# A Dynamic and Robust Random Multiple-Access Scheme for Communication over Satellite Channels with Interference

John T. Metzger
B.S. Electrical Engineering
United States Air Force Academy (2014)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of
Master of Science
in
Electrical Engineering and Computer Science
at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2016



Author ..... Signature redacted
Department of Electrical Engineering and Computer Science
May 20, 2016

Certified by ..... Signature redacted
Vincent W. S. Chan
Joan and Irwin Jacobs Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Certified by ..... Signature redacted
Christopher C. Yu
Division Leader – Signals, Sensors, and Navigation - Charles Stark Draper Laboratory
Thesis Supervisor

Accepted by ..... Signature redacted
Leslie A. Kolodziejski
Chair, Department Committee on Graduate Students

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

# A Dynamic and Robust Random Multiple-Access Scheme for Communication over Satellite Channels with Interference

by

John T. Metzger

Submitted to the Department of Electrical Engineering and Computer Science on May 20, 2016 in partial fulfillment of the requirements for the degree of Master of Science in Electrical Engineering and Computer Science

## Abstract

SATCOM is a critical capability that is increasingly in demand among civilian and military users. The past several years have seen a dramatic increase in electronic warfare capabilities available to potential adversaries that will pose a significant threat to SATCOM systems. Additionally, the circuit-oriented architecture of current SATCOM systems is ill-suited to support future traffic demands and a random multiple-access mode that can dynamically adapt to user traffic, as well as the number of users, will be required for future systems. Given that military operations often take place in contested environments, future systems must also be able to operate in the presence of complex and powerful interference platforms.

This thesis proposes a combined system using the slotted ALOHA protocol as its random multiple-access scheme along with direct sequence spread spectrum coding to provide channel robustness and low probability of detection. We estimate the transmission power achievable by a transportable interferer using commercially available technologies and develop limits on the maximum channel capacity achievable for different numbers of channels operating in the same frequency band. We show that the combined system can support a large number of channels operating at low data rates when the interferer is present, and higher data rates under benign circumstances.

We also investigate the stability of the slotted ALOHA control algorithm under dynamically varying traffic loads and show that the system remains uncongested as long as the average traffic load is kept below the maximum throughput of the channel. The system is shown to be able to return to an uncongested state after periods of time where the traffic load exceeds the maximum throughput of the channel. Two methods for implementing dual-class service are developed and their effects on throughput and latency are discussed.

Finally, we anticipate attack strategies an interferer may use to target the physical and media access control layers of the system and develop techniques for mitigating these attacks. A technique known as code switching is developed and shown to significantly improve the system's robustness to attacks targeting both the physical and media access control layers.

Thesis Supervisor: Vincent W. S. Chan
Title: Joan and Irwin Jacobs Professor of Electrical Engineering and Computer Science

Thesis Supervisor: Christopher C. Yu
Title: Division Leader – Signals, Sensors, and Navigation - Charles Stark Draper Laboratory

## Acknowledgments

I must first offer a word of praise to God, whose guiding hand has been unmistakable during my time here at MIT. I am extremely grateful for the grace and mercy he has shown me in my work as well as the wonderful friends and community he has blessed me with here in Cambridge.

Next, I would like to thank my advisors Professor Vincent Chan and Dr. Christopher Yu for their support and guidance during my time at MIT. I was truly fortunate to have such patient and wise mentors. It was my sincere pleasure to work for both of you. I am also grateful for the financial support of the U.S. Air Force and the Charles Stark Draper Laboratory that made this opportunity possible.

I owe my gratitude to Litian Liu for her work on simulating an ALOHA system that serves as the foundation for much of my work in Chapter 3.

I am very fortunate to have had such wonderful lab mates. Antonia, thank you for being such a great office mate. I appreciate your willingness to listen to my concerns about classes and research. Anny, thank you for carrying me through 6.450! I am going to miss our Sunday night homework sessions. Matt and Henna, thank you for welcoming me to the group. I believe the openness and camaraderie of our group is due in large part to your leadership. Arman, thank you for being a great TA and a good friend. I am going to miss teaming up with you to annoy Shane. Manishika, I'm so glad there was someone else in the lab who shares a mutual love for rock climbing and T-Swift! It was a pleasure to be your designated study break. Esther, thank you for your willingness to be open and genuine with me. I highly value our conversations on school, relationships, faith, and life in general. Andrew, I enjoyed being part of the group's 6.262 crew with you. I wish you the best in your future studies. Finally, to the most delightfully sarcastic man I have ever known,

Shane, thank you for being a great friend, mentor, and office mate. I am extremely impressed by your work ethic and I hope to imitate it as best I can. Thank you for taking me under your wing and for the many lessons on how to be a good officer.

I would also like to thank my mentor Paul Carter. Paul, thank you for all the wisdom you've shared with me over the past two years. You helped me find purpose in my work and showed me how to freely receive God's gift of grace. I will miss our noontime conversations.

Finally, to the members of Tang Small Group, thank you for being such a loving and supportive community. You came alongside me during a very difficult first semester and have become some of my closest friends. May God continue to bless and grow your fellowship.

# Contents

**Acknowledgments** ..... **7**

**Table of Figures** ..... **13**

**Acronyms** ..... **19**

**Notation** ..... **21**

**Chapter 1 Introduction** ..... **27**

1.1 Future SATCOM Requirements and Current Systems ..... 28

1.2 A Potential Solution for Future Systems ..... 29

1.3 Thesis Scope and Organization ..... 30

**Chapter 2 System Description and Threat Estimate** ..... **33**

2.1 System Description ..... 33

2.1.1 Physical Layer Description ..... 34

2.1.2 MAC Layer Description ..... 37

2.1.3 System Capacity under Benign Circumstances ..... 39

2.1.4 System LPI Characteristics ..... 43

2.1.4.1 Comparison of Spreading Techniques ..... 44

2.1.4.2 Vulnerability of Frequency Hopping to Detection ..... 46

2.2 Threat Estimate ..... 48

2.2.1 Estimate of Interferer Strength ..... 49

2.2.2 System Capacity with Broadband Interferer ..... 51

2.3 Summary ..... 55

**Chapter 3 Control Algorithm and Dual-Class Service ..... 57**

3.1 The Rivest Control Algorithm ..... 57

3.1.1 Performance Metrics ..... 59

3.1.2 System Response to Delayed Feedback ..... 62

3.1.3 Control Algorithm Stability ..... 69

3.2 Control Algorithm Performance ..... 70

3.2.1 Heavy Traffic Simulations ..... 79

3.2.2 Time to Clear Heavy Traffic Bursts ..... 92

3.3 Implementation of Dual-Class Service ..... 96

3.3.1 Estimating Arrival Rates ..... 97

3.3.2 Throughput Scaling with Random Drops ..... 105

3.3.3 Simulations with Priority Users ..... 109

3.3.4 Strict Time Deadline Service ..... 125

3.4 Summary ..... 129

**Chapter 4 Physical Layer Defenses ..... 131**

4.1 Downlink Power Robbing ..... 131

4.1.1 Performance Comparison of Signal Processing Schemes ..... 132

4.1.2 Limiting Effect of Power Robbing on Interference Mitigation ..... 137

4.2 Concentrated Interference Attacks ..... 139

4.2.1 Uncoded Channel with Pulsed Interference ..... 140

4.2.2 Coded Channel with Pulsed Interference ..... 143

4.2.3 Channel-Selective Interference ..... 145

4.2.4 Channel-Selective Interference with Code Switching ..... 148

4.3 Summary ..... 150

**Chapter 5 MAC Layer Defenses ..... 151**

5.1 Modified Rivest Algorithm with Channel-Selective Interference ..... 151

5.1.1 Maximum Achievable Throughput with Interference ..... 152

5.1.2 Derivation of Feedback Parameters for Modified Algorithm ..... 153

5.1.3 Estimating Interferer Transmission Rate ..... 157

5.1.4 Simulated Results ..... 160

5.1.4.1 Simulated Throughput ..... 161

5.1.4.2 Simulated Estimation of Backlog ..... 163

5.1.4.3 Simulated Recovery Time from Interferer ..... 165

5.2 Performance Improvements from Using Code Switching ..... 167

5.3 Defense against a Collision-Spoofing Interferer ..... 172

5.4 Summary ..... 177

**Chapter 6 Conclusion ..... 179**

**Appendix A Derivations for Equations in Chapter 2 ..... 181**

A.1 Physical Parameter Calculations for Section 2.1.3 ..... 181

A.2 Supporting Calculations for Section 2.1.4.2 ..... 184

**Appendix B Derivations for Equations in Chapter 3 ..... 187**

B.1 Derivation of Expected Delay for Section 3.1.1 ..... 187

B.2 Derivation of Expected Delay for Section 3.1.2 ..... 188

B.3 Derivation of Expected Delay for Section 3.3.4 ..... 189

**Appendix C Derivations for Equations in Chapter 4 ..... 193**

C.1 SNR Derivations for Section 4.1.1 ..... 193

C.2 Derivation of Limit for Section 4.1.2 ..... 196

**Appendix D Derivations for Equations in Chapter 5 ..... 201**

D.1 Derivations of Results for Section 5.1.2 ..... 201

D.2 Optimization for Section 5.1.3 ..... 204

D.3 Derivation of Chernoff Bound for Section 5.3 ..... 205

**Bibliography ..... 209**

# Table of Figures

Fig. 1 Diagram of DS Signal Spreading and Recovery ..... 35

Fig. 2 Slotted ALOHA Departure Rate vs. Attempted Transmission Rate ..... 38

Fig. 3 Maximum Channel Capacity (Bps) vs. Processing Gain for Benign Channel ..... 41

Fig. 4 Total System Capacity (Bps) vs. Processing Gain for Benign Channel ..... 43

Fig. 5 Comparison of Power Spectral Densities for $G_p = 10$ ..... 45

Fig. 6 Comparison of Power Spectral Densities for $G_p = 1000$ ..... 46

Fig. 7 Interferer EIRP vs. Frequency ..... 51

Fig. 8 Channel Capacity (Bps) vs. Processing Gain for Channel with Broadband Interference ..... 53

Fig. 9 Total Capacity (Bps) vs. Processing Gain for Channel with Broadband Interference ..... 53

Fig. 10 Channel Capacity (Bps) versus Processing Gain with Interference and 20 dB Antenna Nulling ..... 54

Fig. 11 Total Capacity (Bps) versus Processing Gain with Interference and 20 dB Antenna Nulling ..... 54

Fig. 12 Simulated Actual and Estimated Backlog for the Continuous Transmission Attempt Scheme ..... 65

Fig. 13 Simulated Actual and Estimated Backlog for the Wait-for-Feedback Scheme ..... 65

Fig. 14 Simulated Expected Channel Delay for the Continuous Transmission Attempt Scheme ..... 66

Fig. 15 Simulated Expected Channel Delay for the Wait-for-Feedback Scheme ..... 66

Fig. 16 Simulated Long-Term Averages for Continuous Transmission Attempt Scheme ..... 67

Fig. 17 Simulated Long-Term Averages for Wait-for-Feedback Scheme ..... 67

Fig. 18 Simulated Local Averages for Continuous Transmission Attempt Scheme ..... 68

Fig. 19 Simulated Local Averages for Wait-for-Feedback Scheme ..... 68

Fig. 20 Step Function Poisson Arrival Rate Test Case ..... 71

Fig. 21 Square Pulse Poisson Arrival Rate Test Case ..... 72

Fig. 22 Sinusoid Poisson Arrival Rate Test Case ..... 72

Fig. 23 Simulated Actual and Estimated Backlog for Step Function Case ..... 73

Fig. 24 Simulated Expected Delay for Step Function Case ..... 73

Fig. 25 Simulated Local Averages for Step Function Case ..... 74

Fig. 26 Simulated Long-Term Averages for Step Function Case ..... 74

Fig. 27 Simulated Actual and Estimated Backlog for Square Pulse Case ..... 75

Fig. 28 Simulated Expected Delay for Square Pulse Case ..... 75

Fig. 29 Simulated Local Averages for Square Pulse Case ..... 76

Fig. 30 Simulated Long-Term Averages for Square Pulse Case ..... 76

Fig. 31 Simulated Actual and Estimated Backlog for Sinusoid Case ..... 77

Fig. 32 Simulated Expected Delay for Sinusoid Case ..... 77

Fig. 33 Simulated Local Averages for Sinusoid Case ..... 78

Fig. 34 Simulated Long-Term Averages for Sinusoid Case ..... 78

Fig. 35 Heavy Traffic Load with a Step Function Poisson Arrival Rate Test Case ..... 81

Fig. 36 Heavy Traffic Load with a Square Pulse Poisson Arrival Rate Test Case ..... 81

Fig. 37 Heavy Traffic Load with a Double Pulse Poisson Arrival Rate Test Case ..... 82

Fig. 38 Heavy Traffic Load with a Sinusoid Poisson Arrival Rate Test Case ..... 82

Fig. 39 Simulated Actual and Estimated Backlog for Step Function Case ..... 83

Fig. 40 Simulated Expected Delay for Step Function Case ..... 83

Fig. 41 Simulated Local Averages for Step Function Case ..... 84

Fig. 42 Simulated Long-Term Averages for Step Function Case ..... 84

Fig. 43 Simulated Actual and Estimated Backlog for Square Pulse Case ..... 85

Fig. 44 Simulated Expected Delay for Square Pulse Case ..... 85

Fig. 45 Simulated Local Averages for Square Pulse Case ..... 86

Fig. 46 Simulated Long-Term Averages for Square Pulse Case ..... 86

Fig. 47 Simulated Actual and Estimated Backlog for Double Pulse Case ..... 88

Fig. 48 Simulated Expected Delay for Double Pulse Case ..... 88

Fig. 49 Simulated Local Averages for Double Pulse Case ..... 89

Fig. 50 Simulated Long-Term Averages for Double Pulse Case ..... 89

Fig. 51 Simulated Actual and Estimated Backlog for Sinusoid Case ..... 90

Fig. 52 Simulated Expected Delay for Sinusoid Case ..... 90

Fig. 53 Simulated Local Averages for Sinusoid Case ..... 91

Fig. 54 Simulated Long-Term Averages for Sinusoid Case ..... 91

Fig. 55 Visualization of System Clear Time ..... 93

Fig. 56 Example Poisson Arrival Rate for Clear Time Analysis ..... 95

Fig. 57 Simulated and Estimated System Clear Time versus Pulse Width for Square Pulse Arrival Rate ... 95

Fig. 58 Simulated Arrival Rate Estimation for $k_w = 1$ ..... 99

Fig. 59 Simulated Arrival Rate Estimation for $k_w = 2$ ..... 99

Fig. 60 Simulated Actual and Estimated for the Constant Value Update Method ..... 101

Fig. 61 Simulated Actual and Estimated Backlog for the Updated Method from (3.10) with $k_w = 2$ ..... 101

Fig. 62 Simulated Arrival Rate Estimation for Updated Method from (3.10) with $k_w = 2$ ..... 102

Fig. 63 Simulated Arrival Rate Estimation for a Synchronized Change in User Traffic ($k_w = 2$) ..... 103

Fig. 64 Simulated Arrival Rate Estimation for a Change in Normal User Traffic ($k_w = 2$) ..... 104

Fig. 65 Simulated Arrival Rate Estimation for a Change in Priority User Traffic ($k_w = 2$) ..... 104

Fig. 66 Simulated Arrival Rate Estimation for an Unsynchronized Change in User Traffic ($k_w = 2$) ..... 105

Fig. 67 Initial Poisson Arrival Rates for Synchronized Traffic Increase ..... 111

Fig. 68 Simulated Estimated and Scaled Poisson Arrival Rates for Synchronized Traffic Increase ..... 111

Fig. 69 Simulated Actual and Estimated Backlog for Synchronized Traffic Increase ..... 112

Fig. 70 Simulated Expected Delay for Synchronized Traffic Increase ..... 112

Fig. 71 Simulated Local Averages for Synchronized Traffic Increase ..... 113

Fig. 72 Simulated Long-Term Averages for Synchronized Traffic Increase ..... 113

Fig. 73 Initial Poisson Arrival Rates for Normal User Traffic Increase ..... 114

Fig. 74 Simulated Estimated and Scaled Poisson Arrival Rates for Normal User Traffic Increase ..... 114

Fig. 75 Simulated Actual and Estimated Backlog for Normal User Traffic Increase ..... 115

Fig. 76 Simulated Expected Delay for Normal User Traffic Increase ..... 115

Fig. 77 Simulated Local Averages for Normal User Traffic Increase ..... 116

Fig. 78 Simulated Long-Term Averages for Normal User Traffic Increase ..... 116

Fig. 79 Initial Poisson Arrival Rates for Priority User Traffic Increase ..... 118

Fig. 80 Simulated Estimated and Scaled Poisson Arrival Rates for Priority User Traffic Increase ..... 118

Fig. 81 Simulated Actual and Estimated Backlog for Priority User Traffic Increase ..... 119

Fig. 82 Simulated Expected Delay for Priority User Traffic Increase ..... 119

Fig. 83 Simulated Local Averages for Priority User Traffic Increase ..... 120

Fig. 84 Simulated Long-Term Averages for Priority User Traffic Increase ..... 120

Fig. 85 Initial Poisson Arrival Rates for Unsynchronized Traffic Increase ..... 121

Fig. 86 Simulated Estimated and Scaled Poisson Arrival Rates for Unsynchronized Traffic Increase ..... 121

Fig. 87 Simulated Actual and Estimated Backlog for Unsynchronized Traffic Increase ..... 122

Fig. 88 Simulated Expected Delay for Unsynchronized Traffic Increase ..... 122

Fig. 89 Simulated Local Averages for Unsynchronized Traffic Increase ..... 123

Fig. 90 Simulated Long-Term Averages for Unsynchronized Traffic Increase ..... 123

Fig. 91 Expected Delay for a Strict Time Deadline User versus Number of Transmissions ..... 126

Fig. 92 Minimum Expected Delay for other Users versus Number of Transmissions by a Strict Time Deadline User ..... 128

Fig. 93 Bit Error Probability Comparison with $N_C = 100$ for a System Serving as a Relay and a System Using Onboard Signal Processing ..... 135

Fig. 94 Bit Error Probability Comparison with $N_C = 1000$ for a System Serving as a Relay and a System Using Onboard Signal Processing ..... 136

Fig. 95 Required Interferer-to-Signal Ratio versus Spreading Factor for Generic and Power Robbing Cases ..... 138

Fig. 96 Bit Error Probability for Pulsed Interferer on Uncoded Channel ..... 141

Fig. 97 Bit Error Probability Comparison for Constant Power and Optimally Pulsed Interferers ..... 142

Fig. 98 Bit Error Probability for Pulsed Interferer on a Channel with $m = 9$ Repeat Coding ..... 144

Fig. 99 Bit Error Probability Comparison for Optimal Channel-Selective and Broadband Interferers ..... 147

Fig. 100 Bit Error Probability for Channel-Selective Interferer with Code Switching ..... 150

Fig. 101 Normalized Expected Interferer Rate Estimation Error versus Number of Slots Observed ..... 159

Fig. 102 Simulated Throughput Comparison for $\lambda = 1 - \alpha e^{-1}$ ..... 161

Fig. 103 Simulated Throughput Comparison for $\lambda = e^{-1}$ ..... 162

Fig. 104 Estimation of Packets in System by Original Rivest Algorithm ..... 164

Fig. 105 Estimation of Packets in System by Modified Rivest Algorithm ..... 164

Fig. 106 Extended Estimation of Packets in System by Original Rivest Algorithm ..... 166

Fig. 107 Extended Estimation of Packets in System by Modified Rivest Algorithm ..... 167

Fig. 108 Comparison of Effective Interference Rates for System Using a Static DS Code and System Using Code Switching ..... 170

Fig. 109 Maximum Achievable Throughput versus Interferer Rate for Systems Using Code Switching and Static DS Codes ..... 172

Fig. 110 Probability of Detection versus Probability of False Alarm for $N_{sys} = 100$, $P_D = 0.8$, $P_f = 0.2$ ..... 176

## Acronyms

| | |
|---|---|
| ADC | analog-to-digital converter |
| ASAT | anti-satellite |
| Bps | bits per second |
| BPSK | binary phase-shift-keying |
| CDMA | code division multiple access |
| DOD | department of defense |
| DS | direct sequence |
| dB | decibels |
| dBW | decibel watts |
| EHF | extremely high frequency |
| EIRP | effective isotropic radiated power |
| EW | electronic warfare |
| FFT | fast Fourier transform |
| Hz | hertz |
| IID | independent identically distributed |
| LPI | low probability of intercept |
| MAC | media access control |
| PN | pseudo-noise |
| RTT | round trip time |
| SATCOM | satellite communications |
| SHF | super high frequency |
| SNR | signal-to-noise ratio |

## Notation

| | |
|---|---|
| $A_E$ | area between arrival rate pulse and residual arrival rate during congested period |
| $A_{RX}$ | area of receiver antenna |
| $C$ | maximum channel capacity |
| $C_q(N)$ | probability of a collision slot given $N$ packets in the system |
| $C_{sys}$ | total system capacity |
| $d_I$ | interferer antenna diameter |
| $d_{RX}$ | receiver antenna diameter |
| $E_I$ | EIRP of the interferer |
| $E_{sat}$ | EIRP available for satellite downlink |
| $E_{TX}$ | EIRP of the transmitter |
| $e_I$ | interferer antenna efficiency |
| $e_{RX}$ | receiver antenna efficiency |
| $F_p$ | signal path loss |
| $F_{sys}$ | system loss |
| $f$ | frequency |
| $f_{co}$ | co-channel interference factor |
| $f_{ss}$ | spreading sequence frequency |
| $G$ | attempted transmission rate |
| $G_I$ | gain of interferer antenna |
| $G_n$ | gain over interferer due to antenna nulling |
| $G_p$ | processing gain |
| $G_{RX}$ | gain of receiver antenna |
| $G_{TX}$ | gain of transmitter antenna |

| | |
|---|---|
| $H_q(N)$ | probability of a hole slot given $N$ packets in the system |
| $\mathbb{I}_C(i)$ | indicator variable for a collision slot |
| $\mathbb{I}_H(i)$ | indicator variable for a hole slot |
| $\mathbb{I}_S(i)$ | indicator variable for a success slot |
| $k$ | Boltzmann constant |
| $k_w$ | window scaling constant |
| $L$ | signal path distance |
| $L_p$ | packet length in bits |
| $m$ | number of repeated symbols per bit |
| $N$ | number of packets ready for transmission in an ALOHA slot |
| $N_A$ | number of ALOHA slots required for a packet to pass its transmission test |
| $N_B$ | number of bit periods in a packet using the same DS code for transmission |
| $N_C$ | number of user channels occupying a single frequency band |
| $N_{drop}$ | threshold number of backlogged packets to trigger a drop of normal users |
| $N_{FFT}$ | number of FFT points required |
| $N_{flop}$ | number of flops required |
| $N_h$ | number of hole slots observed in observation window |
| $N_I$ | power spectral density of broadband interferer |
| $N_{obv}$ | number of time slots included in observation window |
| $N_p$ | number of packets ready for transmission by priority users |
| $N_{Rep}$ | number of repeated transmissions of a strict time deadline packet |
| $N_{RTT}$ | number of ALOHA slots in a single channel round trip time |
| $N_S$ | number of transmission attempts required for success given that a success occurred |
| $N_{SW}$ | number of success slots observed in a window |

| | |
|---|---|
| $N_{sym}$ | maximum number of independent collision detection tests that can be performed on symbol periods |
| $N_T$ | total power spectral density of broadband interferer and ambient channel noise |
| $N_{TS}$ | number of transmitted packets in a time slot |
| $N_{TX}$ | number of transmission attempts required for a successful transmission of a single packet |
| $N_0$ | power spectral density of ambient channel noise |
| $n_s$ | number of shift registers |
| $n_{start}$ | first slot included in local average at nth ALOHA slot |
| $P_b$ | bit error probability |
| $P_{clear}$ | probability that an ALOHA slot is clear when a strict time deadline user is present |
| $P_D$ | probability that the system correctly detects a genuine collision |
| $P_d$ | probability that an individual collision detection test correctly detects a genuine collision |
| $P_{DP}$ | probability of bit error on downlink for system with onboard signal processing |
| $P_{DR}$ | probability of bit error on relay downlink |
| $P_{FA}$ | probability that the system incorrectly determines a hole slot to be a collision |
| $P_f$ | probability that an individual collision detection test incorrectly determines a hole slot to be a collision given that an interferer is not present |
| $P_{f,T}$ | total probability that an individual collision detection test incorrectly determines a hole slot to be a collision |
| $P_I$ | interferer transmitter power |
| $P_{N-1}$ | probability that $N-1$ of the packets in an ALOHA channel do not transmit on a given slot |
| $P_{N-2}$ | probability that $N-2$ of the packets in an ALOHA channel do not transmit on a given slot |
| $P_{N\|C}(n)$ | normalized distribution of the number of packets in the system $N$ given that a collision is observed |

| | |
|---|---|
| $P_{N\|H}(n)$ | normalized distribution of the number of packets in the system $N$ given that a hole is observed |
| $P_{N\|S}(n)$ | normalized distribution of the number of packets in the system $N$ given that a success is observed |
| $P_{N_\alpha\|N_h\cap\alpha}(n_\alpha)$ | probability of observing $N_\alpha$ time slots with a transmission from a channel-selective interferer out of $N_h$ total slots observed given that the probability that interferer affects a time slot is $\alpha$ |
| $P_{Proc}$ | probability of bit error for system using onboard signal processing |
| $P_{Rel}$ | probability of bit error for relay system |
| $P_{Total}$ | total power observed by uplink receiver |
| $P_{TX}$ | transmitter power |
| $P_{UP}$ | probability of bit error on uplink for system with onboard signal processing |
| $P_v(n)$ | Poisson distribution with mean $v$ of number of packets in the system $N$ |
| $p_{N_S}(n_s)$ | probability mass function of the random variable $N_S$ |
| $q$ | probability of transmission for user operating under ALOHA protocol |
| $q_{drop}$ | probability that a normal user is dropped from the ALOHA channel |
| $q_{in}$ | absorbed thermal energy per unit time to receiver |
| $q_{out}$ | emitted thermal energy per unite time from receiver |
| $r_I$ | fraction of downlink power devoted to interferer's signal |
| $r_n$ | fraction of normal users retained by the channel during a drop |
| $r_p$ | fraction of arrivals in window from priority users |
| $r_U$ | fraction of downlink power devoted to signals from legitimate users |
| $S_D(f)$ | power spectral density of data signal |
| $S_{DS}(f)$ | power spectral density of DS spread signal |
| $S_{FH}(f)$ | power spectral density of frequency hopped signal |
| $S_q(N)$ | probability of a success slot given $N$ packets in the system |

| | |
|---|---|
| $SNR$ | signal-to-noise ratio |
| $SNR_{DP}$ | downlink signal-to-noise ratio for system with onboard signal processing |
| $SNR_{DR}$ | downlink signal-to-noise ratio for relay system |
| $SNR_{UP}$ | uplink signal-to-noise ratio for system with onboard signal processing |
| $T$ | temperature in Kelvin |
| $T_b$ | data bit period |
| $T_{clear}$ | channel clear time in number of ALOHA slots required |
| $\hat{T}_{clear}$ | estimated channel clear time in number of ALOHA slots required |
| $T_{drop}$ | threshold channel delay in seconds to initiate a drop of normal users |
| $T_w$ | time in seconds a packet spends in the ALOHA channel |
| $v$ | estimated number of packets ready for transmission in an ALOHA slot |
| $W_d$ | data signal bandwidth |
| $W_{ss}$ | spread signal bandwidth |
| $\alpha$ | fraction of channels transmitted on by channel-selective interferer |
| $\alpha'$ | effective interference rate of channel-selective interferer |
| $\alpha^*$ | optimum fraction of channels transmitted on by channel-selective interferer |
| $\hat{\alpha}$ | estimated rate at which a channel-selective interferer affects the channel |
| $\hat{\alpha}'$ | estimated effective interference rate of channel-selective interferer |
| $\bar{\alpha}_{err}$ | normalized estimation error of rate at which a channel-selective interferer affects the channel |
| $\alpha_{sat}$ | receiver thermal absorptivity |
| $\Gamma$ | throughput in successful packets per time slot |
| $\Gamma_{Lo}$ | local throughput |
| $\Gamma_{LT}$ | long-term throughput |
| $\Gamma_{max}$ | maximum achievable throughput |

| | |
|---|---|
| $\varepsilon$ | symbol error probability |
| $\varepsilon_{sat}$ | receiver thermal emissivity |
| $\eta$ | Threshold number of collision detection tests that declare that a collision occurred for the system to declare that the current slot is a collision |
| $\theta(\tau)$ | cross-correlation function |
| $\lambda$ | Poisson arrival rate for packet arrivals to ALOHA channel in packets per slot |
| $\hat{\lambda}$ | estimated packet arrival rate to ALOHA channel in packets per slot |
| $\lambda_c$ | center frequency wavelength |
| $\lambda_n$ | arrival rate of packets from normal users in packets per slot |
| $\hat{\lambda}_n$ | estimated arrival rate of packets from normal users in packets per slot |
| $\lambda_p$ | arrival rate of packets from priority users in packets per slot |
| $\hat{\lambda}_p$ | estimated arrival rate of packets from priority users in packets per slot |
| $\lambda_R$ | residual packet arrival rate in packets per slot |
| $\lambda_S$ | supportable packet arrival rate in packets per slot |
| $\lambda_U$ | unsupportable packet arrival rate in packets per slot |
| $\rho$ | interferer pulse rate |
| $\rho^*$ | optimum interferer pulse rate |
| $\sigma_{SB}$ | Stefan-Boltzmann constant |
| $\omega_P$ | pulse width in number of ALOHA slots |

# Chapter 1

## Introduction

A defining feature of conflicts involving the U.S. military over the past two decades has been its unchallenged use of space-based assets for command, control, communications, and reconnaissance. Space systems have provided a tremendous advantage to U.S. forces by enabling capabilities such as precision airstrikes, satellite imagery, and communication to infrastructureless areas. Due to the technological inferiority of the U.S. military's recent opponents, space has been taken for granted as an uncontested domain. The availability of space-based assets is integral to significant portions of U.S. military strategy and any disruption in these systems would have significant consequences for future military operations.

The U.S. military's reliance on space-based assets, particularly communication systems, has not gone unnoticed by its rivals. Anti-satellite (ASAT) capabilities have proliferated around the world in recent years and electronic warfare (EW) systems in particular have improved dramatically [1]. Additionally, this increasing availability of commercially available components with significant EW capabilities will enable new players to operate in the space domain. Unlike ASAT systems, EW systems interfere with the signals transmitted and received by satellite communication (SATCOM) systems and can therefore attack SATCOM systems terrestrially without the added cost of being sent into space, and often without confirmed attribution. For this reason, EW capabilities will likely proliferate much faster than ASAT technologies and will pose the most significant threat to U.S. SATCOM systems.

Unfortunately, current SATCOM systems are ill-suited to meet the growing threat posed by the proliferation of EW technologies. A new generation of SATCOM systems is needed which can operate in an increasingly contested space environment and meet an evolving set of user requirements.

## 1.1 Future SATCOM Requirements and Current Systems

In order to survive in a contested space environment, future SATCOM systems must be robust in the sense that they can operate effectively in the presence of strong and deliberate interference. Future systems must also have a low probability of intercept (LPI) by an adversary in order for them to service users who need to operate undetected, such as special forces and stealth aircraft. In addition to mitigating the threat from new EW capabilities, future SATCOM systems must also be able to service a very large number of user terminals[1] with traffic that is often bursty in nature. Given that many of these terminals will be on highly mobile platforms, future SATCOM systems must be able to dynamically adjust to user traffic while remaining as efficient as possible in allocating channel resources. In light of these challenging user requirements, a Defense Science Board Task Force has recommended that future SATCOM systems employ a random multiple-access scheme to allow a large number of users to share a single channel [2]. A final requirement for future SATCOM systems is that they be able to support different levels of service [3]. Future systems must be able to provide minimal delay for priority communications while achieving as high a throughput as possible for remaining traffic.

While current SATCOM systems satisfy the requirement for a robust channel through their use of frequency hopping, they cannot provide sufficient LPI, nor can they support the desired number of user terminals. Frequency hopping in high frequency bands has typically been regarded as a good LPI scheme, but advances in signal processing, particularly in analog-to-digital converters and fast processors, are

[1] Most likely on the order of 100,000 terminals.

rendering this strategy obsolete. Additionally, the quasi-static nature of the circuit-oriented architecture employed by current SATCOM systems does not scale well and is unsuitable for servicing a large number of users with bursty traffic. For these reasons, new SATCOM systems are needed that are dynamic and robust, provide sufficiently low LPI, have an adaptive anti-interference capability, incorporate a random multiple-access scheme, and support different levels of service.

## 1.2 A Potential Solution for Future Systems

While updates at all levels of SATCOM systems are necessary to meet the requirements for future systems, changes to subsystems in the physical and media access control (MAC) layers will play the largest role in satisfying these requirements. Using the spread spectrum technique known as direct sequence (DS) spreading is a promising physical layer solution to provide robustness and an increased degree of LPI to a satellite channel. Additionally, as a form of code division multiple access (CDMA), DS spreading naturally lends itself to supporting multiple channels in a single frequency band. A potential solution at the MAC layer is the use of a multiple random-access ALOHA protocol to provide a dynamic system response to user traffic. An added benefit of the ALOHA protocol is that it requires very little coordination between users and the receiver, which is desirable for highly mobile systems that commonly experience brief channel outages.

The work in this thesis explores the merits of a combined DS/ALOHA scheme as a potential physical and MAC layer solution to the requirements for future SATCOM systems. The performance of a DS/ALOHA channel as part of a SATCOM system is simulated under various conditions to determine the capacity and robustness of the system. Additionally, modifications to both the DS spreading technique and the ALOHA control algorithm are developed in order to mitigate various interference strategies.

## 1.3 Thesis Scope and Organization

The following is a brief description of the scope and organization of this thesis, by chapter:

Chapter 2 outlines the proposed system description and reviews the direct sequence spread spectrum technique as well as the ALOHA MAC protocol. System parameters are recommended for the system such as antenna beam width, transmission power, and processing gain. Next, the maximum power available to a transportable interferer is developed and used to estimate the system's maximum achievable capacity under benign and hostile conditions. Finally, the vulnerability of frequency hopping to hostile detection is analyzed and its LPI characteristics are compared with direct sequence spreading.

Chapter 3 briefly reviews the Rivest Algorithm [4] as a method for controlling an ALOHA channel and examines the algorithm's stability. Performance metrics including the number of backlogged packets in the system and the expected system delay are developed and applied to simulations of an ALOHA channel controlled by the Rivest Algorithm under various traffic loads. These simulations include the delayed feedback present in a real satellite channel. A method for providing two different classes of service is also developed and simulated in this chapter.

Chapter 4 examines physical layer strategies for defending against deliberate interference. Onboard signal processing is analyzed as a means to prevent power robbing by an interferer. Direct sequence spreading combined with repeat coding is also evaluated as a means to mitigate pulsed and channel-selective interferers. Additionally, the concept of code switching is also developed in this chapter and its ease of implementation is briefly discussed.

Chapter 5 explores strategies for defending against attacks on the MAC layer. The impact of a stationary interferer on the throughput and stability achieved by the Rivest Algorithm is explored, and a modified

Rivest Algorithm with user authentication is developed to mitigate this attack. Code switching is demonstrated to provide superior protection against the stationary interferer and also prevents the interferer from spoofing collisions on hole slots.

Chapter 6 summarizes the main results of the thesis and suggests additional work to further improve future SATCOM systems. Other areas for improvement in SATCOM systems are also identified.

# Chapter 2

# System Description and Threat Estimate

This chapter outlines the physical and MAC layers of the DS/ALOHA system, briefly reviews DS spectrum spreading as a technique to provide robustness, and presents the ALOHA protocol as a method for providing random multiple-access to a large number of users[2]. The channel and total system capacities of the DS/ALOHA system are shown to support a large number of high data rate channels under benign circumstances. Additionally, the LPI characteristics of DS spectrum spreading and frequency hopping are compared and frequency hopping is shown to be vulnerable to detection due to advances in analog-to-digital converter (ADC) technology. Next, the capabilities of a transportable interference platform are estimated and are shown to pose a significant threat to future SATCOM systems. Finally, the effect of a transportable interferer on the DS/ALOHA system is analyzed and is shown to justify the need for antenna nulling at the satellite's receiver.

## 2.1 System Description

The DS/ALOHA system proposed in this thesis is composed of a channel utilizing DS spreading and an ALOHA protocol controlled by the Rivest Algorithm that manages user transmissions. Under this scheme, each channel uses its own DS code and maintains its own control parameter for the ALOHA protocol. In order to increase robustness[3] channels can routinely change which DS code they are using in a manner

[2] The outstanding question of the effect of the feedback delay on this system will be addressed in Chapter 3.
[3] See Chapter 4's discussion of code switching.

that appears random to an outside observer. Thus, for the purposes of this thesis, a channel in the DS/ALOHA system is considered to be a specific pattern of DS codes used by a single group of users governed by its own ALOHA protocol. It is important to make the distinction between the channel described here and the frequency band it occupies. Multiple DS codes can be used over the same frequency band simultaneously, and therefore a single frequency band will have multiple channels. This concept is somewhat counterintuitive since a channel is often synonymous with the frequency band it occupies. A more thorough description of the physical and MAC layers of the system is given in the following two sections.

### 2.1.1 Physical Layer Description

The primary feature of the physical layer is the spread spectrum scheme it uses. The purpose of a spread spectrum system is to spread a signal over a larger bandwidth than is necessary for that signal's transmission [5]. The spreading of a signal in DS spreading is accomplished by multiplying the data sequence[4] by a pseudo-noise (PN) sequence whose elements have values of $\pm 1$ and are changing at a faster rate than the data sequence [6]. The resulting signal will use the same underlying modulation scheme, but will appear to have a data rate equal to the rate of the PN sequence and will therefore occupy a larger bandwidth [6]. The data sequence is recovered at the receiver by correlating the received signal and multiplying the resulting sequence by the same PN sequence used at the transmitter [6]. Fig. 1 contains a conceptual diagram of the spreading and recovery process for a DS signal.

[4] It is assumed here that the data sequence only takes on values $\pm 1$.

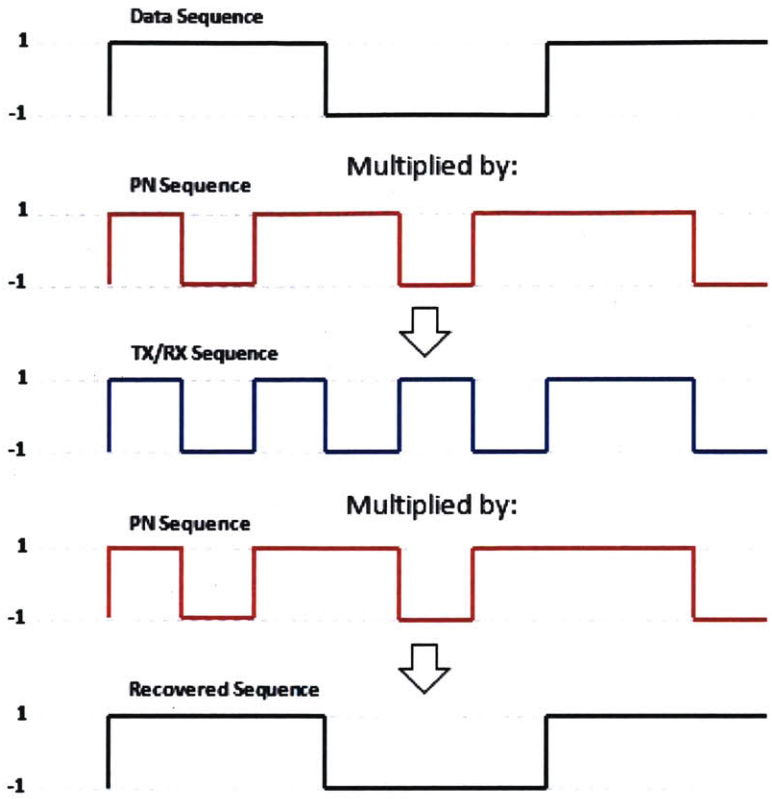


Fig. 1 Diagram of DS Signal Spreading and Recovery

An important parameter when discussing the DS spread spectrum technique is the processing gain $G_p$, which is defined as the ratio between the bit period of the data sequence and the symbol period of the PN sequence. The processing gain is effectively a measure of how much signal spreading occurs beyond the bandwidth required to transmit the underlying signal. Noting that bit period is the inverse of signal bandwidth, it is shown in [5] that the processing gain can also be expressed as:

$$G_p = \frac{W_{ss}}{W_d} \ , \tag{2.1}$$

where $W_{ss}$ is the bandwidth of the spread signal and $W_d$ is the bandwidth to the data signal before spreading. It is also shown in [5] that the processing gain is proportional to the power advantage of a DS signal over a broadband interferer, regardless of how it distributes its power. Thus, as long as an interferer does not know the particular DS PN code being used, it must transmit $G_p$ times more power to the receiver than the DS signal to be received with equal power. It is this power advantage that is the primary source of robustness for the DS/ALOHA system.

In order to preserve the power advantage afforded to the DS signal by the processing gain, it is necessary to develop PN codes with long periods that are difficult to reconstruct from a short segment of intercepted code [5]. It is also necessary to routinely change the DS code used by a signal since consecutive transmissions using the same code will greatly increase the likelihood of an adversary acquiring the DS code being used. An adversary that obtains the channel's DS code can eliminate the processing gain of the signal by transmitting an interfering signal spread using the same DS code as the channel. For these reasons, the DS/ALOHA system will switch the DS code it is using to transmit after every 10 data bit periods[5]. This technique will be referred to as code switching. An advantage of using code switching is that the transmitter can routinely vary its transmission parameters to avoid detection by an adversary without requiring resynchronization by the receiver since changing channel's the DS code does not affect the phase or timing of the transmitted signal.

In addition to using the DS code switching scheme outlined previously, several system parameters are assumed for the physical layer. The DS/ALOHA system is assumed to operate over a bandwidth of 1 GHz centered at 44.5 GHz in the 43.5 to 45.5 GHz DOD EHF satellite uplink frequency band [7]. Additionally, the receiver is assumed to be mounted on a satellite operating in a geosynchronous orbit at an altitude

[5] The choice of 10 data bit periods is motivated by the results in Chapter 5.

of 35,786 kilometers with an antenna diameter of 3 meters. In order to withstand strong interference, it is assumed that all user terminals are designed to have 10 watts available for transmission and use an aperture antenna with a beam width of 10 degrees.

### 2.1.2 MAC Layer Description

The MAC layer of the proposed system uses an ALOHA multiple random-access protocol with a back-off scheme controlled by the Rivest Algorithm[6]. A slotted ALOHA protocol is used which divides the channel into time slots for user transmissions[7]. Each user that has a packet to send during the current time slot will transmit it with a probability $q$ specified by the control algorithm at the satellite receiver that is broadcast to the users. Under the slotted ALOHA protocol, each time slot will contain a hole, a success, or a collision. A hole occurs when no users transmit during a time slot. A success occurs when only one user transmits during a time slot, resulting in a single packet being successfully received. A collision occurs when two or more users transmit during a time slot, resulting in interfering packet transmissions, none of which are received successfully. Therefore, the only time a successful transmission occurs is during a success slot. Packets that collide become backlogged and will attempt to retransmit with probability $q$ on subsequent slots.

The slotted ALOHA model assumes that the arrivals of users to the system form a Poisson process with rate $\lambda$ and that each arrival and each packet originates from a different user [8]. Using the approximation [8] that the total number of transmissions from both new arrivals and backlogged packets is a Poisson random variable with parameter $G > \lambda$, the departure rate of the ALOHA system is equal to the

[6] See Chapter 3 for an explanation of the Rivest Algorithm.
[7] The timing is acquired through the same algorithms used for processing satellites.

probability that a success occurs on a time slot, which is $Ge^{-G}$ [8]. Note that the parameter $G$ models the total attempted transmission rate of the system. A plot of departure rate versus $G$ is shown in Fig. 2.

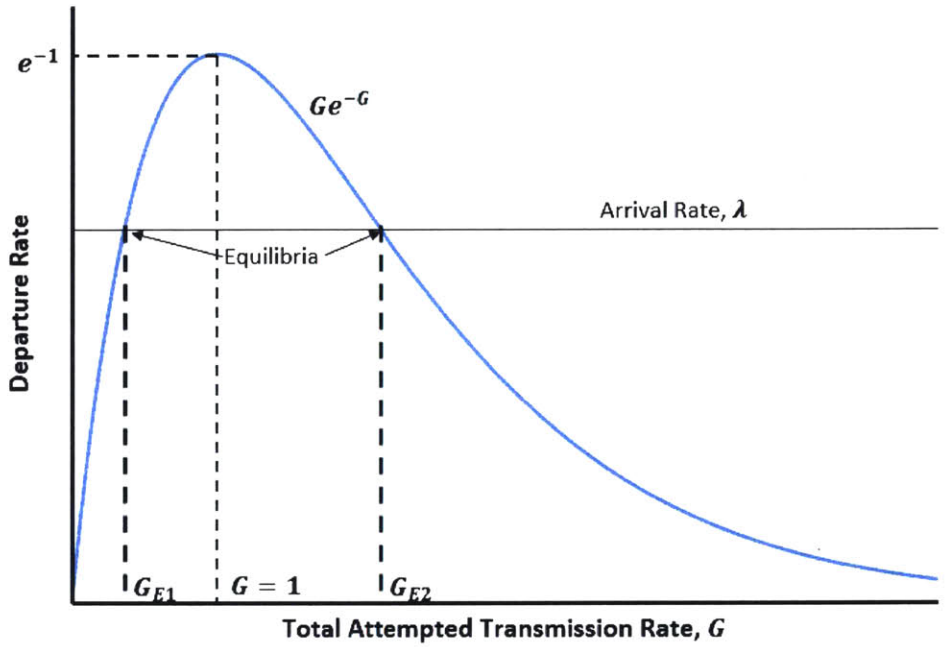


Fig. 2 Slotted ALOHA Departure Rate vs. Attempted Transmission Rate

We see from Fig. 2 we see that the maximum departure rate achievable by the slotted ALOHA system is $e^{-1}$, which occurs at $G = 1$. Since the departure rate of packets from the system is equivalent to its throughput, the slotted ALOHA protocol has a maximum throughput of $e^{-1} \approx 0.3678$. While $e^{-1}$ is a relatively low maximum throughput, it must be kept in mind that the primary advantage of an ALOHA system is the low coordination that is required between users and the receiver. We also see from Fig. 2 that there are two equilibria for arrival rates smaller than $e^{-1}$ that occur at $G_{E1}$ and $G_{E2}$. At these points, the system's departure rate is equal to its arrival rate, and the backlog is expected to be small. However, for values of $G$ greater than $G_{E2}$, the system departure rate is less than its arrival rate and runaway instability occurs as the system backlog grows to infinity [8]. For this reason, it is important to implement

a control scheme to ensure that the system remains stable and is biased as close to the maximum departure rate of $e^{-1}$ as possible. The DS/ALOHA system discussed in this thesis uses the Rivest Algorithm to stabilize its slotted ALOHA protocol.

