

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**

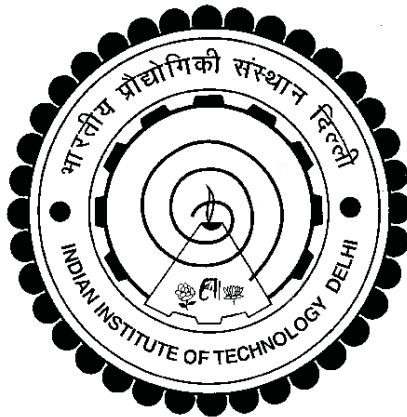
by

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 प्रत्युपायो 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

ACKNOWLEDGEMENTS	i
ABSTRACT	ii
LIST OF FIGURES	x
LIST OF TABLES	xi
ABBREVIATIONS	xii
NOTATION	xiv
1 INTRODUCTION	1
1.1 Overview	1
1.2 Objective and Scope of the Thesis	4
1.3 Contributions and Outline of the Thesis	5
1.4 List of Publications	8
2 BACKGROUND	10
2.1 Wireless Jamming Attacks: A Survey	10
2.1.1 Constant Jammer	11
2.1.2 Intermittent Jammer	12
2.1.3 Reactive Jammer	12
2.1.4 Adaptive Jammer	13
2.1.5 Intelligent Jammer	14
2.2 Full-Duplex Radios	14
2.2.1 Propagation Domain Cancellation	15
2.2.2 Analogue Domain Cancellation	16
2.2.3 Digital Domain Cancellation	17
2.3 Full-Duplex Cognitive Radios: A Survey	18
2.3.1 Cognitive Radios	18

2.3.2	Need for Full-Duplex Cognitive Radios	20
2.3.3	Full-Duplex Cognitive Radios as Adversaries: A Big Picture	21
3	Fast-Forward Mitigation Schemes for Reactive Adversaries for Slow-Fading Channels	22
3.1	Introduction	22
3.1.1	Contributions	22
3.1.2	Related Works	23
3.2	System Model	24
3.3	Semi-Coherent Fast-Forward Half-Duplex Relaying Scheme	26
3.3.1	Signal Model: SC-F2HD Relaying Scheme	26
3.3.2	Error Performance: SC-F2HD Relaying Scheme	27
3.4	Semi-Coherent Fast-Forward Full-Duplex Relaying Scheme	30
3.4.1	Signal Model: SC-F2FD Relaying Scheme	31
3.4.2	Error Performance at Charlie	33
3.4.3	Error Performance at Bob	34
3.5	SC-F2FD Joint Dominant Decoder	35
3.5.1	Probability of Error using SC-F2FD JD Decoder	36
3.5.2	Validation of SC-F2FD JD Decoder	40
3.5.3	Dominant Error Events and a Near-Optimal Solution	40
3.6	Simulation Results on the Performance of SC-F2FD Relaying Scheme	46
3.7	Covertness Analysis of the Relaying Schemes	50
3.7.1	Covertness of SC-F2FD Relaying Scheme	50
3.7.2	Simulation Results on Covertness	54
3.8	Chapter Summary	56
4	Fast-Forward Mitigation Schemes for Reactive Adversaries for Fast-Fading Channels	58
4.1	Introduction	58
4.1.1	Contributions	58
4.1.2	Related Work and Novelty	60
4.2	System Model	60
4.3	Non-Coherent Fast-Forward Full-Duplex Relaying Scheme	62
4.3.1	NC-FFFD: Signal Model	63

4.3.2	The Complementary Energy Levels and Distribution of r_B	66
4.3.3	Joint Maximum A Posteriori (JMAP) decoder for NC-FFFD Relaying Scheme	68
4.3.4	Joint Dominant (JD) Decoder for NC-FFFD Relaying Scheme	70
4.4	Optimization of Energy Levels	72
4.4.1	Optimization of Energy Levels for $M = 2$	73
4.4.2	Optimization of Energy Levels for $M \geq 2$	81
4.4.3	Energy Backtracking (EB) Algorithm	85
4.5	Delay-Tolerant NC-FFFD (DT NC-FFFD) Relaying Scheme	86
4.5.1	Delay Tolerant Energy Backtracking (DT-EB) Algorithm	88
4.6	Covertness Analysis of NC-FFFD Relaying Scheme	91
4.6.1	Energy Detector (ED)	92
4.6.2	Correlation Detector (CD)	95
4.7	Chapter Summary	97
5	Delay-Aware Full-Duplex Relaying Scheme Against Reactive Jammers	99
5.1	Introduction	99
5.1.1	Contributions	100
5.1.2	Related Work and Novelty	101
5.2	System Model	101
5.3	Delay-Aware Semi-Coherent Multiplex-and-Forward Relaying Scheme	102
5.3.1	Signal Model	105
5.3.2	Error Analysis at Bob	106
5.4	3ϕ Delay-Tolerant Semi-Coherent Multiplex-and-Forward Relaying Scheme	108
5.4.1	Signal Model and Error Analysis of Phase-I	111
5.4.2	Signal Model and Error Analysis of Phase-II	112
5.4.3	Signal Model and Error Analysis of Phase-III	115
5.4.4	Optimization of N_C and β for 3ϕ DASC-MF Relaying Scheme	120
5.4.5	Simulation Results for 3ϕ DASC-MF Relaying Scheme	122
5.5	Semi-Coherent Multiple Access Channel Scheme	125
5.5.1	Error Analysis of SC-MAC	126
5.5.2	Simulation Results for SC-MAC	130

