F2FD	Semi-Coherent Fast-Forward Full-Duplex
NC-FFFD	Non-Coherent Fast-Forward Full-Duplex
DT NC-FFFD	Delay Tolerant NC-FFFD
DASC-MF	Delay-Aware Semi-Coherent Multiplex-and-Forward
SC-MAC	Semi-Coherent Multiple Access Channel
NR	Newton Raphson

NOTATION

α,	Energy-splitting factor
$\gamma(\cdot,\cdot)$	Lower-incomplete Gamma function
$\Gamma(\cdot,\cdot)$	Upper-Incomplete Gamma function
$\Gamma(\cdot)$	Complete Gamma function
$Q(\cdot)$	Q-function
$\delta(\cdot)$	Dirac-delta function
$Q_1(\cdot,\cdot)$	Marcum-Q function
N_o	Noise variance
N_C	Receive antennas at Charlie
N_B	Receive antennas at Bob
$\mathbf{0}_{N_C}$	$N_C \times 1$ vector of zeros
$\mathbf{I}_{N_C}$	$N_C \times N_C$ Identity Matrix
$\max$	Maximum
$\min$	Minimum
$\mathbb{E}[\cdot]$	Expectation operator
$\mathbf{P}_{FA}$	Probability of false-alarm
$\mathbb{P}_{MD}$	Probability of miss-detection
Φ_{ij}	Probability of decoding bit-i and bit-j at Charlie
$(\cdot)^H$	Hermitian operator
σ^2_{AC}	Variance of Alice-to-Charlie link
σ^2_{AB}	Variance of Alice-to-Bob link
σ^2_{CB}	Variance of Charlie-to-Bob link
$\mathcal{CN}(\cdot,\cdot)$	Complex Normal distribution
$\bar{i}$	complement of i
$\ln(\cdot)$	Natural logarithm
λ	Residual SI
f_{AB}	Alice-to-Bob uplink frequency
f_{CB}	Charlie-to-Bob uplink frequency

$\mathcal{E}_{AB}$	Average energy level on f_{AB}
$\mathcal{E}_{CB}$	Average energy level on f_{CB}
h_{AB}	Rayleigh fading channel coefficient of Alice-to-Bob link
h_{CB}	Rayleigh fading channel coefficient of Charlie-to-Bob link
h_{AC}	Rayleigh fading channel coefficient of Alice-to-Charlie link
$I(X;Y)$	Mutual Information between X and Y