### 2.1.3 System Capacity under Benign Circumstances

An important performance metric of the DS/ALOHA system is its capacity since the system must be able to support a large number of channels at sufficiently high data rates in order to be viable as a future SATCOM system. It is assumed here that the uplink to the SATCOM system will be the limiting factor on system capacity. An upper bound on the channel capacity of the uplink can be easily developed using the Shannon limit which has the following form [9]:

$$C = W_d \log_2(1 + SNR) \quad , \tag{2.2}$$

where $C$ is the maximum channel capacity in bits per second (Bps), $W_d$ is the data signal bandwidth in Hertz (Hz), and $SNR$ is the signal-to-noise ratio. Under benign circumstances, the signal-to-noise ratio can be expressed as [9]:

$$SNR = \frac{E_{TX} G_{RX} F_p}{W_d N_0 + (N_C - 1) f_{co} E_{TX} G_{RX} F_p} \quad , \tag{2.3}$$

where $E_{TX}$ is the effective isotropic radiated power (EIRP) of a user, $G_{RX}$ is the gain of the receiver's antenna, $F_p$ is the signal path loss, $N_0$ is the power spectral density in watts per Hz of the ambient channel noise, $N_C$ is the number of DS channels occupying the same frequency band, and $f_{co}$ is the co-channel interference factor modelling the fraction of power from other DS channels that is present as interference in the channel of interest. The co-channel interference factor is determined by the construction of the DS

codes being used. It is assumed in this thesis that maximal linear sequences are used for the system's DS codes. For a family of maximal linear sequences, $f_{co}$ has the following form [10]:

$$f_{co} = \frac{|\theta(\tau)|}{2^{n_s} - 1} \ , \tag{2.4}$$

where $\theta(\tau)$ is the cross-correlation function between the maximal linear sequence of interest and the other maximal linear sequences being used, $2^{n_s} - 1$ is the period of the maximal linear sequences, and $n_s$ is the number of shift registers used to generate the sequences. The cross-correlation function is itself a function of $n_s$ and has the following upper bound [10]:

$$|\theta(\tau)| \leq \begin{cases} 2^{(n_s+1)/2} + 1 & for \quad n_s \ odd \\ 2^{(n_s+2)/2} + 1 & for \quad n_s \ even \quad n_s \neq mod \ 4 \end{cases} \tag{2.5}$$

Since the cross-correlation of two DS spread signals decreases with increasing sequence length until the sequence begins to repeat, it is assumed that the entire chipping sequence is used for each data bit period. Under this assumption, the processing gain $G_p$ is equal to the sequence period since the sequence maximum chipping rate is $2^{n_s} - 1$. Thus, the processing gain can only take on values that satisfy $2^{n_s} - 1$, where $n_s$ is a positive integer. A plot of maximum channel capacity $C$ under benign circumstances versus the processing gain of the channel for various numbers of channels $N_C$ is given in Fig. 3. See Appendix A.1 for a derivation of the values of $E_{TX}$, $G_{RX}$, $F_p$, $W_d$, and $N_0$ used in (2.3) to produce the results in Fig. 3. Note that the number of shift registers $n_s$ used to generate the DS codes governs both the maximum channel capacity and the processing gain in Fig. 3 since $G_p = 2^{n_s} - 1$. Also note that there cannot be more channels than the number of DS codes available, which is $2^{n_s} + 1 \approx G_p$. Therefore, the additional requirement that $N_C \leq G_p$ is included in Fig. 3.

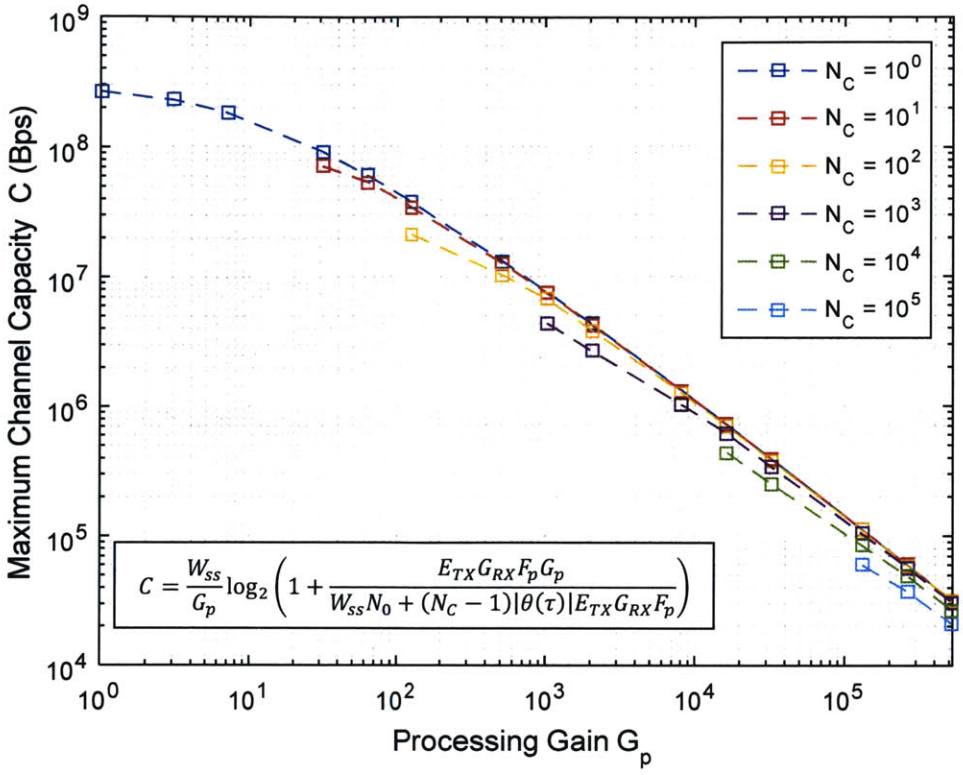


Fig. 3 Maximum Channel Capacity (Bps) vs. Processing Gain for Benign Channel

We see from Fig. 3 that channel capacity monotonically decreases with increasing processing gain because the capacity gained from a reduction in co-channel interference is less than the capacity lost due to the reduction in data bandwidth that results from an increase in processing gain. It should be noted that under benign circumstances, the DS/ALOHA system can support up to 10,000 channels operating at 436 kBps with a processing gain of 16,383 or 1,000 channels operating at 4.3 MBps with a processing gain of 1023. This is a significant improvement in the number of available channels over current circuit-based SATCOM systems. Note that the equation in Fig. 3 is (2.2) with substitutions from (2.3), (2.4), and $G_p = 2^{n_s} - 1$.

From Fig. 3 it is evident that there is a tradeoff between the number of channels and the data rate each channel can support. However, the appropriate number of channels to maximize the total capacity of the system $C_{sys}$ is not readily apparent because increasing the number of channels may lower individual

channel capacity, but could also increase the total system capacity due to the added channels. Total system capacity is defined as:

$$C_{sys} = N_C \cdot C \quad , \tag{2.6}$$

where $C_{sys}$ is simply the number of channels multiplied by their individual capacities. A plot of total system capacity $C_{sys}$ versus $G_p$ for various values of $N_C$ is given in Fig. 4 and reveals that $C_{sys}$ is largest when $N_c = 10^5$ and $G_p = 131{,}071$. However, when $N_c = 10^3$ channels with are used with a processing gain of 1023, $C_{sys}$ is still close to 70 percent of the capacity achieved when $N_c = 10^5$ channels are used, and provides a significantly higher individual channel capacity (4.3 MBps versus 60 kBps). Therefore, depending on user requirements it may be preferable to use a smaller number of channels with higher individual channel capacity, but lower total system capacity.

It is important to remember that the capacities plotted in Fig. 3 and Fig. 4 are produced using the Shannon limit and therefore represent a bound on the maximum capacities achievable under benign conditions. These capacities also do not take into account efficiency losses from higher network layers (above the physical layer). For example, using ALOHA as a MAC layer protocol would reduce these capacities by a factor of $e^{-1}$.

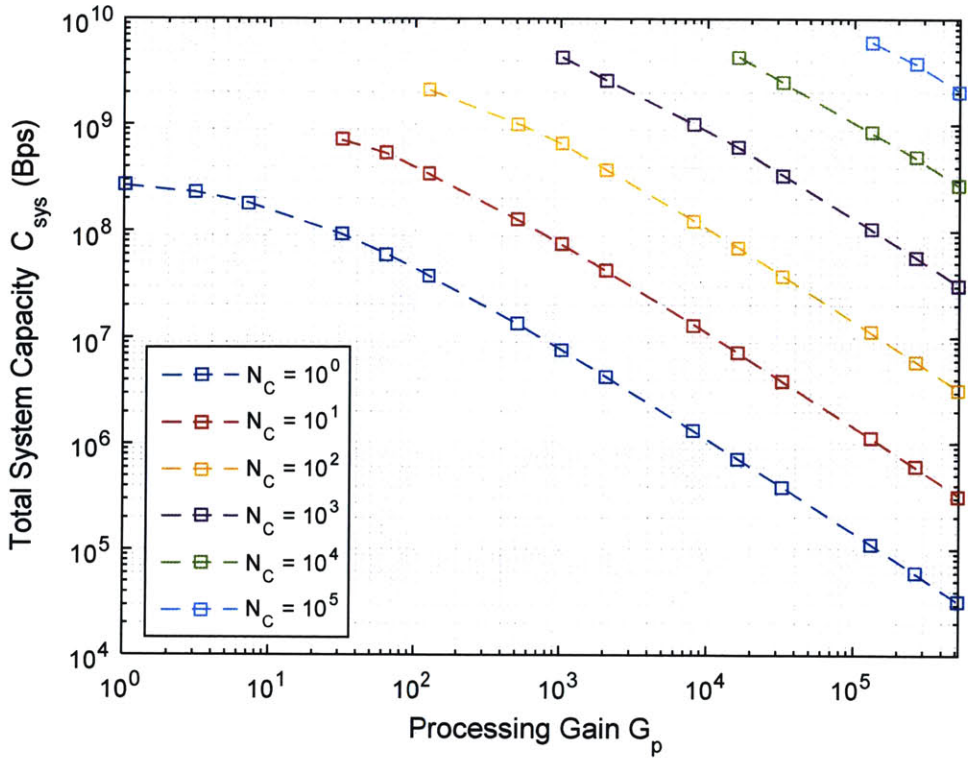


Fig. 4 Total System Capacity (Bps) vs. Processing Gain for Benign Channel

## 2.1.4 System LPI Characteristics

In addition to achieving high capacity, it is important that the DS/ALOHA system maintains a low probability of intercept (LPI) by adversaries. Using DS coding achieves LPI by spreading the signal power over a very large bandwidth so that the signal is difficult to differentiate for the ambient noise floor of the channel. Current SATCOM systems do not use signal power spreading to achieve LPI. Instead they use a form of spread spectrum called frequency hopping. Frequency hopping is accomplished by dividing the spread spectrum bandwidth into smaller channels with identical bandwidths to the data signal bandwidth. A user transmits on one or more of the channels at a time and rapidly hops their transmission from channel to channel in a pseudo-random fashion that makes it difficult for an adversary to track their hopping pattern. Frequency hopping itself has some inherent LPI, but SATCOM transmissions in the EHF band have typically been at frequencies that are too high for an adversary to detect due to limits in analog-

to-digital converter (ADC) and processing technology. Unfortunately for current SATCOM systems, ADC and processor technology has made significant steps forward since these systems were launched and the EHF band has become much more vulnerable.

### 2.1.4.1 Comparison of Spreading Techniques

The LPI advantage of DS spectrum spreading over frequency hopping can be easily seen by comparing the power spectrums of their respective signals. Assume that a DS signal and frequency hopped signal share the same data bit period $T_b$. From [5] the power spectrum for the data signal before spreading $S_D(f)$ is then:

$$S_D(f) = T_b\left(\frac{\sin \pi f T_b}{\pi f T_b}\right)^2 , \tag{2.7}$$

where $f$ is frequency in Hz. Since frequency hopping only changes which channel the signal uses, the power spectral density of the frequency hopped signal $S_{FH}(f)$ is the same as $S_D(f)$. Assuming the DS signal uses a spreading sequence with frequency $f_{ss}$, the power spectral density of the DS spread signal $S_{DS}(f)$ is then [5]:

$$S_{DS}(f) = \frac{1}{f_{ss}}\left(\frac{\sin \pi f/f_{ss}}{\pi f/f_{ss}}\right)^2 \tag{2.8}$$

A plot of $S_{FH}(f)$ and $S_{DS}(f)$ versus $f$ for a processing gain of 10 is shown in Fig. 5. Even with a relatively low processing gain, the difference in power concentrations between the DS and frequency hopped signals is significant. The more concentrated peak of the frequency hopped signal is easier for an adversary to detect than the spread peak of the DS signal. In this way, DS spectrum spreading offers an LPI advantage

over frequency hopping at the same data rate. As processing gain increases, the LPI advantage of DS spreading over frequency hopping also increases because the DS signal power is spread over a larger bandwidth. A plot of $S_{FH}(f)$ and $S_{DS}(f)$ versus $f$ for a more realistic processing gain of 1000 is shown in Fig. 6. It is apparent from Fig. 6 that the difference in power concentrations between the DS and frequency hopped signals is significant and that relative to the frequency hopped signal, the DS signal is virtually indistinguishable from the noise floor.

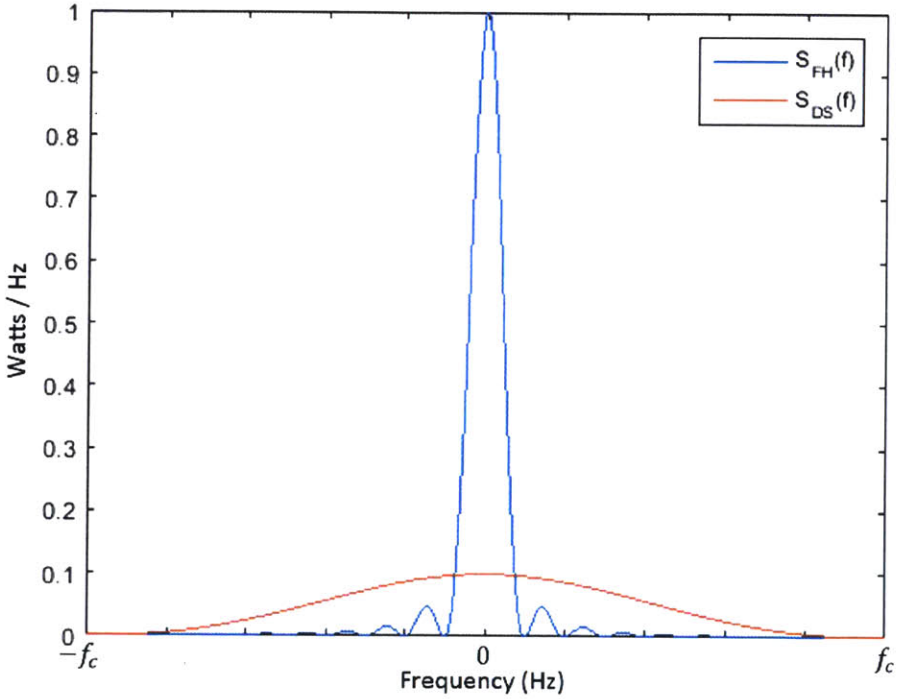


Fig. 5 Comparison of Power Spectral Densities for $G_p = 10$

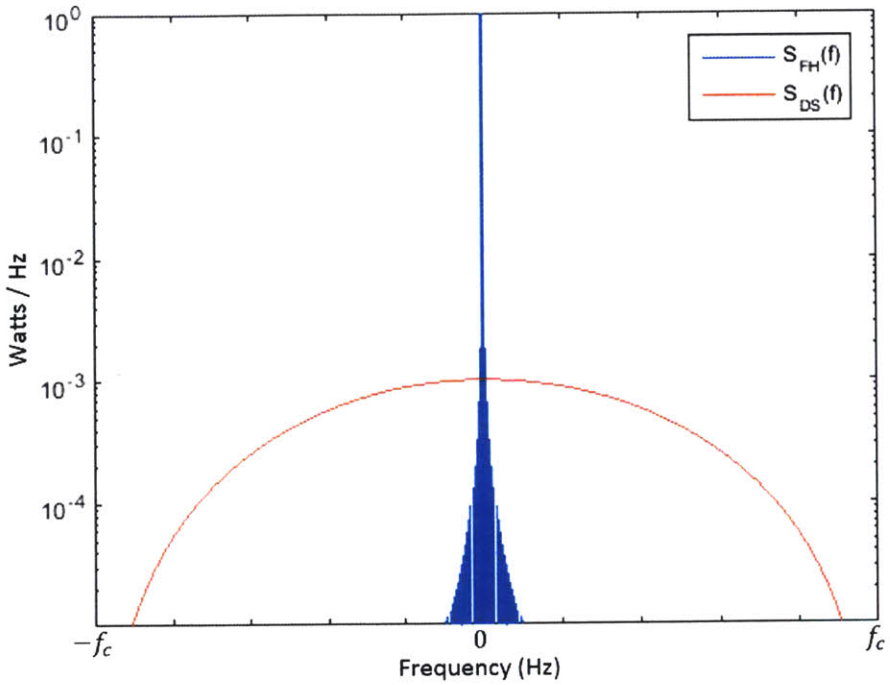


Fig. 6 Comparison of Power Spectral Densities for $G_p = 1000$

Since several arbitrary parameter choices ($T_b$ and $f_{ss}$) were made to generate Fig. 5 and Fig. 6, no particular significance should be ascribed to the values of the primary axes of these plots. The purpose of these figures is to examine the relative difference in power concentrations between frequency hopping and DS spreading, not the particular values of the concentrations themselves.

## 2.1.4.2 Vulnerability of Frequency Hopping to Detection

As shown in the previous section, frequency hopped signals have a far more distinctive power distribution than their DS spread counterparts that makes them easier to detect. Current SATCOM systems compensate for frequency hopping's poor LPI characteristics by operating in a high enough frequency band that most ADC's cannot observe the channel. However, recent advances in ADC technology, such as Fujitsu's 56 Giga-sample per second 8-bit ADC, are beginning to render high frequency channels more vulnerable to observation [11]. As ADC technology progresses, it is reasonable to assume that the EHF

band (43.5 - 45.5 GHz) will become observable. Assuming that an ADC is developed that allows a fast Fourier transform (FFT) to be performed over the entire EHF band, the processing power required to perform the FFT is the final obstacle an adversary must overcome in order to detect a frequency hopped signal. It is therefore important to investigate the processing power required to perform an FFT on the EHF band.

Assuming that an ADC can provide a 100 Giga-sample per second input to a processor, and that a frequency hopped signal in the EHF band is using a data bandwidth of 2.4 kHz, a $4.17 \times 10^7$ point FFT is required in order to observe the channel in fine enough detail to detect the FH signal[8]. However, assuming that the split-radix algorithm is used to compute the FFT, the number of points in the FFT must be a power of 2 [12]. Therefore, a $2^{26} \approx 6.71 \times 10^7$ point split-radix FFT must be computed. From [12], a split-radix FFT of this size will require approximately 13.154 Giga-flops to compute assuming that each flop from the algorithm also requires a flop of overhead.

Unfortunately for current SATCOM systems, 13.154 Giga-flops is a trivial processing requirement for current processors. An Intel Core i7 processor can provide 90 Giga-flops per second of processing power and could compute the entire FFT in approximately 146 milliseconds [13]. This result suggests that once ADC technology progresses to the point where a 100 Giga-sample per second input is possible, the processing power to perform the FFT to detect a frequency hopped signal in the EHF band is trivial. Therefore, it is only a matter of time before current SATCOM systems lose their ability to provide channels with good LPI characteristics. It is imperative that an alternative LPI scheme such as DS spreading be implemented in future SATCOM systems.

[8] See Appendix A.2 for supporting calculations for this section.

An additional drawback of frequency hopping's vulnerability to detection is that its power advantage over an interferer it also compromised. If an adversary can reliable detect a frequency hoppeds signal in real-time, it can concentrate its interference in the same band as the user and can follow the user's hopping pattern, thereby eliminating the user's power advantage over the interferer. In order to perform this kind of interference, the adversary would have to be able to compute an FFT faster than the user is hopping their signal, which would require a processing time on the order of microseconds for most FH systems. While a single Intel Core i7 processor cannot perform the required FFT in this amount of time, more powerful processors or cloud computing services could be used to reduce the computation time. Given these weaknesses, frequency hopping may no longer be viable in terms of LPI or robustness as a solution for future SATCOM systems.

## 2.2 Threat Estimate

While previous sections of this chapter have dealt with the description and performance of the DS/ALOHA system, it is equally important to have an understanding of the systems an adversary can use to threaten such a system. The primary focus in developing an estimate of the threats SATCOM systems will face in the future is the transmission power an adversary can achieve on a mobile platform. While stationary platforms can be larger, and therefore transmit interference at greater power, their static nature renders them vulnerable to other prevention strategies such as kinetic strikes, mission planning, and satellite positioning. Mobile platforms are far more difficult to account for in planning and are also less vulnerable to targeting. Therefore, the design of the DS/ALOHA system in this thesis focuses primarily on the maximum transmission power achievable by a transportable interferer.

### 2.2.1 Estimate of Interferer Strength

The metric used to gauge the interference power achievable by a transportable interferer will be its effective isotropic radiated power $E_I$. The interferer's EIRP is simply a product of the power available to the interferer for transmission $P_I$ and the gain of its antenna $G_I$. It is somewhat difficult to estimate the values of $P_I$ and $G_I$ since the capabilities of many advanced interferers are kept secret by the nations that develop them. Therefore, this thesis uses estimates of $P_I$ and $G_I$ based on information that is publicly available, but it should be kept in mind that more powerful systems may be achievable.

A reasonable estimate for $P_I$ is 1000 watts based on commercially available travelling wave tube amplifiers. Several companies advertise compact amplifiers operating near the EHF band that can achieve 500 watts of output power [14]. Additionally, these amplifiers can be aggregated to achieve significantly higher total output power [15]. It is therefore plausible that several 500 watt amplifiers could be combined to produce a kilowatt of output power in a configuration that is physically small enough to mount on a mobile platform.

A reasonable estimate for $G_I$ is developed by estimating the largest diameter antenna a mobile system can support. Given an estimate of the diameter $d_I$ of the interferer's antenna, the antenna's gain can be expressed as [16]:

$$G_I = \frac{\pi^2 d_I^2 e_I}{\lambda_c^2} \quad , \tag{2.9}$$

where $e_I$ is the interferer antenna's efficiency (assumed to be 0.7) and $\lambda_c$ is the wavelength of the center frequency of the frequency band the interferer is transmitting in (approximately 0.006742 meters at 44.5

GHz). Assuming that $d_I = 5$ meters is the largest diameter aperture antenna a transportable platform can support, the estimated value for $G_I$ at 44.5 GHz is 65.80 dB of gain.

Given the dependence of $G_I$ on frequency, the estimated EIRP of the transportable interferer can be calculated over a range of frequencies used by SATCOM systems. A plot of $E_I$ versus frequency for the super high frequency (SHF) and EHF bands is shown in Fig. 7. This is a highly useful result as it allows users of other SATCOM terminals to determine how effectively a transportable interferer can degrade their systems. From Fig. 7 it is evident that the EIRP of the transportable interferer increases with increasing frequency due to the resulting increase in antenna gain. At 44.5 GHz, the center frequency of interest for the DS/ALOHA system, the estimated EIRP achievable by a transportable interferer is approximately 95.8 decibel watts (dBW). This is a considerable amount of interference power, especially since users of the DS/ALOHA system are expected to transmit with only 10 watts of power and an EIRP of only 36.15 dBW. Given this significant difference in EIRP, DS spectrum spreading and effective channel coding are required to mitigate the transportable interferer.

Given that the results in Fig. 7 are developed using commercially available components from open sources, it is reasonable to assume that transportable interferers with high interference powers will be a fairly ubiquitous technology in the future since any organization with even a modest amount of technical knowledge and resources could acquire or assemble such a system. Therefore, it is necessary for future SATCOM systems, including the DS/ALOHA system proposed in this thesis, to possess the ability to operate in an environment in which a powerful transportable interferer is present.

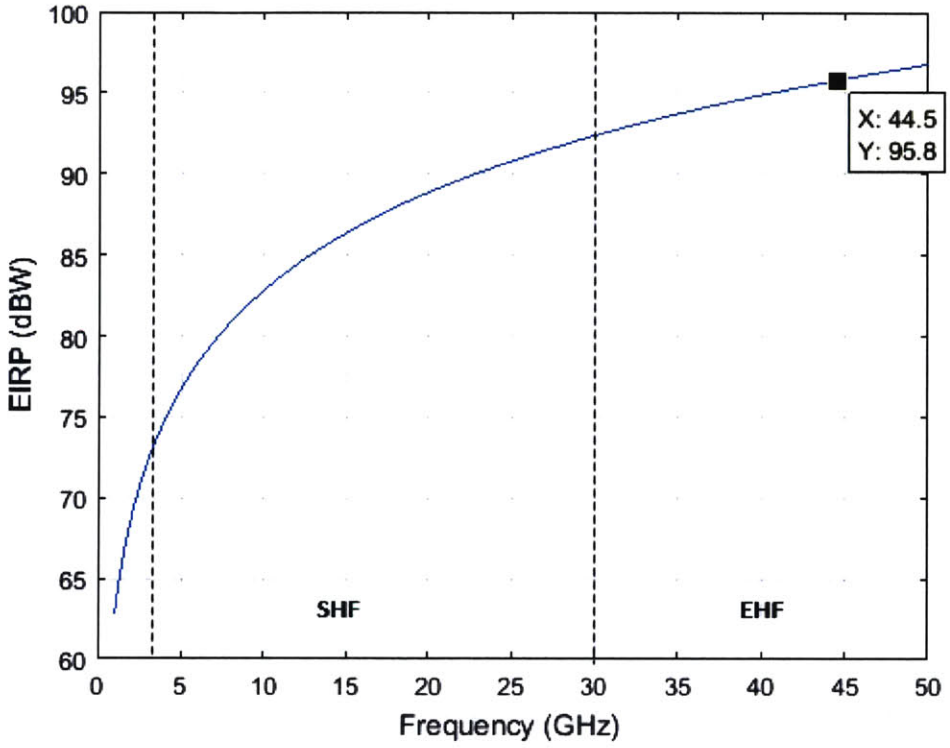


Fig. 7 Interferer EIRP vs. Frequency

## 2.2.2 System Capacity with Broadband Interferer

In order for the DS/ALOHA system to be a viable solution for future SATCOM requirements, it must be able to achieve reasonable channel and total system capacity when subjected to interference from a transportable platform. The channel capacity $C$ with an interferer present can again be determined using (2.2) with the following modification to the expression for SNR in (2.3):

$$SNR = \frac{E_{TX}G_{RX}F_p}{W_d N_0 + G_p^{-1}E_I G_{RX}F_p G_n^{-1} + (N_C - 1)f_{co}E_{TX}G_{RX}F_p} \quad , \tag{2.10}$$

where $G_n$ is the power advantage over the interferer afforded to the user due to antenna nulling. It is assumed here that the transportable interferer has no knowledge of the sequence of DS codes being used

by a channel and therefore defaults to spreading its power uniformly over the entire spread bandwidth. Thus, users have a transmission power advantage over the interferer equal to the processing gain $G_p$. It is also assumed that the signal path loss is the same for both the interferer and the user. Given the updated expression for SNR in (2.10), the total system capacity $C_{sys}$ can again be determined using (2.6). A plot of channel capacity versus processing gain with no antenna nulling ($G_n = 1$) and the same physical parameters from Appendix A.1 is given in Fig. 8. A plot of total system capacity versus processing gain and the same parameters is given in Fig. 9.

The effect of the transportable interferer is readily apparent in Fig. 8 and Fig. 9 where the channel and total system capacities have been significantly reduced from the capacities shown in Fig. 3 and Fig. 4. Users can now expect to achieve a data rate no higher than 1560 Bps and the maximum total system capacity is now only slightly greater than 100 MBps. These capacities may be too low to accommodate many types of user messages over the DS/ALOHA system. The only way to improve the situation is to further increase the power advantage of the user's signal over the interferer's signal through a method like antenna nulling. Assuming that antenna nulling can provide 20 dB of suppression to the interferer's signal ($G_n = 100$), the channel and total system capacities can be increased to those shown in Fig. 10 and Fig. 11.

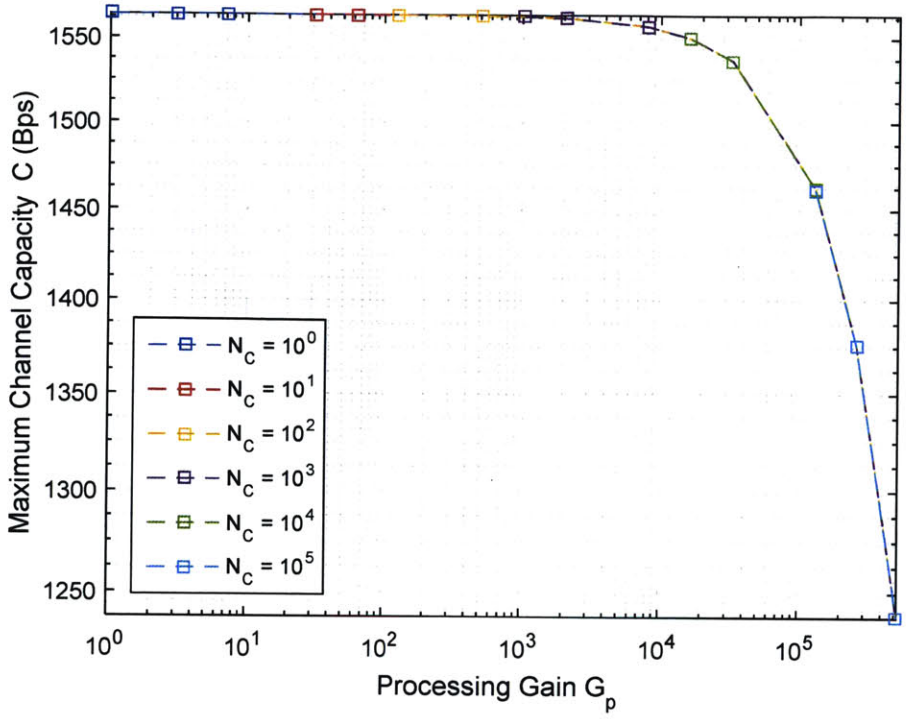


Fig. 8 Channel Capacity (Bps) vs. Processing Gain for Channel with Broadband Interference

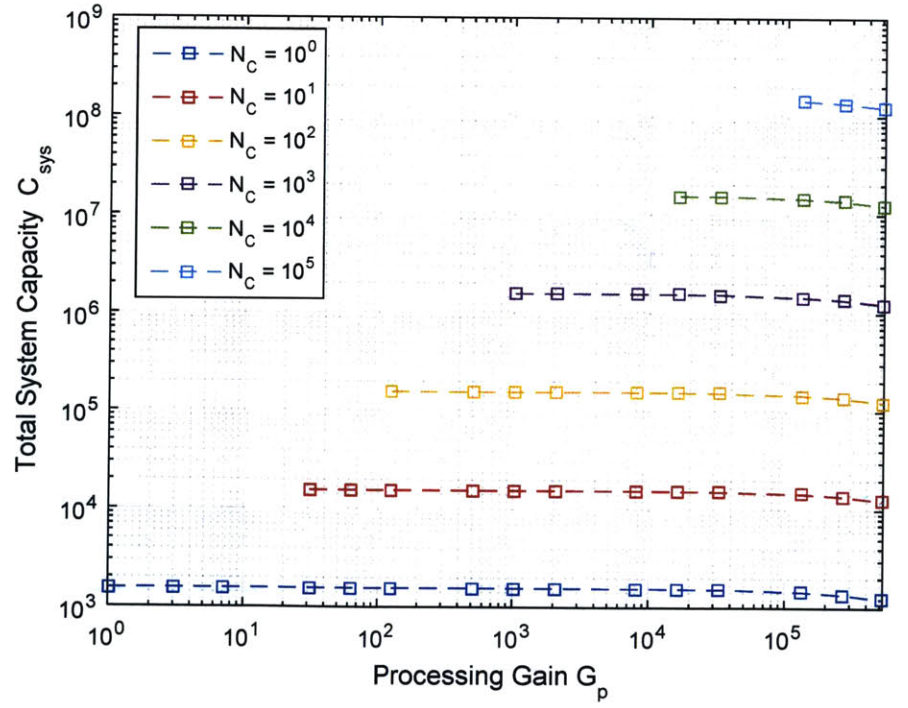


Fig. 9 Total Capacity (Bps) vs. Processing Gain for Channel with Broadband Interference

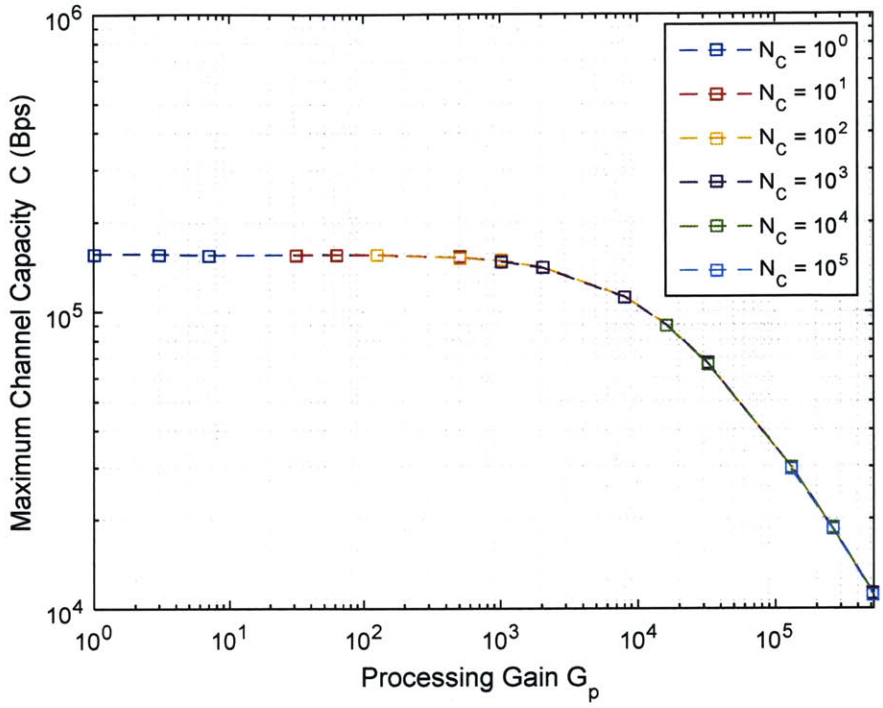


Fig. 10 Channel Capacity (Bps) versus Processing Gain with Interference and 20 dB Antenna Nulling

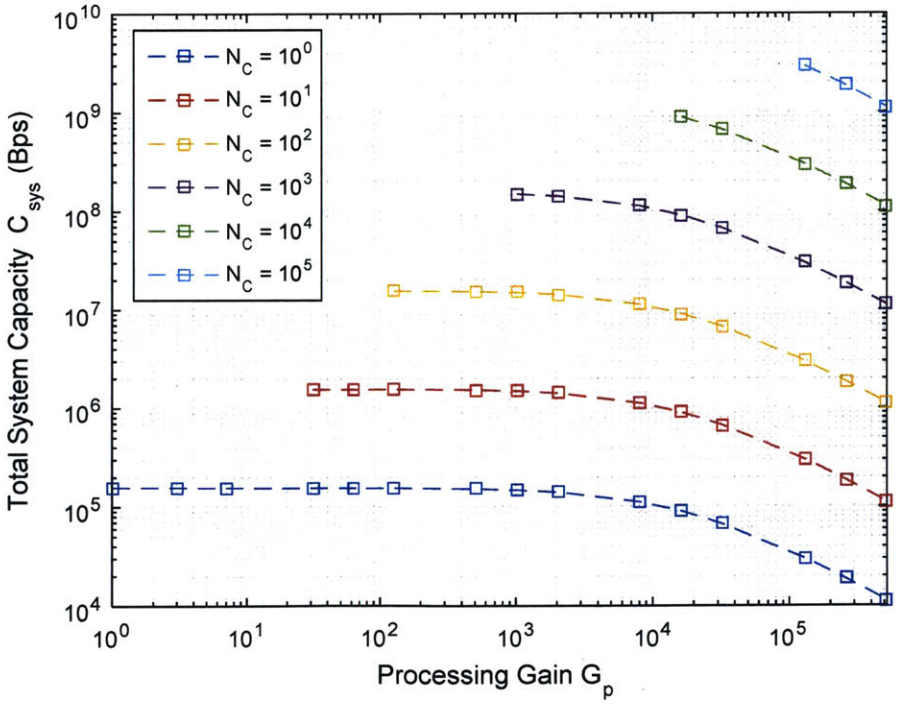


Fig. 11 Total Capacity (Bps) versus Processing Gain with Interference and 20 dB Antenna Nulling

From Fig. 10 and Fig. 11 it is apparent that 20 dB of antenna nulling is sufficient for the DS/ALOHA system to support a large number of channels at a reasonably high data rate close to 100 kBps, though the channel and total system capacities still suffer a significant reduction from their benign channel counterparts. It should be noted that the reason that $C_{sys}$ is fairly invariant versus $G_p$ in Fig. 9 and Fig. 11 is that the number of channels $N_C$ dominates the expression for $C_{sys}$ when an interferer is present.

From this analysis of channel and total system capacities, it is evident that users must transmit at a lower data rate when a strong interferer is present in the channel. In order to take advantage of the high data rate afforded under benign circumstances, the DS/ALOHA system should be able to detect an interferer, estimate its power, and dynamically adjust the data rates of its channels accordingly. This functionality will be discussed in greater detail in Chapter 5.

## 2.3 Summary

This chapter outlined the DS/ALOHA system and estimated the threats that SATCOM systems will face in the future. Section 2.1 described the physical and MAC layers of the system and estimated the maximum achievable channel and total system capacities under benign circumstances. It was demonstrated in this section that the DS/ALOHA system can support a large number of channels operating at a high data rate under these conditions. This section also investigated the LPI characteristics of both DS spectrum spreading and frequency hopping and showed that improvements in ADC technology will render frequency hopping vulnerable to detection. Section 2.2 outlined the kinds of systems adversaries may construct to threaten SATCOM systems and developed an estimate for the EIRP achievable by a transportable interferer. This section also examined the performance of the DS/ALOHA system when subjected to a transportable interferer and revealed that antenna nulling will be required to achieve acceptable channel data rates.

# Chapter 3

# Control Algorithm and Dual-Class Service

This chapter investigates the performance of the Rivest Algorithm [4] in stabilizing the ALOHA protocol on a system with significant feedback delay. The Rivest Algorithm is shown to be able to effectively stabilize the system and achieves high throughput with time-varying user arrival rates and significant feedback delay. Furthermore, the algorithm is shown to be able to clear congestion that develops during periods of congestion in the subsequent sufficiently long period of supportable traffic. An estimation of the time required by the algorithm to clear congestion is also developed. Next, a technique for implementing dual-class service for normal and priority users via random drops is developed, along with a means for estimating user arrival rates. The dual-class scheme is simulated and found to be reasonably effective in maintaining channel efficiency while offering two levels of service. Finally, the implementation of a stricter time-deadline service is discussed and is shown to be effective only for a small number of users.

## 3.1 The Rivest Control Algorithm

As previously discussed in Section 2.1.2, the ALOHA protocol requires a control algorithm to ensure that the attempted transmission rate remains biased close to $G = 1$ in order to ensure that the system remains stable and that the optimum throughput of $e^{-1}$ is achieved. In other words, a control algorithm is needed to set the transmission probability $q$ on each slot so that the expected number of packets transmitted on each slot is one. It is important to note that it is assumed that system feedback, including $q$, is received by

all users without error. In order to develop an algorithm to modify $q$ based on observations from the channel, it is first necessary to determine the optimum $q$ as a function of the number of packets $N$ ready for transmission in the current slot. It is shown in [4] that the optimal transmission probability for $N$ packets is $q = 1/N$. However, since the receiver only observes holes, successes, and collisions it must estimate the number of packets ready for transmission $v$ and uses this estimate to specify the transmission probability as $q = 1/v$ [4].

The primary function of the control algorithm is to develop an accurate estimate of $N$ based solely on observations of holes, successes, or collisions on each time slot. Developing an estimation technique is difficult because the arrival rate of new packets to the channel $\lambda$ is also unknown and affects the number of packets ready for transmission. In order to address this issue, the Rivest Algorithm is developed from a technique known as Pseudo-Bayesian inference. This technique approximates $N$ as a Poisson random variable and uses the conditional distributions of $N$ given a hole, success, or collision to estimate the number of packets in the system [4]. Performing the Pseudo-Bayesian inference method leads to the surprising simple result that the value of $v$ is updated after each slot by incrementing it or decrementing it by constant values determined by the outcome of the most recently observed time slot [4].

The Rivest Algorithm uses $v = 1$ as its initial estimate of $N$ and then increments or decrements $v$ after each slot based on whether a hole, success, or collision was observed during the slot [4]. If a hole or success is observed, the algorithm decrements $v$ by one [4]. If a collision is observed, the algorithm increments $v$ by $(e-2)^{-1} \approx 1.392211$ [4]. Finally, the algorithm sets $v$ to $max\{v + \hat{\lambda}, 1\}$ where $\hat{\lambda}$ is the estimated arrival rate of new packets to the channel [4]. A discussion of estimation techniques for $\lambda$ is given in Section 3.1.3.

### 3.1.1 Performance Metrics

In order to analyze the effectiveness of the Rivest Algorithm as a control mechanism for an ALOHA channel it is first necessary to develop several performance metrics. Four different metrics will be considered: the number of backlogged packets, the expected channel delay, the long-term throughput of the system, and the local throughput of the system. The number of backlogged packets is used as a means to gauge the level of congestion present in the ALOHA system and will be specified as the value of $N$ during the current time slot. A backlog that appears to grow without bound will indicate instability in the ALOHA system. The expected channel delay is primarily used to gauge the channel quality from the perspective of the individual user. The higher the expected channel delay, the greater the message delivery latency a user can expect to experience. The channel delay is defined as the expected amount of time $T_w$ that a packet will spend in the ALOHA system based on the current value of $N$. Note that $T_w$ includes the time the packet spends waiting to be transmitted over the channel as well as the time it takes for the packet's transmission to traverse the channel and receive feedback from the receiver. The expected value of $T_w$ can be expressed in the following manner (see Appendix B.1 for a derivation of this result):

$$E[T_w] = e(v + N_{RTT})L_p T_b \quad , \tag{3.1}$$

where $N_{RTT}$ is the number of ALOHA time slots in a round trip time (RTT) of the channel, $L_p$ is the length in bits of a packet sent during a time slot, and $T_b$ is the data bit period. In addition to estimating the number of packets ready for transmission using the parameter $v$, the ALOHA control mechanism maintains an estimate of the expected channel delay $E[\hat{T}_w]$ using the same relationship:

$$E[\hat{T}_w] = e(v + N_{RTT})L_p T_b \tag{3.2}$$

This expression allows the control mechanism to estimate the latency experienced by the channel's users and is used as a control parameter for the dual-class service discussed in Section 3.3. The number of slots per round trip time $N_{RTT}$ can be determined by the following relationship:

$$N_{RTT} = \frac{T_{RTT}}{L_p T_b} \quad , \tag{3.3}$$

where $T_{RTT}$ is the channel's round trip time in seconds. A reasonable estimate of $T_{RTT}$ for a satellite in geosynchronous orbit is 250 milliseconds. Additionally, there will also be some processing delay at the satellite receiver. Therefore, if the system is operating at a data rate of 1 MBps there will be at least 250 time slots in a single round trip time, each lasting 1 millisecond. Simulations of the DS/ALOHA system in subsequent sections operate under this assumption.

The long-term average throughput of the system $\Gamma_{LT}$ is used to gauge the convergence of the DS/ALOHA system towards a steady state when the packet arrival rate is constant, and is also used as means of measuring how well the system maintains a throughput near $e^{-1}$ when the arrival rate is time-varying. For a slotted ALOHA system, the long-term average throughput is computed as an average starting from the first simulated time slot up to the current time slot. In other words, for the nth slot since the ALOHA system was initialized, $\Gamma_{LT}$ is expressed as:

$$\Gamma_{LT} = \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}_S(i) \quad , \tag{3.4}$$

where $\mathbb{I}_S(i)$ is an indicator variable associated with the ith time slot and has a value of 1 if the slot contains a success and a value of zero otherwise. Similar time-averages will also be computed for hole and collision slots using the same technique as (3.4) where $\mathbb{I}_S(i)$ is replaced by $\mathbb{I}_H(i)$ and $\mathbb{I}_C(i)$ for holes and collisions

respectively. The variables $\mathbb{I}_H(i)$ and $\mathbb{I}_C(i)$ behave in a manner similar to $\mathbb{I}_S(i)$ except that they have a value of one when the slot contains a hole or collision respectively.

The local throughput of the system $\Gamma_{Lo}$ is used to gauge the throughput achieved by the DS/ALOHA system over a short window of time in order to gain an understanding of how well the system is performing at a specific point in time. The local throughput is computed in a manner similar to the long-term throughput, except that the average is performed over the last 250 time slots instead of all previous slots. The choice of 250 time slots as the window length for $\Gamma_{Lo}$ is based on the assumption that there are 250 time slots in a single round trip time for the channel. Thus, $\Gamma_{Lo}$ is a local average over the time it takes the system to update after it observes the outcome of the current time slot. An expression for $\Gamma_{Lo}$ is:

$$\Gamma_{Lo} = \frac{1}{max\{n - n_{start} + 1\}} \sum_{i=n_{start}}^{n} \mathbb{I}_S(i) \quad , \tag{3.5}$$

where $n_{start}$ is the first slot included in the average and is determined by the following expression:

$$n_{start} = max\{1, n - 249\} \tag{3.6}$$

The expression in (3.6) is used to account for the initial 249 slots after initialization where the system has not yet been active for 250 slots and therefore cannot average over an entire window of 250 time slots. In this case, the system simply averages over as many slots as are available. As in the long-term throughput case, local averages for holes and collisions are computed using (3.6) with $\mathbb{I}_S(i)$ replaced by $\mathbb{I}_H(i)$ and $\mathbb{I}_C(i)$ respectively.

### 3.1.2 System Response to Delayed Feedback

The Rivest Algorithm was developed under the assumption that feedback from the previous slot is available when the transmission parameter $q$ for the next slot is determined. However, this assumption is not reasonable for a SATCOM system due to the long round trip time of the channel. Assuming that the channel data rate is 1 MBps, and therefore that $N_{RTT} = 250$ slots, the Rivest Algorithm implemented on a SATCOM system operates based on feedback that is delayed by 250 time slots. Another way to think about this delay in a physical system is to imagine that the Rivest Algorithm operating at the receiver is observing transmissions that occurred 125 time slots ago (half an RTT). The algorithm updates the transmission parameter $q$ based on the delayed feedback and transmits the updated value to all users who will receive it 125 slots later. Thus, users transmit based on feedback that is delayed by a total of 250 time slots.

There are two schemes that users can employ to interact with the delayed ALOHA channel. We refer to these two strategies as the continuous transmission attempt scheme and wait-for-feedback scheme. Under the continuous transmission attempt scheme, packets that pass their transmission test will continue to attempt transmissions on subsequent time slots with probability $q$ until they receive feedback that their transmission has been received successfully. A potential advantage of this scheme is that latency may be reduced because transmitted packets that collide will not wait for feedback from the receiver before attempting retransmission. However, this comes at the cost of stability and congestion as transmitted packets that are received successfully will continue to attempt retransmission for 250 more time slots before they get feedback that their initial transmission attempt was successful.

Under the wait-for-feedback scheme, packets that pass their transmission test wait for feedback from the receiver before attempting to pass their transmission test again (if the feedback indicates that a

retransmission is necessary) [17]. The advantage of this scheme is that it has a better stability because packets will only attempt retransmission if they are not received correctly. The disadvantage of this scheme is its potentially higher latency because packets that collide will not attempt another retransmission for 250 time slots.

The continuous transmission attempt and wait-for-feedback schemes were compared by simulating an ALOHA system controlled by the Rivest Algorithm for 20,000 time slots using each scheme. For these simulations, the arrival rate to the channel was held constant with a value of $\lambda = 0.3$ packets per slot[9]. Both simulations used the same random seed to ensure that a fair performance comparison was made. Plots of the actual and estimated backlog over time for both schemes are given in Fig. 12 and Fig. 13. Plots of the expected channel delay for both schemes are given in Fig. 14 and Fig. 15. Finally, plots for long-term and local average throughput, holes, and collisions for both schemes are given in Fig. 16 through Fig. 19.

A comparison of the backlog plots from Fig. 12 and Fig. 13 reveals that the wait-for-feedback scheme has significantly less congestion than the continuous transmission attempt scheme. Additionally, under the wait-for-feedback scheme, $v$ remains relatively close to $N$ while under the continuous transmission attempt scheme, $v$ oscillates significantly above and below $N$. The oscillations seen in Fig. 12 are due to the repeated transmissions that occur before users receive updated feedback. These repeated transmissions result in an increased number of collisions which causes the algorithm to overestimate $N$, the number of packets in the system. As the overestimate of $N$ increases, eventually a point is reached where the value of $v$ is so large that the system is highly suppressed and few transmissions are attempted. As the system slowly begins to allow more retransmissions due to the large number of hole slots observed during the period of suppression, throughput improves until $v$ drops to a low enough value

[9] Note that a constant estimate of $\hat{\lambda} = e^{-1}$ is used in these simulations. An explanation for this choice is given in Section 3.1.3.

that the backlog begins to rapidly increase again and the cycle repeats. Thus, the continuous transmission attempt scheme is more prone to instability and is more congested than the wait-for-feedback scheme.