5.6	Covertness Analysis	130
5.6.1	Covertness Analysis for ED when using 3 ϕ DASC-MF Relaying Scheme	132
5.6.2	Covertness Analysis for ED when using SC-MAC Scheme	135
5.6.3	Simulation Results	136
5.7	Chapter Summary	137
6	CONCLUSION AND FUTURE WORK	138
6.1	Conclusion	138
6.2	Future Work	140

LIST OF FIGURES

1.1	Pictorial representation of jamming.	2
1.2	Pictorial depiction of cognitive jamming.	4
1.3	System model for jamming attack by a cognitive adversary.	5
2.1	Block diagram of FD transceiver showing three types of SIC, as depicted in [1].	15
2.2	Dynamic spectrum management for an interweave network as depicted in [2, 3].	20
3.1	The network model for <i>cognitive</i> jamming, where Dave can <i>jam and measure</i>	24
3.2	Average error performance of Alice and Charlie prior and after SC-F2HD relaying scheme for various SNR values.	29
3.3	Average error performance of Alice in the SC-F2HD scheme with increasing interference (I_{Dave}) from Dave at Charlie.	30
3.4	Network model depicting SC-F2FD relaying scheme. Alice and Charlie use $1 - \alpha$ and α fractions of their energies on the frequency band f_{CB} , respectively. Concurrently, Alice and Charlie also pour α and $1 - \alpha$ fraction of their energy on the frequency band f_{AB} , respectively. SI at Charlie is $\sim \mathcal{CN}\left(0, \lambda \frac{(1+\alpha)}{2}\right)$	31
3.5	Constellations diagrams in the SC-F2FD scheme.	36
3.6	Average error performance of JMAP, JMAX, and JD decoder as a function of $\alpha \in (0, 1)$ at 35 dB for 4- and 8-PSK used by Charlie. Each decoder (along with the union bound in (3.18)) experiences a dip which is close to $\alpha = 1$	41
3.7	The intersection of $\Phi_{11,FD}P_{3,avg}$ and $\Phi_{10,FD}(P_{2,avg}^c + 0.5)$ and the actual minima of (3.18) at 35 dB.	46
3.8	Comparison of average error performance of JMAP and JD decoder for SC-F2FD and JMAP decoder for SC-F2HD, at high SNRs.	47
3.9	Individual performance using α^* as energy-splitting factor: Charlie uses 4-PSK constellation and has $\lambda = 10^{-5}$ as residual SI.	47
3.10	Joint error performance at Bob using α^* -JMAP decoder for various degree of residual SI at Charlie.	48
3.11	Plots showcasing the effect on the average error performance of Alice and Charlie when FD radio at Charlie has large residual SI ($\lambda = 10^{-3}$).	49

3.12	$\mathbf{P}_{FA} + \mathbf{P}_{MD}$ as a function of n at 35 dB for simulation as well as analytical expression (from approximation) for various combinations of ϑ and λ	55
3.13	$\mathbf{P}_{FA} + \mathbf{P}_{MD}$ as a function of ϑ for $n = 250$ and SNR = 35 dB. For $\lambda = 10^{-2}$, analytical result is approximately 1, the simulated sum fluctuates around 1.	55
4.1	A network model consisting legitimate nodes Alice and Charlie communicating with Bob, on f_{AB} , and f_{CB} , respectively. Dave is the FD cognitive adversary, jamming f_{AB} . He also measures the energy level on f_{AB} and computes the correlation between the symbols on f_{AB} and f_{CB}	61
4.2	System model of NC-FFFD relaying scheme.	64
4.3	Illustration of multiplexing at Charlie and corresponding energy levels received at Bob.	67
4.4	Variation of P'_e , its increasing and decreasing terms as a function of η_2 , when η_1 and α are fixed.	75
4.5	Variation of P'_e , its increasing and decreasing terms as a function of α , when η_1 and η_2 are fixed.	77
4.6	Performance of NC-FFFD using energy levels obtained using TLGD and the exhaustive search.	79
4.7	Performance of NC-FFFD for fixed $N_B = 8$ and varying N_C	80
4.8	Alice's performance when using NC-FFFD scheme for $N_C = 1$ and $N_B = 8$	80
4.9	Error performance of NC-FFFD when energy levels are computed using EB algorithm for $M = 2$	84
4.10	Error performance of NC-FFFD when energy levels are computed using EB algorithm for $M = 4$	85
4.11	N_C^\dagger as a function of SNR for $M = 2$ and $M = 4$	86
4.12	Error performance for $nT = 0$ and $nT = T$	87
4.13	Variation of $\frac{\Phi_{01} + \Phi_{10}}{2}$ as a function of N_C and α	88
4.14	Performance of DT NC-FFFD when energy levels are computed using DT-EB algorithm for $M = 2$	89
4.15	Performance of DT NC-FFFD when energy levels are computed using DT-EB algorithm for $M = 4$	90
4.16	N_C^\dagger as a function of SNR for $M = 2$ and $M = 4$	90
4.17	DT NC-FFFD scheme, when $nT = 0$ and $nT = T$ for $M = 2$, $N_B = 8$, $\Delta_{RE} = 10^{-2}$, and $\Delta_{DT} = 10^{-1}$	91