It is important to note that the expression for expected channel delay from (3.2) is developed under the assumption that the system is operating under the wait-for-feedback scheme. An expression for the expected channel delay for the continuous transmission attempt scheme is:

$$E[\hat{T}_w] = (e \cdot v + N_{RTT})L_p T_b \tag{3.7}$$

See Appendix B.2 for a derivation of this result. A plot of expected channel delay for the continuous transmission attempt scheme is given in Fig. 14. A comparison of Fig. 14 and Fig. 15 reveals that the wait-for-feedback scheme achieves lower expected channel delay on the average than the continuous transmission attempt scheme. This is due to the fact that the congestion of the continuous transmission attempt scheme is so severe that it eliminates the latency advantage packets gain from being able to continuously attempt to transmit on time slots.

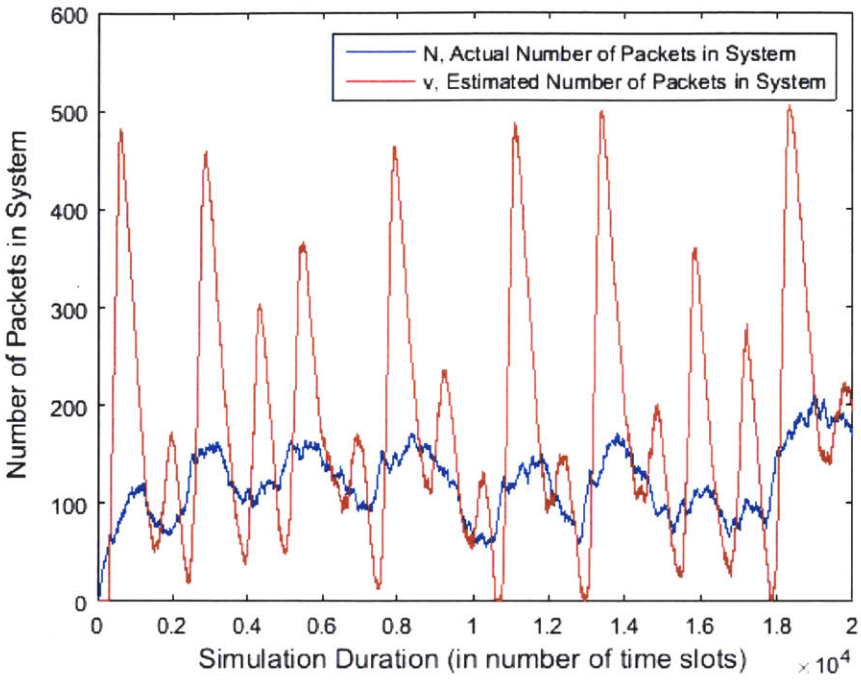


Fig. 12 Simulated Actual and Estimated Backlog for the Continuous Transmission Attempt Scheme

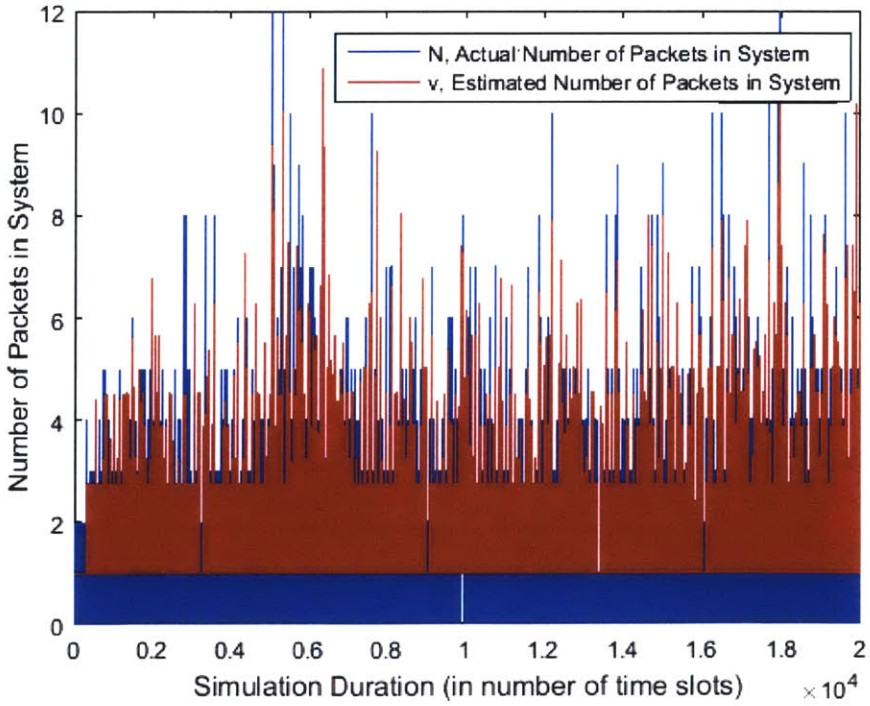


Fig. 13 Simulated Actual and Estimated Backlog for the Wait-for-Feedback Scheme

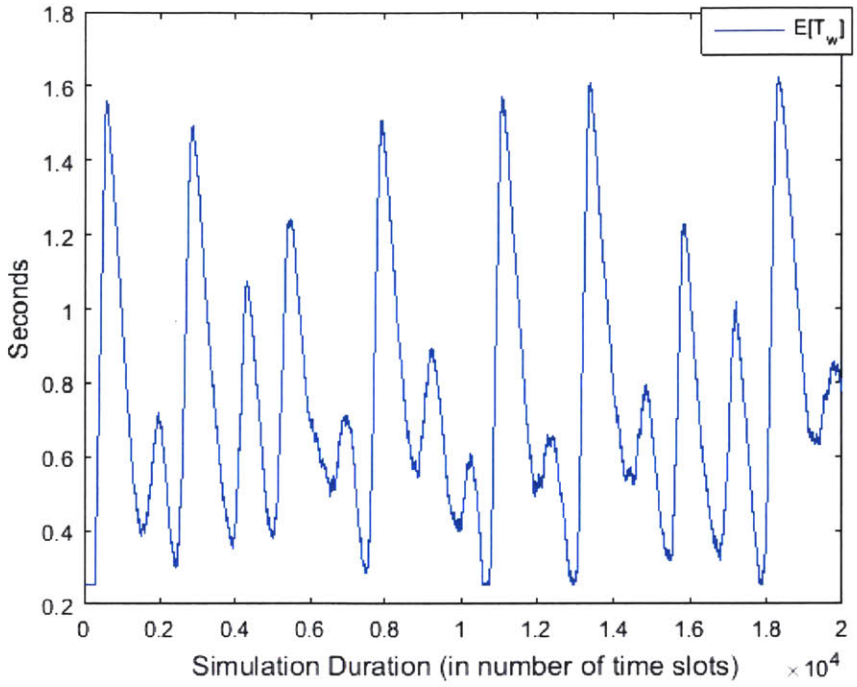


Fig. 14 Simulated Expected Channel Delay for the Continuous Transmission Attempt Scheme

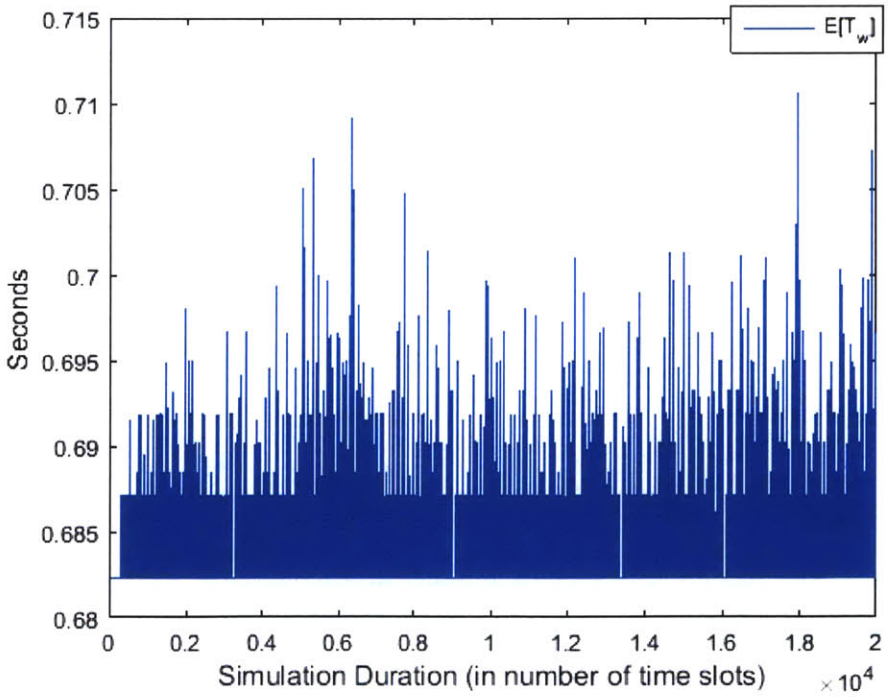


Fig. 15 Simulated Expected Channel Delay for the Wait-for-Feedback Scheme

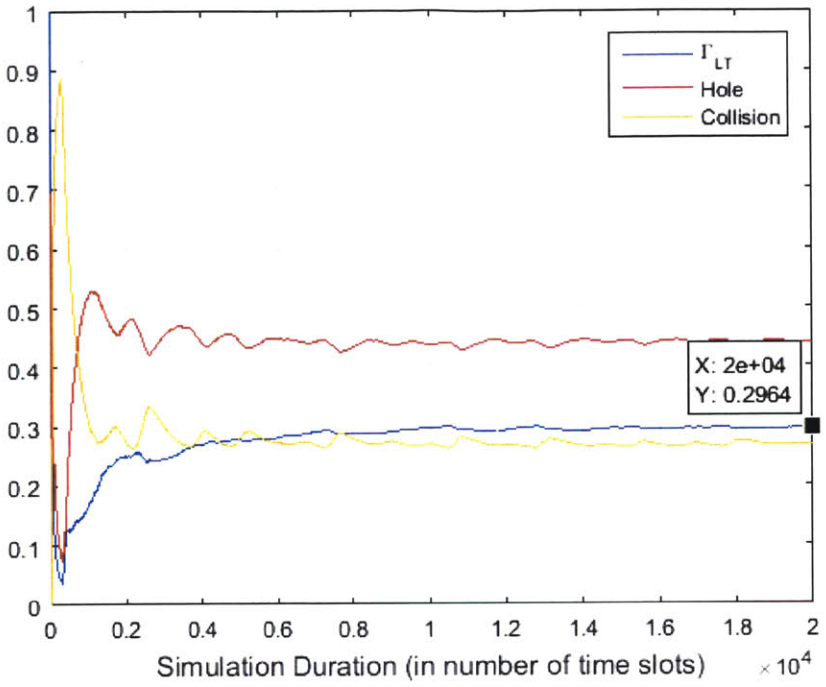


Fig. 16 Simulated Long-Term Averages for Continuous Transmission Attempt Scheme

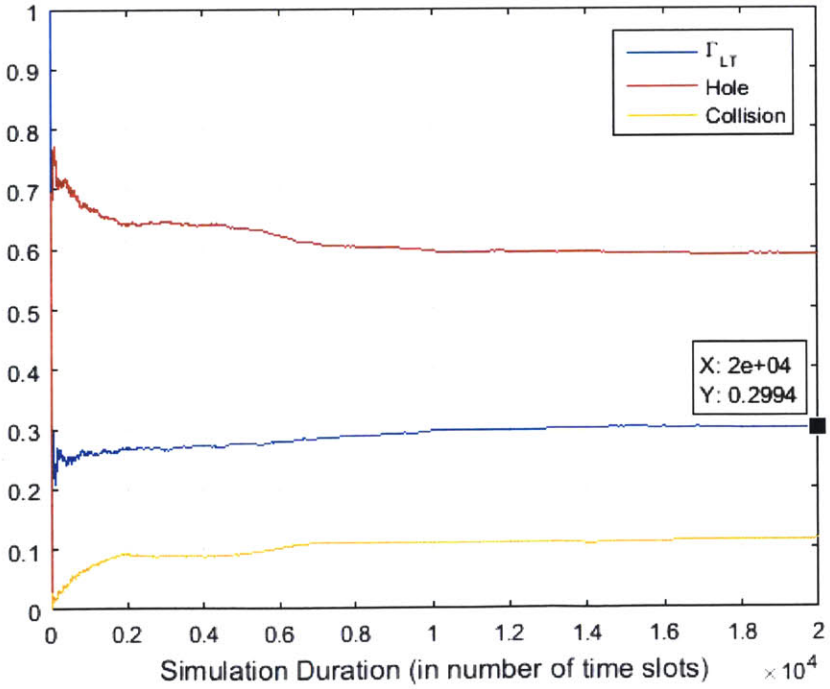


Fig. 17 Simulated Long-Term Averages for Wait-for-Feedback Scheme

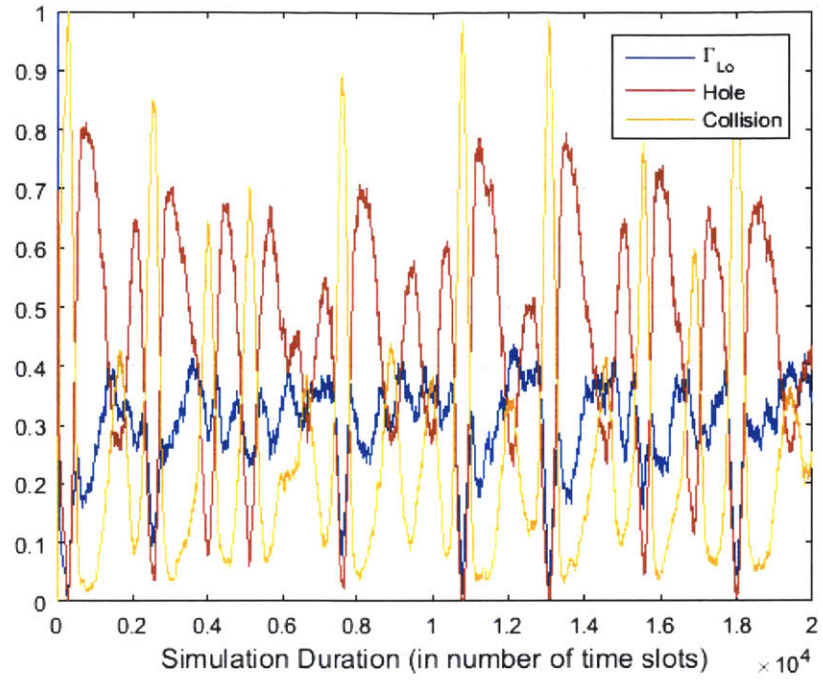


Fig. 18 Simulated Local Averages for Continuous Transmission Attempt Scheme

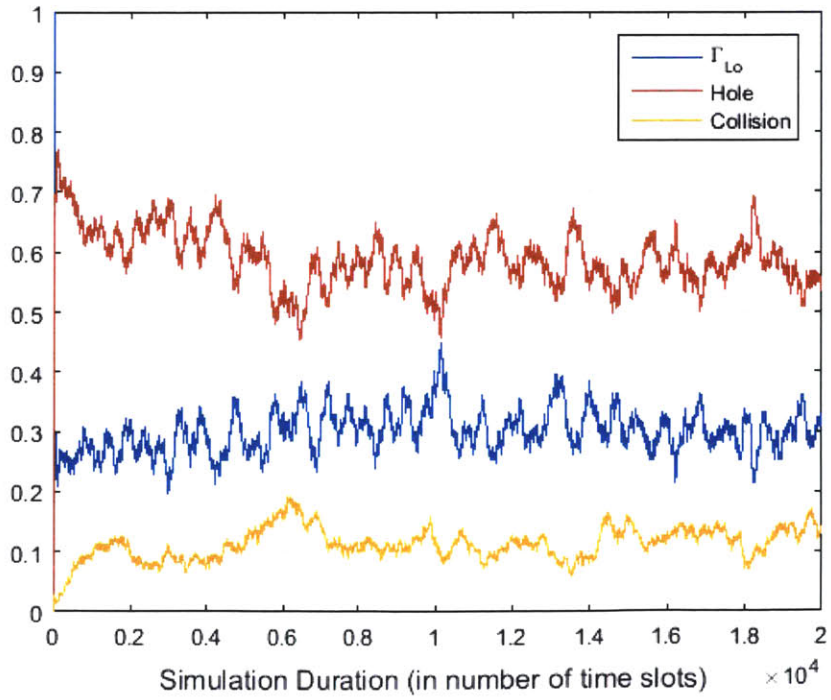


Fig. 19 Simulated Local Averages for Wait-for-Feedback Scheme

From Fig. 16 and Fig. 17 we see that both schemes achieve similar long-term throughputs and that the continuous transmission attempt scheme has more collisions and less holes on the average than the wait-for feedback scheme. Comparing the local averages from Fig. 18 and Fig. 19 reveals that the local throughput is far more consistent under the wait-for-feedback scheme. Since the wait-for-feedback scheme also achieves lower delay on average, it is clearly superior as a means for managing packet retransmissions. For this reason, the DS/ALOHA system in this thesis uses the wait-for-feedback scheme.

### 3.1.3 Control Algorithm Stability

A key performance requirement for the DS/ALOHA system discussed in the previous section is the stability of the control algorithm. Runaway instability occurs when the number of backlogged packets begins to grow without bound when the system is biased at a throughput that is less than the arrival rate of new packets to the channel. A good control algorithm must be able to bias the ALOHA protocol close to its optimal throughput of $e^{-1}$ while preventing the system from entering a state of runaway instability due to sharp changes in the packet arrival rate . It is worth noting that for $\lambda > e^{-1}$ the system will always be congested since packets are arriving faster than they can be cleared by the system. However, a good control algorithm will be able to tolerate brief periods where $\lambda$ exceeds the system's maximum throughput as long as they are followed by sufficiently long periods where $\lambda < e^{-1}$ which allow the system to clear the backlog created by unsupportable surges in user traffic.

While the relative stability of user retransmission schemes has been discussed in the previous section, the impact of the estimation of the arrival rate $\lambda$ on the stability of the ALOHA system has not yet been explored. The work in [4] outlines the Rivest Algorithm's method for updating $v$ and $q$, but it is less concrete in its treatment of the estimated arrival rate $\hat{\lambda}$ and its effect on system stability. Fortunately, the stability of the ALOHA system in terms of $\hat{\lambda}$ is discussed in great detail in [18], Where it is shown that for

a constant arrival rate satisfying $\lambda \leq e^{-1}$, setting $\hat{\lambda}$ to the constant value $e^{-1}$ results in a stable system that achieves the same throughput as the case where the true value of $\lambda$ is known. It is also shown in [18] that if a different method is used to estimate $\hat{\lambda}$, such as averaging or inference, instability in the system can result if $\lambda > \hat{\lambda}$ even if $\lambda < e^{-1}$. Therefore, based on these results, the DS/ALOHA system in this thesis uses the constant value of $e^{-1}$ for $\hat{\lambda}$.

It should be noted that the results derived in [18] are developed under the assumption that there is no delay in feedback and that the arrival rate of packets to the channel is constant. It is briefly argued in [18] that the proof of stability can be extended to a channel with fixed finite delay in its feedback when the arrival rate is constant. However, it is unrealistic to model the arrival rate of packets to the channel as time-invariant since real-world traffic changes significantly over time. Unfortunately, a time-variant arrival rate significantly increases the complexity of the analysis performed in [18]. Under these conditions it is very difficult to determine the stability of the system, but the system can be simulated with delayed feedback and a time-varying arrival rate can be simulated to gain a sense of its stability. These simulations are the focus of Section 3.2.1.

## 3.2 Control Algorithm Performance

In order to better understand how a DS/ALOHA system controlled by the Rivest Algorithm performs when the arrival rate is time-varying and the feedback is delayed by 250 slots, the system is simulated for three test cases. These simulations use the wait-for-feedback scheme and the constant value of $e^{-1}$ for $\hat{\lambda}$. The three test cases use different time-varying arrival rates $\lambda$ which are modelled as a step function, a pulse function, and a sinusoid. The value of $\lambda$ never exceeds $e^{-1}$ in each test case, resulting in a time-varying traffic load this is never greater than the system's maximum throughput. Plots of the arrival rate versus

simulation time for the three test cases are given in Fig. 20 through Fig. 22. The resulting backlog, delay, local averages, and long-term averages for each case are given in Fig. 23 through Fig. 34.

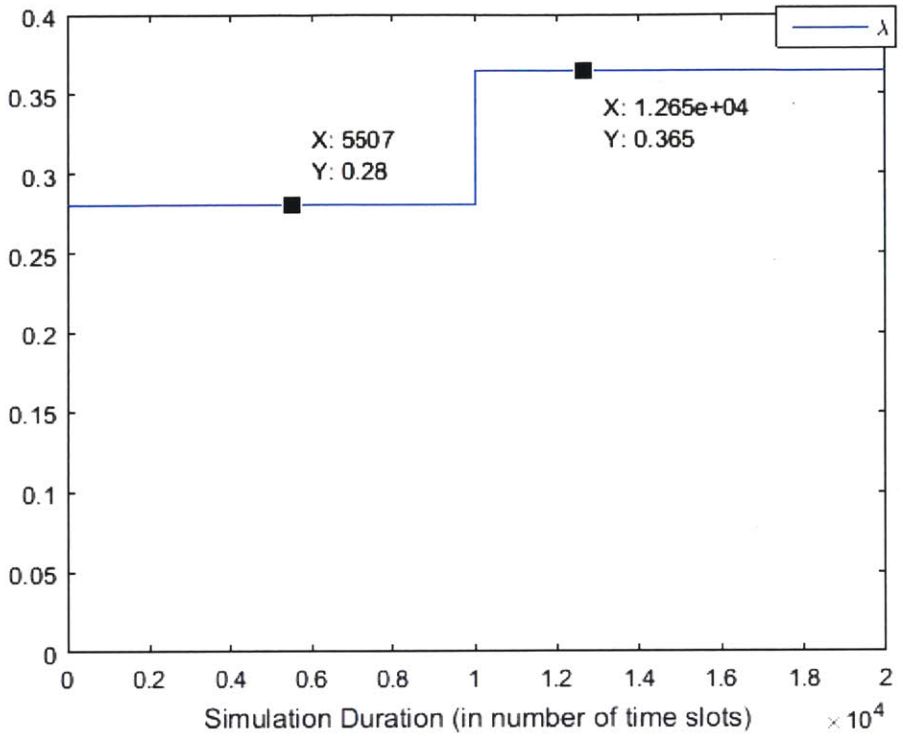


Fig. 20 Step Function Poisson Arrival Rate Test Case

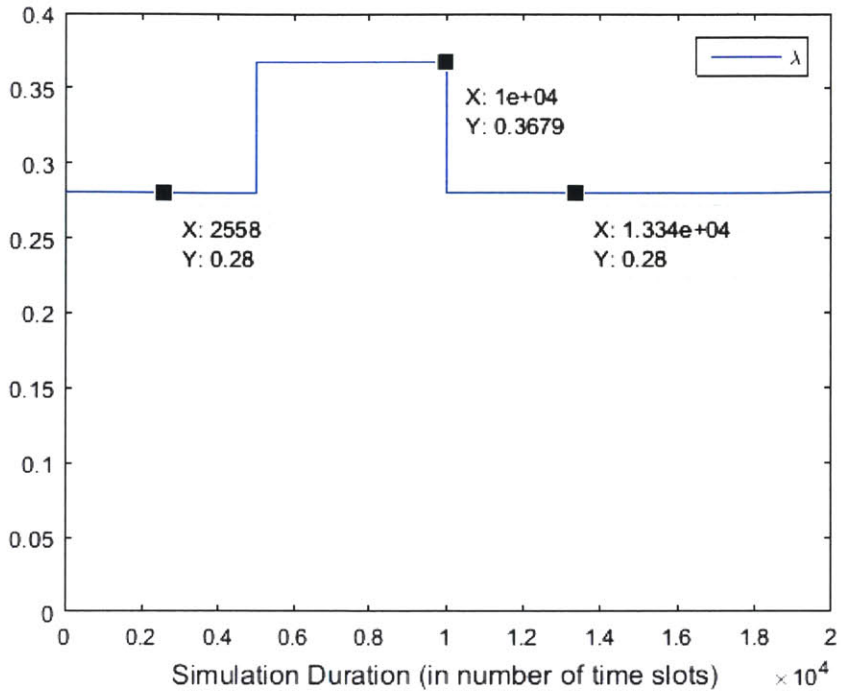


Fig. 21 Square Pulse Poisson Arrival Rate Test Case

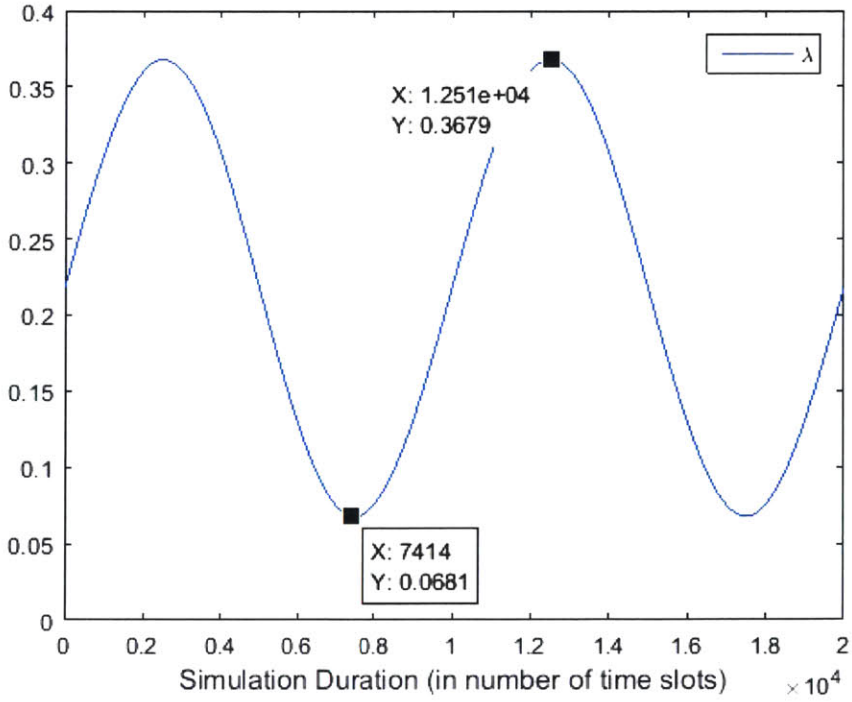


Fig. 22 Sinusoid Poisson Arrival Rate Test Case

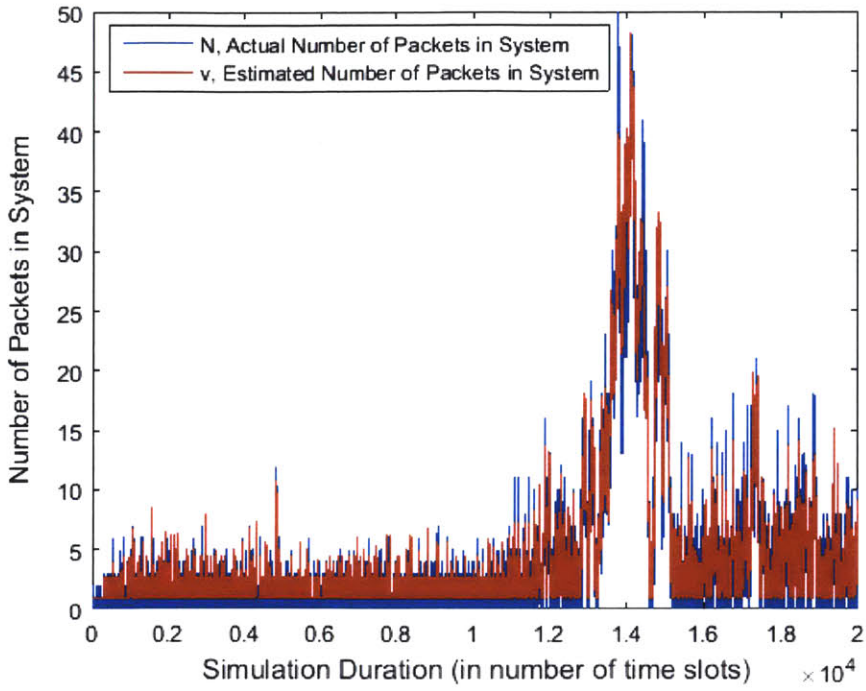


Fig. 23 Simulated Actual and Estimated Backlog for Step Function Case

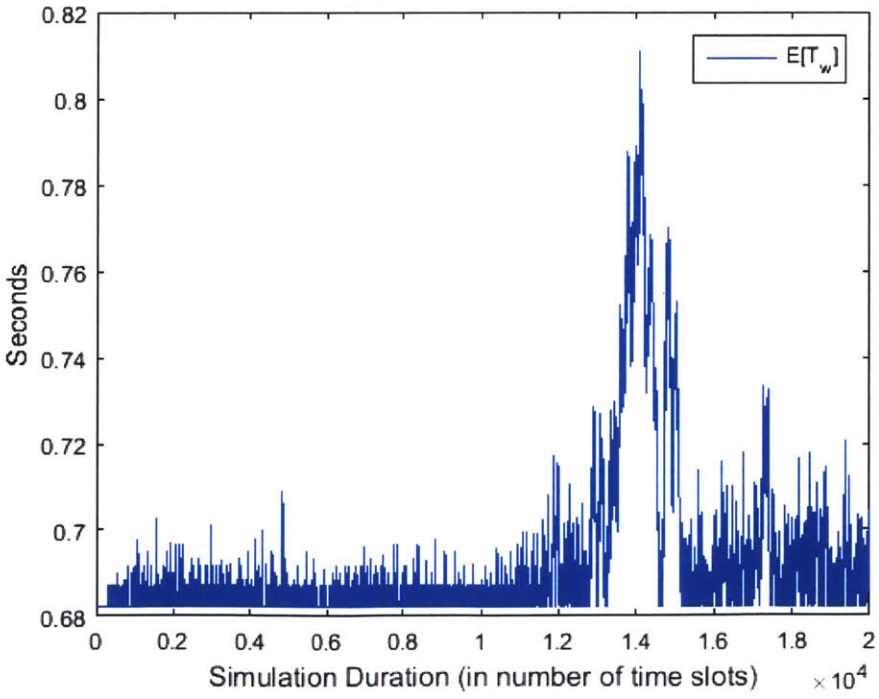


Fig. 24 Simulated Expected Delay for Step Function Case

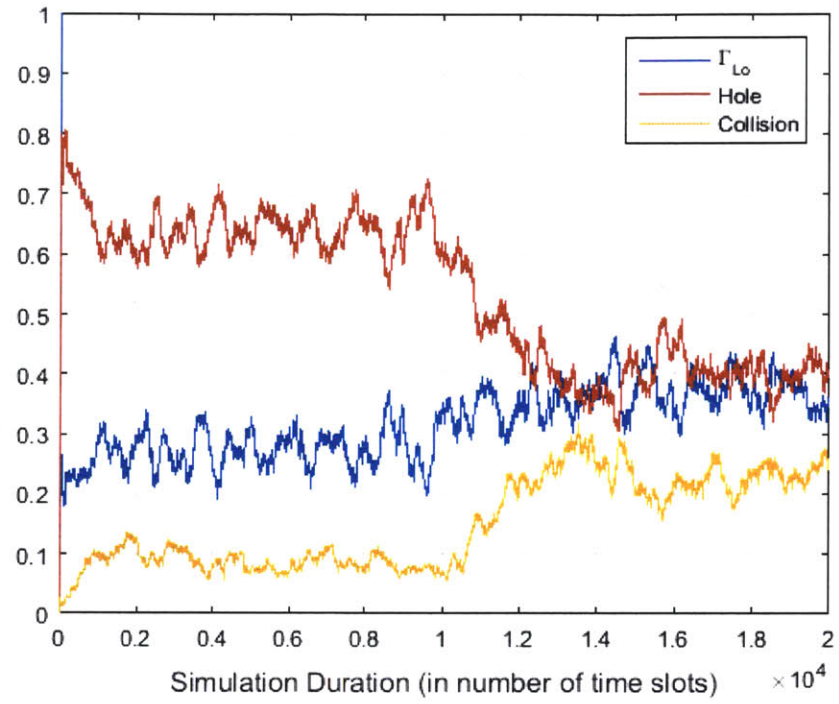


Fig. 25 Simulated Local Averages for Step Function Case

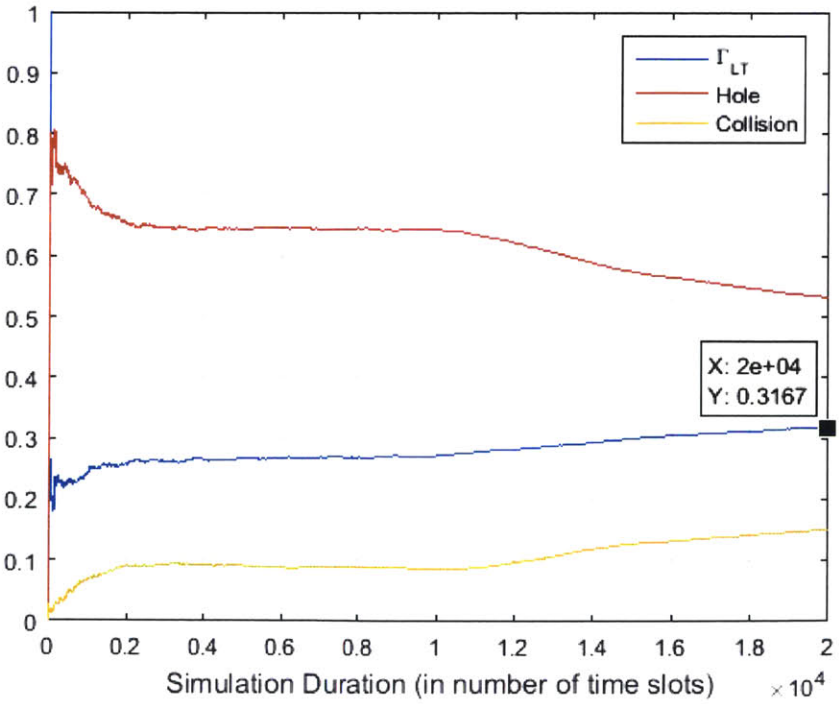


Fig. 26 Simulated Long-Term Averages for Step Function Case

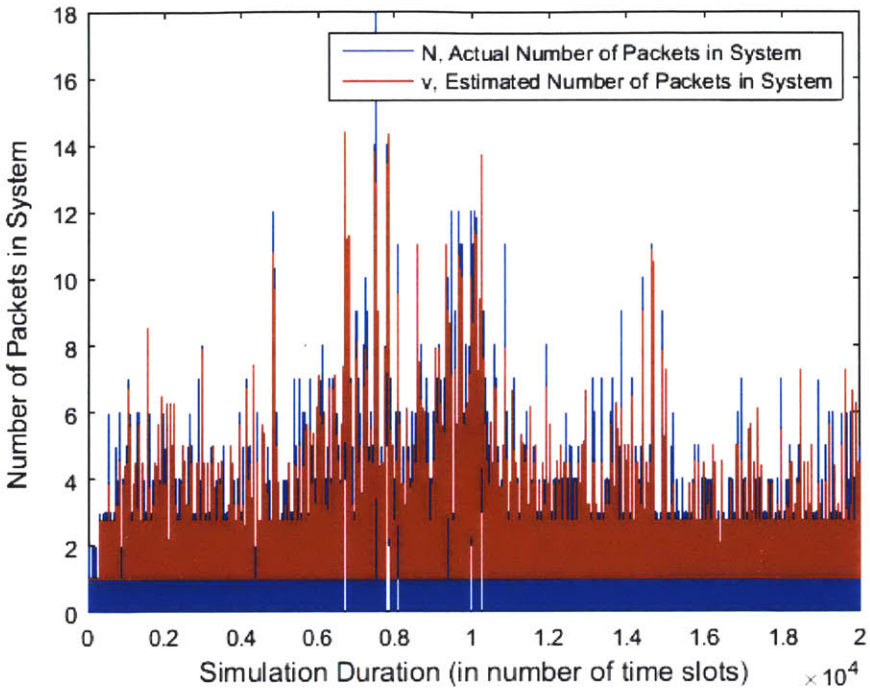


Fig. 27 Simulated Actual and Estimated Backlog for Square Pulse Case

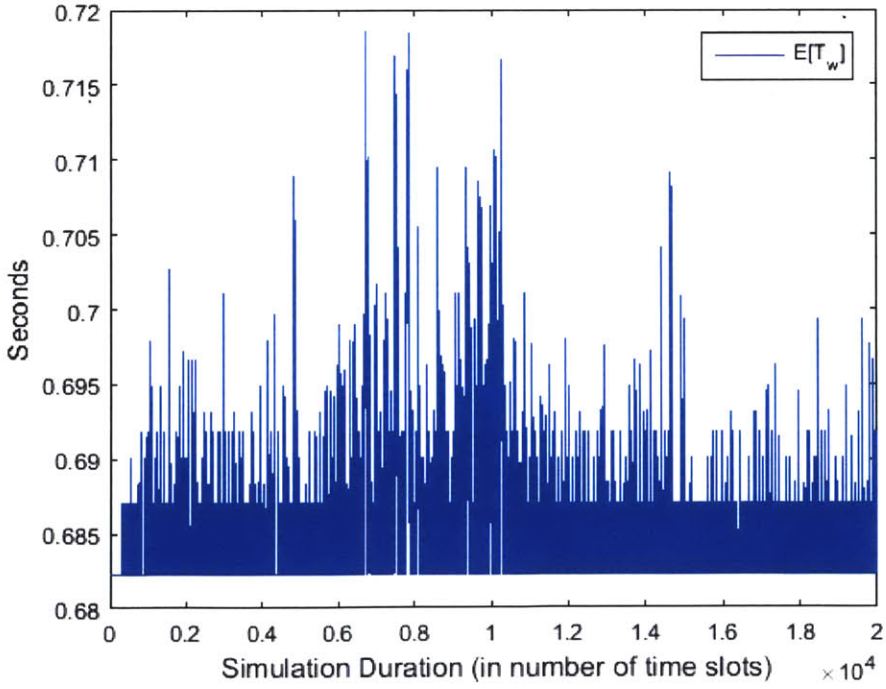


Fig. 28 Simulated Expected Delay for Square Pulse Case

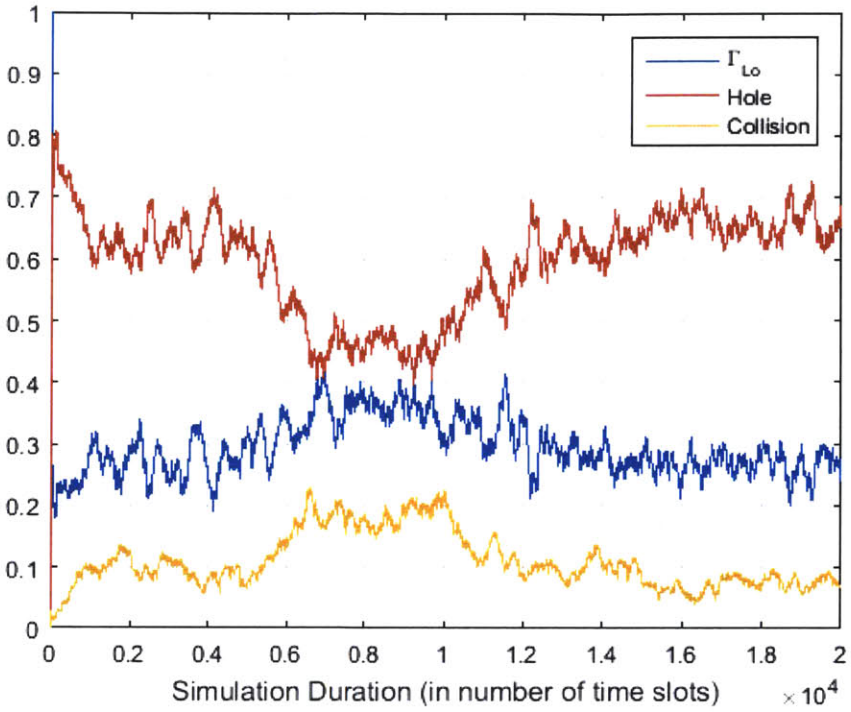


Fig. 29 Simulated Local Averages for Square Pulse Case

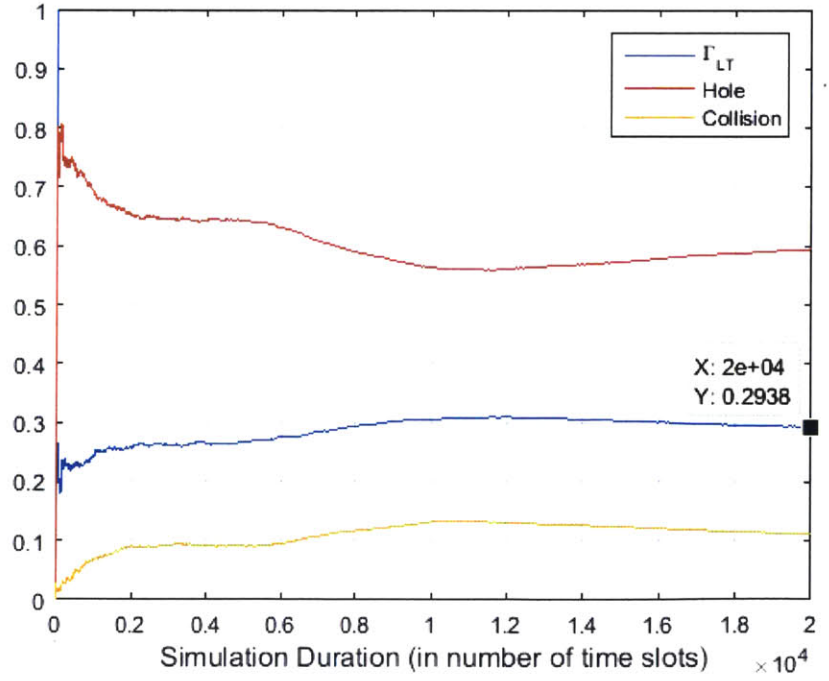


Fig. 30 Simulated Long-Term Averages for Square Pulse Case

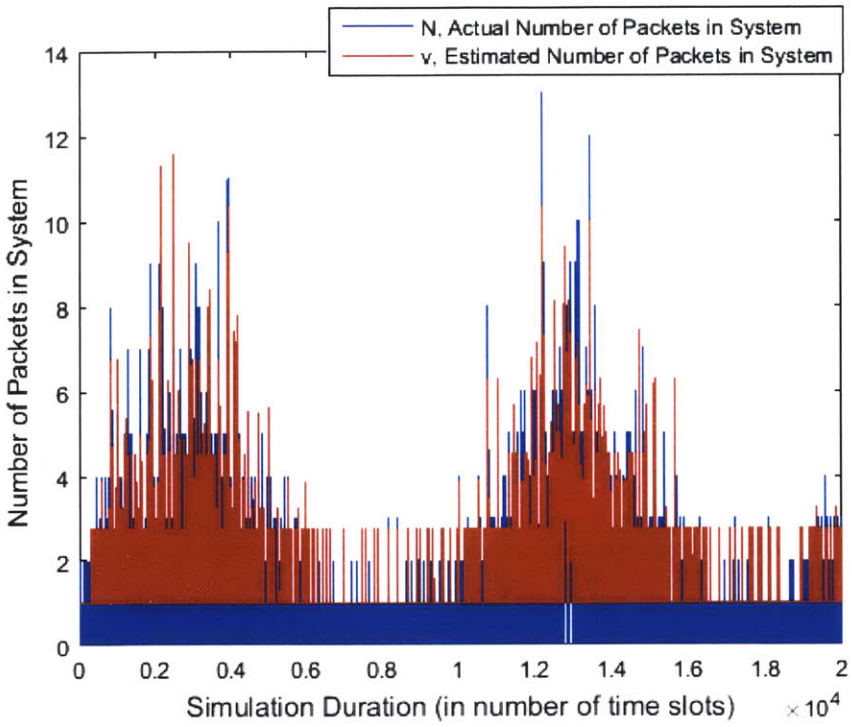


Fig. 31 Simulated Actual and Estimated Backlog for Sinusoid Case

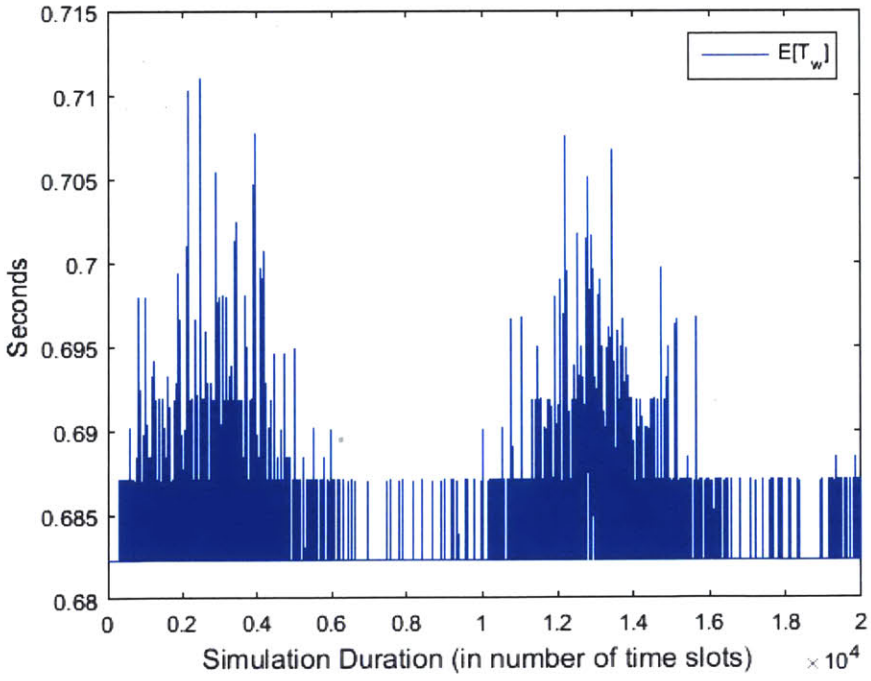


Fig. 32 Simulated Expected Delay for Sinusoid Case

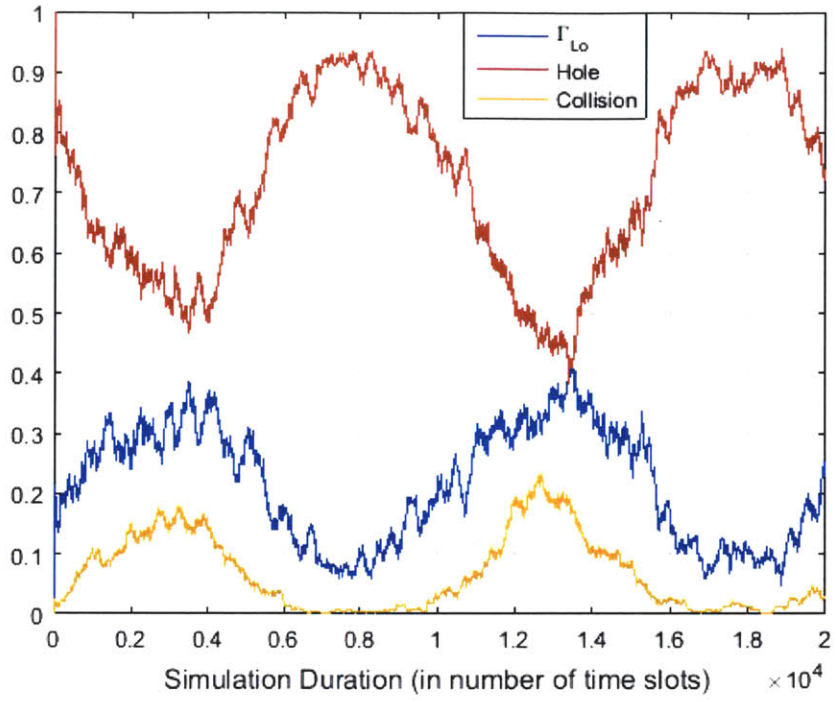


Fig. 33 Simulated Local Averages for Sinusoid Case

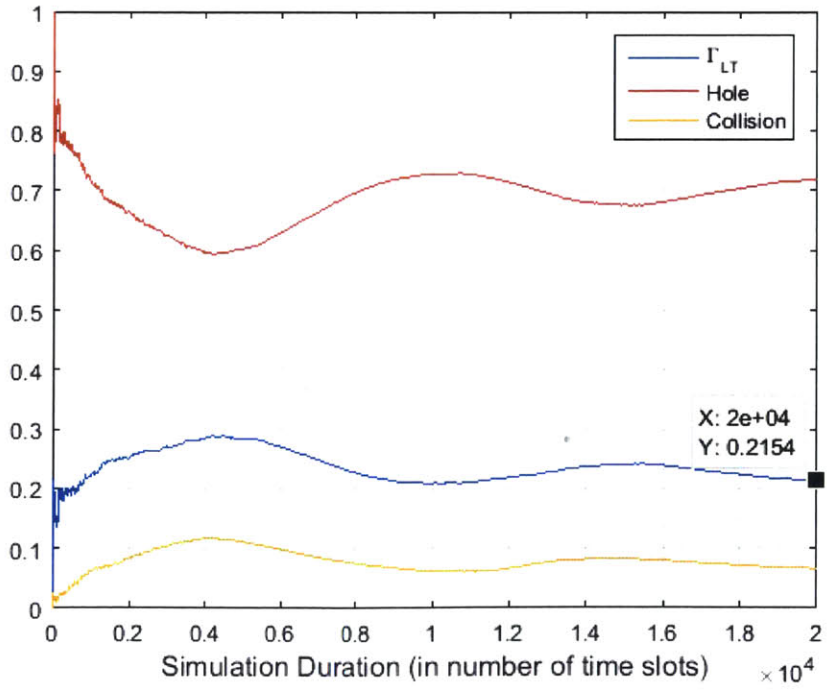


Fig. 34 Simulated Long-Term Averages for Sinusoid Case

In each test case we see that the backlog and delay remain relatively low. Sharp increases in arrival rate result in a temporary increase in backlog and delay, but the system is able to clear the backlog and reduce delay in each case after it adjusts to the change in the arrival rate. Additionally, the local average throughput in each case tends to follow the arrival rate. This is a desirable behavior because it demonstrates that the system is able to adjust its throughput to match the traffic load. Finally, the plots of the long-term averages reveal that the average throughput in each case tends toward the average arrival rate, which is expected for a stable system. Based on these results, it is apparent that the DS/ALOHA system using the Rivest Algorithm and wait-for-feedback scheme remains stable with time-varying arrival rate and a feedback delay of 250 time slots. It is important to remember that the traffic loads in these cases never exceed the maximum throughput of the system.

### 3.2.1 Heavy Traffic Simulations

While the previous section demonstrated that the Rivest Algorithm can provide a stable ALOHA system for a time-varying arrival rate and delayed feedback as long as $\lambda \leq e^{-1}$, it is also important to examine the effects of heavier traffic loads on the system. It is not unreasonable to expect that traffic loads greater than the system's maximum throughput may occur in real situations. Such conditions could arise as the result of a political crisis, military emergency, or natural disaster that triggers increased traffic over the SATCOM network. While an arrival rate of $\lambda > e^{-1}$ will result in a congested system because the maximum throughput of the system is less than the arrival rate of new packets, the ALOHA system must be able to clear as much traffic as possible during this period. Additionally, the system should be able to clear the backlog once traffic returns to a supportable condition where $\lambda \leq e^{-1}$. The performance of the Rivest Algorithm under these conditions is investigated through simulations. Four heavy traffic cases are developed with a time-varying arrival rate that exceeds $e^{-1}$ for a period of the simulation time. The four functions used to model arrival rates are a step function, a square pulse function, a combination of two

square pulse functions, and a sinusoidal function. Plots of the arrival rate for each case are given in Fig. 35 through Fig. 38. Plots of the backlog, delay, local averages, and long-term averages for each case are given in Fig. 39 through Fig. 54.

For the step function case, we see from Fig. 39 and Fig. 40 that the system's backlog and delay begin to grow without bound once the arrival rate changes from $\lambda = 0.3$ to $\lambda = 0.7$. This result makes sense since the traffic load is above the maximum system throughput when $\lambda = 0.7$ and does not change its value for the rest of the simulation. We also see from Fig. 39 that the estimator $v$ begins to diverge away from the true number of packets ready for transmission $N$. A key point of interest in this that the local average throughput remains close to the maximum achievable throughput despite the fact that the backlog is growing without bound. This is an important result because it indicates that the Rivest Algorithm can achieve near-maximum throughput even under congested conditions.

The pulse function case serves as an extension of the step function case where a period of time with a traffic load greater than $e^{-1}$ is followed by a period of time with a traffic load less than $e^{-1}$. We see from Fig. 43 and Fig. 44 that the backlog and delay of the system begin to grow once the arrival rate exceeds $e^{-1}$, but gradually return to relatively low values once the arrival rate returns to a value below $e^{-1}$. This is an excellent example of the Rivest Algorithm's ability to recover from a period of congestion. We also see that the estimator $v$ remains relatively close to $N$, though a delay in estimation response is evident. From Fig. 45 and Fig. 46 we see that the algorithm continues to maintain a high throughput, even during the period of congestion.

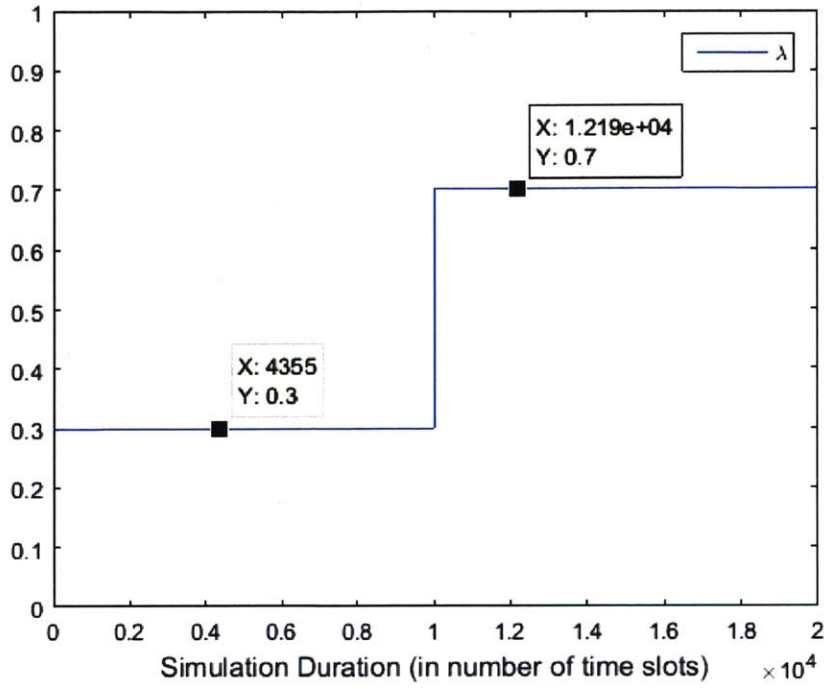


Fig. 35 Heavy Traffic Load with a Step Function Poisson Arrival Rate Test Case

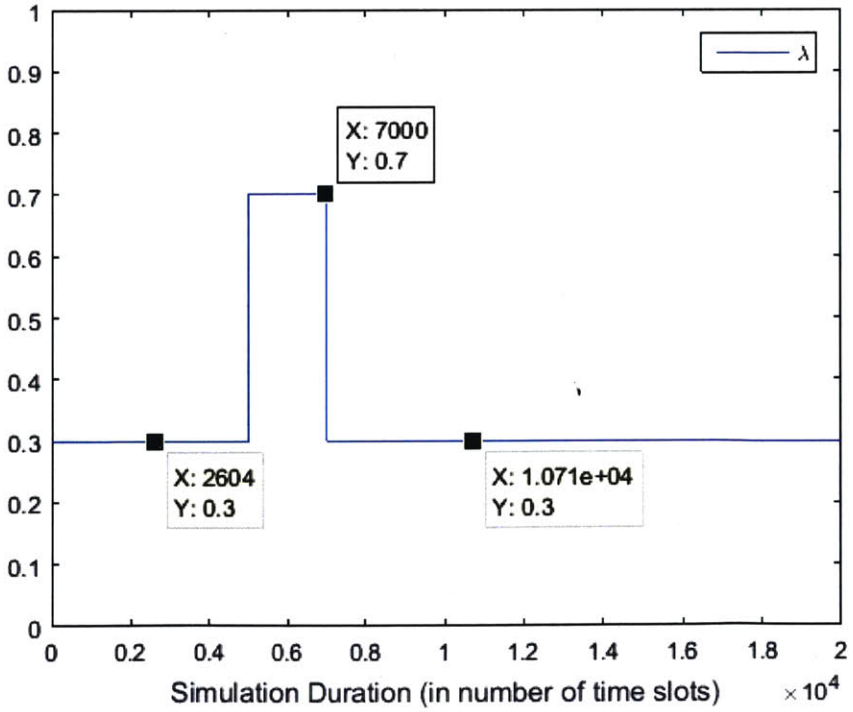


Fig. 36 Heavy Traffic Load with a Square Pulse Poisson Arrival Rate Test Case

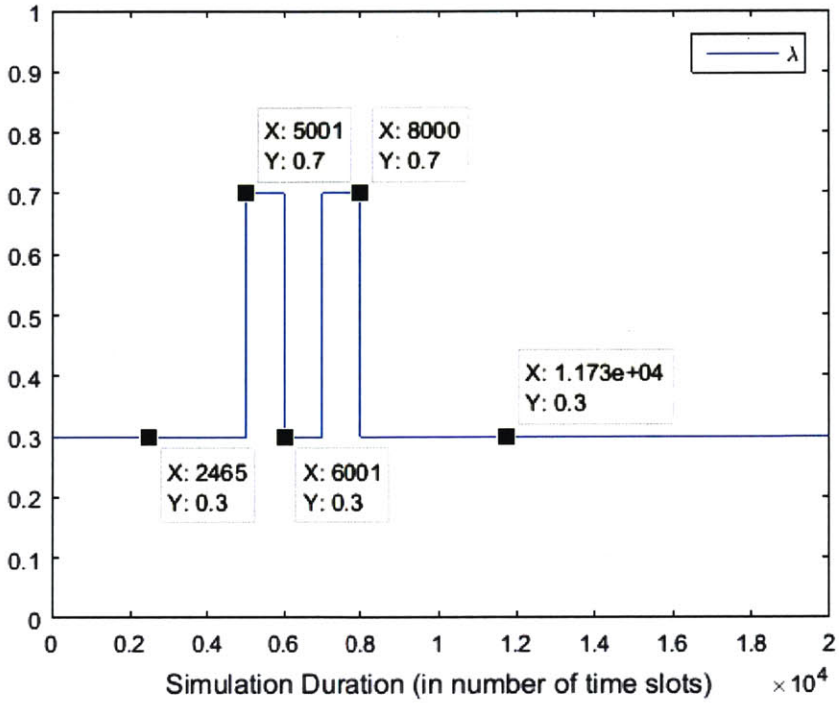


Fig. 37 Heavy Traffic Load with a Double Pulse Poisson Arrival Rate Test Case

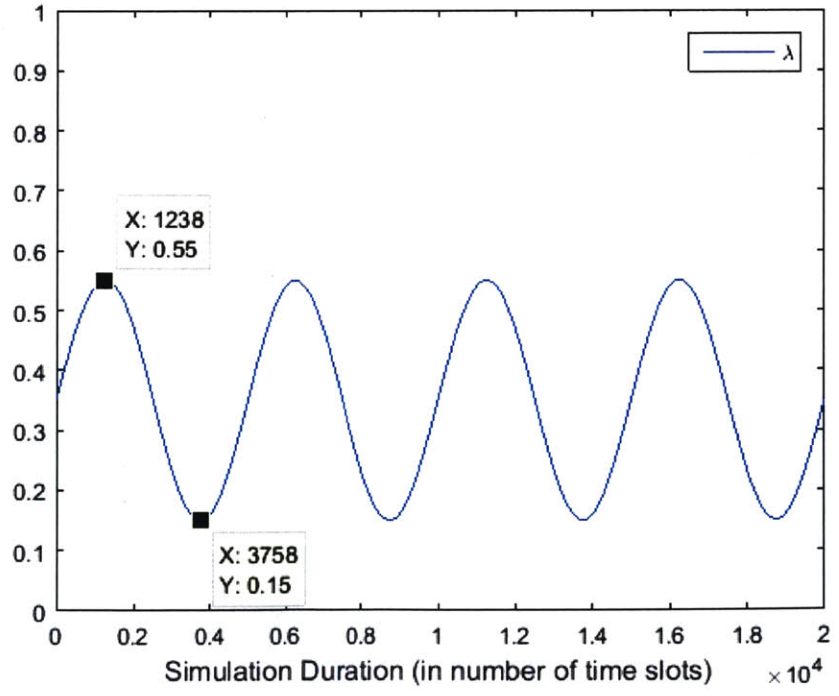


Fig. 38 Heavy Traffic Load with a Sinusoid Poisson Arrival Rate Test Case

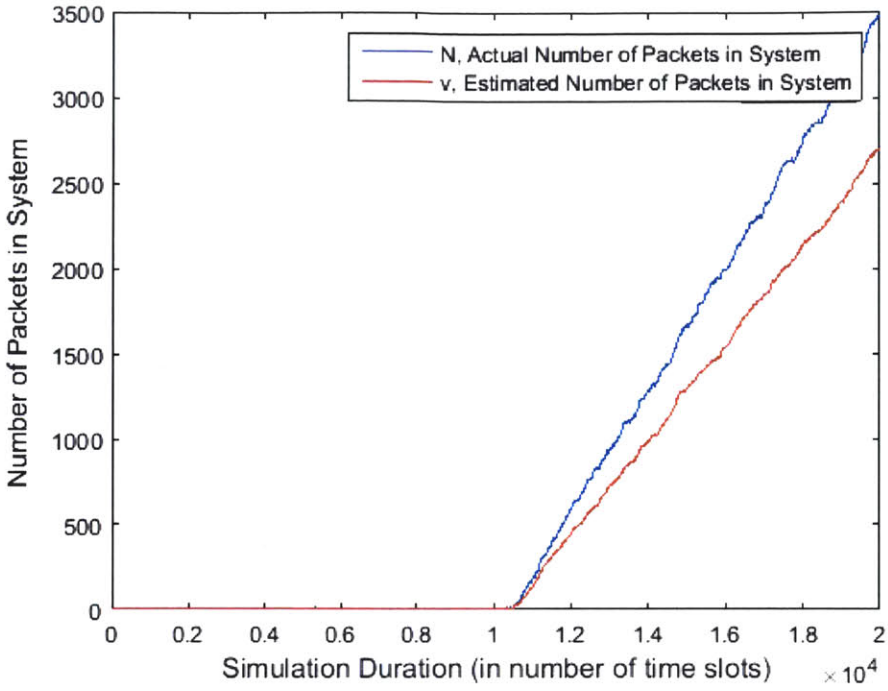


Fig. 39 Simulated Actual and Estimated Backlog for Step Function Case

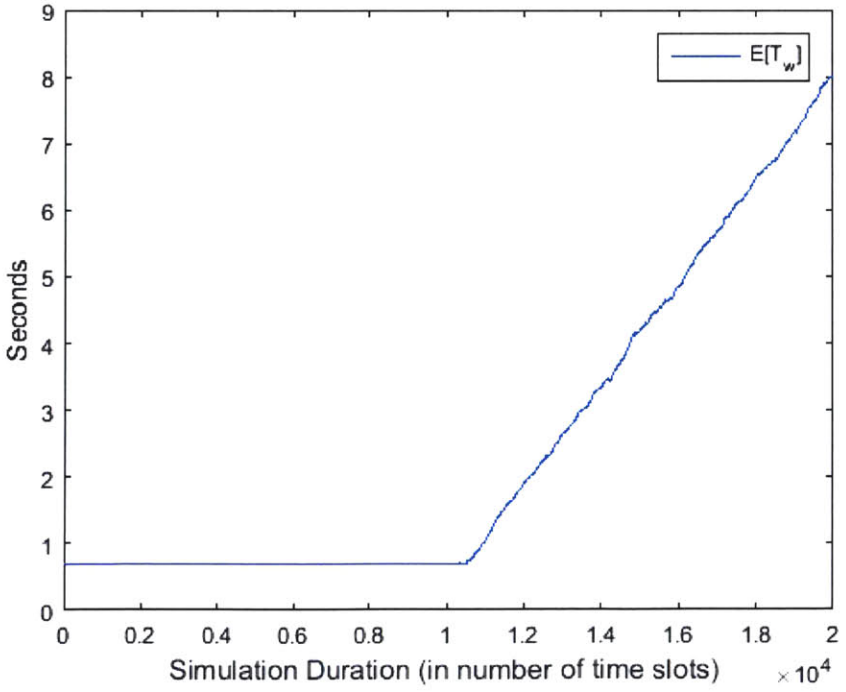


Fig. 40 Simulated Expected Delay for Step Function Case

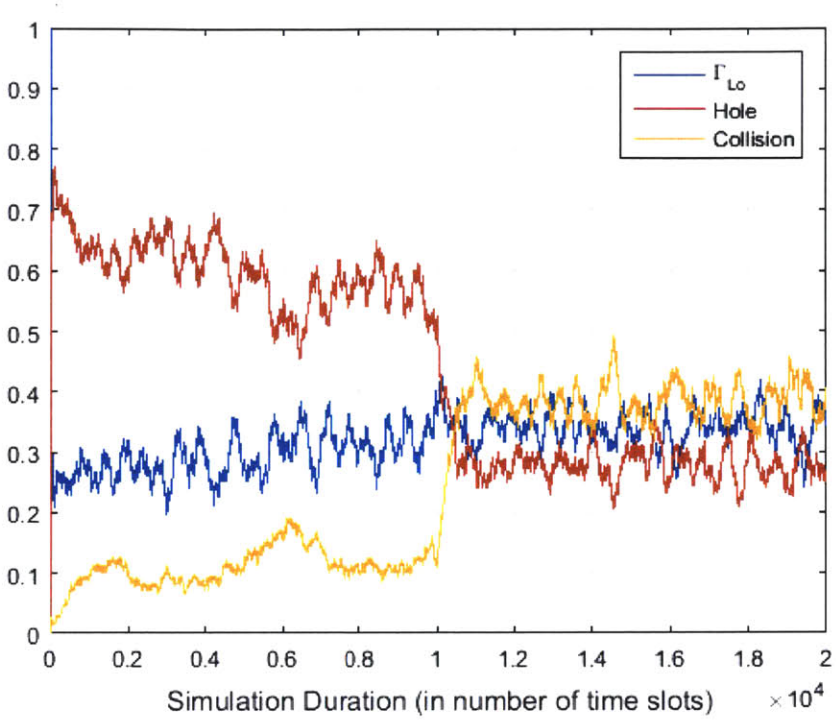


Fig. 41 Simulated Local Averages for Step Function Case

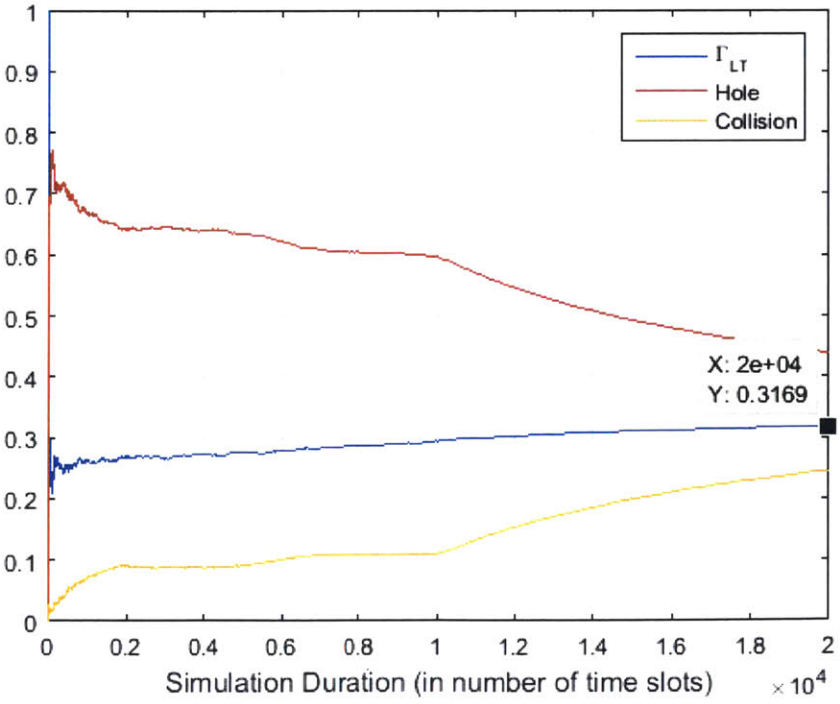


Fig. 42 Simulated Long-Term Averages for Step Function Case

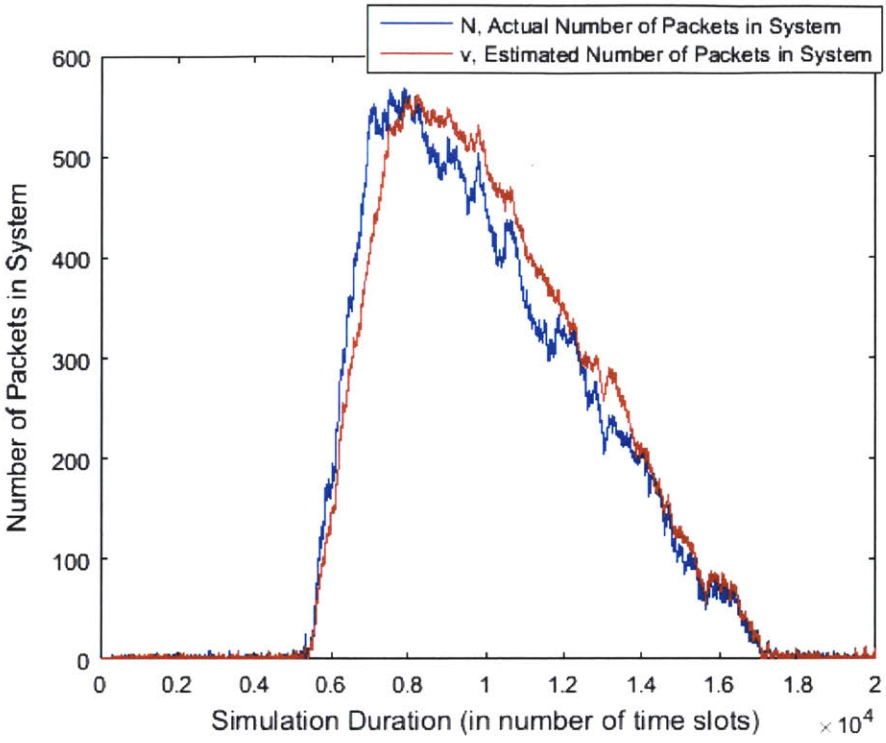


Fig. 43 Simulated Actual and Estimated Backlog for Square Pulse Case

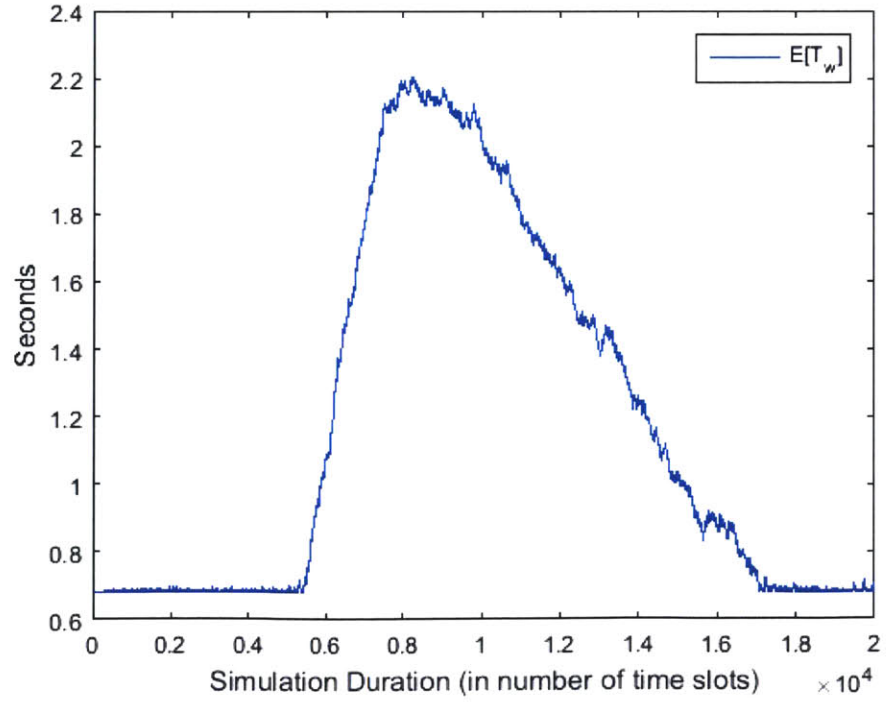


Fig. 44 Simulated Expected Delay for Square Pulse Case

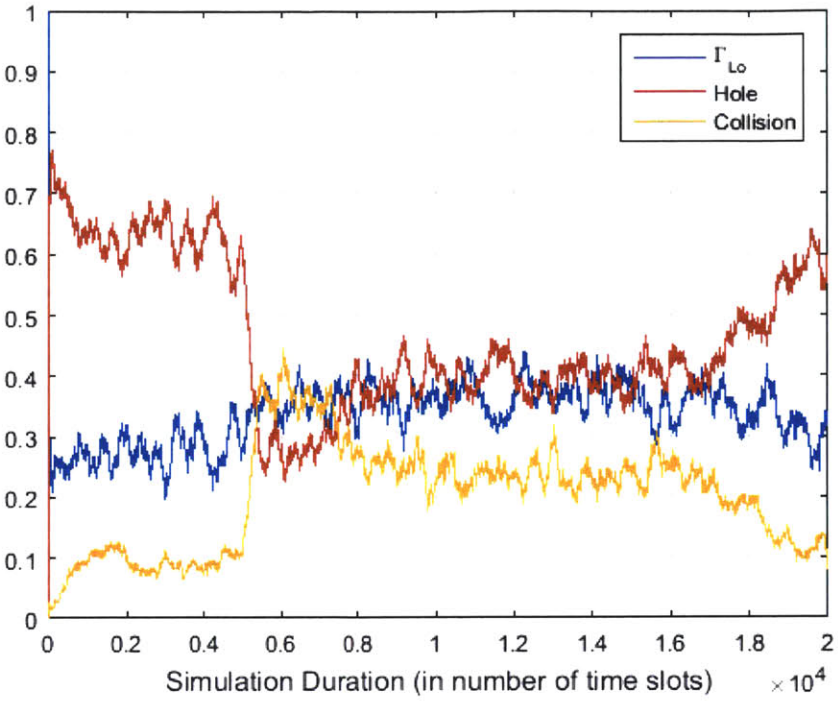


Fig. 45 Simulated Local Averages for Square Pulse Case

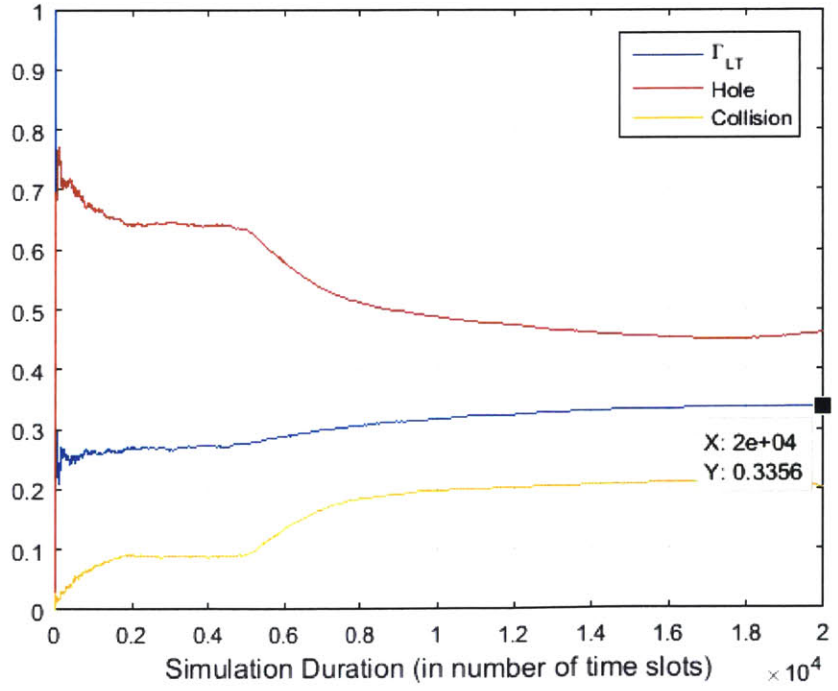


Fig. 46 Simulated Long-Term Averages for Square Pulse Case

The double square pulse case is used to gauge the Rivest Algorithm's ability to respond to several abrupt changes in arrival rate that occur in quick succession. From Fig. 47 through Fig. 50 we see that the performance of the system under these conditions is very similar to the single square pulse case. Once again, the backlog and delay gradually return to relatively low values after the periods of congestion. The effect of the second pulse in the arrival rate is evident in both Fig. 47 and Fig. 48 where the backlog and delay initially begin to decrease after the first pulse, and then increase toward a final maximum value after the second pulse occurs. Despite this double perturbation to the system, its estimate of $N$ manages to remain fairly accurate. From Fig. 49 we see that the local average throughput remains fairly high for the duration of the simulation and is slightly closer to the maximum achievable throughput during the period of high congestion. We also see that the local average number of holes decreases during periods of high congestion and that the local average number of collisions increases during the same periods. Finally, we see from Fig. 50 that the long-term throughput converges towards the average arrival rate, indicating that the system is able to clear all user traffic if given sufficiently long periods of supportable traffic loads.

The sinusoid case is used to evaluate the system's performance when the arrival rate is constantly changing and periodically assumes values greater than the maximum system throughput. From Fig. 51 and Fig. 52 we see that the system is able to accurately update its estimate of $N$ and can clear the backlog during periods where the arrival rate assumes a supportable value. From Fig. 53 we see that the local average throughput remains fairly constant while the local average numbers of collisions and holes vary in a sinusoid-like fashion. This result is reasonable because more collisions are expected to occur during periods of congestion, due to an overabundance of new arrivals, while more holes are expected to occur when the arrival rate is low. Finally, from Fig. 54 we see that long-term throughput converges towards the average arrival rate which indicates that the system is able to clear congestion effectively during periods with supportable traffic loads.

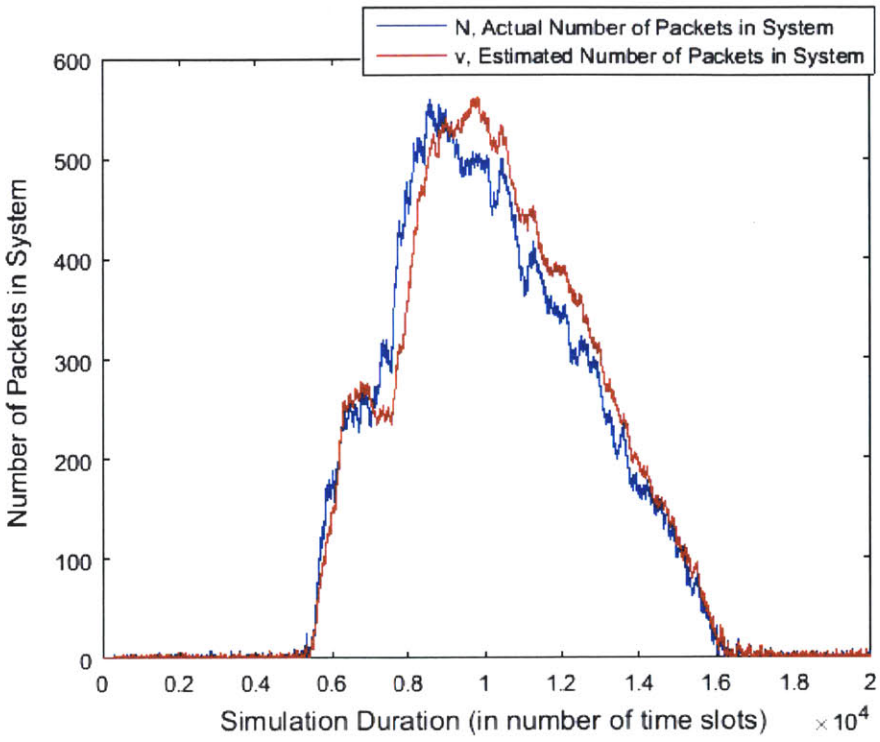


Fig. 47 Simulated Actual and Estimated Backlog for Double Pulse Case

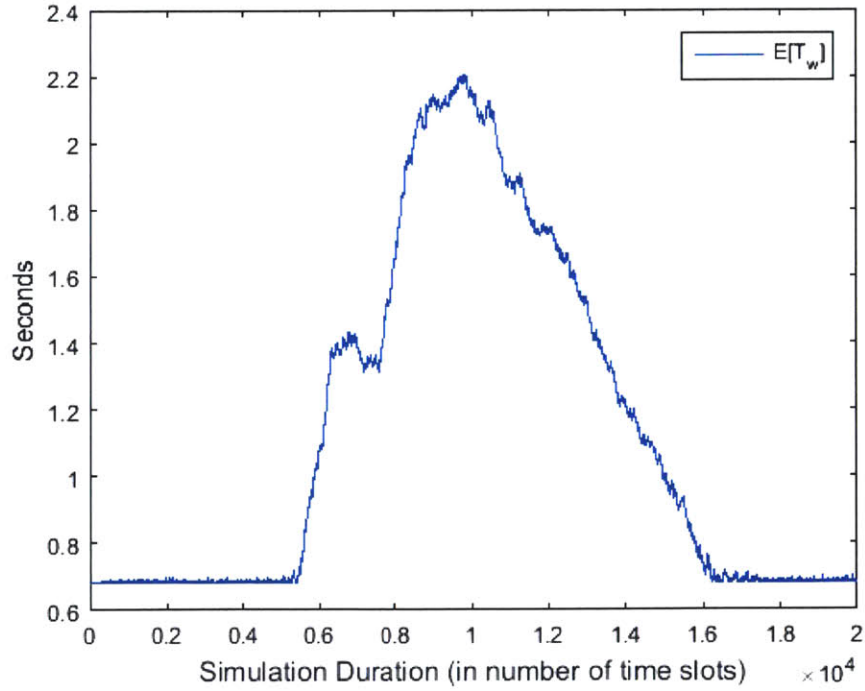


Fig. 48 Simulated Expected Delay for Double Pulse Case

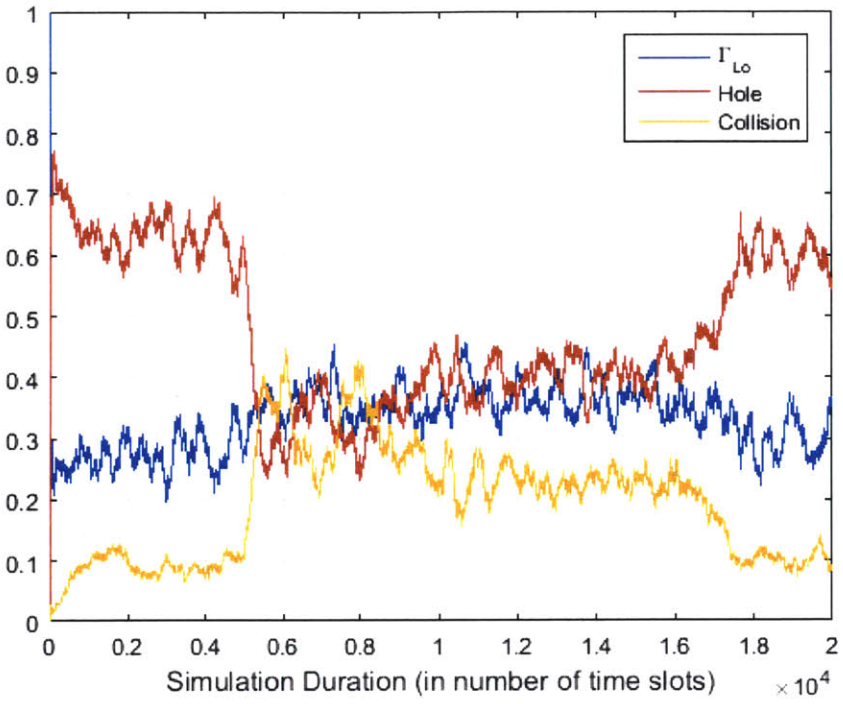


Fig. 49 Simulated Local Averages for Double Pulse Case

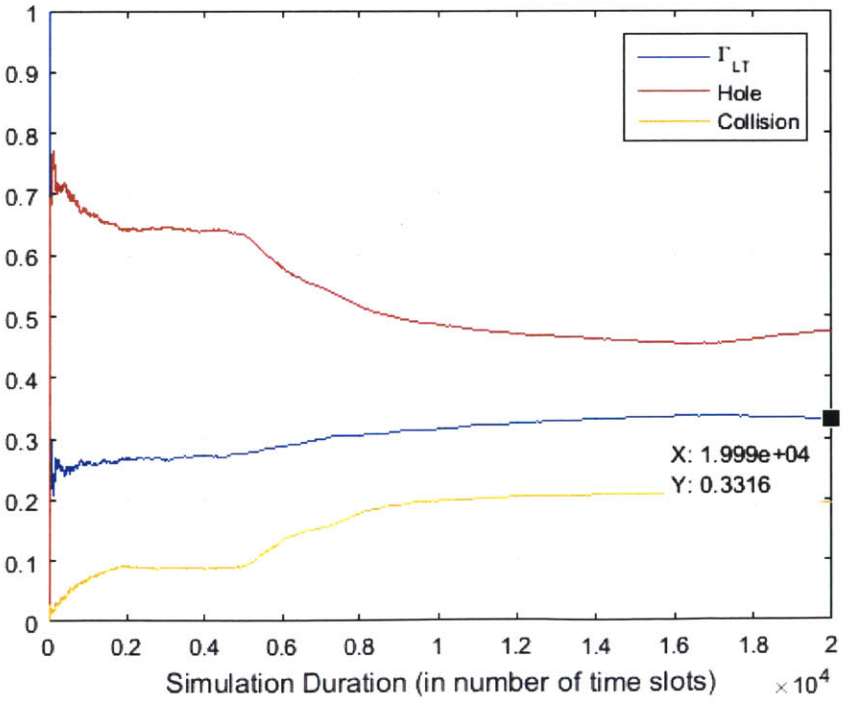


Fig. 50 Simulated Long-Term Averages for Double Pulse Case

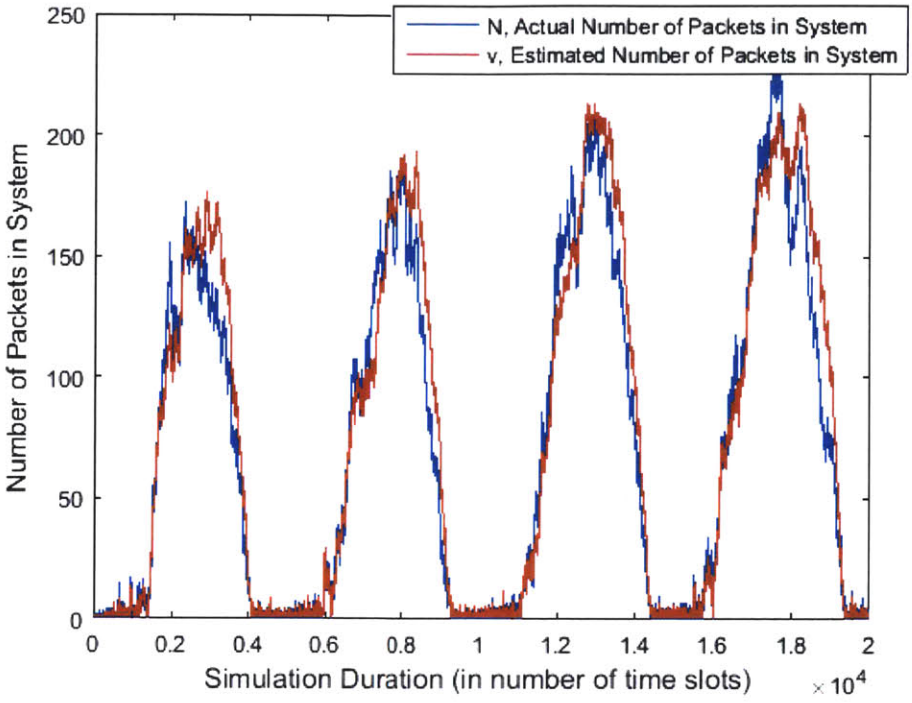


Fig. 51 Simulated Actual and Estimated Backlog for Sinusoid Case

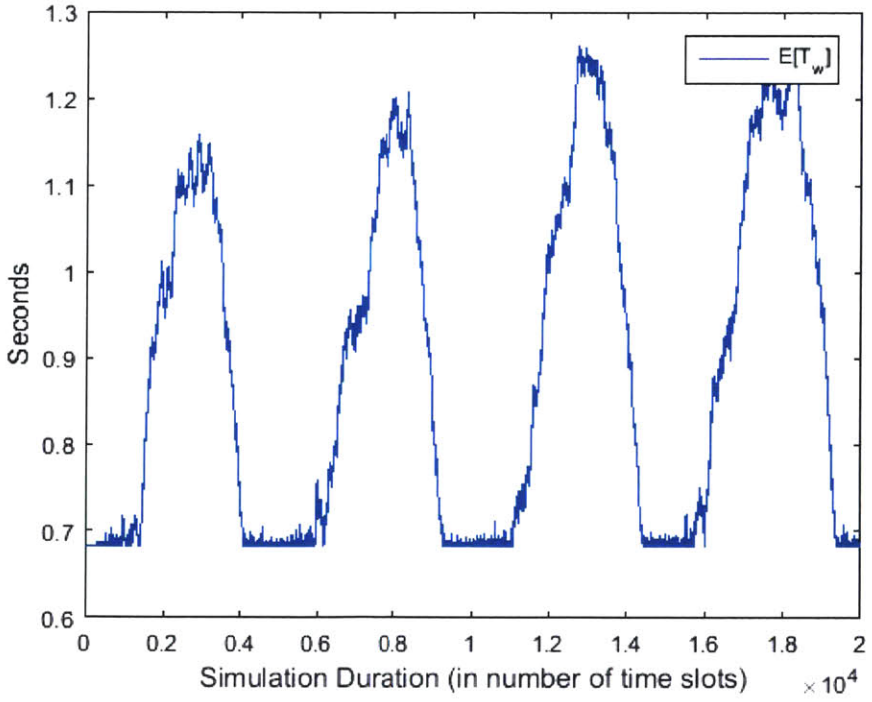


Fig. 52 Simulated Expected Delay for Sinusoid Case

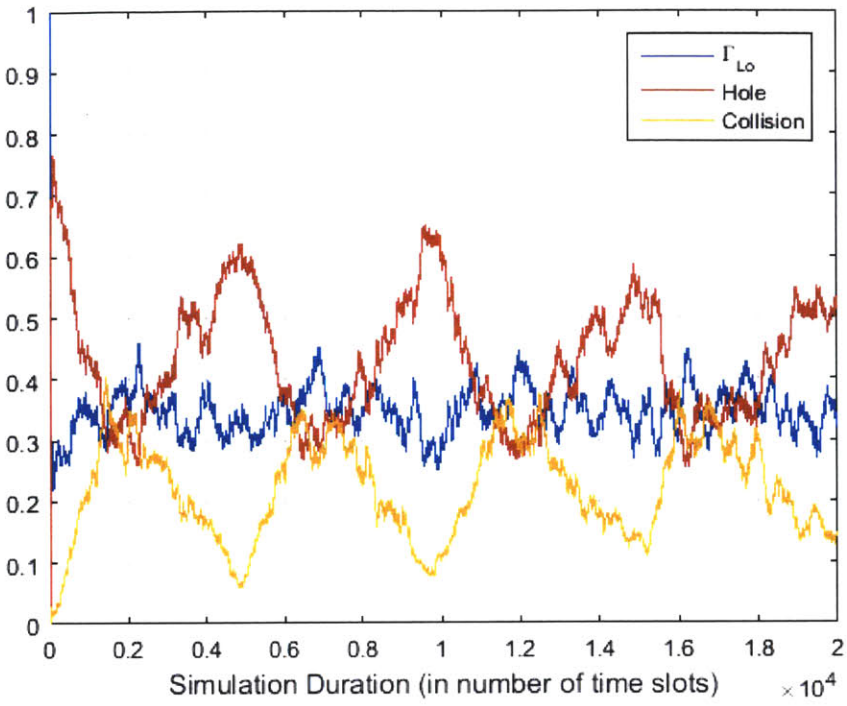


Fig. 53 Simulated Local Averages for Sinusoid Case

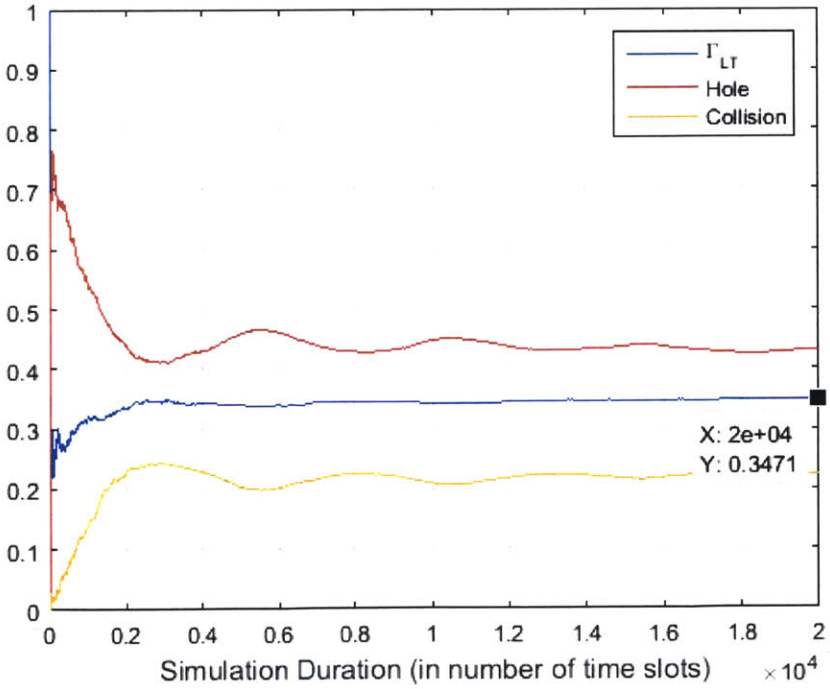


Fig. 54 Simulated Long-Term Averages for Sinusoid Case

The results from these four heavy traffic cases indicate that the Rivest Algorithm has a robust response to unsupportable surges in user traffic. Even during periods of congestion, the algorithm is able to maintain an accurate estimate of $N$. Additionally, the algorithm is able to support a high throughput under these conditions which is close to the system's maximum achievable throughput during periods of high congestion. While the backlog and delay of the system grows during periods of congestion, the system can clear its backlog and reduce its delay during subsequent periods with supportable traffic loads. Based on these results, the Rivest Algorithm is a good choice as a control mechanism for an ALOHA system due to its ability to function well under stable conditions and achieve considerable best-effort performance under highly congested conditions.

### 3.2.2 Time to Clear Heavy Traffic Bursts

The previous section's analysis of the Rivest Algorithm's performance under unsupportable traffic surges revealed that the backlog grows during period of congestion and gradually clears when the arrival rate drops below $e^{-1}$. It is therefore important to understand how long the system must be in a supportable condition in order to recover from a period of congestion. A simple case that can be analyzed to predict how long it takes the system to clear the excess backlog generated during a period of congestion is the case discussed in the previous section where the arrival rate is modelled as a square pulse. In this case, the arrival rate initially assumes a supportable value $\lambda_S$ below $e^{-1}$, jumps to an unsupportable value $\lambda_U$ above $e^{-1}$ for a period of time, and then returns to the same initial supportable value $\lambda_S$ for the rest of the simulation. As was seen in the previous section, the abrupt increase in arrival rate results in a backlog that grows without bound until the subsequent drop in arrival rate allows the system to gradually clear the backlog. The primary metric of concern here is the time it takes for the system to clear the extra backlog generated by the period of the simulation where the traffic load is greater than the maximum system throughput. This metric is referred to as the clear time of the system $T_{clear}$ and is defined as the

number of time slots after the increase in arrival rate from $\lambda_S$ to $\lambda_U$ that are required for the backlog to return to the average backlog observed during the initial period of supportable traffic. To help clarify the definition of clear time, a plot of the backlog for a simulated square pulse arrival rate with $T_{clear}$ identified is given in Fig. 55.