4.18	$\mathbf{P}_{FA} + \mathbf{P}_{MD}$ as a function of L and ∂ at 25 dB (including the residual SI), $N_B = 8$, and $\Delta_{DT} = 0.1$	95
4.19	Scatter-plots representing the energy pairs received at Dave for SNR = 25 dB, $N_B = 8$, $L = 50$, when (a) Dave is not jamming. (b) Alice and Charlie use repetitive coding across f_{AB} and f_{CB} . (c) Alice and Charlie cooperatively use Gold-sequence. (d) MI before jamming and after using NC-FFFD with Gold-sequence and with Repetitive coding as a function of L at SNR = 25 dB, $k = 2$, and $N_B = 8$. (e) $\mathbf{P}_{D,CD}$ when NC-FFFD is implemented with repetitive coding and with Gold-sequence, for $L = 150$ at 25 dB, $N_B = 8$, and $k = 2$	96
5.1	A network model depicting legitimate nodes, Alice and Charlie, and the reactive adversary, Dave.	102
5.2	System model for DASC-MF scheme, where Charlie takes Θ symbols to multiplex-and-forward Alice's symbols to Bob.	103
5.3	Illustration of symbol transmission in DASC-MF scheme.	104
5.4	Frame model for the 3ϕ DASC-MF scheme.	110
5.5	Constellation diagram jointly contributed by Alice and Charlie during Phase-I	112
5.6	Constellation diagram jointly contributed by Alice and Charlie during Phase-II	112
5.7	Constellation diagram jointly contributed by Alice and Charlie during Phase-III	116
5.8	Variation of $\mathcal{P}_{e,3\phi}$ and its increasing and decreasing terms as a function of β at 25 dB.	122
5.9	Joint error-performance when using 3ϕ DASC-MF.	124
5.10	Improvement in Alice's performance when using 3ϕ DASC-MF.	124
5.11	Optimal N_C versus SNR for Phase-III of 3ϕ DASC-MF.	125
5.12	Constellation diagram jointly contributed by Alice and Charlie when using SC-MAC.	127
5.13	Variation of \mathcal{P}_{MAC} and its increasing and decreasing terms as a function of ε at 25 dB.	129
5.14	Joint error performance of SC-MAC scheme.	131
5.15	Improvement in Alice's performance when using SC-MAC.	131
5.16	$\mathbf{P}_{FA,AB} + \mathbf{P}_{MD,AB}$ on f_{AB} as a function of ∂	136
5.17	$\mathbf{P}_{FA,CB} + \mathbf{P}_{MD,CB}$ on f_{CB} as a function of ∂	137

LIST OF TABLES

3.1	Comparison between the proposed SC-F2HD and SC-F2FD relaying schemes	57
4.1	FREQUENTLY OCCURRING NOTATIONS	63
4.2	ERROR-RATES AT BOB WHEN USING JMAP DECODER AND JD DECODER FOR $M = 2$	70
5.1	SYMBOLS TRANSMITTED IN EACH PHASE	110
5.2	ERROR TERMS FOR PHASE-III AS GIVEN IN THEOREM 15	117
5.3	VALUES OF EXACT AND APPROXIMATE (N_C, β) FOR VARIOUS Θ	123
5.4	ERROR TERMS FOR SC-MAC AS GIVEN IN THEOREM 17	127
5.5	EXACT AND APPROXIMATE VALUES OF ε	130

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

$\alpha,$	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_{AC}^2	Variance of Alice-to-Charlie link
σ_{AB}^2	Variance of Alice-to-Bob link
σ_{CB}^2	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