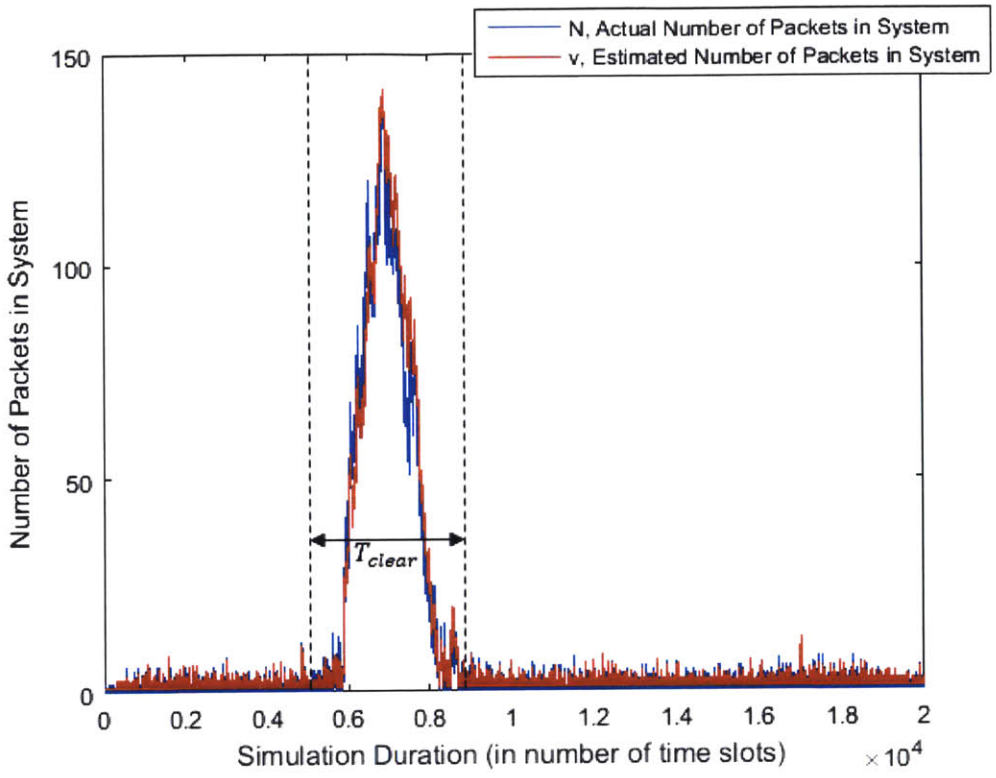


Fig. 55 Visualization of System Clear Time

Note that the square pulse arrival rate used to generate Fig. 55 has its first change in value at 5,000 time slots and therefore $T_{clear}$ is defined as the number of time slots required after the 5,000$^{th}$ slot to reduce the backlog. Given the values of $\lambda_S$ and $\lambda_U$, as well as the number of slots for which $\lambda = \lambda_U$ (defined as the pulse width $\omega_P$), the estimated system clear time $\hat{T}_{clear}$ has following expression:

$$\hat{T}_{clear} = \frac{\omega_P(\lambda_U - \lambda_S)}{(e^{-1} - \lambda_S)} \quad , \tag{3.8}$$

where the term $\omega_P(\lambda_U - \lambda_S)$ is the extra arrivals from the unsupportable traffic surge that must be cleared by the system. Additionally, the term $e^{-1} - \lambda_S$ is the remaining throughput after servicing the nominal traffic arriving with rate $\lambda_S$ that can be devoted to reducing the backlog.

The accuracy of the estimation technique given by (3.8) is analyzed by simulating and measuring the average clear time of a square pulse arrival rate with $\lambda_S = 0.28$, $\lambda_U = 0.5$, and a variable pulse width $\omega_P$. An example of the arrival rate for these simulations is given in Fig. 56. Ten simulations are performed at each value of $\omega_P$ and the average clear time from these simulations is recorded and compared to the corresponding value of $\hat{T}_{clear}$ calculated using (3.8). A comparison of the estimated clear time and the average clear times obtained from simulations is given in Fig. 57. From this comparison we see that the estimated values of $T_{clear}$ are close to the average values obtained from simulation for all simulated values of $\omega_P$ and therefore the expression in (3.8) appears to be a reasonable estimate of the system clear time.

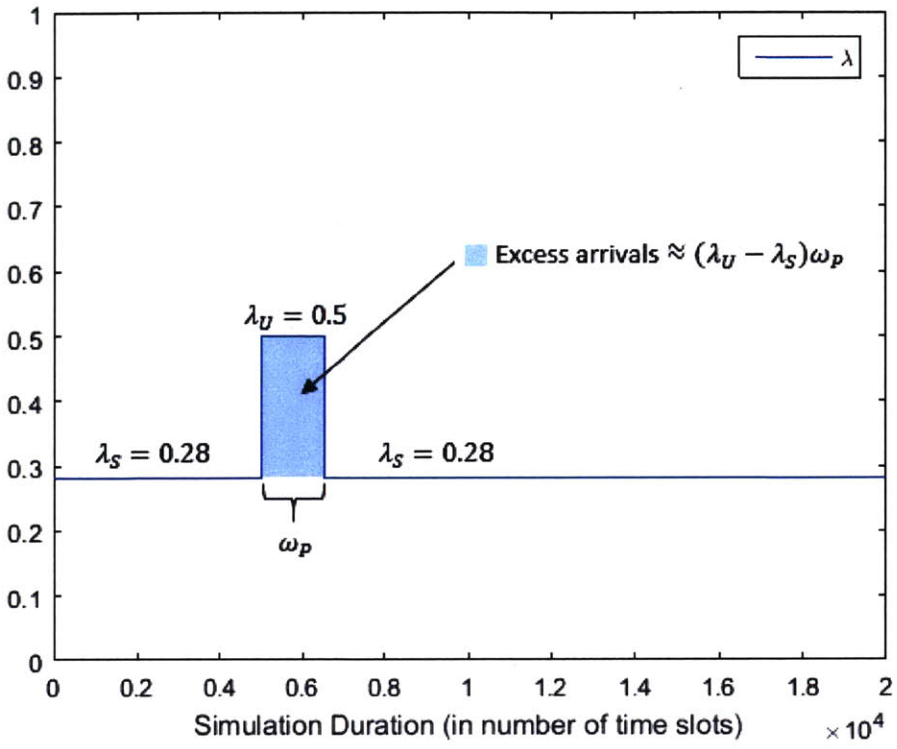


Fig. 56 Example Poisson Arrival Rate for Clear Time Analysis

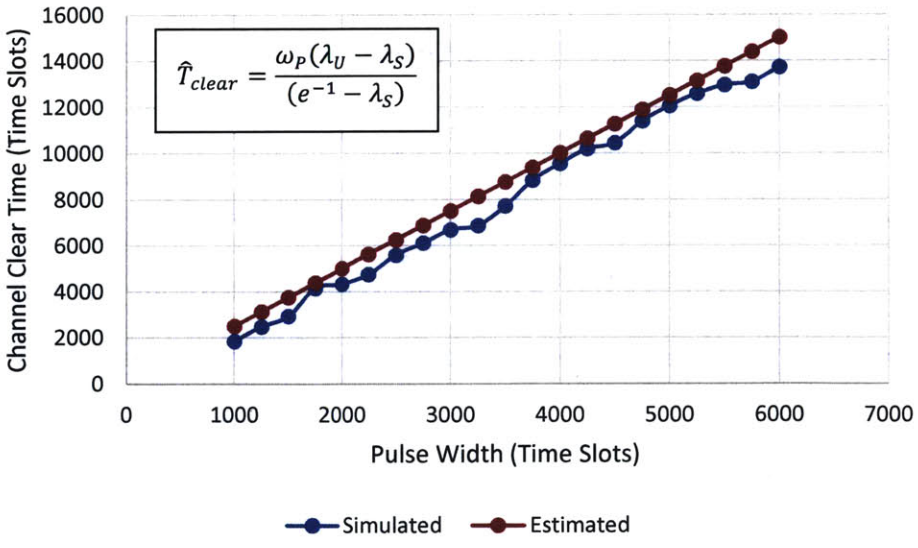


Fig. 57 Simulated and Estimated System Clear Time versus Pulse Width for Square Pulse Arrival Rate

It is important to note that the estimation technique in (3.8) is primarily concerned with the area of the pulse in Fig. 56, rather than its specific shape. This area corresponds to the expected number of extra arrivals to the channel during the unsupportable traffic surge. Therefore, it is possible to generalize the estimation technique developed previously in the following manner:

$$\hat{T}_{clear} = \frac{A_E}{(e^{-1} - \lambda_R)} \quad , \tag{3.9}$$

where $A_E$ is the area between the time-varying arrival rate $\lambda$ and the constant value $\lambda_R$ over the period of congestion. This area corresponds to the extra number of arrivals to the channel during this time. The constant $\lambda_R$ corresponds to the residual arrival rate of packets to the channel during the period where the traffic rate is supportable that follows the traffic surge. The expression given in (3.9) can be used to estimate the clear time for any pulse shape as long as the period of congestion is preceded and followed by periods of supportable traffic with constant arrival rates less than $e^{-1}$.

## 3.3 Implementation of Dual-Class Service

In addition to maintaining high throughput and low delay under various traffic loads, it is important that the DS/ALOHA system be able to offer two classes of service for priority and normal users. Priority users must be able to use as much of the available system capacity as they need in order to keep their expected delay acceptably low, and the remaining system capacity must be used as efficiently as possible by the normal users. The ALOHA protocol is not inherently designed for dual-class service because every packet attempts transmission with the same probability $q$. Thus, every user has the expected delay. It is therefore necessary to introduce a modification to the ALOHA protocol to ensure that priority users receive as much of the system throughput as their traffic requires in order to operate below a maximum tolerable delay while the remaining throughput is allocated to normal traffic as efficiently as possible. One scheme for

implementing dual-class service is to have normal users randomly drop off the channel when a threshold expected channel delay is exceeded. The following two sections develop this scheme.

### 3.3.1 Estimating Arrival Rates

The scheme for dual-class service based on random drops requires accurate estimates of the arrival rate $\lambda_p$ of packets from priority users to the channel and the arrival rate $\lambda_n$ of packets from normal users. It is therefore necessary to develop a method for estimating $\lambda_p$ and $\lambda_n$ before discussing the implementation of random drops. It is assumed that the arrival of priority and normal packets to the channel can be modelled as a combined Poisson process where $\lambda = \lambda_p + \lambda_n$. The value of $\lambda$ at any point in time can be estimated by observing the number of arrivals over a window of time slots ending at the current time slot. The estimated arrival rate is then simply the number of arrivals observed during the window divided by the window length.

One factor that complicates the estimation of $\lambda$ is that the number of new arrivals to the channel over a window of time cannot be observed directly because the system can only see a success, hole, or collision on each time slot. However, noting that $v$ increases with each arrival and decreases with each success, the total number of arrivals in a window is equal to the number of packets cleared by the system plus the change in the number of packets that remain in the system's backlog. Therefore, number of arrivals to the channel can be estimated by adding the number of success slots observed during the window $N_{SW}$ with the change in the estimated backlog $\Delta v$ from the first to the last time slot in the window. Since the arrival rate $\lambda$ is equal to the number of arrivals in a window divided by the window's length, the estimated arrival rate $\hat{\lambda}$ can be expressed as:

$$\hat{\lambda} = \frac{(\Delta v + N_{SW})}{k_w \cdot N_{RTT}} \quad , \tag{3.10}$$

where $\Delta v$ is the change in backlog from first to last time slot in a window of length $k_w \cdot N_{RTT}$, $N_{SW}$ is the number of successes observed during the window, $k_w$ is a positive integer used to scale the window size, and $N_{RTT}$ is the number of ALOHA slots in a round trip time. The choice of $N_{RTT}$ is somewhat arbitrary, but allows the window size to be specified as a multiple of the number of time slots in a RTT. The effectiveness of this estimation method is analyzed by simulating the ALOHA system using this technique with a square pulse arrival rate for two values of $k_w$. Plots of $\lambda$ and $\hat{\lambda}$ for $k_w = 1$ and $k_w = 2$ using the same random seed are given in Fig. 58 and Fig. 59 respectively.

We see from both Fig. 58 and Fig. 59 that the estimation technique from (3.10) is reasonably accurate for a time-varying arrival rate. We also see that the estimation technique exhibits a delay in its response to changes in the arrival rate which is to be expected due to the long feedback delay in the system. Finally, we see that the results for using a smaller window size ($k_w = 1$) are fairly noisy, but the estimator is responsive. Increasing the window size ($k_w = 2$) results in a more stable, but less responsive estimator. This performance difference highlights the fundamental tradeoff between stability and responsiveness in estimation techniques. This all makes sense since the estimation period should be commensurate with the coherence time of the arrival process.

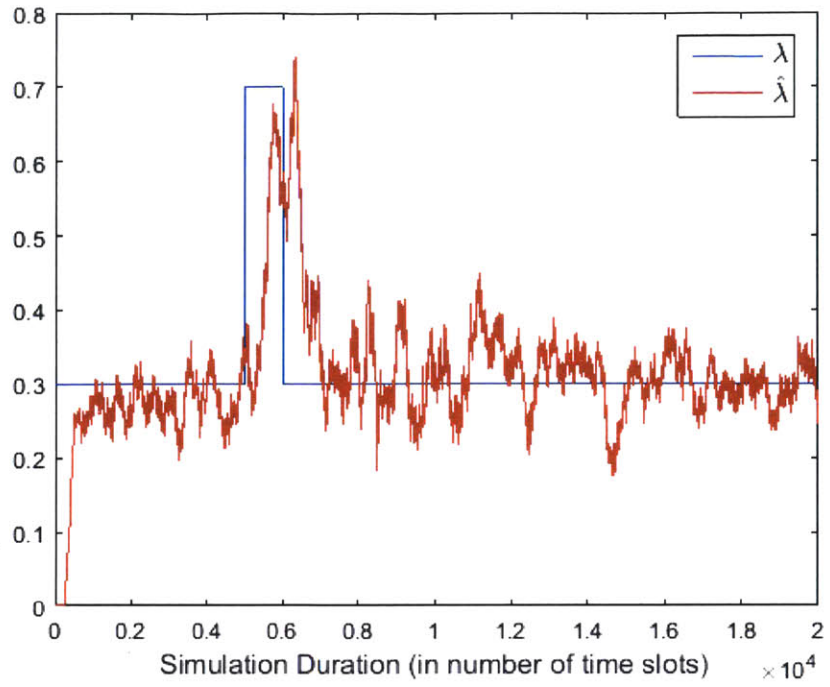


Fig. 58 Simulated Arrival Rate Estimation for $k_w = 1$

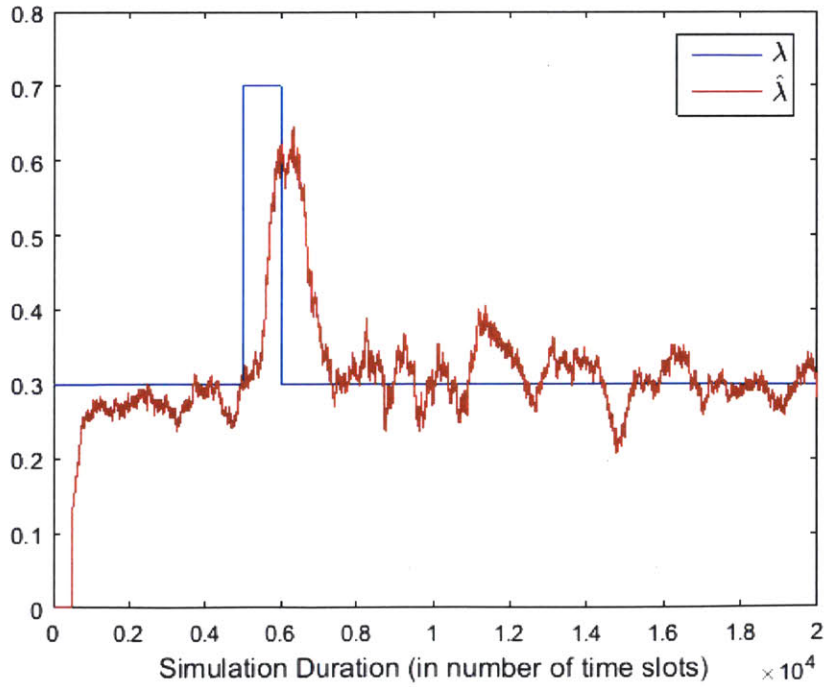


Fig. 59 Simulated Arrival Rate Estimation for $k_w = 2$

Since (3.10) provides a means of estimating $\lambda$, the value of $\hat{\lambda}$ obtained from this method can be used in the Rivest Algorithm's update of the parameter $v$ instead of the constant value $e^{-1}$. A performance comparison of the methods for updating $v$ is made by simulating an ALOHA system that uses each method. The arrival rate in these simulations is modeled by the square pulse function from Fig. 58 and Fig. 59. The system backlog is the primary metric of interest for this comparison because it provides the best insight into the system's stability. Plots of the actual and estimated backlog for each simulated system are given in Fig. 60 and Fig. 61. Note that the more conservative estimate technique with $k_w = 2$ is used in Fig. 61.

A comparison of Fig. 60 and Fig. 61 reveals that the ALOHA system using the method from (3.10) has significantly worse performance than the system using the constant value of $e^{-1}$ for $\lambda$. Not only is the maximum value of the backlog greater in Fig. 61, but it also takes the system longer to clear the backlog, resulting in greater expected channel delay. The estimator $v$ is also significantly more inaccurate and unstable in Fig. 61. Using the method from (3.10) also degrades the estimation accuracy of the arrival rate itself. A plot of $\lambda$ and $\hat{\lambda}$ for the simulation using the method from (3.10) is given in Fig. 62. We see from Fig. 62 that using the method from (3.10) to update $v$ results in significant oscillations in the value of $\hat{\lambda}$ and poor estimation accuracy. From this analysis, it is evident that using the constant value of $e^{-1}$ for $\hat{\lambda}$ when updating $v$ results in better performance over than using the value for $\hat{\lambda}$ obtained from (3.10). Therefore, while the estimation technique from (3.10) is useful as a means for implementing dual-class service, it is not used to update the value of $v$ maintained by the Rivest Algorithm.

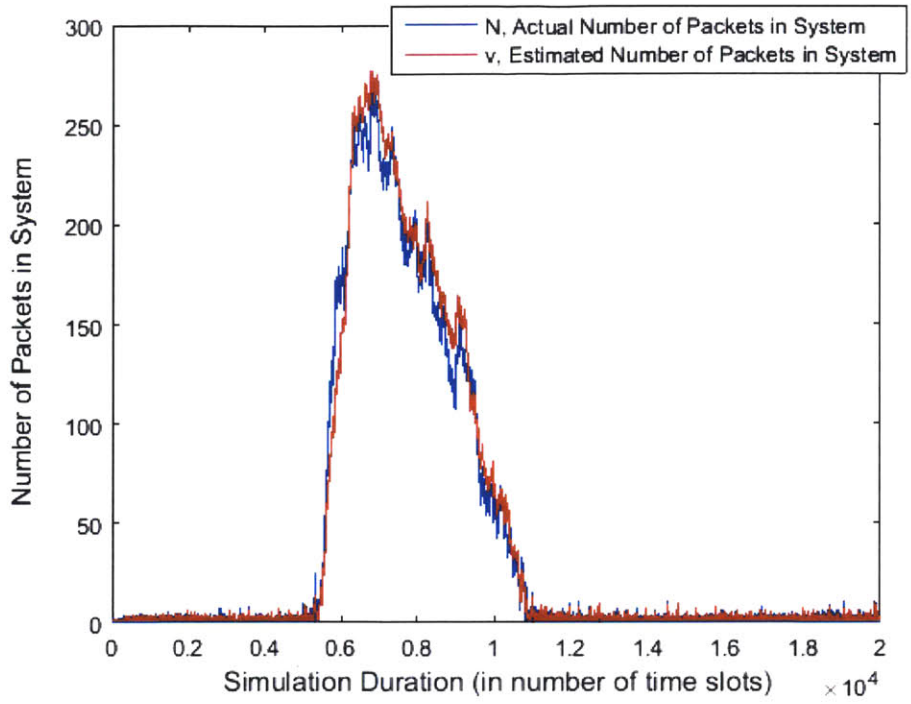


Fig. 60 Simulated Actual and Estimated for the Constant Value Update Method

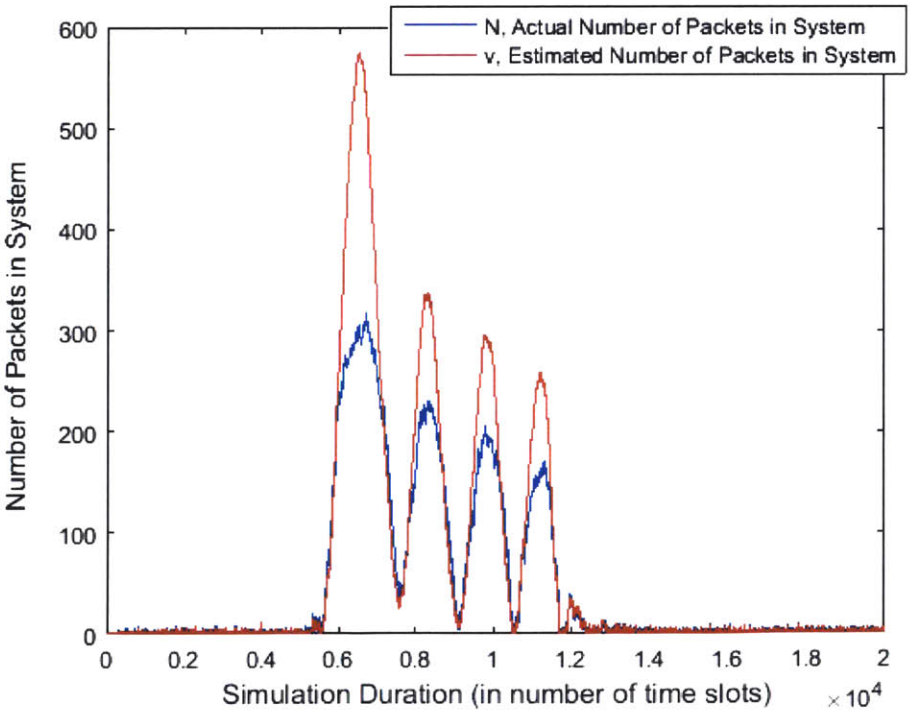


Fig. 61 Simulated Actual and Estimated Backlog for the Updated Method from (3.10) with $k_w = 2$

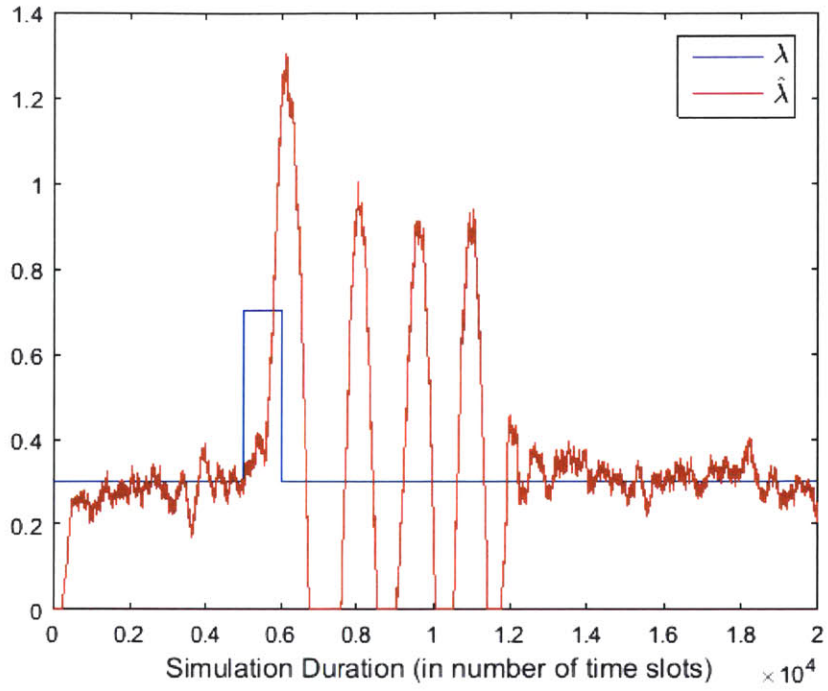


Fig. 62 Simulated Arrival Rate Estimation for Updated Method from (3.10) with $k_w = 2$

In addition to estimating the value of $\lambda$, it is also necessary to develop a means of estimating $\lambda_n$ and $\lambda_p$. Since the arrival to packets to the channel is modelled as a combined Poisson process, the estimators $\hat{\lambda}_n$ and $\hat{\lambda}_p$ are formed using the following two expressions:

$$\hat{\lambda}_n = (1 - r_p) \cdot \hat{\lambda} \quad , \tag{3.11}$$

$$\hat{\lambda}_p = r_p \cdot \hat{\lambda} \quad , \tag{3.12}$$

where $r_p$ is the fraction of successes that come from priority users observed over the window of $k_w \cdot N_{RTT}$ slots. It is assumed that priority successes can be differentiated from normal successes by embedding a code in each packet that indicates whether it originated from a priority or normal user. Note that $r_p$ is set to zero in the ambiguous case where no arrivals of either type are observed over the entire window. The

performance of the estimators developed in (3.11) and (3.12) is analyzed by simulating their behavior under four test cases. Note that (3.11) and (3.12) use the value of $\hat{\lambda}$ obtained from (3.10) with $k_w = 2$. Plots of the estimated and true arrival rates for normal and priority users for these simulations are given in Fig. 63 through Fig. 66. We see from Fig. 63 that the most accurate estimates of arrival rates occur when $\lambda_n$ and $\lambda_p$ both increase at the same time. Conversely, we see from Fig. 66 that the most inaccurate estimates occur when $\lambda_n$ and $\lambda_p$ both increase, but at different times. Additionally, the estimators have a delayed reaction to changes in the arrival rates, which is to be expected given the channel's significant feedback delay.

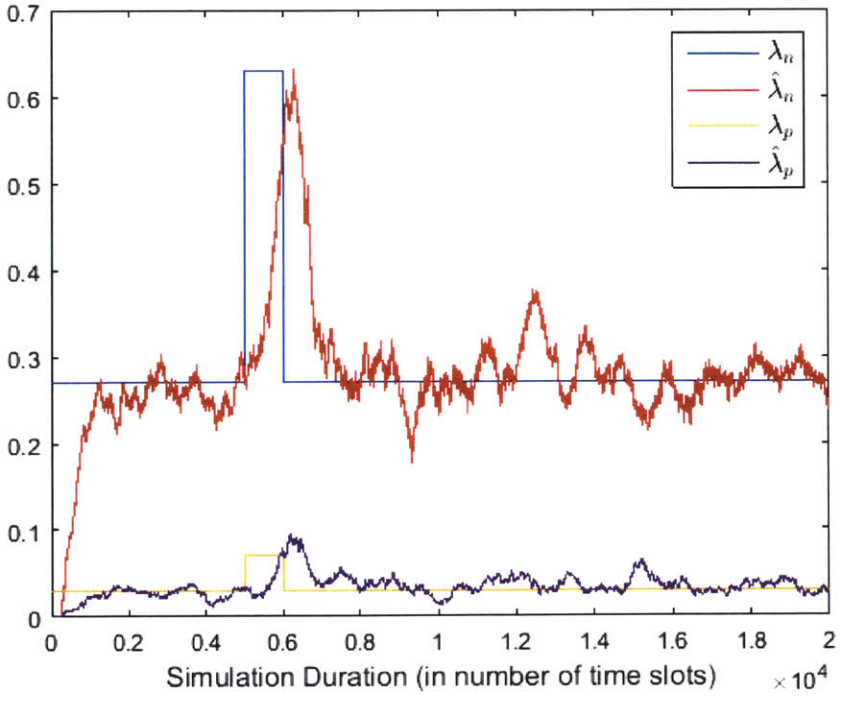


Fig. 63 Simulated Arrival Rate Estimation for a Synchronized Change in User Traffic ($k_w = 2$)

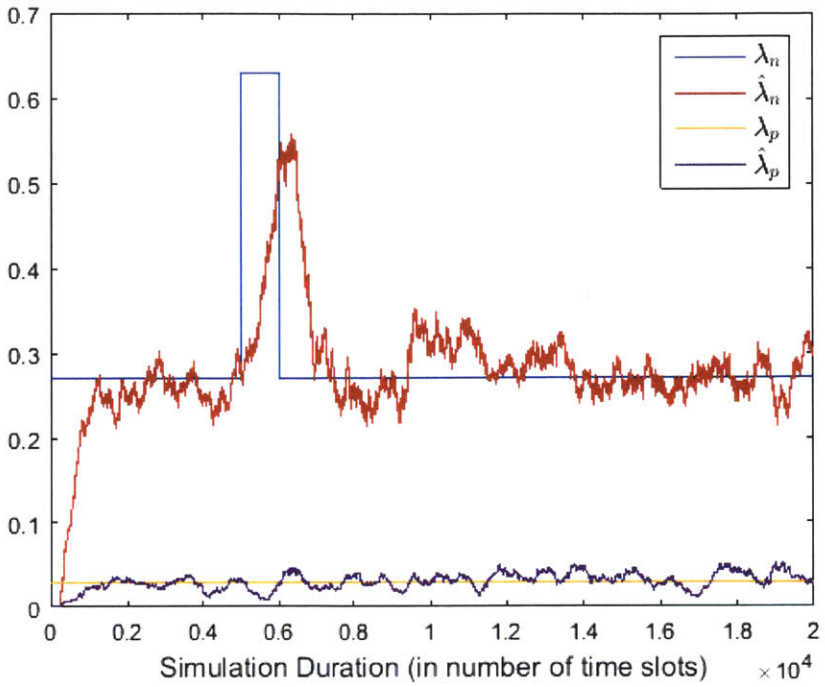


Fig. 64 Simulated Arrival Rate Estimation for a Change in Normal User Traffic ($k_w = 2$)

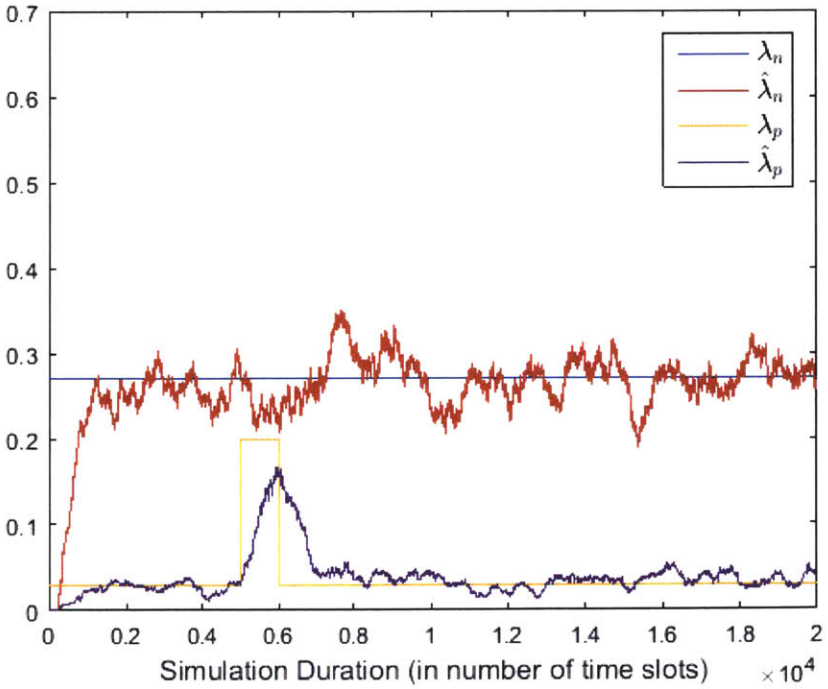


Fig. 65 Simulated Arrival Rate Estimation for a Change in Priority User Traffic ($k_w = 2$)

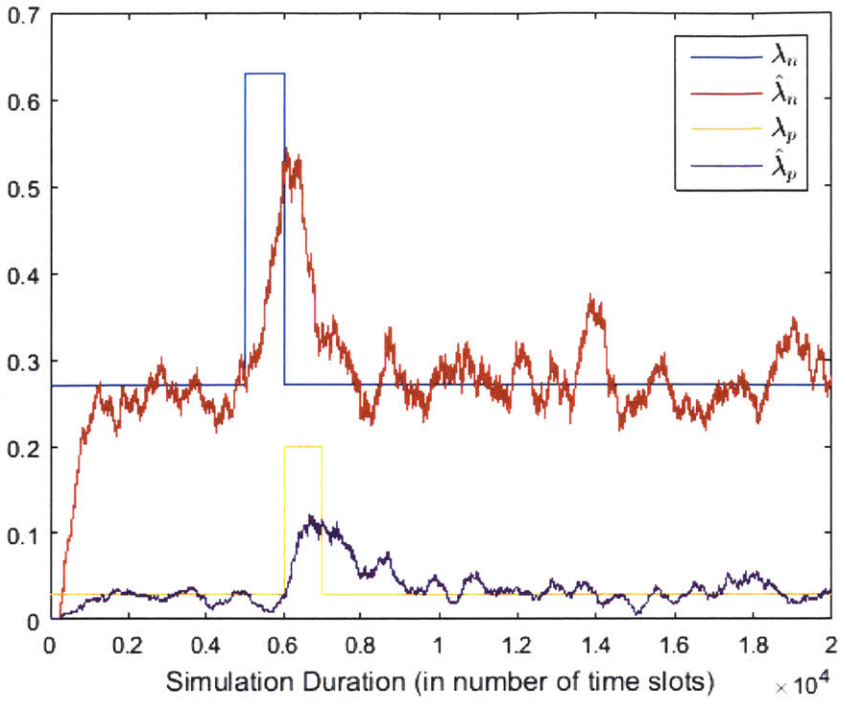


Fig. 66 Simulated Arrival Rate Estimation for an Unsynchronized Change in User Traffic ($k_w = 2$)

A final point of interest from these simulations is that the delayed response of the estimators to increases in the actual arrival rates causes the system to underestimate $\lambda_n$ and $\lambda_p$ initially. Similarly, the delayed response causes the system to overestimate $\lambda_n$ and $\lambda_p$ for a period of time after a decrease in the actual arrival rates occurs. It is shown in the next section that for the purposes of implementing dual-class service, underestimating $\lambda_n$ and $\lambda_p$ is more desirable than overestimating their values. Therefore, the delayed response of the estimators to increases in arrival rates is better than a more responsive, but more unstable, estimation method that may overestimate the arrival rates.

## 3.3.2 Throughput Scaling with Random Drops

With a scheme for estimating the arrival rates in place, the implementation of dual-class service can now be discussed. The goal of the dual-class service scheme is to efficiently scale back the throughput allocated

to normal users when priority user traffic requires additional system capacity in order to maintain a low expected delay. Ideally, this mechanism will scale $\lambda_n$ such that $\lambda_n + \lambda_p = e^{-1}$ true when there is sufficient traffic to require the maximum system capacity. One technique for scaling throughput is to divide the control parameter $q$ into two separate parameters for each class of service. However, doing so violates many of the assumptions used to develop the Rivest Algorithm, and it is unclear how to scale these two control parameters based on channel feedback. A more promising technique for scaling throughput is to order normal users to randomly drop off the channel when the total arrival rate is greater than the system's maximum achievable throughput.

Two criteria will be used to determine when normal users should drop from the channel. First, the estimated number of backlogged packets $v$ must exceed a user-defined threshold $N_{drop}$. The parameter $N_{drop}$ is used to ensure that the channel does not exceed some maximum tolerable delay threshold $T_{drop}$. The relationship between $N_{drop}$ and $T_{drop}$ follows the same form as the relationship between $v$ and $E[\hat{T}_w]$ given in (3.7):

$$T_{drop} = (e \cdot N_{drop} + N_{RTT}) L_p T_b \tag{3.13}$$

Second, the estimated total arrival rate from normal and priority users $\hat{\lambda}$ must exceed the maximum system throughput of $e^{-1}$. This criterion is necessary because the backlog and channel delay will naturally decrease to acceptably low values when $\hat{\lambda} < e^{-1}$ and it is undesirable to drop users from the channel unnecessarily.

When the system detects that the conditions for a random drop have been met, it will broadcast a drop parameter $q_{drop}$ in addition to its regular feedback. Upon reception of $q_{drop}$, normal users will then

individually perform a test to determine whether they will drop off the channel with probability $q_{drop}$, or will remain on the channel with probability $1 - q_{drop}$. Assuming that each packet in the system originates from a different user, a drop of normal users will scale $\lambda_n$ by a factor of $1 - q_{drop}$. Users that are dropped from the channel may then search for other DS/ALOHA channels to join. A dropped user can gauge the availability of other channels by observing the value of the control parameter $q$ broadcast by each channel as a measure of the channel's congestion. Priority users ignore drop commands and continue to transmit in accordance with the Rivest Algorithm.

The drop parameter $q_{drop}$ can be determined by the noting that the desired result from the random drops is to satisfy:

$$r_n \cdot \lambda_n + \lambda_p = e^{-1} \quad , \tag{3.14}$$

where $r_n$ is the fraction of normal users retained by the channel after the drop and is equivalent to $1 - q_{drop}$. Solving (3.14) for $r_n$ yields:

$$r_n = \frac{e^{-1} - \lambda_p}{\lambda_n} \tag{3.15}$$

However, the expression in (3.15) is not sufficient for determining $r_n$ because it fails to account for two cases that may arise during a random drop. First, if $\lambda_p > e^{-1}$, the value of $r_n$ in (3.15) will be negative because the traffic from priority users is greater than the maximum system throughput. Under these conditions, the best the system can do is to drop all normal users and set $r_n$ equal to zero. Second, if the system manages to scale the combined arrival rate exactly to $e^{-1}$, the system will remain stable, but the backlog and delay will remain high since there is no additional throughput available to clear the backlog

that built up during the period where the traffic load is greater than the maximum system throughput. Therefore, the throughput should be scaled to $0.99 \cdot e^{-1}$ to ensure that a small portion of the system throughput is reserved for reducing congestion and latency. The complete expression for determining $r_n$ based on these changes is:

$$r_n = max\left\{\frac{0.99 \cdot e^{-1} - \lambda_p}{\lambda_n}, 0\right\} , \tag{3.16}$$

where the maximum in (3.16) corrects for the case where $\lambda_p > e^{-1}$. Using the expression in (3.16), the drop parameter $q_{drop}$ is calculated using the following expression:

$$q_{drop} = max\{1 - r_n, 0\} , \tag{3.17}$$

where the maximum in (3.17) ensures that $0 \leq q_{drop} \leq 1$.

In addition to setting the appropriate drop parameter, the system must also update its estimators to reflect the reduction in normal user traffic. This is easily accomplished for $r_p$, $\hat{\lambda}_p$, and $\hat{\lambda}_p$ by updating the observation window to exclude time slots observed before the drop is executed. Note that the system must wait half a RTT between the transmission of the drop command and its execution by normal users. During this time, the system will continue to transmit feedback normally. When the drop occurs half a RTT after the drop command is initially broadcast, the estimated number of packets in the backlog $v$ is updated in the following manner:

$$v = v \cdot r_p + v \cdot (1 - r_p) \cdot r_n , \tag{3.18}$$

where the system estimates that $v \cdot r_p$ of the backlogged packets are from priority users, and therefore remain in the system's backlog. Additionally, the system estimates that $v \cdot (1 - r_p)$ of the backlogged packets are from normal users, and therefore only a fraction $r_n$ of them remain after the drop. Note that after the drop occurs the system will have to wait an additional half of a RTT to observe the first time slot that occurs after the drop. During this time, the system will increment $v$ by $\hat{\lambda} = e^{-1}$ and will ignore the outdated channel feedback that was broadcast before the drop command was broadcast.

After a drop occurs, it will take some time for the estimates of $\lambda$, $\hat{\lambda}_p$, $\hat{\lambda}_p$, and $N$ to achieve sufficient accuracy. Therefore, it is necessary to wait for a period of time before initiating the next drop if it is determined that another drop is required. It is shown in the next section that waiting for a window of $2 \cdot k_w \cdot N_{RTT}$ slots before initiating another drop is an acceptable choice for most simulated conditions. A second drop may be necessary due to either a spike in priority user traffic that occurs after in the initial drop or an underestimation of the number of normal users that needed to be dropped initially. Underestimations of the required number of normal users to drop occur when there is an overestimate of $r_n$. An overestimation of $r_n$ is preferable to an underestimation of its value because a second drop can be initiated to remove additional users that remained on the channel due to an overestimation of $r_n$, but the throughput lost from dropping too many users from the channel cannot be easily recovered. We see from (3.16) that overestimations of $r_n$ result from underestimations of $\lambda_n$, $\lambda_p$, or both. Therefore, an underestimating arrival rates is more desirable than overestimation of their values when determining the drop parameter $q_{drop}$.

### 3.3.3 Simulations with Priority Users

The performance of the ALOHA system using the Rivest Algorithm with delayed feedback and the random drop scheme is simulated for four different cases. Plots of initial arrival rates, scaled arrival rates, backlog,

delay, local average throughput, and long-term average throughput are given for each case. The plots of the initial arrival rates show the traffic load users initially offer to the channel. The plots of scaled arrival rates show how the random drop scheme scales the arrival rates to reduce congestion. A new parameter $N_p$, corresponding to the number of backlogged packets from priority users, is included in the backlog plots to better understand how the drop scheme affects the congestion of priority users. The delay threshold to initiate a drop $T_{drop}$ is set to 1.2232 seconds and is included in the delay plots to determine how long the system remains above the drop threshold. The choice of 1.2232 seconds for $T_{drop}$ corresponds to the expected delay for the case where the system will not tolerate more than $N_{drop} = 200$ backlogged packets with $N_{RTT} = 250$ time slots, $L_p = 1000$ bits, and $T_b = 10^{-6}$ seconds. The effect of a drop of normal users on the arrival rate $\lambda_n$ is modeled by having each backlogged packet from a normal user drop from the channel with probability $q_{drop}$, reducing $N$ by the number of packets that drop from the channel, and scaling $\lambda_n$ by the ratio of normal packets dropped to the total number of normal backlogged packets prior to the drop.

The four test cases simulated model a synchronized increase in priority and normal user traffic, an increase in only normal user traffic, an increase in only priority user traffic, and an unsynchronized increase in priority and normal user traffic. The simulated results for the synchronized case are given in Fig. 67 through Fig. 72. The simulated results for the normal user traffic increase are given in Fig. 73 through Fig. 78. The simulated results for the priority user traffic increase are given in Fig. 79 through Fig. 84. Finally, the simulated results for the unsynchronized case are given in Fig. 85 through Fig. 90.

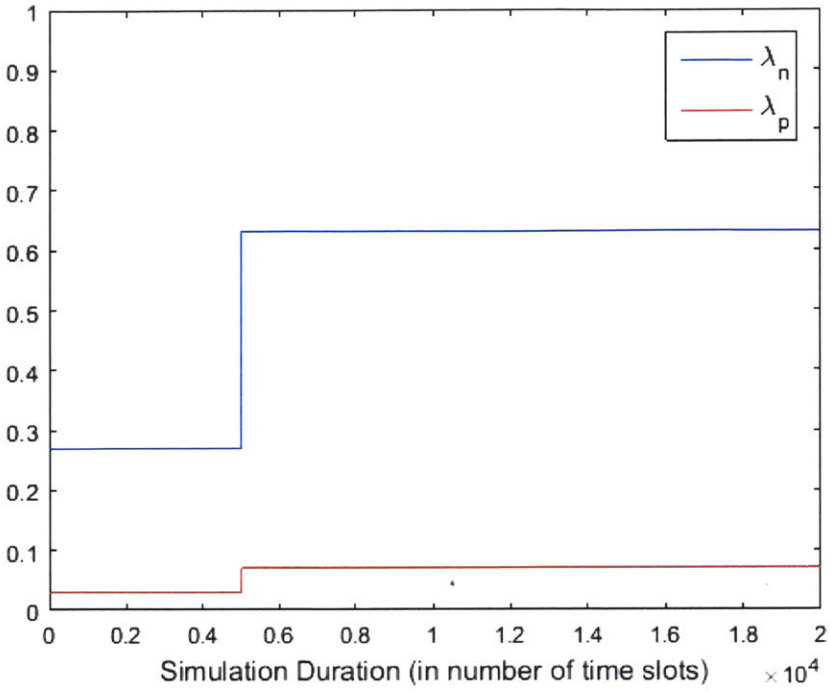


Fig. 67 Initial Poisson Arrival Rates for Synchronized Traffic Increase

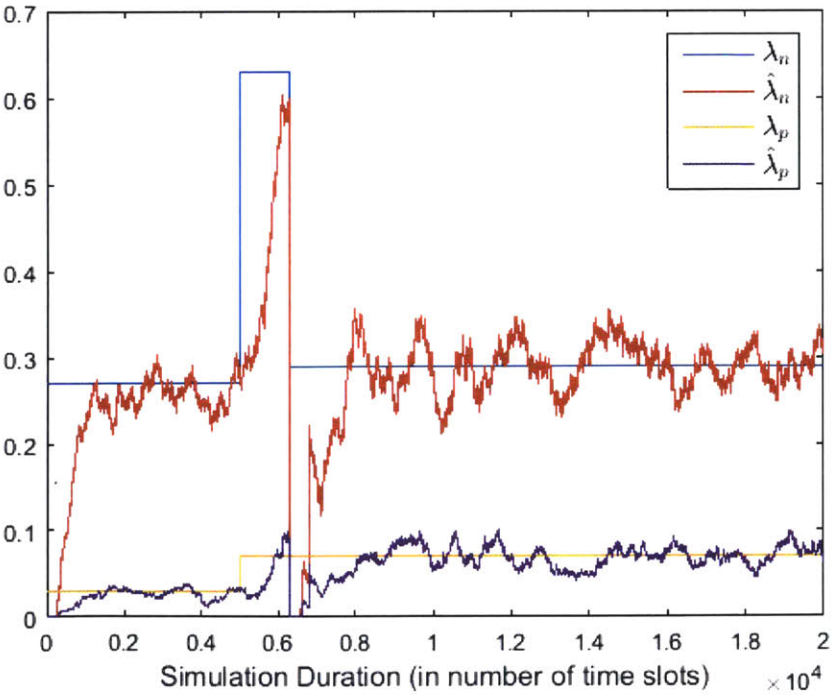


Fig. 68 Simulated Estimated and Scaled Poisson Arrival Rates for Synchronized Traffic Increase

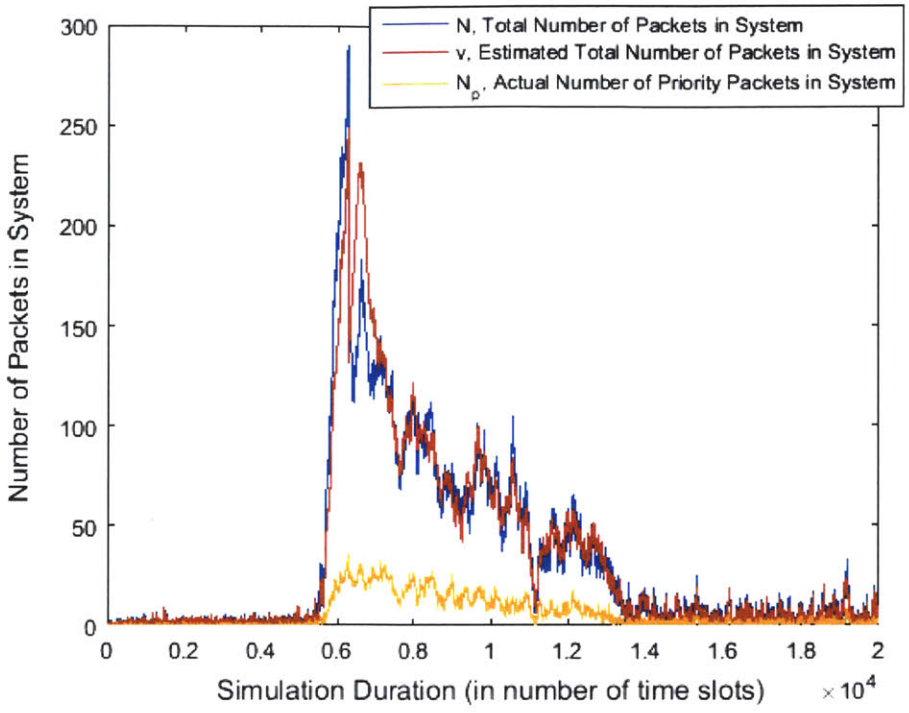


Fig. 69 Simulated Actual and Estimated Backlog for Synchronized Traffic Increase

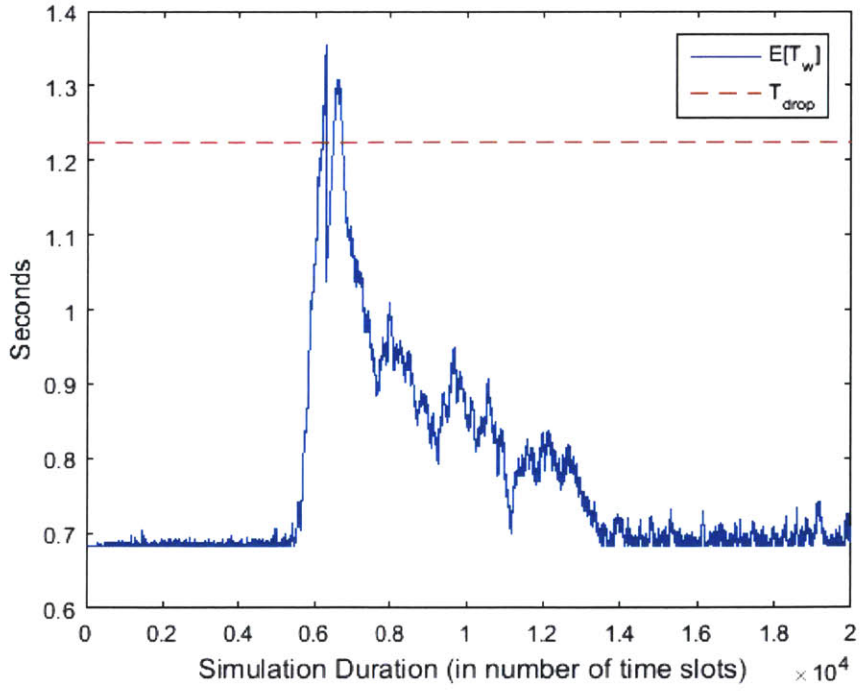


Fig. 70 Simulated Expected Delay for Synchronized Traffic Increase

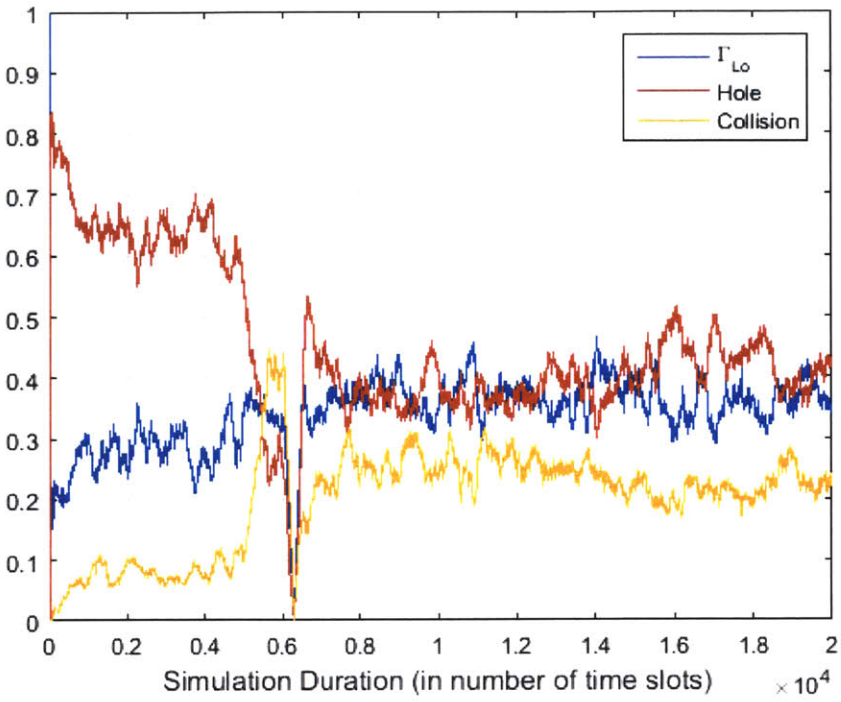


Fig. 71 Simulated Local Averages for Synchronized Traffic Increase

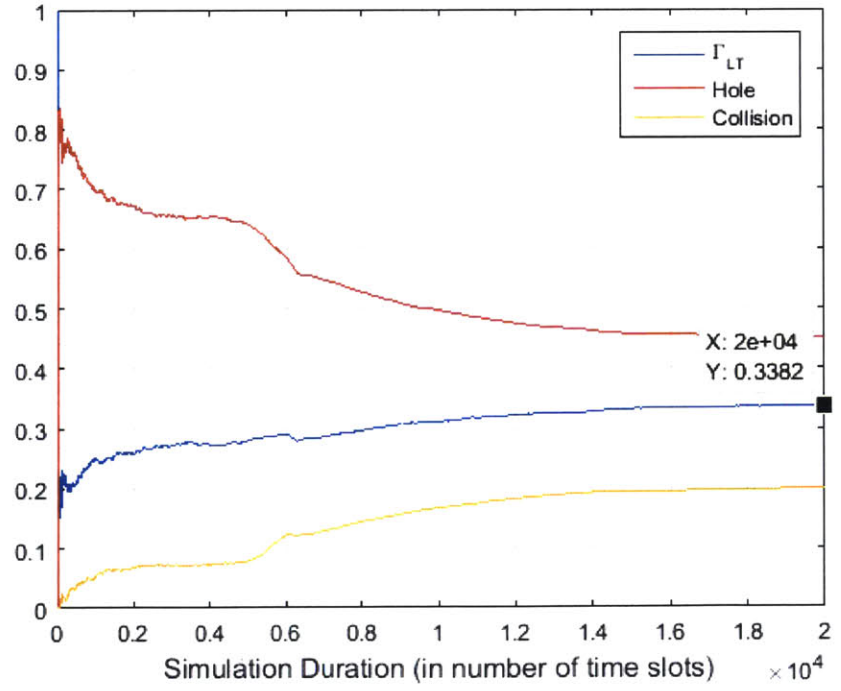


Fig. 72 Simulated Long-Term Averages for Synchronized Traffic Increase

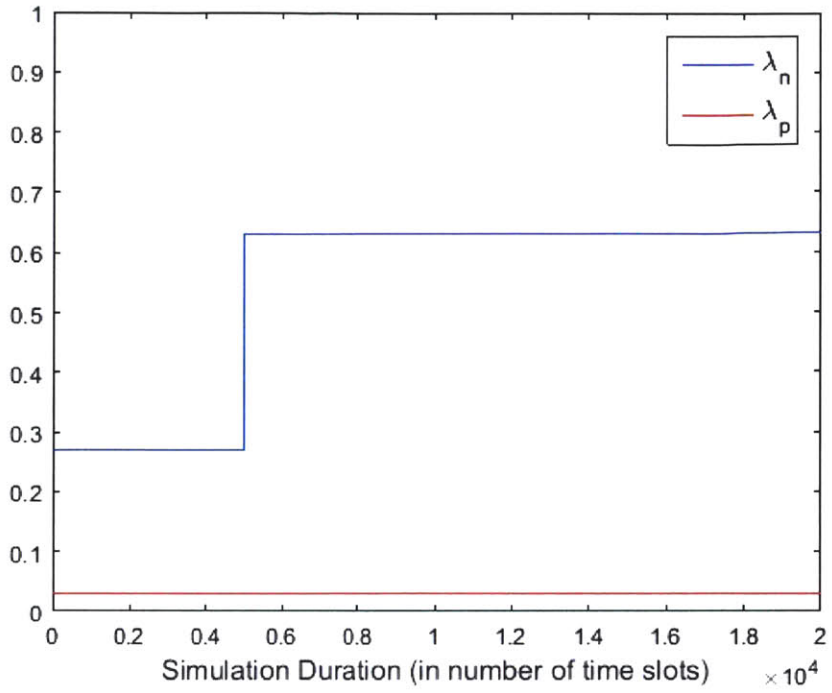


Fig. 73 Initial Poisson Arrival Rates for Normal User Traffic Increase

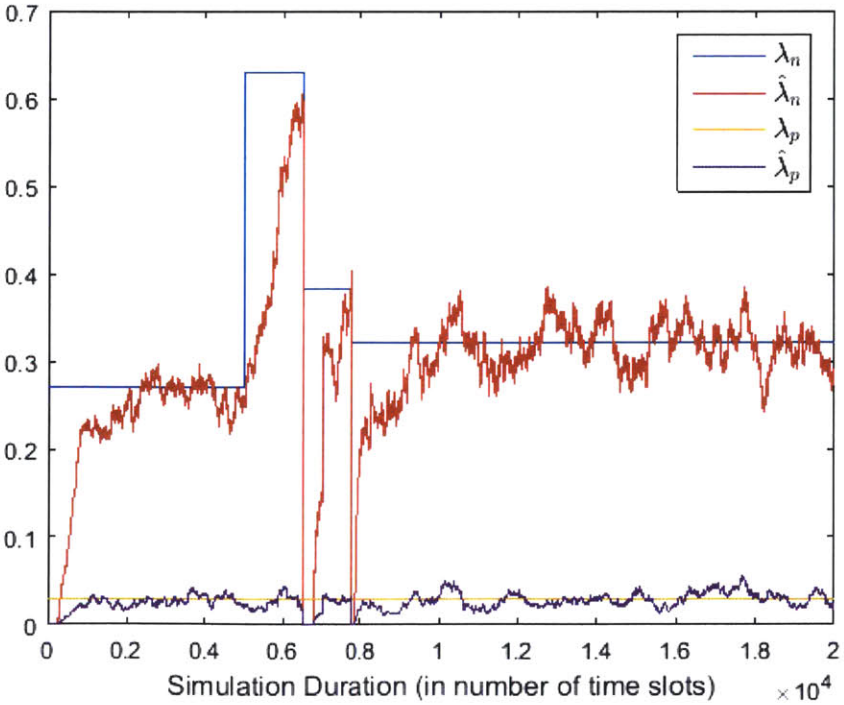


Fig. 74 Simulated Estimated and Scaled Poisson Arrival Rates for Normal User Traffic Increase

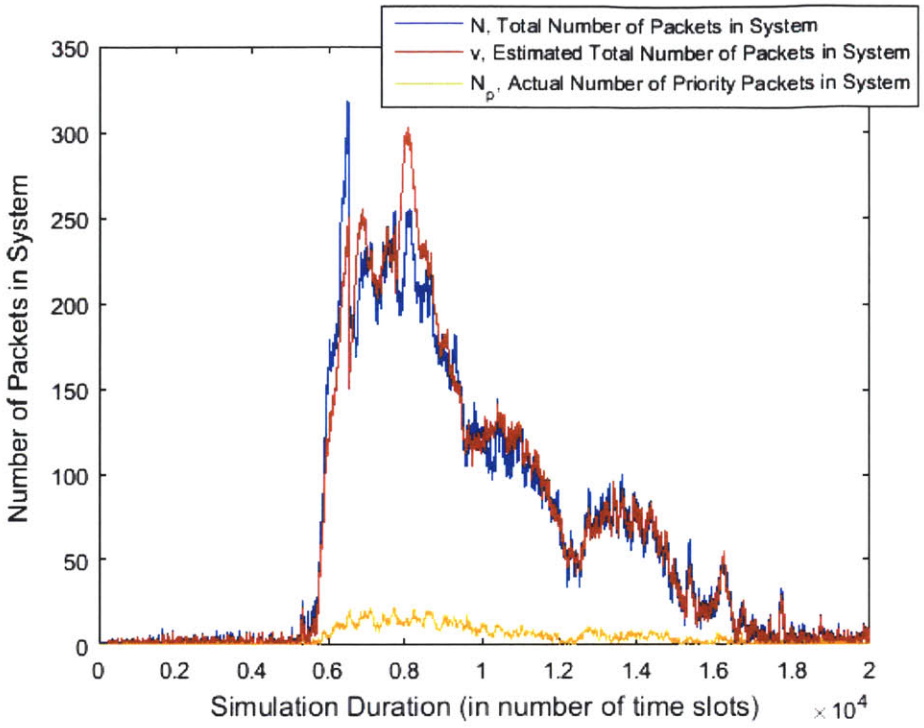


Fig. 75 Simulated Actual and Estimated Backlog for Normal User Traffic Increase

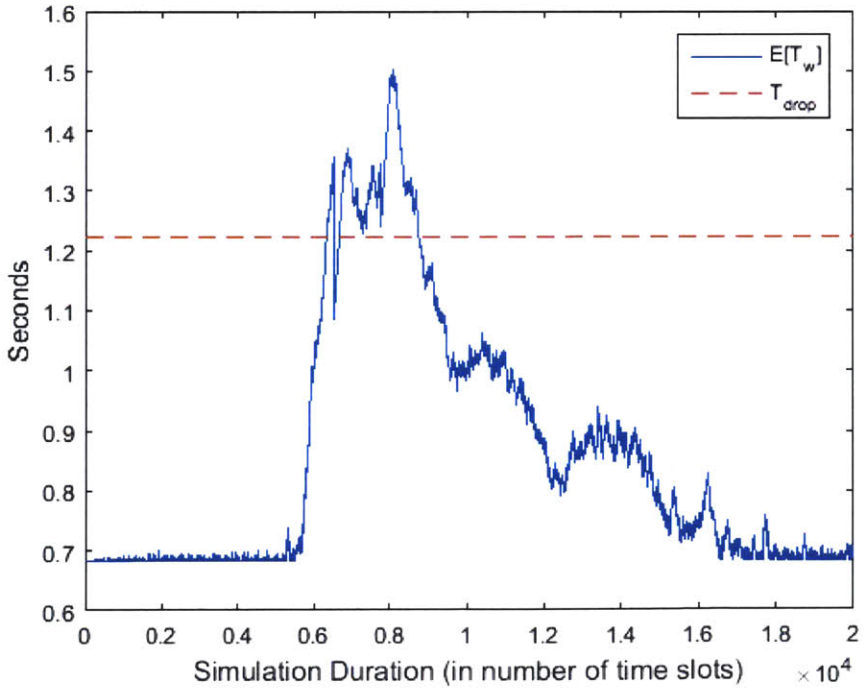


Fig. 76 Simulated Expected Delay for Normal User Traffic Increase

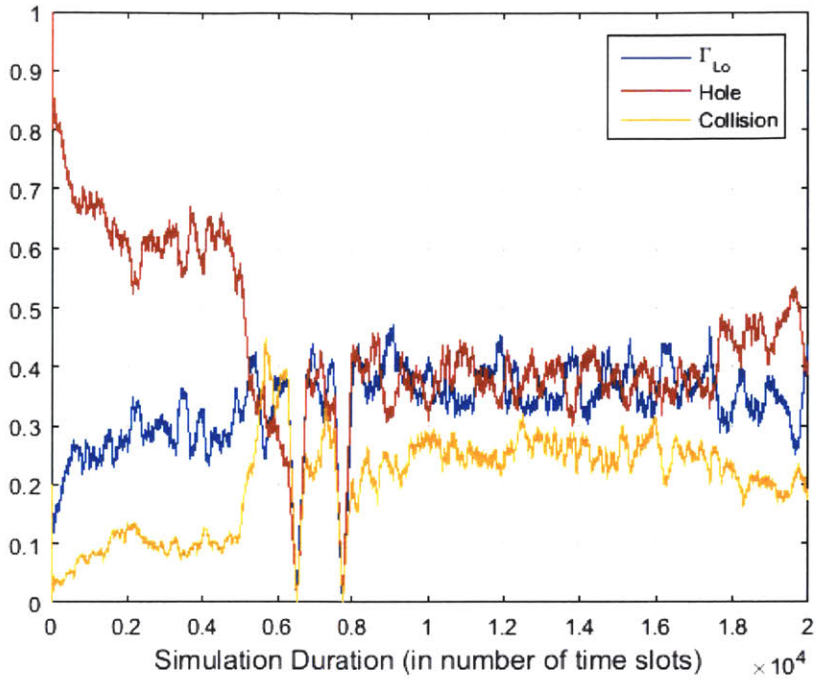


Fig. 77 Simulated Local Averages for Normal User Traffic Increase

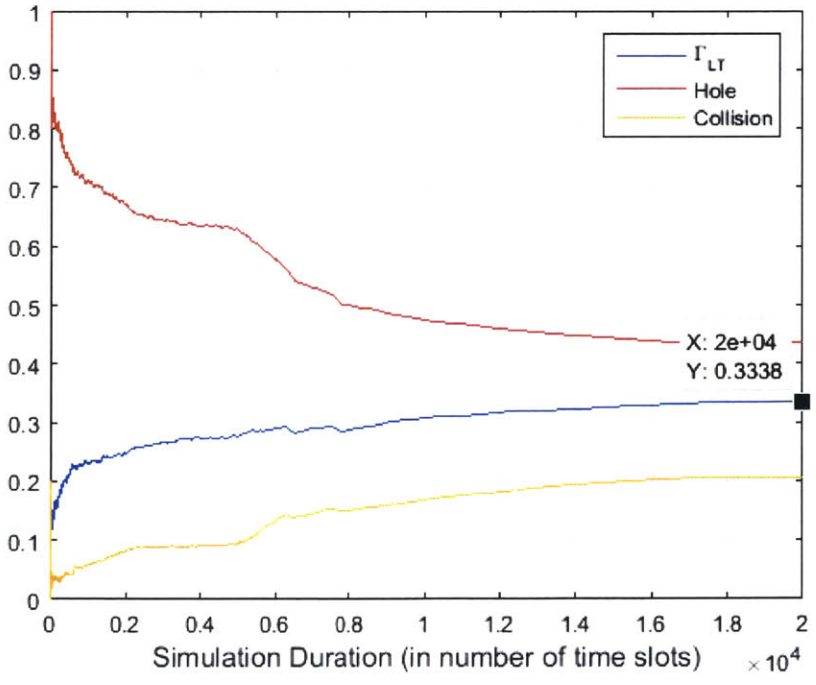


Fig. 78 Simulated Long-Term Averages for Normal User Traffic Increase

We see from Fig. 68 that for the case where there is a synchronized increase in priority and normal user traffic, the dropping scheme effectively scales $\lambda_n$ so that the total arrival rate is reduced to a supportable value below the maximum system throughput and that the backlog is gradually cleared by the system. The location of the drop is easily identifiable in Fig. 68 where the arrival rate for normal users is abruptly scaled down to a supportable value. We also see that the estimates of $\lambda_n$ and $\lambda_p$ take time to achieve acceptable accuracy after the drop is executed. We see from Fig. 69 that $v$ remains fairly close to $N$, except for a brief period after the drop occurs where the system significantly overestimates $N$. This overestimate briefly suppresses the channel and its effect on local throughput can be seen around the 6,000$^{th}$ time slot in Fig. 71. This overestimate also causes the channel delay shown in Fig. 70 to exceed $T_{drop}$ for a second brief period. This behavior highlights the importance of waiting for a window of time before allowing another drop to occur. Without this requirement, a second drop could have been triggered by the temporary increase in delay which would result in more normal users dropping from the channel than necessary. Finally, we see from Fig. 72 that the system is able to achieve a long-term throughput close to the maximum system throughput using the random drop scheme.

Similar behavior is observed for the case where only normal user traffic increases. Note that in this case two drops of normal users occur instead of one. We see from Fig. 74 that the first drop's reduction of $\lambda_n$ is not large enough to achieve a supportable traffic load due to an underestimate of $\lambda_n$. We also see from Fig. 74 that the system is able to correct this error with a second drop that reduces the total arrival rate below the maximum system throughput. We see from Fig. 75 that both drops result in temporary overestimates of $N$ which suppress the channel for a brief period of time. These periods of suppression result temporary reductions of local throughput evident in Fig. 77. We see from Fig. 76 that the channel delay remains above $T_{drop}$ for a longer period of time in this case because the system requires two drops to achieve a supportable arrival rate.

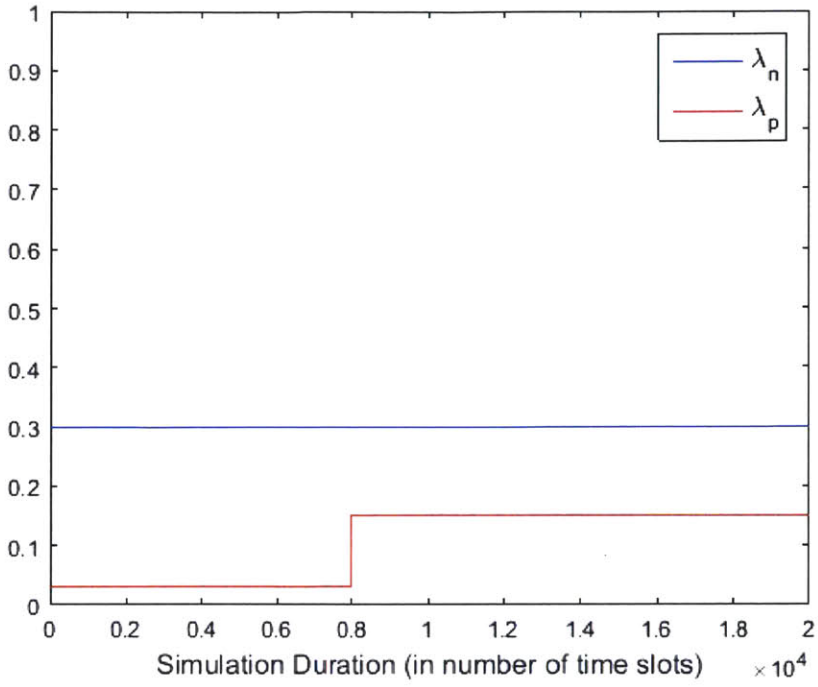


Fig. 79 Initial Poisson Arrival Rates for Priority User Traffic Increase

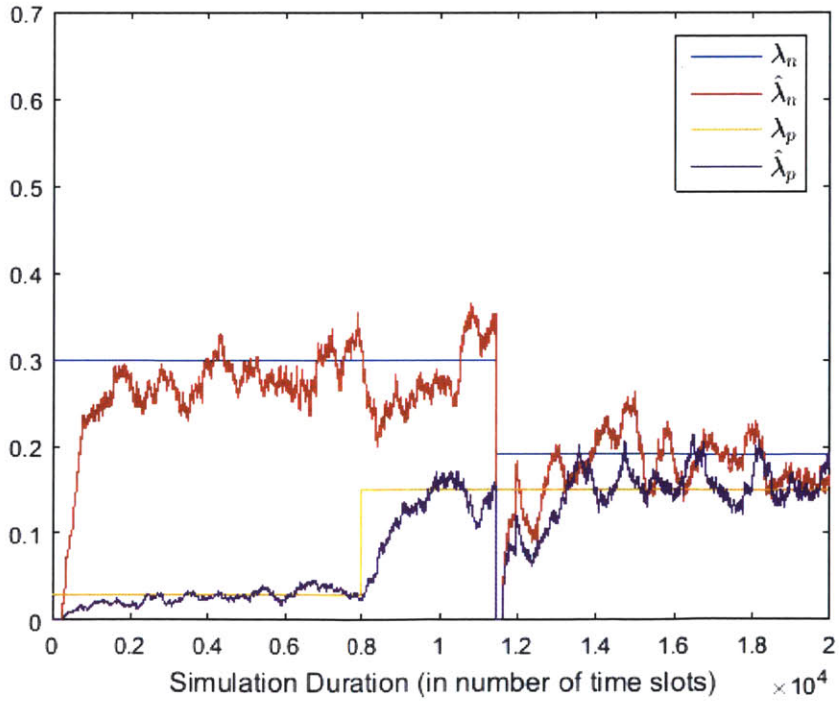


Fig. 80 Simulated Estimated and Scaled Poisson Arrival Rates for Priority User Traffic Increase

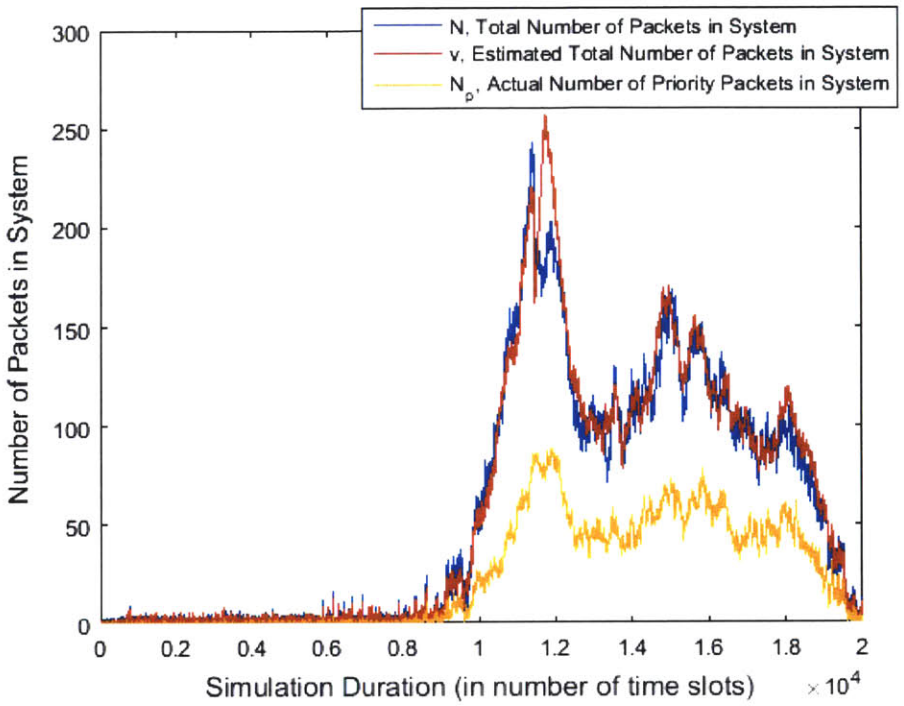


Fig. 81 Simulated Actual and Estimated Backlog for Priority User Traffic Increase

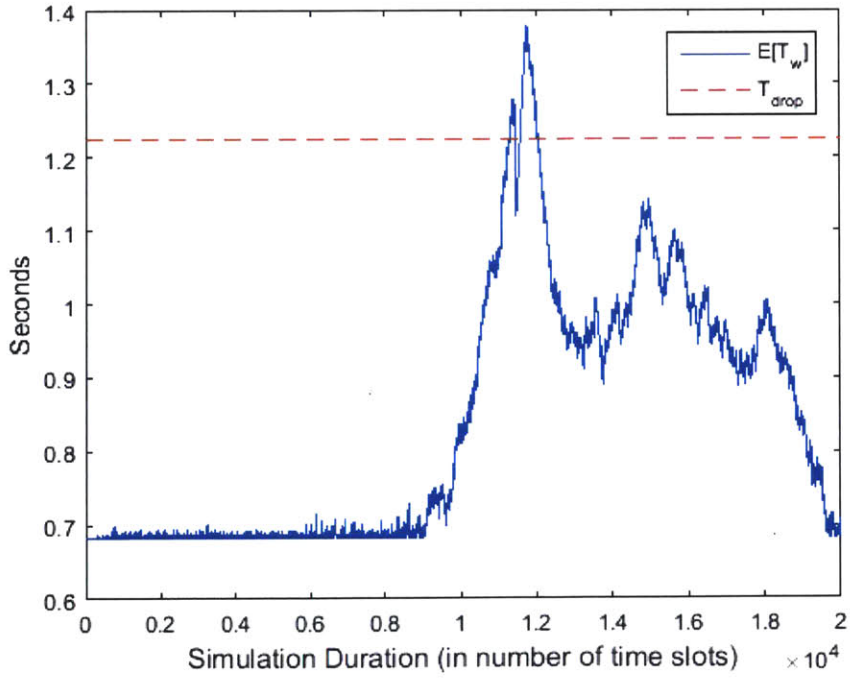


Fig. 82 Simulated Expected Delay for Priority User Traffic Increase

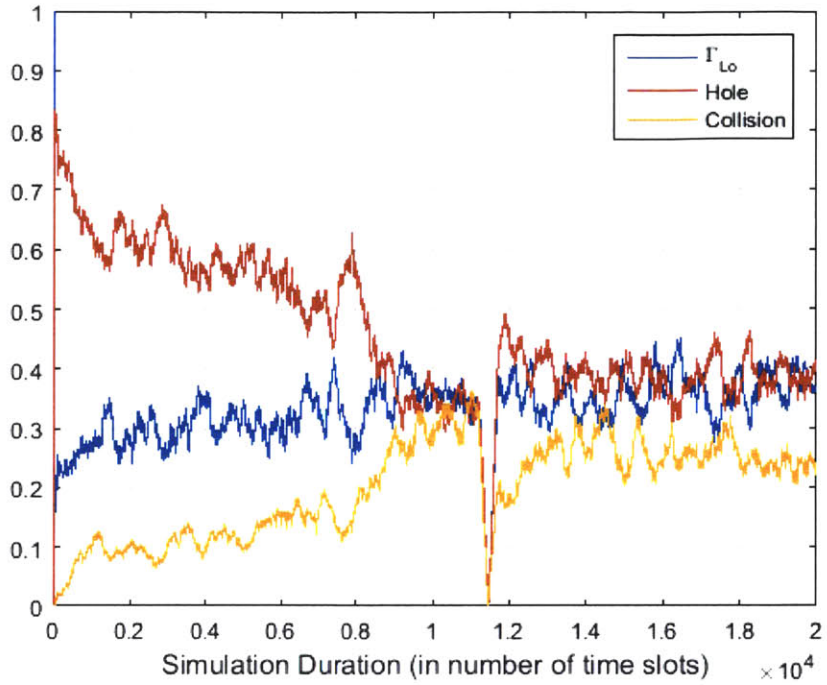


Fig. 83 Simulated Local Averages for Priority User Traffic Increase

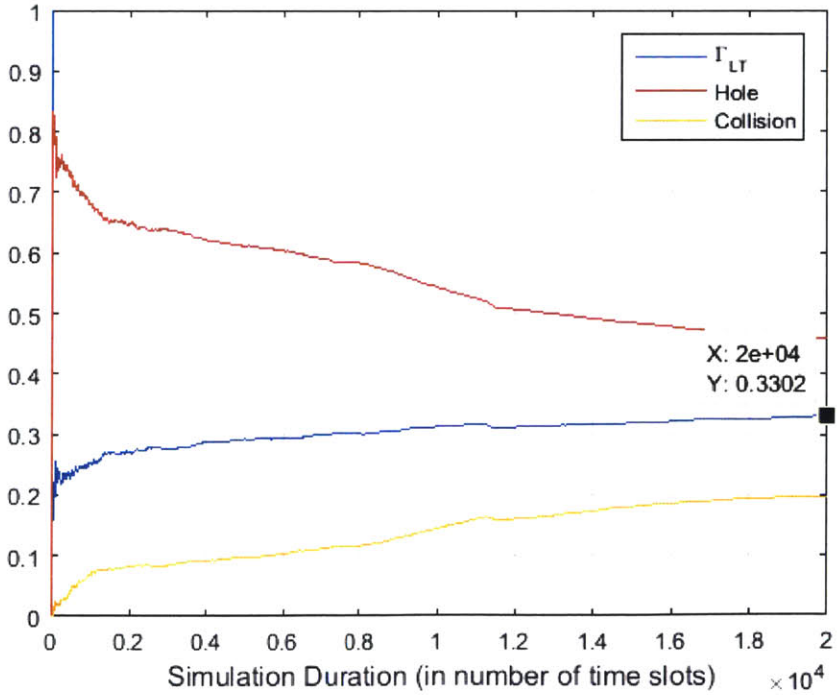


Fig. 84 Simulated Long-Term Averages for Priority User Traffic Increase

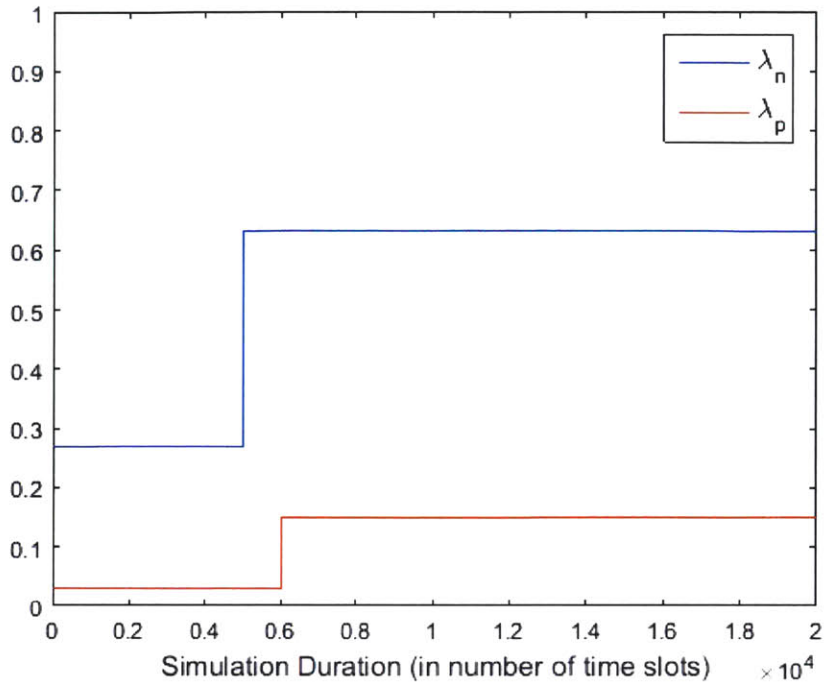


Fig. 85 Initial Poisson Arrival Rates for Unsynchronized Traffic Increase

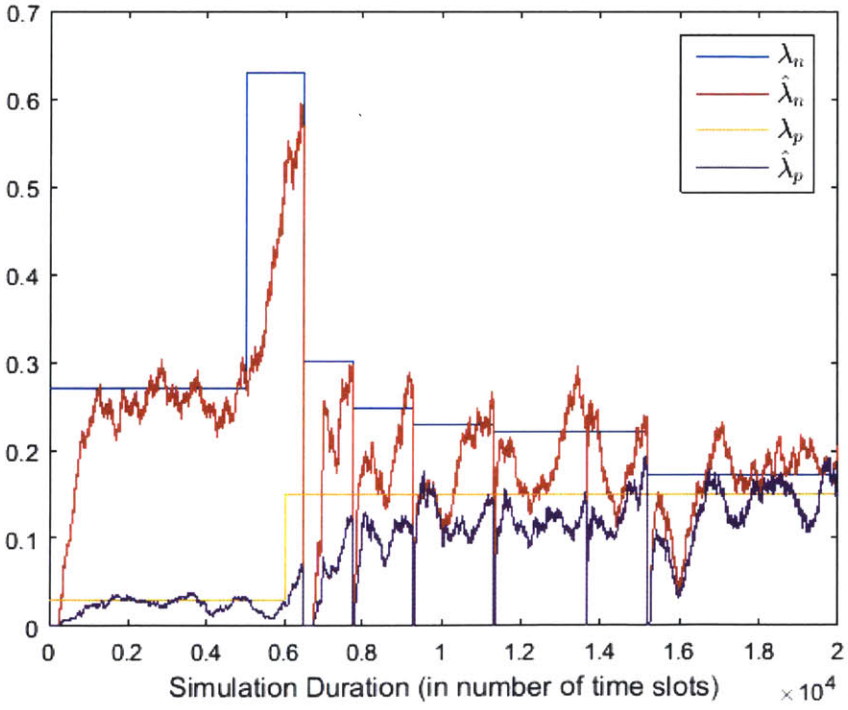


Fig. 86 Simulated Estimated and Scaled Poisson Arrival Rates for Unsynchronized Traffic Increase

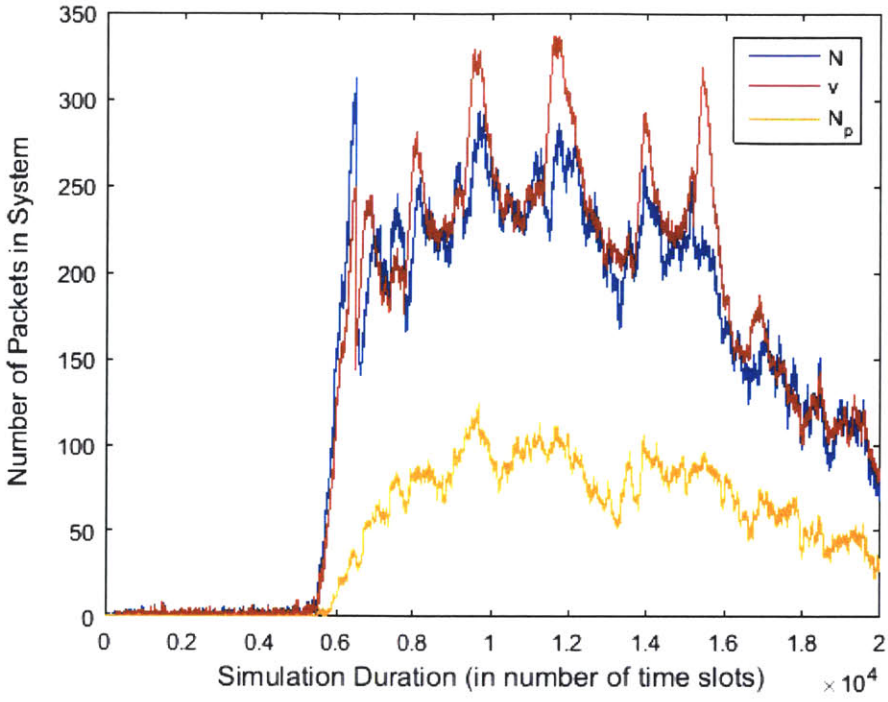


Fig. 87 Simulated Actual and Estimated Backlog for Unsynchronized Traffic Increase

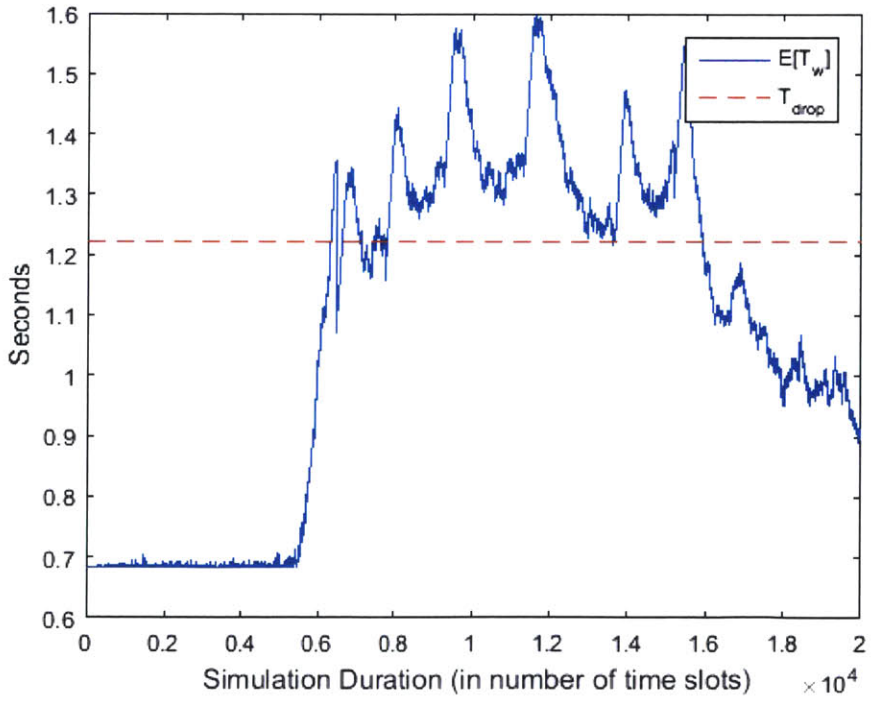


Fig. 88 Simulated Expected Delay for Unsynchronized Traffic Increase

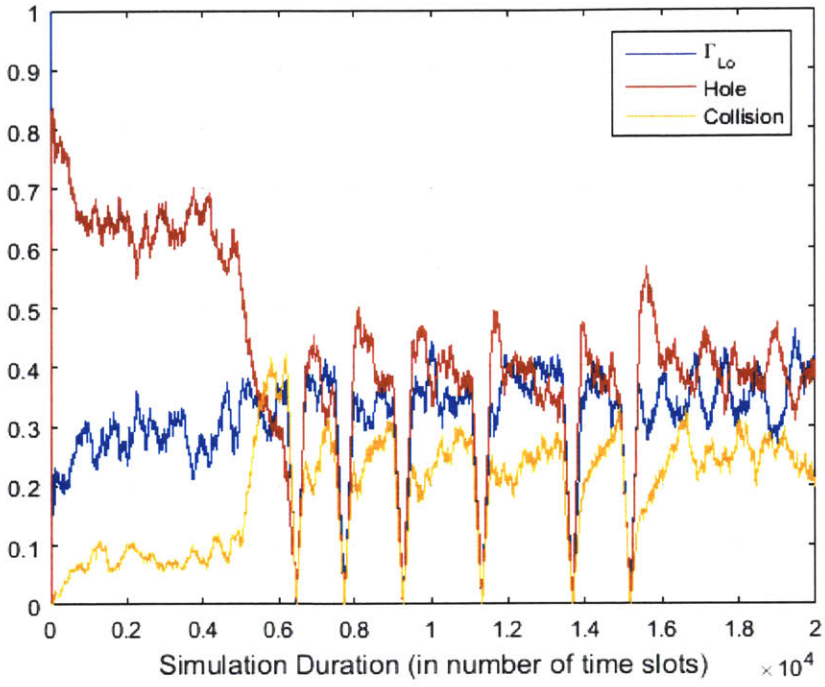


Fig. 89 Simulated Local Averages for Unsynchronized Traffic Increase

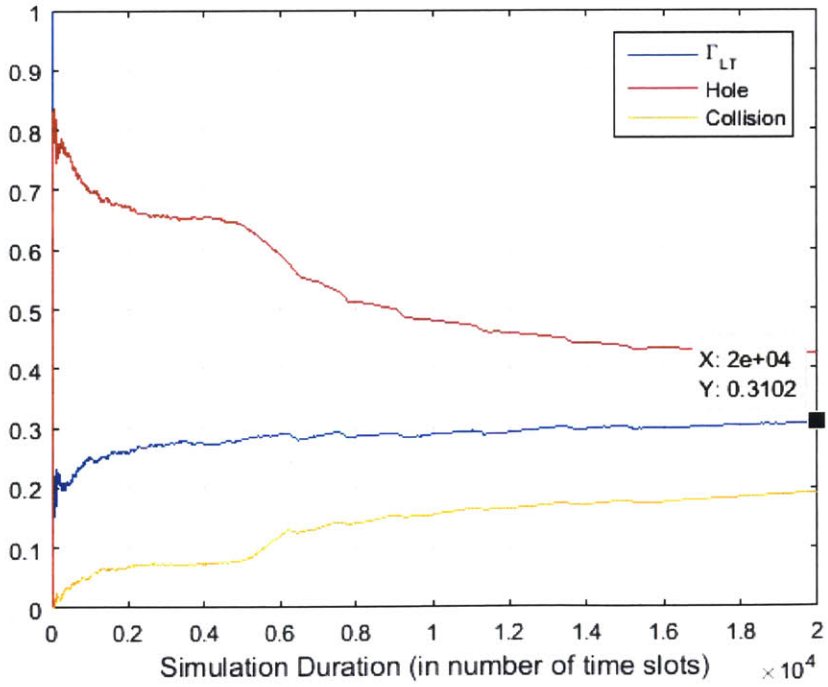


Fig. 90 Simulated Long-Term Averages for Unsynchronized Traffic Increase

We see from Fig. 79 through Fig. 84 that the case where only priority user traffic increases exhibits similar behavior to the case where there is a synchronized increase in user traffic. We see from Fig. 80 that only a single drop is required to achieve a supportable traffic load. Additionally, we see from Fig. 81 and Fig. 82 that backlog and expected delay gradually decrease after the drop. Finally, we see from Fig. 83 and Fig. 84 that the local and long-term throughputs remain close to the maximum system throughput.

The case where there is an unsynchronized increase in user traffic exhibits the most interesting behavior. For this particular simulation, we see from Fig. 86 that the system requires five drops to reach a supportable arrival rate. It is apparent from Fig. 87 and Fig. 88 that the large number of drops used by the system results in the longest time required to reduce backlog and delay among the four test cases. We also see from Fig. 86 that this case has the most inaccurate estimates of $\lambda_n$ and $\lambda_p$. The significantly worse performance of the throughput scaling scheme in this case highlights the need to select the appropriate observation window length in order to ensure accurate estimates of $\lambda_n$ and $\lambda_p$. Accurate estimates of these arrival rates are essential to minimize the number of drops required to achieve a supportable arrival rate.

From an analysis of the four test cases, it is evident that the random drop scheme is a reasonably effective means of implementing dual class service. Even in the worst case observed, the random drop scheme is able to maintain a throughput close to the maximum system throughput while scaling back the arrival rate of normal user traffic to reduce congestion and delay. From the cases where multiple drops are required, we also see that the scheme demonstrates the ability to iteratively apply corrective measures to converge toward a supportable state.

### 3.3.4 Strict Time Deadline Service

While the random drop dual-class service method effectively scales back the throughput of normal users to accommodate priority user traffic, it has an expected delay that may be unacceptable for priority messages with strict time deadlines. We see from (3.2) that even if the system is completely uncongested ($v = 1$) the expected delay for a packet is 0.6823 seconds for $N_{RTT} = 250$, $L_p = 1000$, and $T_b = 10^{-6}$. This means that the minimum expected delay for the random drop dual-class service method is 0.6823 seconds for all users. Therefore, another mode of transmission for users with strict time deadlines may be necessary.

A simple strategy to reduce the expected delay for users with strict time deadlines is to allow these users to transmit their packets repeatedly over a fixed number of slots $N_{Rep}$ before waiting for feedback. From the continuous transmission attempt case in Section 3.1.2 we know that allowing users to transmit packets multiple times before receiving feedback results in greater congestion. However, if the number of users with strict time deadlines is small, these performance losses may be tolerable to reduce the expected delay for strict time deadline users. Assuming that the arrival rate of strict time deadline packets to the channel is sufficiently small such that there is never more than one packet from a strict time deadline user in the system at any given time, the expected delay $E[T_w]$ for the strict time deadline user is:

$$E[T_w] = \left(E[N_S] + \frac{N_{RTT}}{1-(1-e^{-1})^{N_{Rep}}}\right) L_p T_b \quad , \tag{3.19}$$

where $N_S$ is a random variable modelling the number of transmission attempts required for a successful transmission given that a successful transmission occurs within the $N_{Rep}$ attempts. See Appendix B.3 for a derivation of this result. The expected value of $N_S$ is can be expressed as:

$$E[N_S] = \frac{1 - N_{Rep}e^{-1}(1-e^{-1})^{N_{Rep}} - (1-e^{-1})^{N_{Rep}}}{e^{-1} - e^{-1}(1-e^{-1})^{N_{Rep}}} \tag{3.20}$$

See Appendix B.3 for a derivation of this result A plot of the expected delay $E[T_w]$ for the strict time deadline user versus the number of transmissions $N_{Rep}$ by the strict time deadline user is given in Fig. 91.

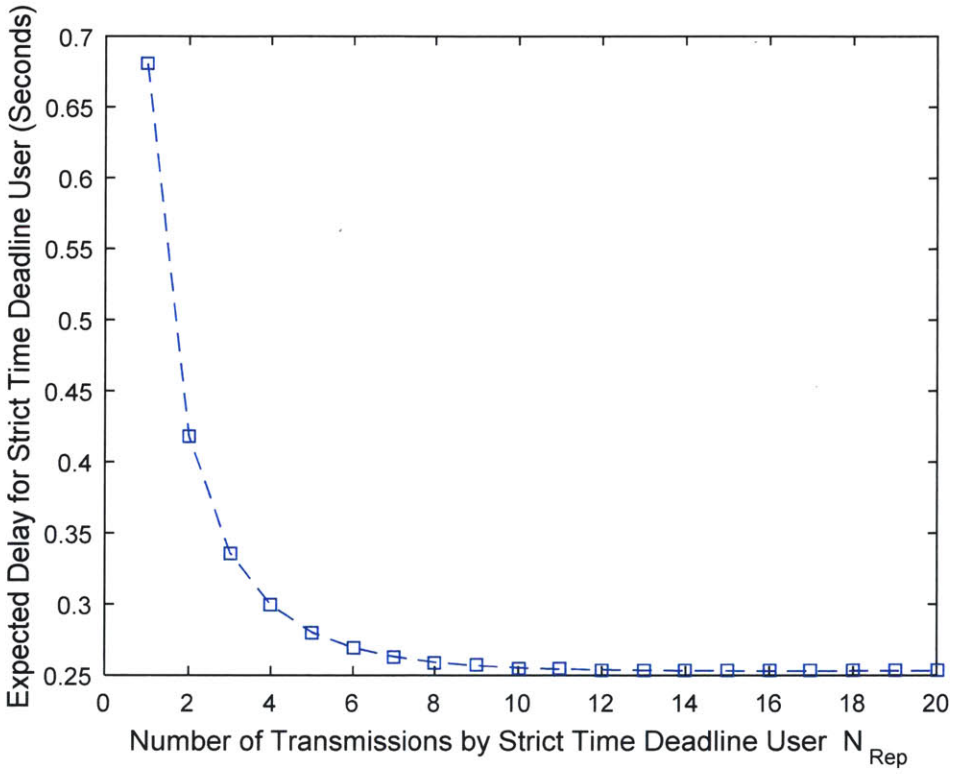


Fig. 91 Expected Delay for a Strict Time Deadline User versus Number of Transmissions

We see from Fig. 91 that the expected delay for the strict time deadline user asymptotically approaches the round trip time of the channel as the number of transmissions increases. This result makes intuitive sense since the expected delay can never be less than the time it takes a packet and its feedback to traverse the channel. We also see from Fig. 91 that the repeated transmission scheme can achieve significantly lower expected delay than the minimum expected delay of 0.6823 seconds achieved by the

random drop dual-class service scheme. Additionally, we see from Fig. 91 that increasing $N_{Rep}$ beyond 10 transmissions offers minimal performance gain as the expected delay is already close to its asymptotic limit.

Unfortunately, the lower expected delay achieved by the repeated transmission scheme comes at the cost of increased expected delay for the other users transmitting on the channel. Assuming that only one strict time deadline user is present on the channel at a time, and that $N_{RTT} > N_{Rep}$, the expected delay $E[T_w]$ for the other users is:

$$E[T_w] = \frac{e \cdot N_{RTT}(v + N_{RTT})L_p T_b}{N_{RTT} - N_{Rep}} \tag{3.21}$$

See Appendix B.3 for a derivation of this result. Note that (3.21) is similar in form to the expected delay given in (3.1), where the additional term $N_{RTT}/(N_{RTT} - N_{Rep})$ represents a reduction in throughput. This reduction in throughput is the result of transmissions from strict time deadline users colliding with transmissions from the other users. A plot of the minimum expected delay $E[T_w]$ for the other users versus the number of transmissions $N_{Rep}$ by the strict time deadline user is given in Fig. 92. Note that the minimum expected delay occurs when $v = 1$.

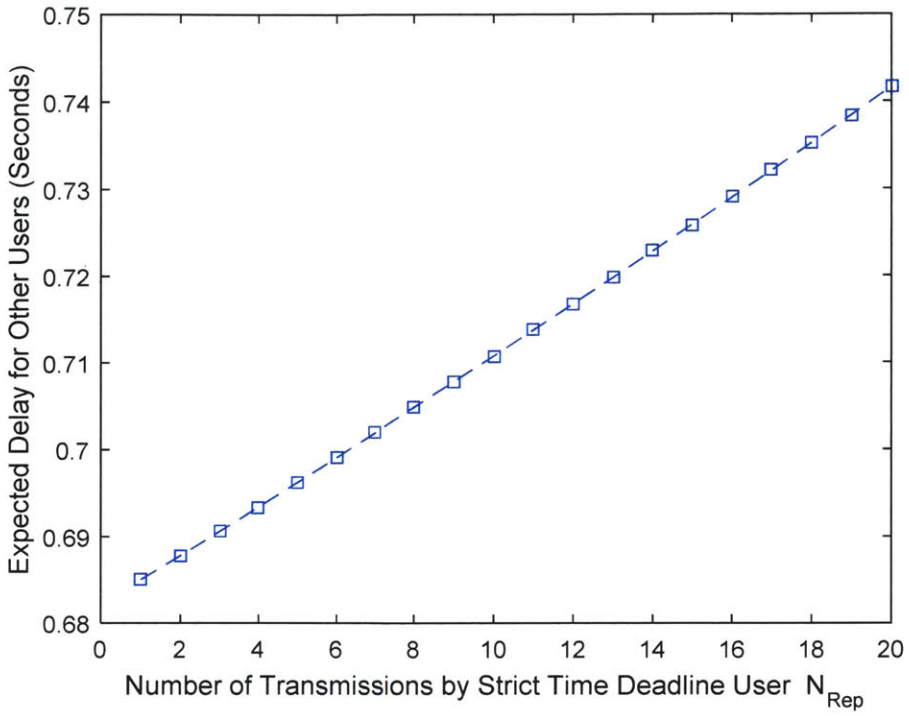


Fig. 92 Minimum Expected Delay for other Users versus Number of Transmissions by a Strict Time Deadline User

We see from Fig. 92 that the minimum expected delay for the other users on the ALOHA channel increases linearly with an increasing number of repeated transmissions by the strict time deadline user. However, for the case where $N_{Rep} = 10$, we see from (3.21) and Fig. 92 that the minimum expected delay for the other users is 0.7107 seconds, which is only a four percent increase in latency from the case where $N_{Rep} = 1$. Given that the expected delay for the strict time deadline user decreases from 0.6823 seconds when $N_{Rep} = 1$, to 0.2552 seconds when $N_{Rep} = 10$, a reduction of approximately 62.6 percent, the small increase in expected delay for the other users may be worth the significant reduction in expected delay for the strict time deadline user. It is important to remember that the results in Fig. 91 and Fig. 92 are developed under the assumption that the arrival rate of packets from strict time deadline users is sufficiently small such that only one packet from a strict time deadline user is present in the channel at any given time. Allowing even one additional packet from a strict time deadline user to be present in the

channel results in a nontrivial increase in expected delay for all users. Therefore, the repeated transmission scheme is only effective for very light traffic from strict time deadline users[10].

## 3.4 Summary

This chapter investigated the performance of a slotted ALOHA protocol using the Rivest Algorithm for a channel with long feedback delay. Section 3.1 outlined the implementation of the Rivest Algorithm and developed performance metrics for analyzing simulations of the ALOHA system. It was also shown in this section that the Rivest Algorithm using $\hat{\lambda} = e^{-1}$ is an effective method for maintaining system stability. Section 3.2 analyzed simulations of the ALOHA system for time-varying arrival rates in both supportable and congested conditions. The Rivest Algorithm was demonstrated to achieve high throughput, even during congested conditions, and to effectively clear congestion during sufficiently long periods of supportable traffic. Additionally, a technique for estimating the time required for a system to clear congestion was developed in this section. Section 3.3 discussed the requirement for dual-class service for priority users and a random drop dual-class service scheme. A technique for estimating the arrival rates of packets from normal and priority users was also developed in this section in order to detect when a random drop is necessary. Additionally, the performance of the random drop dual-class service scheme was simulated and demonstrated to be a reasonably effective means of implementing dual-class service. Finally, the implementation of a strict time deadline service using repeated transmissions was discussed and shown to only be effective for very light traffic from strict time deadline users.

[10] Note that multiple strict time deadline users could be better accommodated by allowing them to transmit on multiple noncontiguous time slots selected randomly in a single RTT.

# Chapter 4

# Physical Layer Defenses

This chapter considers attack vectors an adversary may pursue against the physical layer of DS/ALOHA SATCOM system and techniques to counter such attacks. Power robbing is the first attack method investigated and is shown to be highly effective against a SATCOM system acting as a simple relay. Power robbing is also shown to impose a limiting effect on the power advantage over an interferer that a system can provide to its users. Onboard signal processing is demonstrated to be an effective means of mitigating the effects of power robbing by an interferer. The next attack vector considered is a concentrated interference technique known as a pulsed interferer. The pulsed interferer is shown to be highly effective against an uncoded channel. Repeat coding is introduced as an effective means of mitigating the pulsed interferer. The last attack vector considered in this chapter is another concentrated interference technique that we call channel-selective interference. Channel-selective interference is shown to be effective against a system using repeat coding and a technique we call code switching is developed to mitigate this type of interference. Code switching's ease of implementation is also outlined.

## 4.1 Downlink Power Robbing

Downlink power robbing is a simple and effective interference technique that can be used against a SATCOM system acting as a relay between two ground stations. When serving as a relay, the satellite simply receives and retransmits whatever signals it receives. Since commercial SATCOM systems in this

configuration do not discriminate between where uplink signals originated, these systems are often hijacked by third parties to broadcast their own signals. An interferer can take advantage of the SATCOM system in a similar manner by broadcasting a very powerful signal to the satellite's receiver. Since the relay allocates power to its downlink signals proportionally, the interferer's powerful signal on the uplink can steal a significant portion of the system's downlink power. The power stolen by the interferer results in less downlink power being available for the retransmission of signals from legitimate users and can therefore lead to unacceptably high bit error rates.

An effective method to mitigate downlink power robbing is through onboard signal processing in a SATCOM system. By digitally processing signals before retransmission, the system can identify the interferer's signal and avoid retransmitting it. While onboard signal processing does come at the cost of added weight, expense, and power consumption, it is necessary to ensure that an interferer cannot steal power from the downlink. In order to quantify the performance gain from onboard signal processing, the next section analyzes the effect of an interferer on the bit error rates of a system configured as a simple relay and a system with onboard signal processing.

### 4.1.1 Performance Comparison of Signal Processing Schemes

In order to analyze the effects of an interferer on the system serving as a relay and the system with onboard signal processing, it is assumed that the underlying data signal is generated using binary phase-shift-keying (BPSK). Additionally, it is assumed that the interferer only transmits on the uplink channel, and that its signal power is spread uniformly over $W_{SS}$. Finally, it is assumed that the downlink channel from the SATCOM system has a finite amount of power available for transmission that is allocated proportionally based on the relative strengths of received signals.

Given these assumptions, the bit error rate for the system acting as a relay $P_{Rel}$ is equal to the bit error rate of the relay's downlink channel $P_{DR}$. For a BPSK signal, $P_{DR}$ can be expressed as [6]:

$$P_{DR} = Q\left(\sqrt{2 \cdot SNR_{DR}}\right) \ , \tag{4.1}$$

where $Q$ is the q-function and $SNR_{DR}$ is the downlink signal-to-noise ratio for the relay. Assuming that path loss is uniform among users and the interferer, that the ambient channel noise is the same at both the uplink and downlink receivers, and that co-channel interference is negligible, $SNR_{DR}$ can be expressed as:

$$SNR_{DR} = \frac{E_{sat}\left(\frac{E_{TX}}{(1-e^{-1})E_{TX}N_C + G_n^{-1}E_I}\right)G_{RX}F_P}{E_{sat}\left(\frac{G_n^{-1}E_I}{(1-e^{-1})E_{TX}N_C + G_n^{-1}E_I}\right)G_{RX}F_P G_p^{-1} + N_0 W_d} \ , \tag{4.2}$$

where $E_{sat}$ is the downlink EIRP of the SATCOM system and is assumed to have a value of 30 dBW. A derivation of (4.2) is given in Appendix C.1. Note that the numerator in (4.2) corresponds to the power allocated to the signals from legitimate users while the denominator corresponds to the power allocated to the interferer's signal plus ambient noise power.

Assuming that bit errors occur independently for the uplink and downlink channels of the system using onboard signal processing, the bit error rate for the system $P_{Proc}$ is related to the bit error rates of the uplink and downlink channels in the following manner:

$$P_{Proc} = 1 - (1 - P_{UP})(1 - P_{DP}) \ , \tag{4.3}$$

where $P_{UP}$ is the probability of a bit error on the uplink channel and $P_{DP}$ is the probability of a bit error on the downlink channel. Essentially, the expression in (4.3) states that the probability of a bit error occurring in the system is equal to the complement of the probability that no errors occur on either the uplink or downlink. The uplink and downlink channel error probabilities are:

$$P_{UP} = Q\left(\sqrt{2 \cdot SNR_{UP}}\right) \ , \tag{4.4}$$

$$P_{DP} = Q\left(\sqrt{2 \cdot SNR_{DP}}\right) \ , \tag{4.5}$$

where $SNR_{UP}$ and $SNR_{DP}$ are the signal-to-noise ratios of the uplink and downlink channels, respectively, for the system using onboard signal processing. Using the same assumptions for the relay case, $SNR_{UP}$ and $SNR_{DP}$ can be expressed as:

$$SNR_{UP} = \frac{E_{TX} G_{RX} F_p}{E_I G_{RX} F_p G_n^{-1} G_p^{-1} + N_0 W_d} \tag{4.6}$$

$$SNR_{DP} = \frac{E_{sat} G_{RX} F_p}{(1 - e^{-1}) N_C N_0 W_d} \tag{4.7}$$

See Appendix C.1 for a derivation of the expressions given above. Using the expressions developed for $P_{Rel}$ and $P_{Proc}$ in (4.1) and (4.3), the performance of the system acting as a relay and the system using onboard signal processing can be compared by plotting $P_{Rel}$ and $P_{Proc}$ versus the ratio of user EIRP to interferer EIRP. Using the same parameter values developed in Appendix A.1[11], along with a processing gain of 1023, a plot of $P_{Rel}$ and $P_{Proc}$ versus $E_{TX}/E_I$ for $N_C = 100$ is given in Fig. 93. Note that the results

[11] Note that a receiver gain of 72 dB is used to model a 10 m diameter antenna (a best case for the relay system).

in Fig. 93 are for the best case scenario where the interferer's signal experiences 20 dB of antenna nulling on the uplink.

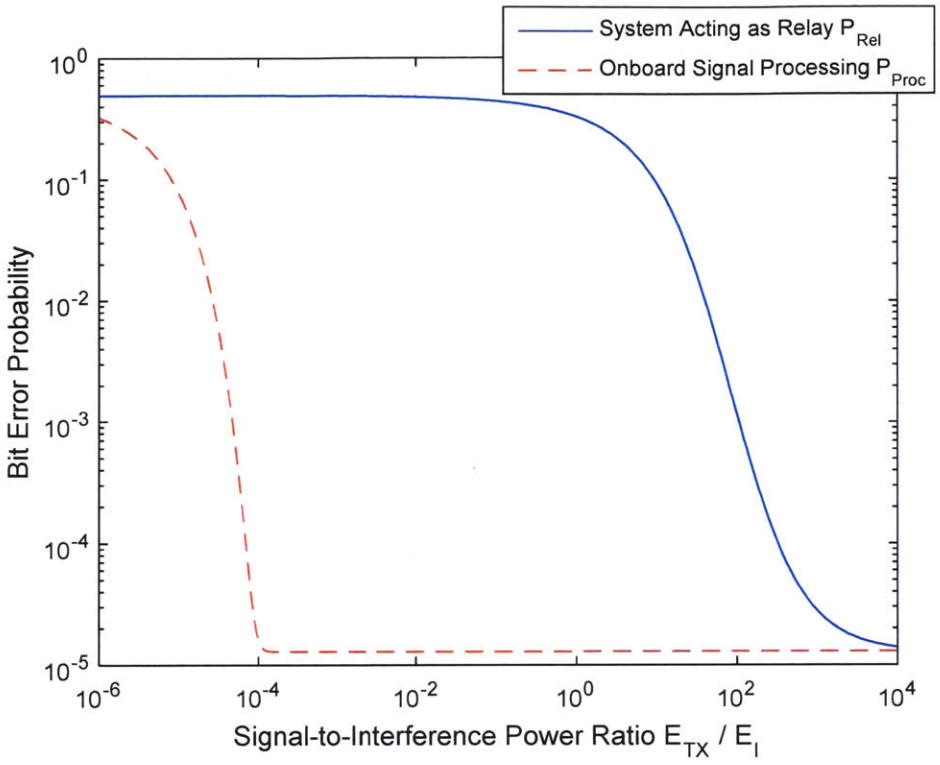


Fig. 93 Bit Error Probability Comparison with $N_C = 100$ for a System Serving as a Relay and a System Using Onboard Signal Processing

We see from Fig. 93 that there is approximately a 30 dB difference in the values of $E_{TX}/E_I$ at which $P_{Rel}$ and $P_{Proc}$ achieve the same bit error rate. In other words, the system with onboard signal processing can achieve the same bit error rate as the system acting as a relay with a signal-to-interference ratio that is 40 dB lower. This significant difference in bit error rates demonstrates that the relay system is highly susceptible to power robbing, and that the system with onboard signal processing is far more resilient to this kind of attack. It should be noted that the bit error rates plotted in Fig. 93 were developed under the assumption that a relatively low number of channels are supported by the SATCOM system. Since the DS/ALOHA system must be able to support a very large number of channels, it is also important to

understand how increasing the number of channels affects $P_{Rel}$ and $P_{Proc}$. A plot of $P_{Rel}$ and $P_{Proc}$ versus $E_{TX}/E_I$ for a greater number of channels ($N_C = 1000$) is given in Fig. 94.

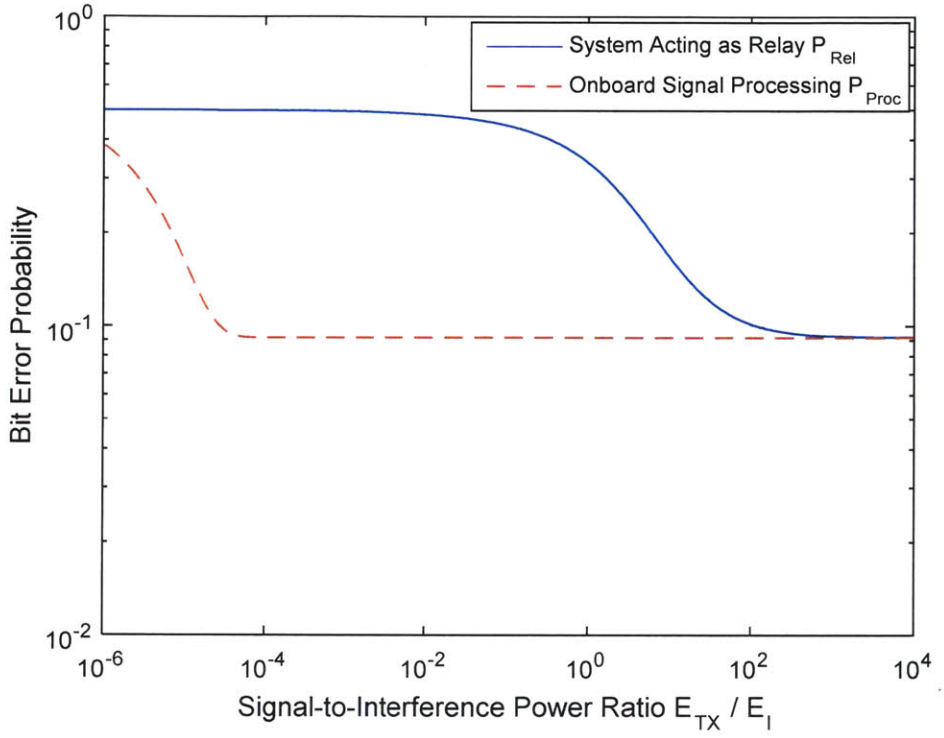


Fig. 94 Bit Error Probability Comparison with $N_C = 1000$ for a System Serving as a Relay and a System Using Onboard Signal Processing

We see from Fig. 94 that the system with onboard signal processing maintains a power advantage of approximately 30 dB over the system acting as a relay. Therefore, as the number of channels supported by the system increases, the system with onboard signal processing maintains a significant power advantage over the system acting as a relay. It should be noted that the minimum bit error rate achievable by both systems is unacceptably high in Fig. 94. This is due to the fact that error correcting code, which considerably reduces the bit error rate, is not included in the models developed in (4.1) through (4.7). Therefore, the ambient noise in the channel is able to impose an unacceptably high limit on the bit error rate achievable by the system. Thus, the primary purpose of Fig. 94 is to provide insight on the relative

difference in vulnerability to power robbing between a relay system and system with onboard signal processing rather than to determine the exact bit error rates achievable by a real system.

### 4.1.2 Limiting Effect of Power Robbing on Interference Mitigation

The negative effect of power robbing on the relay system also imposes a limit on the system's ability to mitigate interference. In order to understand this limiting behavior, it is first necessary to develop the interference-to-signal power ratio $I/S_{Req}$ required for a broadband interferer to cause an unacceptably high bit error rate. For this generic case, $I/S_{Req}$ can be expressed as:

$$I/S_{Req} = G_n \cdot \frac{W_{ss}/W_d}{E_b/N_T} \quad , \tag{4.8}$$

where $N_T$ is the total power spectral density of the interferer and ambient channel noise, and $E_b/N_T$ is the lowest tolerable bit-to-interference energy ratio. Note that it is assumed in (4.8) that the interferer is spreading its power evenly over $W_{ss}$. We see from (4.8) that increasing the processing gain $W_{ss}/W_d$ increases the amount of power required for an interferer to cause an unacceptably high bit error rate. Conversely, increasing $E_b/N_T$ decreases the amount of interferer power required to degrade the channel's bit error rate to an unacceptably high value. Increasing the bandwidth $W_{ss}$ over which the channel's data signal is spread results in a linear increase in $I/S_{Req}$ when $W_d$ and $E_b/N_T$ remain constant. In other words, the power advantage of a user over a broadband interferer can be increased without limit by increasing the spreading factor $W_{ss}/W_d$ of the signal.

For the case where power robbing is present in the system, the required interference-to-signal power ratio $I/S_{Rob}$ has the following form:

$$I/S_{Rob} = \frac{W_{ss}\left[E_{sat}F_pG_{RX} - (1-e^{-1})N_CW_dN_0(E_b/N_T)\right]}{G_n^{-1}(E_b/N_T)W_{ss}W_dN_0 + G_n^{-1}(E_b/N_T)W_dE_{sat}F_pG_{RX}} \tag{4.9}$$

See Appendix C.2 for a derivation of this result. Unlike the previous case, as $W_{ss}$ increases toward infinity the expression for $I/S_{Rob}$ given in (4.9) asymptotically approaches a limiting value $I/S_{Limit}$ instead of infinity. The limiting value $I/S_{Limit}$ is given by:

$$I/S_{Limit} = \frac{G_nE_{sat}F_pG_{RX}}{(E_b/N_T)N_0W_d} - G_n(1-e^{-1})N_C \tag{4.10}$$

See Appendix C.2 for a derivation of this limit. A plot of $I/S_{Req}$, $I/S_{Rob}$, and $I/S_{Limit}$ versus the spreading factor $W_{ss}/W_d$ is shown in Fig. 95.

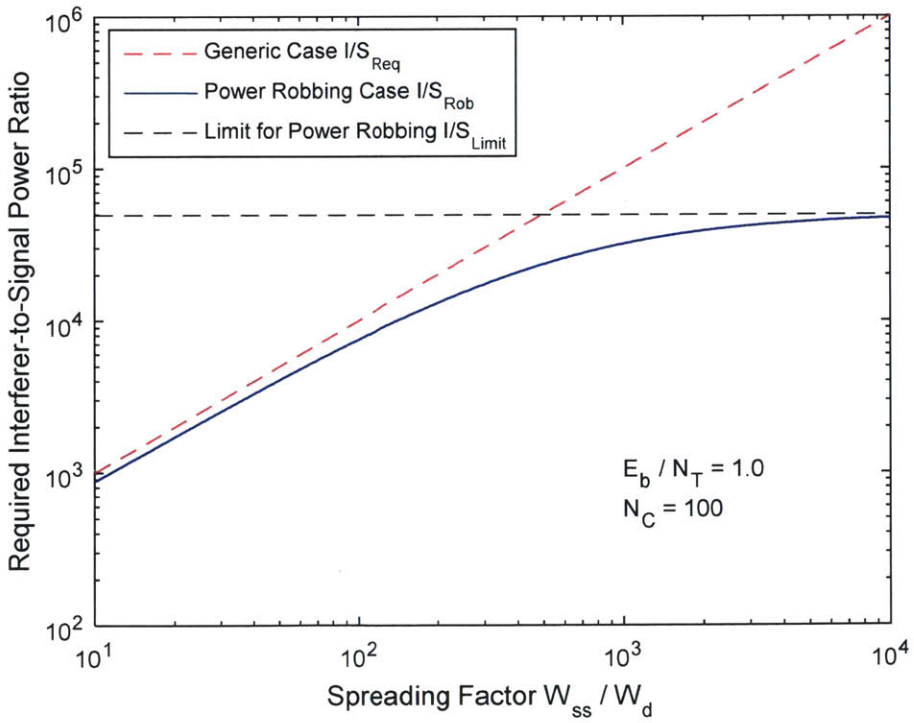


Fig. 95 Required Interferer-to-Signal Ratio versus Spreading Factor for Generic and Power Robbing Cases

Note that the values for $G_n$, $E_{sat}$, $F_p$, $G_{RX}$, $W_d$, and $N_0$ used in Fig. 95 are the same those values used in Section 4.1.1. The limiting effect of power robbing is clearly evident in Fig. 95. As the spreading factor increases beyond $10^2$, $I/S_{Rob}$ diverges away from $I/S_{Req}$ and asymptotically approaches $I/S_{Limit}$. Note that there is a difference of nearly 5 dB between the values of $I/S_{Req}$ and $I/S_{Rob}$ when the spreading factor is $10^3$. In this way, power robbing significantly degrades the power advantage of a user over an interferer for a system serving as a relay.

## 4.2 Concentrated Interference Attacks

In previous sections, it is assumed that the interferer uniformly spreads its power over $W_{ss}$ and broadcasts continuously in time. Such an interferer is known as a constant power broadband interferer [6]. Since the broadband interferer can be effectively mitigated through the use of spectrum spreading, an adversary may use a different transmission strategy which is more effective. Two possible strategies are concentrating the interferer's power in time, by pulsing its signal on and off, or concentrating its power in a specific subset of DS codes. The pulsed interference strategy is analyzed in Section 4.2.1 and is shown to be more effective in degrading the bit error rate of the channel than the constant power broadband interferer. The strategy of concentrating interference in a subset of DS codes is analyzed in Section 4.2.3 and is shown to have equivalent behavior to the pulsed interferer when the system does not change DS codes over the transmission of a single packet. Note that we call this strategy a channel-selective interferer. Since the constant power broadband interferer is effectively mitigated by spectrum spreading, techniques are developed in Sections 4.2.2 and 4.2.4 to reduce the effectiveness of the pulsed and channel-selective interference strategies to the same level as the constant power broadband interferer.

### 4.2.1 Uncoded Channel with Pulsed Interference

Similar to the constant power broadband interferer, the pulsed interferer spreads its power uniformly over the entire spread bandwidth $W_{ss}$. However, the pulsed interferer only transmits for a fraction of the time $\rho$. Assuming $P_I$ is the time-average power available to the interferer, transmitting for a fraction of the time allows the pulsed interferer to transmit with power $P_I/\rho$. Note that this signal power is greater than the power $P_I$ used by the constant power broadband interferer [6]. However, this increased transmission power comes at the cost of only being able to affect the channel for a fraction of the time. Assuming again that the channel is using BPSK as the underlying data modulation scheme, the bit error rate of the channel $P_b$ is [6]:

$$P_b = \rho Q\left(\sqrt{2 \cdot SNR(\rho)}\right) \ , \tag{4.11}$$

where it is assumed that the pulsed interferer either transmits for the entire duration of a bit period with probability $\rho$, or does not transmit for the entire duration of a bit period with probability $1-\rho$ [6]. It is also assumed that these probabilities are independent between different bit periods and that no bit errors occur when the interferer is not transmitting [6]. The signal-to-noise ratio from (4.11) is a function of $\rho$ and has the following form [6]:

$$SNR(\rho) = \frac{E_{TX} G_p G_n}{E_I} \rho \ , \tag{4.12}$$

where ambient channel noise is assumed to be negligible when an interferer is present. Note that the path loss $F_p$ and the receiver antenna gain $G_{RX}$ are assumed to be the same for the user's and the interferer's signals and therefore cancel out of the ratio. A plot of $P_b$ versus the signal-to-interference ratio $E_{TX}/E_I$ for $G_p = 1023$, $G_n = 100$, and various values of $\rho$ is given in Fig. 96. Noting that the case

where $\rho = 1$ is equivalent to the constant power broadband interferer, we see from Fig. 96 that there exist pulse rates $\rho \neq 1$ that yield significantly worse values of $P_b$ for a given value of $E_{TX}/E_I$ than the constant power broadband interference strategy. For example, $E_{TX}/E_I$ must be roughly 17 dB higher to achieve a bit error rate of $10^{-6}$ when $\rho = 0.01$ than when $\rho = 1$. In other words, $P_I$ can be 17 db lower for an interferer to successfully increase the bit error rate above $10^{-6}$ if it pulses its transmissions with rate $\rho = 0.01$ than when it continuously transmits. Thus, a pulsed interferer is a far more effective strategy for an adversary than the constant power broadband interferer.

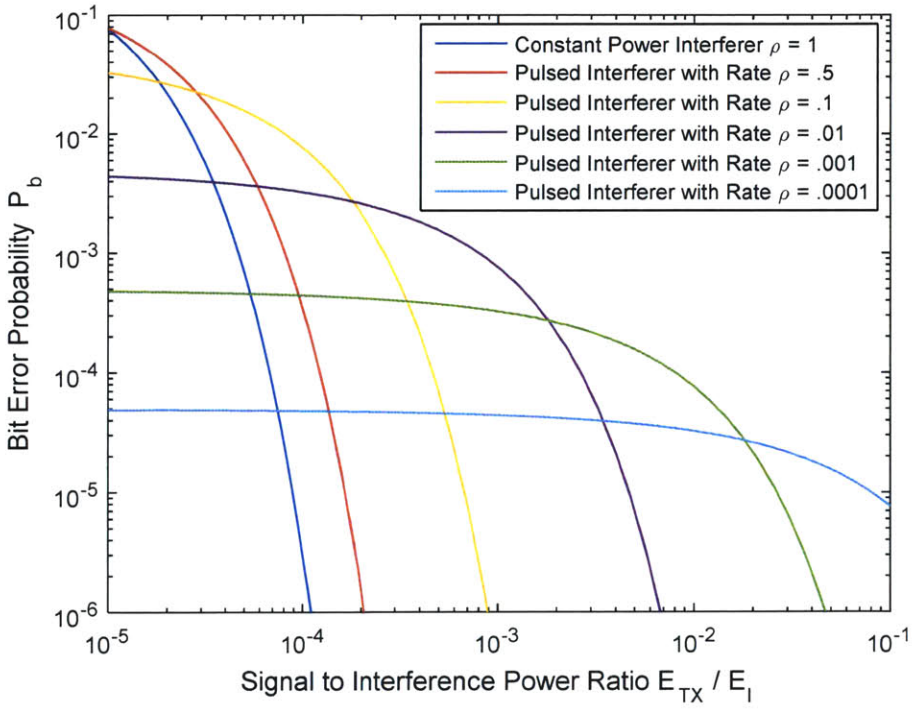


Fig. 96 Bit Error Probability for Pulsed Interferer on Uncoded Channel

To understand the maximum effectiveness of a pulsed interferer against an uncoded channel, the optimal choice of $\rho$ for every value of $E_{TX}/E_I$ is developed in [6] by differentiating (4.11) with respect to $\rho$. The optimal $\rho^*$ is shown to be [6]:

$$\rho^* = \begin{cases} \dfrac{0.709}{E_{TX}G_pG_n/E_I} & for \;\; E_{TX}G_pG_n/E_I > 0.709 \\ 1 & for \;\; E_{TX}G_pG_n/E_I \leq 0.709 \end{cases} \tag{4.13}$$

A plot of the bit error rate versus $E_{TX}/E_I$ for the constant power broadband interferer ($\rho = 1$) and a pulsed interferer with $\rho = \rho^*$ is given in Fig. 97.

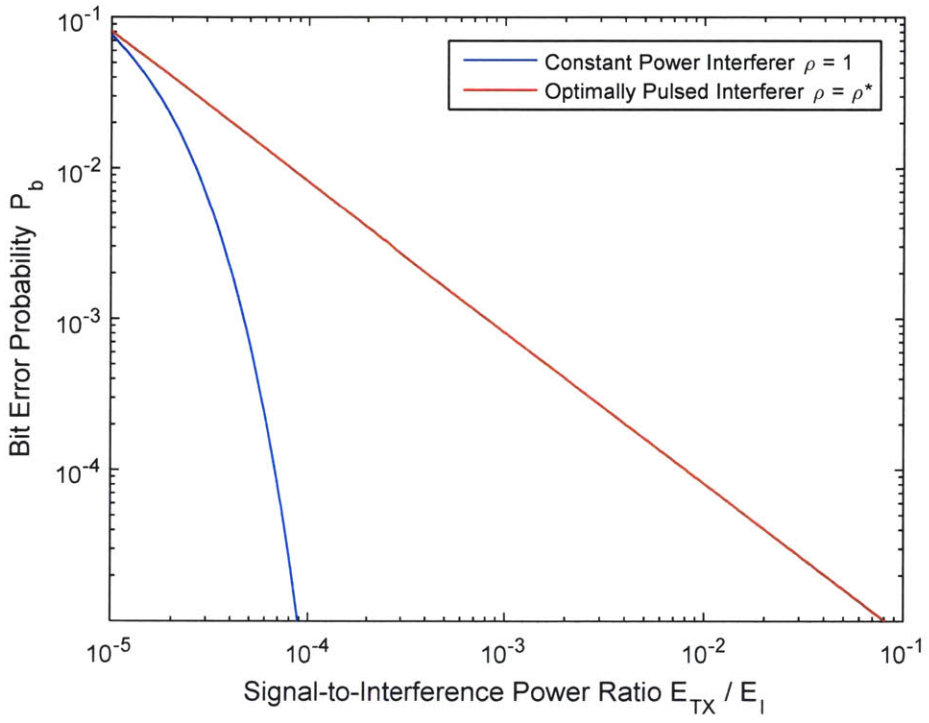


Fig. 97 Bit Error Probability Comparison for Constant Power and Optimally Pulsed Interferers

We see from Fig. 97 that there is nearly a 30 dB difference between the values of $E_{TX}/E_I$ required to achieve a bit error rate of $10^{-6}$ for the constant power broadband interferer and the interferer using the optimal pulse rate. Given this significant difference in the interference strategies' ability to degrade the channel, it is evident that the pulsed interference case must be addressed if the SATCOM system is to be considered robust.

### 4.2.2 Coded Channel with Pulsed Interference

A simple coding scheme known as repeat coding can mitigate the effectiveness of a pulsed interferer. Under the repeat coding scheme, each transmitted bit is divided into an odd number of symbols $m$, each with symbol period $T_b/m$ and power $E_{TX}/m$ [6]. The transmitted symbols also have the same value as their corresponding data bit. Thus, repeat coding is essentially transmitting the same bit $m$ times with each transmission having $1/m$ of the power and $m$ times the rate as the transmitted bit. Even though the symbol rate is $m$ times faster than the bit rate, it is shown in [6] that this does not result in a larger required signal bandwidth due to the DS spreading technique being used. If the symbols are interleaved, the probabilities that symbols from the same data bit are affected by the interferer are independent. The probability of a symbol error $\varepsilon$ for a transmission with interleaved symbols is [6]:

$$\varepsilon = \rho Q\left(\sqrt{2 \cdot SNR(\rho)}\right) \tag{4.14}$$

Note that it is assumed that no symbol errors occur when the interferer is not transmitting. The signal to noise ratio in (4.14) has the form:

$$SNR(\rho) = \frac{E_{TX} G_p G_n}{m E_I} \rho \tag{4.15}$$

Thus, the probability of a symbol error under the repeat coding scheme has the same form as the probability of a bit error for the uncoded channel, except that the SNR for the repeat coding scheme is worse by a factor of $1/m$. While this result does not appear to show any improvement over the uncoded channel, the advantage of the repeat coding scheme is that some of a data bit's transmitted symbols may be received while the interferer is not transmitting. If a hard decision decoder is used, where the receiver

makes a decision on each symbol's value individually, the probability of a bit error for the repeat coding scheme is [6]:

$$P_b = \sum_{i=(m+1)/2}^{m} \binom{m}{i} \varepsilon^i (1-\varepsilon)^{m-i} \quad , \tag{4.16}$$

where a bit error occurs if more than half of its symbols are received incorrectly. Note that this is why $m$ is defined as an odd integer in order to avoid the ambiguous case where exactly of the symbols are received incorrectly. The requirement that the interferer must degrade at least half of the transmitted symbols in order to cause an error is the principle advantage of the repeat coding scheme over the uncoded channel. A plot of $P_b$ for the repeat coding scheme versus $E_{TX}/E_I$ for $G_p = 1023$, $G_n = 100$, $m = 9$, and various values of $\rho$ is given in Fig. 98.

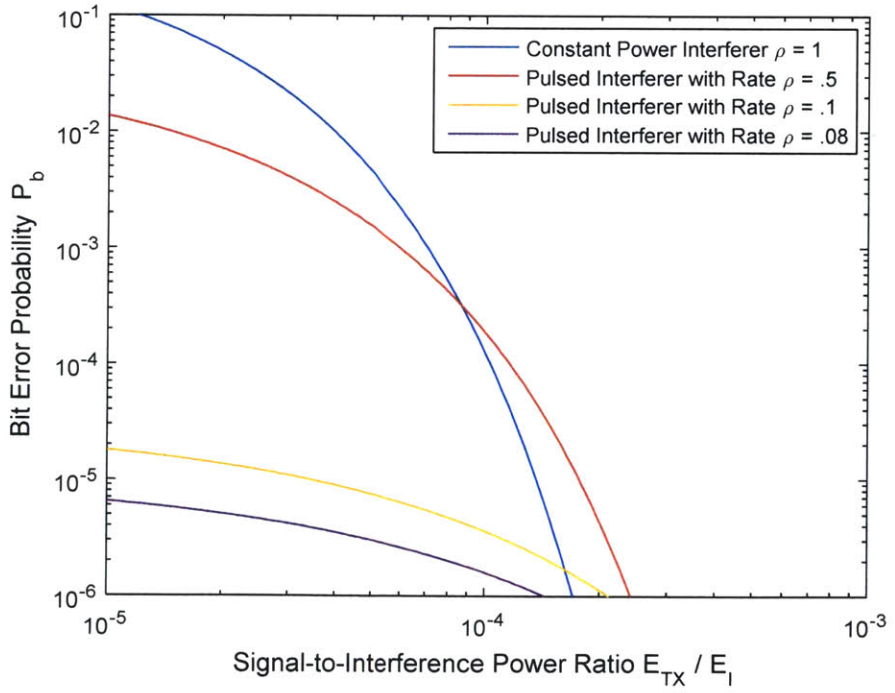


Fig. 98 Bit Error Probability for Pulsed Interferer on a Channel with $m = 9$ Repeat Coding

Note that the smaller values of $\rho$ from Fig. 96 have been excluded from Fig. 98 since these pulse rates have a significantly smaller effect on the coded channel than the constant power broadband interferer. We see from Fig. 98 that the use of $m = 9$ repeat coding on the channel significantly reduces the effectiveness of the pulsed interferer. The value of $E_{TX}/E_I$ required by the system to achieve a bit error rate of $10^{-6}$ for the case with a pulsed interferer with rate $\rho = 0.5$ is only 2 dB greater than the case with a constant power interferer. Thus, the impact of a pulsed interferer on the channel has been reduced to nearly the same effectiveness as the constant power broadband interferer. It should be noted that there are more effective coding techniques than the $m = 9$ repeat coding scheme used in this example. Repeat coding is chosen for its simplicity in order to illustrate how coding can reduce the effectiveness of a pulsed interferer.

### 4.2.3 Channel-Selective Interference

Another attack strategy that an interferer may use is to concentrate its power in specific DS codes. Since different codes correspond to different channels, this type of interferer will be referred to as a channel-selective interferer. It is assumed for now that users transmit on the same DS code for an entire time-slot. If the interferer transmits with equal power on a fraction $\alpha$ of all possible DS codes, the user will transmit on a channel affected by the interferer with probability $\alpha$, and will transmit on a channel free of interference with probability $1 - \alpha$. In this case, repeat coding and interleaving do not offer any advantage to the user because the interferer either affects all or none of the transmitted symbols for a data bit, depending on whether or not the user is transmitting on the same channel as the interferer. Assuming that no bit errors occur when a user transmits a packet on a clear channel, the probability of a bit error is:

$$P_b = \alpha Q\left(\sqrt{2 \cdot SNR(\alpha)}\right) \ , \tag{4.17}$$

where the signal-to-noise ratio in (4.17) is a function of $\alpha$:

$$SNR(\alpha) = \frac{E_{TX} G_p G_n}{E_I} \alpha \tag{4.18}$$

Note that in (4.18) the user has lost the power advantage afforded by the processing gain because the interferer is spreading its signal in the same manner as the user, with its power evenly divided among the $\alpha G_p$ channels it is transmitting on. We see from (4.17) and (4.18) that the bit error probability for the channel-selective interferer has the same form as the case where an uncoded channel is subjected to a pulsed interferer. It is shown in [6] that repeat coding has approximately the same bit error rate as the uncoded channel when all symbols are transmitted in the presence of an interferer. Therefore, the bit error probability given for the uncoded channel in (4.17) is approximately the same for the case where repeat coding is used. Given the duality between the channel-selective interferer and the pulsed interferer on an uncoded channel, the optimal fraction of DS codes $\alpha^*$ for the interferer to transmit on is then:

$$\alpha^* = \begin{cases} \dfrac{0.709}{E_{TX} G_p G_n / E_I} & for \ \ E_{TX} G_p G_n / E_I > 0.709 \\ 1 & for \ \ E_{TX} G_p G_n / E_I \leq 0.709 \end{cases} \tag{4.19}$$

As in the pulsed interferer case, the effectiveness of the channel-selective interferer is compared against the effectiveness of the constant power broadband interferer ($\alpha = 1$). A plot of the bit error rate versus the signal-to-interference power ratio $E_{TX}/E_I$ for the constant power broadband interferer and a channel-selective interferer with $\alpha = \alpha^*$ is given in Fig. 99. We see from Fig. 99 that there is a difference of almost 25 dB in the values of $E_{TX}/E_I$ required to achieve a bit error rate of $10^{-6}$ for the constant power

broadband interferer and the optimal channel-selective interferer. Thus, the channel-selective interferer can achieve a significantly worse bit error probability than the constant power broadband interferer for equivalent values of $E_{TX}/E_I$. Note that these results are based on the assumption that the interferer can synthesize and transmit signals simultaneously on the desired fraction of channels $\alpha$. Given that the cross-correlation of DS codes is low, but is not zero, it is likely that this assumption is impractical as $\alpha$ approaches a large fraction of channels because the interferer's transmissions will cancel out significant portions of one another.

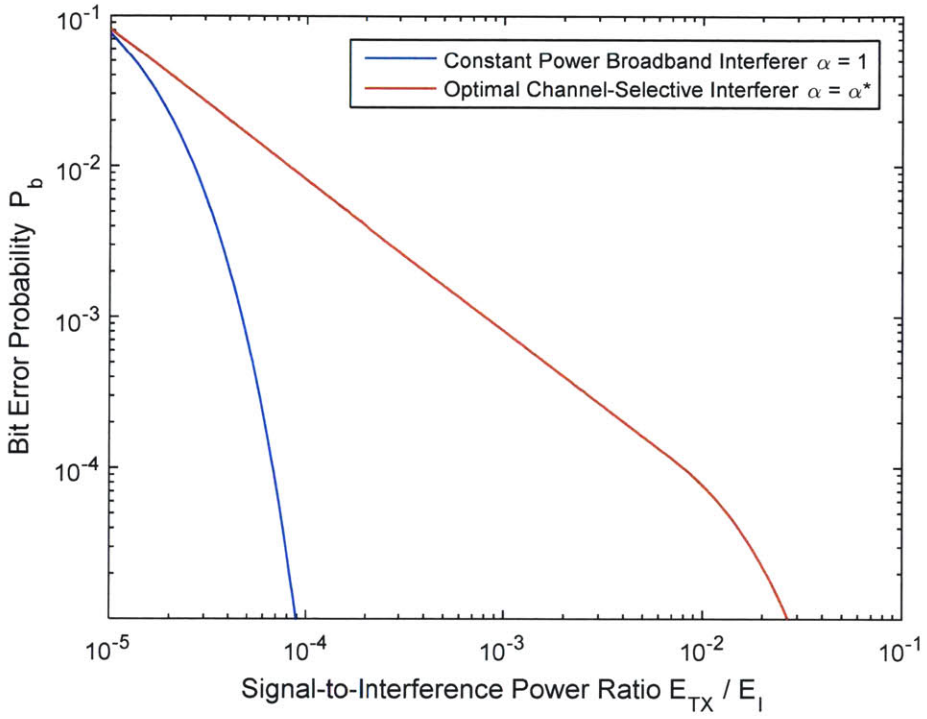


Fig. 99 Bit Error Probability Comparison for Optimal Channel-Selective and Broadband Interferers

Since the results in Fig. 99 can be achieved by the channel-selective interferer when repeat coding is used, an additional system modification is required to mitigate the effects of this interference scheme. The following section develops a technique called code switching to address the channel-selective interferer's threat to the SATCOM system.

### 4.2.4 Channel-Selective Interference with Code Switching

The primary vulnerability of a channel to a channel-selective interferer is that either all, or none, of a bit's symbols are affected by the interferer. As was seen with repeat coding and the pulsed interferer, if the symbols' probability of being affected by the interferer can be made independent with probability $\alpha$, the effectiveness of the interferer can be significantly reduced. Therefore, it is necessary to develop a modification to the system that prevents an interferer from easily affecting the entire transmission of a packet. A simple means of achieving independent probabilities that symbols are affected by the interferer is to change which DS code the system is using after a fixed number of bit periods $N_B$. If the repeated symbols for data bits are interleaved over the entire packet length $L_p$, then a single bit can have up to $L_p/N_B$ symbols whose probabilities of being affected by an interferer are independent. These independent probabilities are achieved by transmitting a symbol from the same data bit over each of the $L_p/N_B$ different DS codes used in the transmission. The technique of switching DS codes over the course of a single transmitted packet will be referred to as code switching. If code switching is used, then the probability of a symbol error is:

$$\varepsilon = \alpha Q\left(\sqrt{2 \cdot SNR(\alpha)}\right) \tag{4.20}$$

Note that it is assumed that no symbol errors occur when the interferer is not present on the channel. The signal to noise ratio in (4.20) has the form:

$$SNR(\alpha) = \frac{E_{TX} G_p G_n}{m E_I} \alpha \tag{4.21}$$

Using a hard decision decoder, the bit error probability has the same form as the channel with repeat coding subjected to a pulsed interferer:

$$P_b = \sum_{i=(m+1)/2}^{m} \binom{m}{i} \varepsilon^i (1-\varepsilon)^{m-i} \tag{4.22}$$

We see from (4.20), (4.21), and (4.22) that code switching allows the channel to take full advantage of repeat coding to achieve a bit error probability with the same form as the case where repeat coding is used to mitigate a pulsed interferer.

If code switching with $N_B = 100$ bit periods per DS code change is used with a packet length of $L_p = 1000$ bits, then the channel can support up to 10 repeated symbols per transmitted bit that will each have an independent probability $\alpha$ of being affected by the channel-selective interferer. Thus, repeat coding with $m = 9$ symbols can be applied to the channel[12]. A plot of $P_b$ for the repeat coding scheme versus $E_{TX}/E_I$ for $G_p = 1023$, $G_n = 100$, $m = 9$, and various values of $\alpha$ is given in Fig. 100. We see from Fig. 100 that the addition of code switching to the channel significantly reduces the effectiveness of the channel-selective interferer. The value of $E_{TX}/E_I$ required to achieve a bit error probability of $10^{-6}$ for the channel selective interferer with rate $\alpha = 0.5$ is now only 1.5 dB above the required value for the constant power broadband interferer ($\alpha = 1$). Thus, the introduction of code switching is an effective strategy to mitigate a channel-selective interferer.

Another benefit of DS code switching is that it is fairly easy to implement in a system. Since the system's DS code sequence is changed periodically, but not its timing, the receiver does not need to reacquire the signal each time the DS code is changed. Thus, the phase and timing of the signal lock are unaffected by switching which DS code is being used by the system [6].

[12] Note that $m = 9$ repeat coding is used even though up to 10 symbols are supported by code switching since $m$ must be an odd integer.

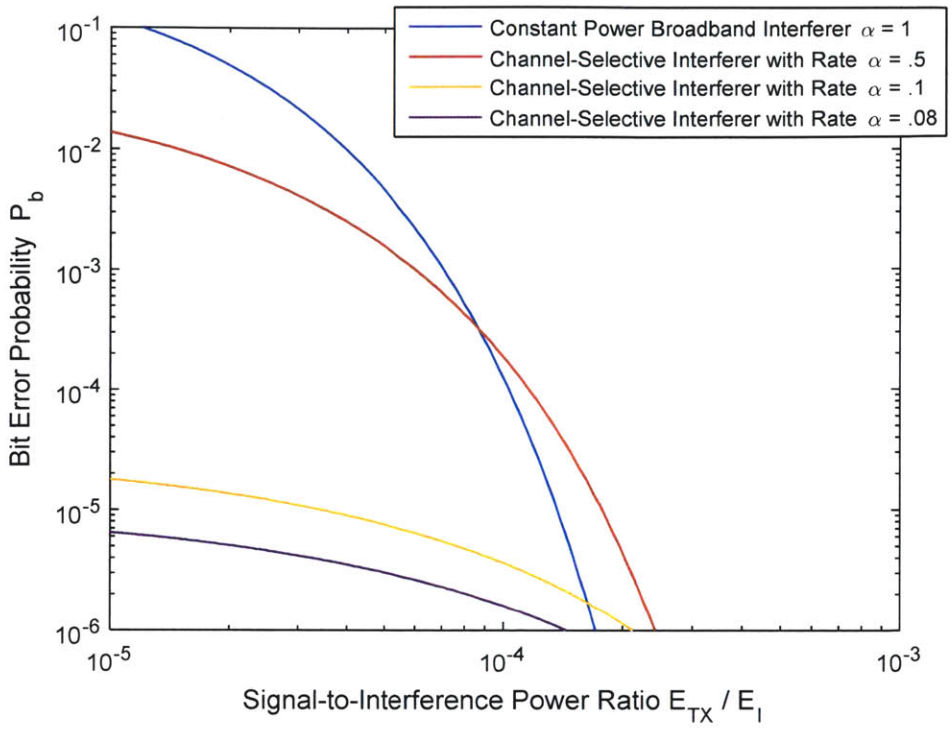


Fig. 100 Bit Error Probability for Channel-Selective Interferer with Code Switching

## 4.3 Summary

This chapter explored possible attacks an adversary may use against the DS/ALOHA system at the physical layer and techniques to mitigate them. Section 4.1 outlined the power robbing interference strategy and how it can be used against a relay system to significantly degrade channel quality. Power robbing was also shown to impose a limiting effect on the system's ability to provide a power advantage over an interferer to its users. Finally in this section, the inclusion of onboard signal processing was demonstrated to effectively mitigate the power robbing attack. Section 4.2 explored concentrated interference attacks in the form of pulsed and channel-selective interferers. Repeat coding was shown to be an effective mitigation technique against a pulsed interferer. Additionally, code switching was shown to be required in order to effectively mitigate the effects of a channel-selective interferer.

# Chapter 5

# MAC Layer Defenses

This chapter considers attacks an interferer may use against the MAC layer of the DS/ALOHA system and develops techniques for mitigating these attacks. The channel-selective interference strategy is reexamined in this chapter from a MAC layer perspective. A modified version of the Rivest Algorithm is developed to achieve close to the maximum throughput allowed by the channel-selective interferer and is shown to achieve better throughput and congestion clearing than the original algorithm. Next, the introduction of code switching to the channel is shown to improve the system's ability to mitigate the channel-selective interferer. Finally, a collision-spoofing interferer is considered and is shown to be mitigated by code switching.

## 5.1 Modified Rivest Algorithm with Channel-Selective Interference

In this section, we again consider a channel-selective interferer that transmits on each time slot with probability $\alpha$. We assume that code switching is not used by the system and that the interferer transmits with the same power as a legitimate user. Under these conditions, the interferer behaves as a malicious user who transmits with fixed probability $\alpha$, regardless of the transmission probability broadcast by the system. Thus, the interferer will cause additional collisions and congestion in the channel, resulting in a degradation in throughput. The additional collisions observed by the channel will also cause the Rivest Algorithm to overestimate the number of packets in the system, since the satellite cannot differentiate

between collisions involving only legitimate users and collisions caused by the interferer. Therefore, in order to achieve as high a throughput as the interferer will allow, it is necessary to develop a modified version of the Rivest Algorithm that takes the interferer's behavior into account when updating its estimate $v$ of the number of packets in the system.

### 5.1.1 Maximum Achievable Throughput with Interference

Before developing the modified Rivest Algorithm, it is important to understand what the maximum achievable throughput $\Gamma_{max}$ is when a channel-selective interferer is present in the system. Assuming that each legitimate packet in the system originates from a different user and that the total transmission rate for all legitimate packets in the system can be approximated as a Poisson process with rate $G$, the departure rate of packets from the system $\Gamma$ is:

$$\Gamma = (1-\alpha)Ge^{-G} \quad , \tag{5.1}$$

where each time slot has a probability of $1-\alpha$ of being free of transmissions from the interferer. Noting that the departure rate from the system is equivalent to throughput, $\Gamma$ is also the system throughput in packets per time slot. The maximum achievable throughput $\Gamma_{max}$ in the presence of a channel selective interferer is obtained by optimizing (5.1) with respect to the total packet transmission rate $G$. Differentiating (5.1) with respect to $G$ results in an optimal value of $G^* = 1$. Substituting $G^*$ into (5.1) yields the following expression for $\Gamma_{max}$:

$$\Gamma_{max} = (1-\alpha)e^{-1} \tag{5.2}$$

The effect of the channel-selective interferer on the DS/ALOHA channel is readily apparent in (5.2). As the probability $\alpha$ of a time slot containing a transmission by the interferer increases, $\Gamma_{max}$ decreases linearly

and reaches a value of zero at $\alpha = 1$. Thus, a channel-selective interferer that is able to achieve a high interference rate $\alpha$ can significantly degrade system throughput below $e^{-1}$. It should be noted that the modified Rivest Algorithm developed in the following section cannot recover the throughput lost to the additional congestion caused by the channel selective interferer, but can ensure that the system is operating as close to $\Gamma_{max}$ as possible.

### 5.1.2 Derivation of Feedback Parameters for Modified Algorithm

A modified Rivest Algorithm is developed using the same pseudo-Bayesian method used to develop the original algorithm [4]. It is assumed that some form of authentication is used so that a transmission by the interferer that occurs on a hole slot is not misinterpreted as a success by the system. Given these assumptions, the interferer has no effect on hole slots. Such authentication can be achieved by embedding a code in each user packet that is unknown to the interferer. Collision slots are also unaffected by interferer transmissions because the Rivest Algorithm is unconcerned with how many users were involved in a collision. Thus, the only way the channel-selective interferer affects the system is when it transmits on a time slot containing a single transmission from a legitimate user. This "success" slot becomes a collision slot due to the interferer's transmission and results in the legitimate user having to attempt to transmit its packet again on another time slot.

Following the pseudo-Bayesian method, the distribution $P_v(n)$ of the number of packets in the system $N$ is approximated as a Poisson distribution with mean $v$:

$$P_v(n) = \frac{v^n e^{-v}}{n!} \tag{5.3}$$

Assuming that there are $N$ packets in the system that are each transmitted with probability $q$ on the current time slot, the probability of a hole $H_q(N)$ is:

$$H_q(N) = (1-q)^N \tag{5.4}$$

We see from (5.4) that the interferer has no effect on the probability of a hole due to our assumption that legitimate users can be authenticated by the system. The probability of a success $S_q(N)$ for a system with $N$ packets is:

$$S_q(N) = (1-\alpha)\binom{N}{1} q(1-q)^{N-1} \ , \tag{5.5}$$

where a success occurs if and only if one user transmits during the time slot and the interferer does not transmit. The probability of a collision $C_q(N)$ for a system with $N$ packets is:

$$C_q(N) = 1 - H_q(N) - S_q(N) \ , \tag{5.6}$$

where a collision occurs if two or more users transmit during the time slot or if a single user and the interferer both transmit. Using the results from (5.3) through (5.6), the unnormalized distributions for $N$ given a hole, success, and a collsion during the current slot are, respectively:

$$P_v(n) \cdot H_q(n) = e^{-vq} \cdot P_{vw}(n) \tag{5.7}$$

$$P_v(n) \cdot S_q(n) = (1-\alpha)vq \cdot e^{-vq} \cdot P_{vw}(n-1) \tag{5.8}$$

$$P_v(n) \cdot C_q(n) = P_v(n) \cdot \left[1 - H_q(n) - S_q(n)\right] \ , \tag{5.9}$$

where $w = 1 - q$. See Appendix D.1 for a derivation of these distributions. Normalizing each distribution given above to obtain the final distributions for $N$ given a hole, a success, or a collision:

$$P_{N|H}(n) = P_{vw}(n) \ , \tag{5.10}$$

$$P_{N|S}(n) = P_{vw}(n-1) \ , \tag{5.11}$$

$$P_{N|C}(n) = \frac{P_v(n) \cdot \left[1 - H_q(n) - S_q(n)\right]}{1 - e^{-vq} - (1-\alpha)vq \cdot e^{-vq}} \ , \tag{5.12}$$

where $P_{N|H}(n)$ is the final distribution of $N$ given that a hole is observed on the most recent time slot, $P_{N|S}(n)$ is the final distribution of $N$ given that a success is observed, and $P_{N|C}(n)$ is the final distribution of $N$ given that a collision is observed. See Appendix D.1 for a derivation of these distributions. Noting that $P_{N|H}(n)$ and $P_{N|S}(n)$ have the same form as the final Poisson distributions derived in [4] for the original Rivest Algorithm, the appropriate change to $v$ given that a hole or success is observed is to decrement $v$ by one, as is done in the original Rivest Algorithm. This result makes intuitive sense since hole slots are unaffected by the interferer due to authentication and the number of packets in the system decreases by one when a success occurs (excluding new arrivals).

Similar to the collision case in [4], $P_{N|C}(n)$ does not simplify to a Poisson distribution. Instead, it can be approximated as a Poisson distribution with the same mean as the distribution in (5.12). Taking the expectation of the distribution in (5.12) yields:

$$E[N|C] = \frac{v(\alpha + e^{vq} + q - 2)}{e^{vq} - 1 - (1-\alpha)vq} \tag{5.13}$$

Assuming that $q = 1/v$ and that $v \geq 1$, the expression in (5.13) simplifies to:

$$E[N|C] = v + \frac{1}{e - 2 + \alpha} \tag{5.14}$$

See Appendix D.1 for a derivation of the results in (5.13) and (5.14). From (5.14) we see that the estimated number of packets in the system $v$ should be incremented by the constant value $(e - 2 + \alpha)^{-1}$ when a collision is observed. Noting that the incremental value $(e - 2 + \alpha)^{-1}$ decreases with increasing probability of the interferer being present in the channel $\alpha$, this result can be interpreted as attributing a fraction of the collisions observed by the system to the interferer rather than to congestion among the users. Since the probability of the interferer being present in the channel influences the increment of $v$ when a collision is observed, it will be necessary for the system to have a means of estimating $\alpha$ (see the next section). Given the results in (5.10), (5.11), and (5.14), the modified Rivest Algorithm can be formulated as a protocol where the system maintains an estimate of the current number of packets in the system $v$, and during each slot,

- users with packets to send transmit with probability $q = 1/v$;
- the system decrements $v$ by 1 if a hole or success is observed on the most recent slot, and increments $v$ by $(e - 2 + \hat{\alpha})^{-1}$ if a collision is observed on the most recent slot (where $\hat{\alpha}$ is an estimate of the interferer's transmission rate);
- the system sets $v$ to $max\{v + \hat{\lambda}, 1\}$, where $\hat{\lambda}$ is the estimated user arrival rate and is chosen to be the constant value $e^{-1}$ based on the results in [18].

### 5.1.3 Estimating Interferer Transmission Rate

In order to estimate the probability of the interferer being present on a time slot $\alpha$, the system observes the outcomes of the most recent $N_{obv}$ slots and counts the number of holes $N_h$. From the set of hole slots observed, the system counts the number of hole slots that contain an unauthenticated transmission from the interferer. Given that $N_h$ hole slots were observed in the most recent $N_{obv}$ slots where an interferer is transmitting with constant rate $\alpha$, the probability of observing $N_\alpha$ hole slots where the interferer transmitted is:

$$P_{N_\alpha|N_h \cap \alpha}(n_\alpha) = \binom{N_h}{n_\alpha} \alpha^{n_\alpha}(1-\alpha)^{N_h - n_\alpha} \quad , \tag{5.15}$$

where it is assumed that all unauthenticated transmissions originate from the interferer. Since the distribution of the interferer's transmission rate is unknown to the system, the value of $\alpha$ can be estimated by maximizing (5.15) with respect to $\alpha$ according to the maximum likelihood hypothesis test. Differentiating (5.15) with respect to $\alpha$ results in an optimal value of $\alpha^* = n_\alpha / N_h$ (see Appendix D.2 for a derivation of this result). Thus the estimate of $\alpha$ for the most recent $N_{obv}$ slots observed should be set to $\hat{\alpha} = N_\alpha / N_h$ to maximize the probability of correctly choosing $\hat{\alpha}$. The technique for estimating the rate at which the interferer affects time slots $\alpha$ can be summarized as:

- observing the outcomes of the most recent $N_{obv}$ slots;
- identifying the set and total number of slots that contain a hole $N_h$;
- counting the number of slots that contain an unauthenticated transmission from the set of hole slots $N_\alpha$;
- estimating the interferer's transmission rate as $\hat{\alpha} = N_\alpha / N_h$.

Note that the estimation of the interferer's rate is also an estimation of the interferer's transmission power, since the rate at which the interferer can affect the channel is governed by its effective isotropic radiated power (EIRP). For a satellite system using a spread-spectrum technique like direct sequence coding, the interferer's EIRP $E_I$ is related to its rate $\alpha$ by:

$$\alpha = \frac{E_I W_d}{E_{TX} W_{ss} G_n} \quad , \tag{5.16}$$

where $E_{TX}$ is the transmission EIRP used by legitimate users, $W_d$ is the data signal bandwidth, $W_{ss}$ is the spread-spectrum bandwidth, and $G_n$ is the power advantage of a user over the interferer due to antenna nulling. Note that it is assumed in (5.16) that the interferer's signal experiences the same path loss as signals from legitimate users.

The choice of the number of slots $N_{obv}$ to include in the estimation of $\alpha$ involves a tradeoff between accuracy and responsiveness. If the interferer abruptly changes the rate at which it affects the channel, the system will have to wait for $N_{obv}$ slots for its estimate to fully reflect the change in transmission rate. Thus, as $N_{obv}$ increases, the system becomes less responsive to a change in the interferer's behavior. To determine how the choice of $N_{obv}$ affects the accuracy of the estimation, the metric of expected estimation error is introduced. Given that there are $N_h$ hole slots in the most recent $N_{obv}$ slots observed, the system is expected to observe $N_\alpha = \alpha N_h$ hole slots with an unauthenticated transmission. If $N_\alpha \neq \alpha N_h$, the estimate $\hat{\alpha}$ will have a normalized error of $\bar{\alpha}_{err} = |N_\alpha - \alpha N_h| / \alpha N_h$. The normalized expected error of $\hat{\alpha}$ given that $N_h$ hole slots occur during the most recent $N_{obv}$ time slots is:

$$E[\bar{\alpha}_{err}] = \sum_{i=1}^{N_h} \frac{|i - \alpha N_h|}{\alpha N_h} \binom{N_h}{i} \alpha^i (1-\alpha)^{N_h - i} \quad , \tag{5.17}$$

where a normalized error of zero occurs when $N_\alpha = \alpha N_h$. The expression in (5.17) can be related to $N_{obv}$ by noting that there is a direct relation between $N_h$ and $N_{obv}$ (as the system observes more slots it is expected to observe more holes). From [4], assuming that the system is stable and has a large number of packets in the system, the expected number of holes observed given $N_{obv}$ is $E[N_h|N_{obv}] \approx e^{-1} \cdot N_{obv}$. Thus, the expected error from (5.17) can be expressed in terms of $N_{obv}$ by setting $N_{obv} = e \cdot N_h$. A plot of the normalized expected estimation error versus $N_{obv}$ is given in Fig. 101.

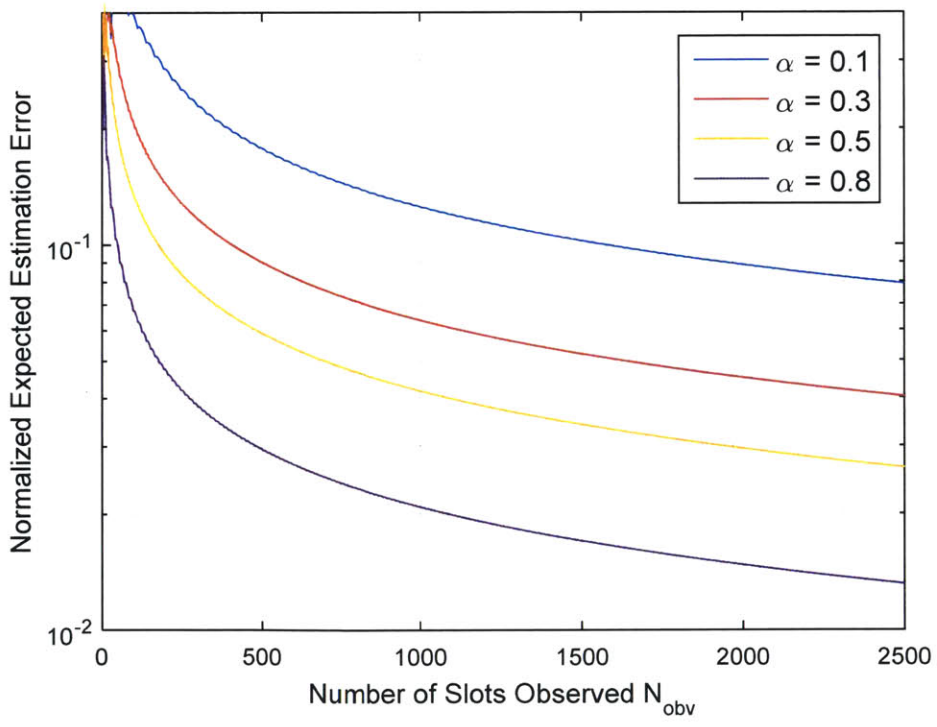


Fig. 101 Normalized Expected Interferer Rate Estimation Error versus Number of Slots Observed

From Fig. 101 we see that the normalized expected estimation error of the interferer's transmission rate is monotonically decreasing with an increasing number of observed slots. Thus, the estimate of $\alpha$ becomes more accurate as $N_{obv}$ is increased. It should also be noted that the expected estimation error decreases with increasing interferer transmission rate $\alpha$ as well. An intuitive explanation for this behavior is that $E[N_\alpha] = \alpha N_h$ increases with increasing $\alpha$, so the same deviation in the observed value of $N_\alpha$ from its expected value causes a proportionally smaller error when the interferer transmission rate $\alpha$ is larger. The tradeoff between accuracy and responsiveness in the choice of $N_{obv}$ is now apparent. Increasing $N_{obv}$ decreases the expected estimation error, resulting in greater accuracy. However, this comes with the tradeoff of reduced responsiveness because the system must wait for a fully up-to-date estimation of $\alpha$ when the interferer changes its rate. Since the expected estimation error asymptotically approaches zero as $N_{obv}$ is increased toward infinity, there is no "optimal" value of $N_{obv}$. Therefore, the value of $N_{obv}$ should be chosen to be as accurate as possible while satisfying any responsiveness requirements dictated by the system.

### 5.1.4 Simulated Results

The performance of an ALOHA channel subjected to a channel-selective interferer with constant rate $\alpha$ using both the original and modified Rivest Algorithms was simulated for various interferer transmission rates. For each value of $\alpha$, simulations were run with two values of the packet arrival rate $\lambda$. The maximum stable arrival rate of $\lambda = (1 - \alpha)e^{-1}$ was simulated in order to understand how well each algorithm functions when run at the system's maximum achievable capacity. The maximum benign arrival rate of $\lambda = e^{-1}$ was also simulated in order to determine how each algorithm handles instability introduced into the system by the interferer. Note that for a particular simulation the values of $\alpha$ and $\lambda$ remain constant. Each simulation was run for 20,000 time slots with a feedback delay of 250 time slots. The value of $N_{obv}$

was chosen to be 1,000 slots (equivalent to 4 round trip times) to model a system that must be reasonably responsive to changes in an interferer's transmission rate.

### 5.1.4.1 Simulated Throughput

Three simulations were run for each set of $\alpha$ and $\lambda$ values and the average throughput of the three simulations was recorded. Note that throughput is defined here as the fraction of simulated time slots that resulted in a successful transmission by a legitimate user. A plot of the average simulated throughput versus interferer transmission rate $\alpha$ for the original and modified Rivest Algorithms with $\lambda = (1-\alpha)e^{-1}$ is given in Fig. 102 Similarly, a plot of the average simulated throughput versus $\alpha$ for the two algorithms with $\lambda = e^{-1}$ is given in Fig. 103.

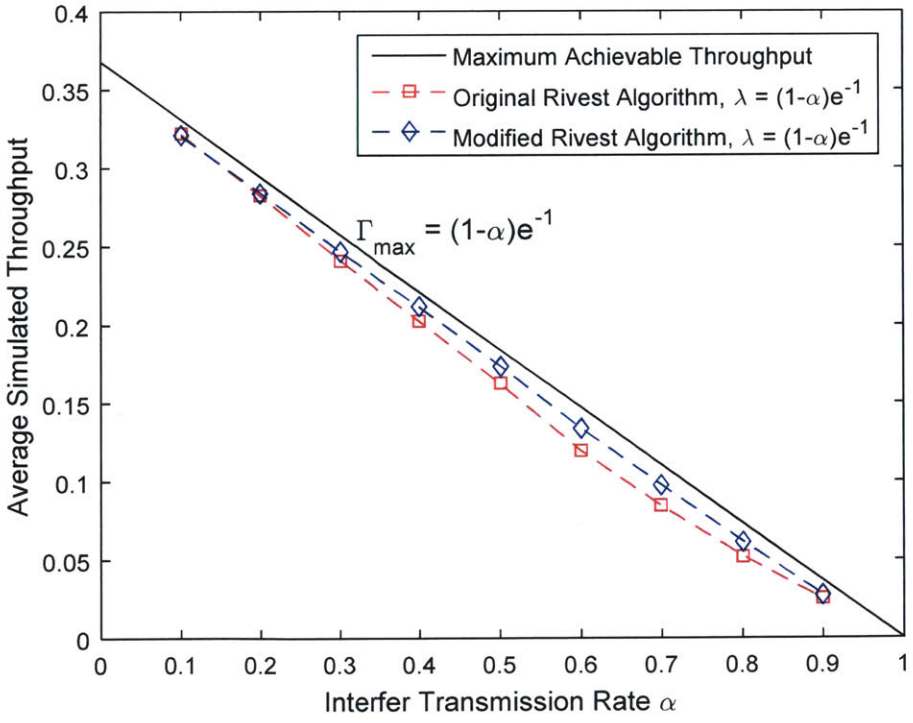


Fig. 102 Simulated Throughput Comparison for $\lambda = (1-\alpha)e^{-1}$

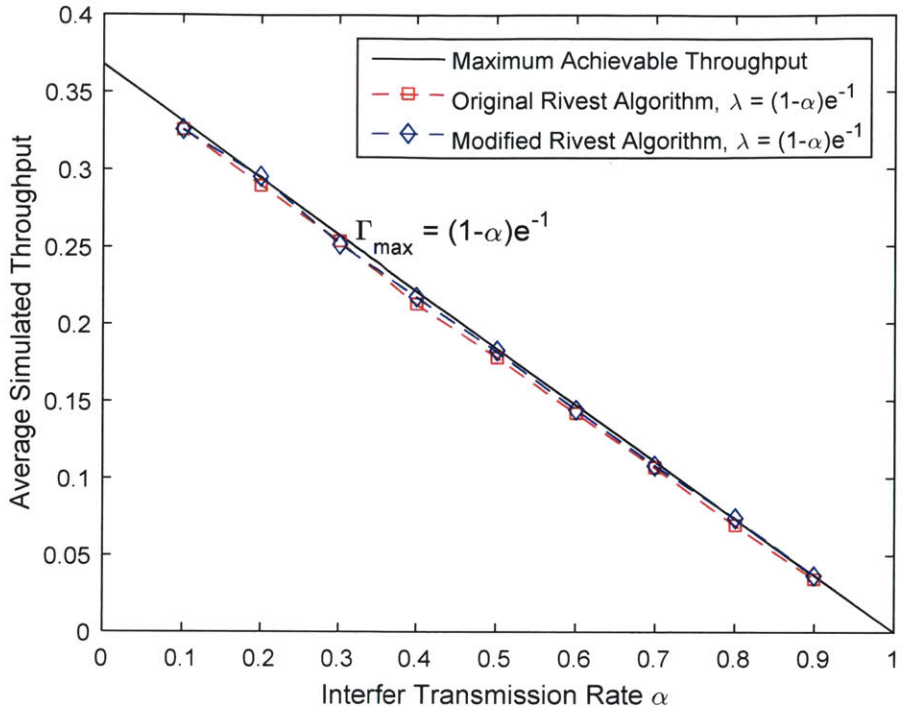


Fig. 103 Simulated Throughput Comparison for $\lambda = e^{-1}$

From the results in Fig. 102 we see the somewhat surprising result that the original Rivest Algorithm performs reasonably close to the maximum achievable throughput $\Gamma_{max}$ despite a significant delay in feedback and an overestimation the number of packets in the system (see the next section). We also see that the modified Rivest Algorithm offers a slight throughput improvement over the original algorithm when the system is run at its maximum stable arrival rate.

From Fig. 103 we see that both algorithms achieve average throughputs very close to $\Gamma_{max}$ when $\lambda = e^{-1}$. The reason that this case offers improved throughput over the case shown in Fig. 102 is that the higher arrival rate of packets mitigates the overestimation of the backlog by both algorithms to some degree and allows the system to set a more accurate probability of transmission $q$. Note that since $\lambda > \Gamma_{max}$ in this case, more packets arrive to the system on average than it can clear and the number of backlogged

packets and delay both grow without bound. This case reveals that when a system operating under benign circumstances (where $\lambda = e^{-1}$ is a stable arrival rate) is suddenly subjected to an interferer, the system can still perform close to its maximum achievable throughput despite increasing congestion. This is an important result as it demonstrates that the sudden introduction of the interferer cannot significantly disturb the Rivest Algorithm. Thus, the system can continue to clear packets at as high a rate as possible while it reduces its packet arrival rate below $\Gamma_{max}$ (which is accomplished by dropping users or having them reduce their data rates).

### 5.1.4.2 Simulated Estimation of Backlog

In addition to recording the throughput of each simulation, the number of packets in the system $N$ and the system's estimate $v$ were recorded in order to compare the estimation accuracy of the two algorithms. In general, the modified Rivest Algorithm achieved a more accurate estimate of $N$ than the original algorithm. An example of the difference in estimation accuracy between the two algorithms is shown in Fig. 104 and Fig. 105. These results were generated from the case where $\alpha = 0.5$ and $\lambda = 0.5e^{-1}$. From these results we see that both algorithms overestimate $N$, but that the modified algorithm achieves a much more accurate value of $v$ than the original Rivest Algorithm. The improved performance of the modified algorithm is due to the fact that the interferer's presence is accounted for when collisions are observed by the system. The primary benefit of the modified algorithm's more accurate estimation of $N$ is that congestion can be cleared more quickly once the interferer leaves the channel. An overestimate of $N$ results in a transmission probability $q$ that is smaller than optimal value of $q = 1/N$. Therefore, overestimating $N$ suppresses the system and users will attempt transmissions less frequently than they ought to. In this way, the modified Rivest Algorithm doesn't suppress the channel to the same degree as the original algorithm and allows the channel to take advantage of the interferer's departure more quickly.

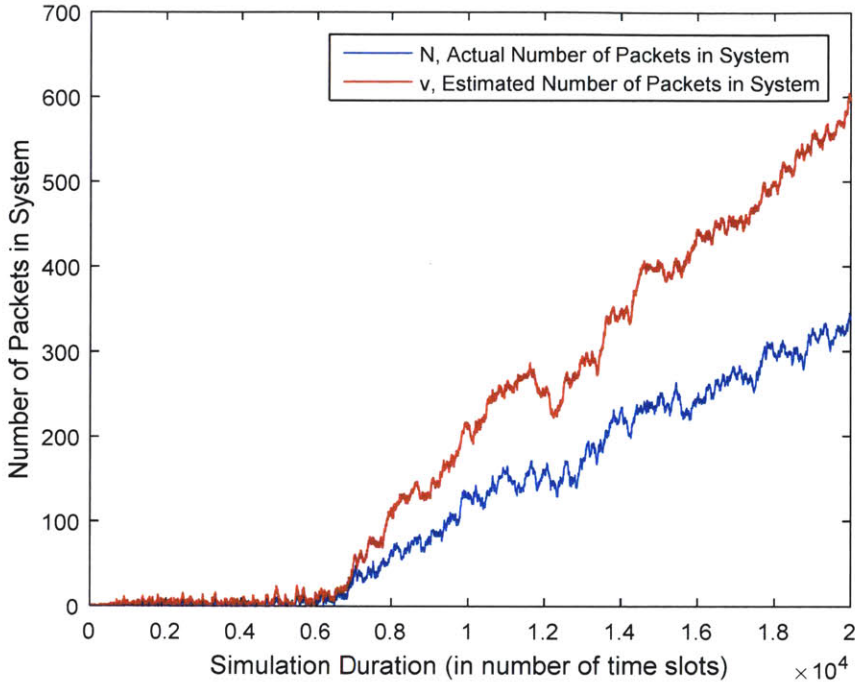


Fig. 104 Estimation of Packets in System by Original Rivest Algorithm

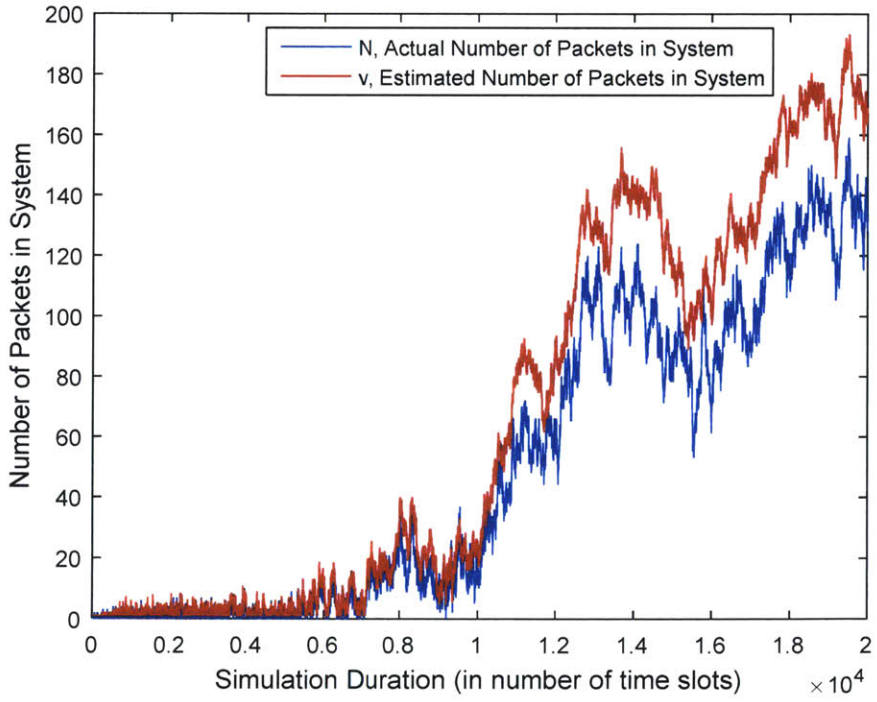


Fig. 105 Estimation of Packets in System by Modified Rivest Algorithm

### 5.1.4.3 Simulated Recovery Time from Interferer

In order to understand how quickly the original and modified Rivest Algorithms clear congestion once the channel-selective stops attacking the system, the simulations shown in Fig. 104 and Fig. 105 were run for an additional 10,000 time slots with an interferer rate of $\alpha = 0$. These extended simulations model an interferer attacking the channel for the first 20,000 time slots with $\alpha = 0.5$ and then leaving the system. After the interferer's departure the system is able to clear its congestion for the remaining 10,000 time slots. Additionally, the arrival rate of user packets is increased from $\lambda = 0.5e^{-1}$ to $\lambda = 0.95e^{-1}$ four round trip times (1000 time slots) after the interferer's departure. The increase in arrival rates models a system that detects the interferer's departure within 4 RTT's and increases its arrival rate to take advantage of the additional throughput available. A plot of the actual and estimated number of packets in the system for the extended simulation of the original Rivest Algorithm is given in Fig. 106. A plot of the actual and estimated number of packets in the system for the extended simulation of the modified Rivest Algorithm is given in Fig. 107.

The primary performance metric of interest in these simulations is how long it takes for the system to clear the congestion generated by the channel-selective interferer after it stops attacking the channel. We call this metric the recovery time of the system and define it as the number of time slots required after the interferer leaves the channel for the control algorithm to reduce the number of packets in the system below 20 packets. The choice of 20 packets as the threshold for successfully clearing congestion is made based on the results from previous simulations where $N$ rarely exceeds 20 packets when the arrival rate of packets to the system is less than the system's maximum throughput. A comparison of Fig. 106 and Fig. 107 reveals that the modified Rivest Algorithm has a much faster recovery time than the original Rivest Algorithm. Given that there are nearly twice as many packets in the system using the original Rivest Algorithm than the system using the modified Rivest Algorithm when the interferer leaves the channel,

one might expect the recovery time of the original Rivest Algorithm to be approximately twice as long as the recovery time of the modified Rivest Algorithm. However, the recovery time of the original algorithm is 5364 time slots while the recovery time of the modified algorithm is only 752 time slots – more than seven times shorter.

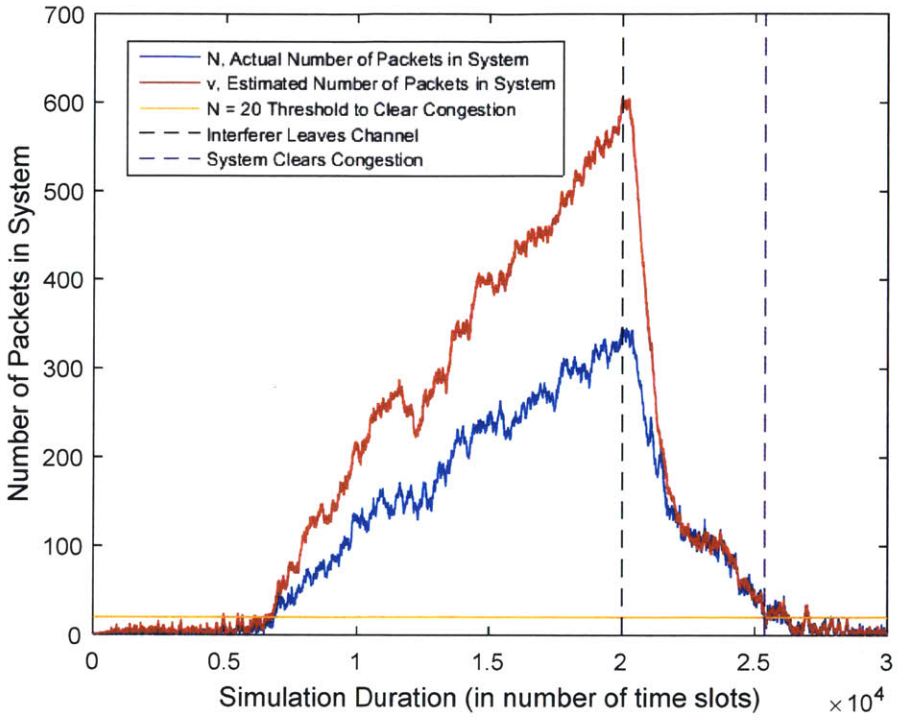


Fig. 106 Extended Estimation of Packets in System by Original Rivest Algorithm

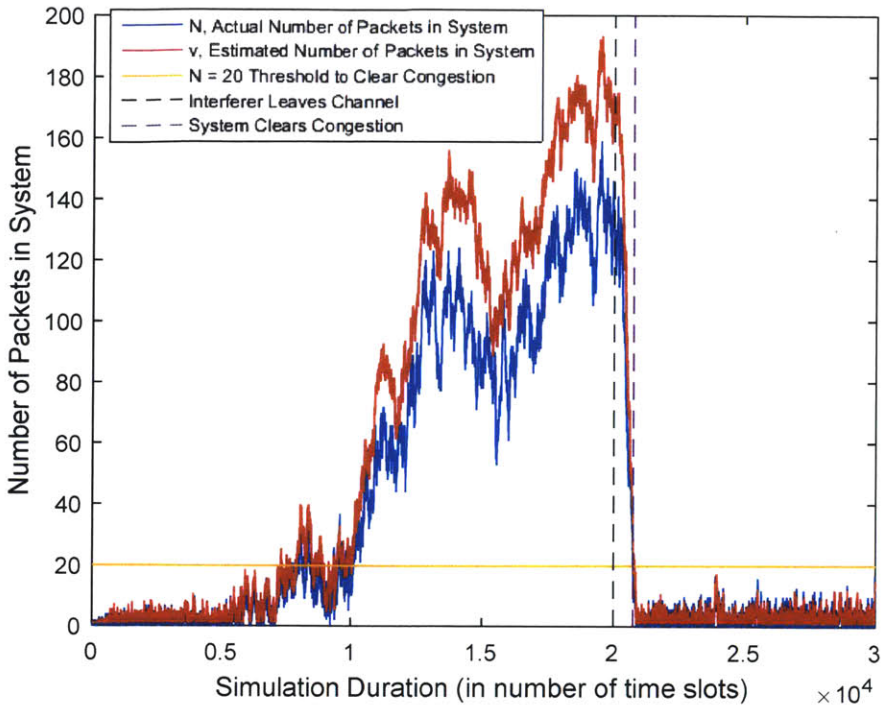


Fig. 107 Extended Estimation of Packets in System by Modified Rivest Algorithm

The primary reason for the difference in performance between the two algorithms is that the original Rivest Algorithm significantly overestimates the number of packets in the system and therefore suppresses transmissions in the channel for a longer period of time than the modified Rivest Algorithm. Thus, the modified Rivest Algorithm's more accurate estimation of the number of packets in the system results in superior performance in clearing congestion after the interferer leaves the channel.

## 5.2 Performance Improvements from Using Code Switching

It is apparent from (5.2) that a channel-selective interferer that transmits on a large fraction of channels can significantly reduce the system's maximum achievable throughput. While the modified Rivest Algorithm is able to ensure that the system operates close to the maximum achievable throughput, it cannot recover any of the lost throughput. Fortunately, implementing code switching in the system can mitigate the throughput loss caused by the interferer. The effect of code switching on the interference

rate $\alpha$ can be understood by introducing a metric known as the effective interference rate $\alpha'$. We define the effective interference rate as the fraction of success slots the interferer can degrade to collision slots. For the DS/ALOHA system that does not use code switching, $\alpha'$ is simply the probability $\alpha$ of the interferer transmitting on a time slot. However, for the system using code switching, the interferer may only transmit during a fraction of a time slot since the channel changes the DS code it uses for transmission during the transmission of a single packet. In this case, it is unclear when the system will interpret a single user transmission affected by the interferer as a collision, and when it will interpret it as a success with potential bit errors. To resolve this ambiguity, it is assumed that bit errors due to ambient noise in the channel occur with negligible probability and that any bit errors in a transmission are the result of a collision or the interferer. If the system assumes that any time slot containing a transmission with bit errors is a collision, then the interferer only needs to cause a single bit error in a transmitted user packet to degrade the success slot to a collision. Note that it is assumed that the system can detect any bit errors that occur in a transmitted packet. Under this scheme, $\alpha'$ is equivalent to the probability that a success slot contains one or more bit errors after decoding when an interferer is attacking the system:

$$\alpha' = 1 - (1 - P_b)^{L_p} \quad , \tag{5.18}$$

where $P_b$ is the bit error probability and $L_p$ is the length in bits of transmitted packet. It is assumed that the channel changes the DS code it is using for transmission after every $N_B = 10$ bit periods. If repeat coding is used, a coding rate of up to $m = 99$ symbols per bit can be used without violating the assumption that symbol error probabilities are independent and identically distributed. The bit error probability for $m = 99$ repeat coding is [6]:

$$P_b = \sum_{i=50}^{99} \binom{99}{i} \varepsilon^i (1-\varepsilon)^{99-i} \quad , \tag{5.19}$$

where $\varepsilon$ is the probability of a symbol error and has the following form for a channel using BPSK modulation [6]:

$$\varepsilon = \alpha Q\left(\sqrt{2 \cdot SNR(\alpha)}\right) \quad , \tag{5.20}$$

where $SNR(\alpha)$ is the signal to noise ratio as a function of $\alpha$ and has the following form when ambient noise is assumed to be negligible:

$$SNR(\alpha) = \frac{E_{TX} G_p G_n}{99 \cdot E_I} \alpha \quad , \tag{5.21}$$

where $E_{TX}$ is the EIRP of a single user, $G_p$ is the processing gain due to DS spectrum spreading, $G_n$ is the power advantage of a user over the interferer due to antenna nulling, and $E_I$ is the EIRP of the interferer. A plot of the effective interference rate $\alpha'$ versus the interferer rate $\alpha$ for a system using code switching and a system using a static DS code is given in Fig. 108. Note that the values for $E_{TX}$, $G_n$, and $E_I$ used to generate Fig. 108 are the same as the those from Section 2.2.2. Additionally, a processing gain of 40 dB is used in Fig. 108. This processing gain is achieved by spreading a 100 kHz data signal bandwidth over a bandwidth of 1 GHz.

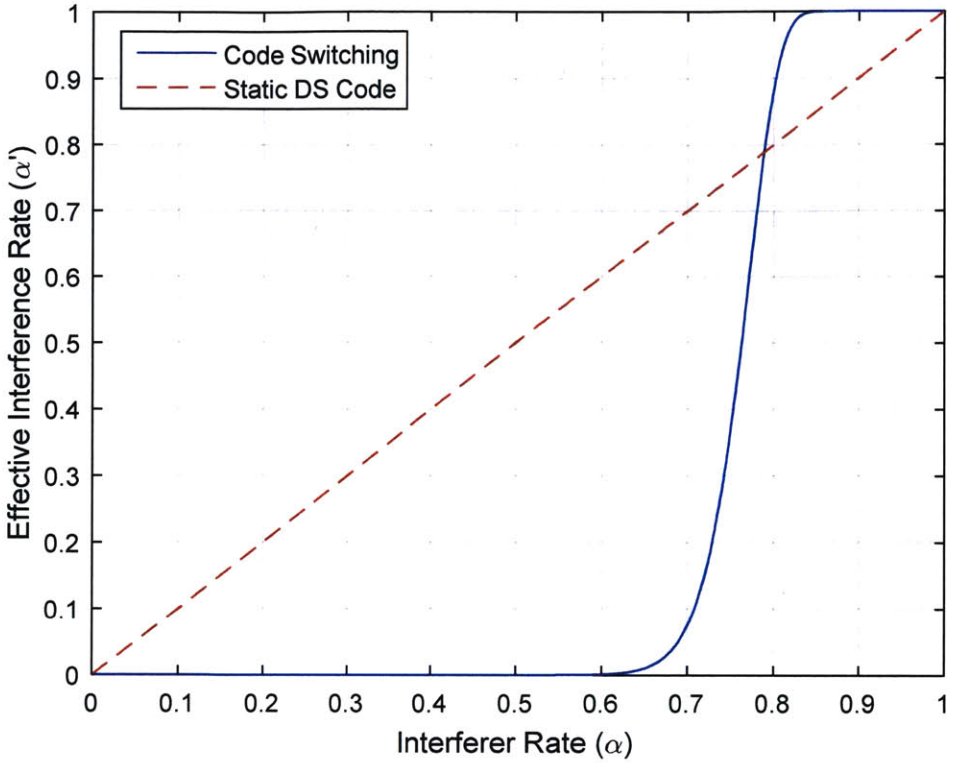


Fig. 108 Comparison of Effective Interference Rates for System Using a Static DS Code and System Using Code Switching

We see from Fig. 108 that the system using code switching can achieve a lower effective interference rate for interferer rates below approximately $\alpha = 0.8$. Thus, the inclusion of code switching in the system significantly reduces the rate at which the interferer can degrade success slots for $\alpha < 0.8$. We also see from Fig. 108 that code switching performs worse that the system with a static DS code for $\alpha > 0.8$. The reason for this behavior is that for high interferer rates, the system is better off not changing its DS code since the probability that the system changes its DS code to a code affected by the channel-selective interferer is very high. Thus, as $\alpha$ increases, the probability that a channel initially selects a DS code free of interference eventually becomes greater than the probability that the channel switches among enough DS codes free of interference during the duration of a packet transmission to avoid a bit errors. Thus, for sufficiently large values of $\alpha$, the system is better offer using static DS code assignments.

Another way to represent the performance improvement achieved by code switching for $\alpha < 0.8$ is to compare the maximum achievable throughput $\Gamma_{max}$ for systems using code switching and static DS codes. An expression for $\Gamma_{max}$ can be derived by substituting $\alpha'$ for $\alpha$ in (5.2):

$$\Gamma_{max} = (1 - \alpha')e^{-1} \tag{5.22}$$

A comparison of the maximum achievable throughput for a system using code switching and a system using static DS codes is given in Fig. 109. We see from Fig. 109 that the system using code switching can achieve a throughput close to $e^{-1}$ for $\alpha < 0.7$ and a higher throughput than the system using static DS codes for $\alpha < 0.8$. It should be noted that smaller values of $\alpha$ are of more interest for this interference strategy since an interferer with enough transmission power to achieve a large value of $\alpha$ would be able to cause more damage to the system by using a different strategy. Thus, for the interference rates of interest, code switching can significantly improve performance over a system using static DS code assignments.

Finally, it should be noted that the modified Rivest Algorithm described in Section 5.1.2 can be used with code switching. This is accomplished by incrementing $v$ by $(e - 2 + \hat{\alpha}')^{-1}$, where $\hat{\alpha}'$ is an estimate of the effective interference rate. An estimate of the effective interference rate $\alpha'$ can be made by estimating the interferer rate $\alpha$ using the same method as described in Section 5.1.3 and then using (5.18) through (5.21) to compute $\hat{\alpha}'$. Note that this method assumes that transmissions by the interferer on hole slots can still be reliably detected by whatever authentication mechanism the system is using.

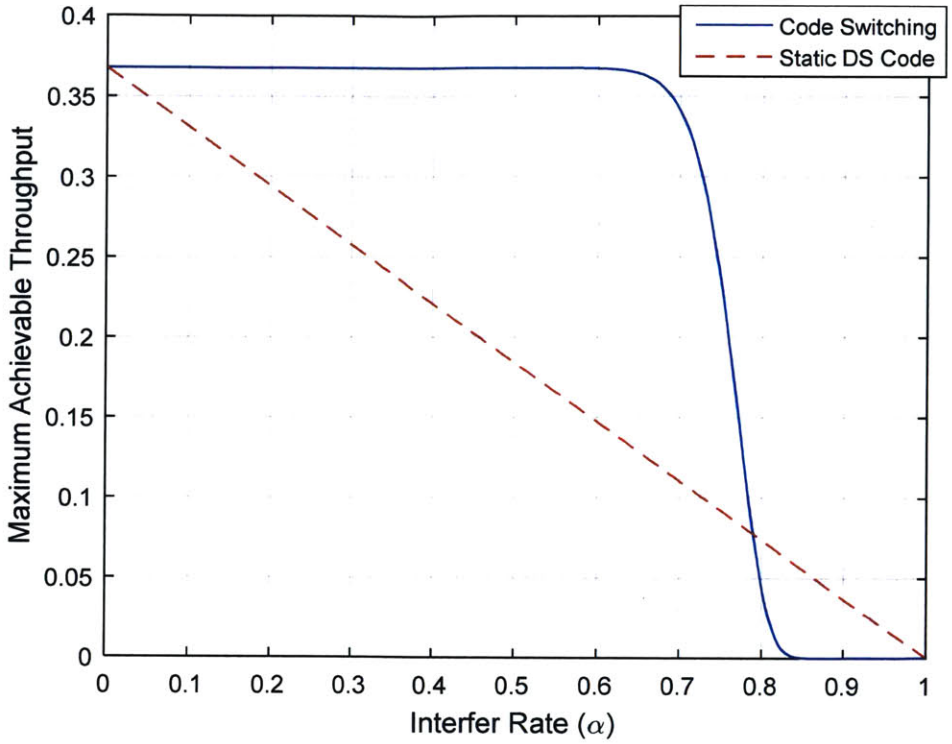


Fig. 109 Maximum Achievable Throughput versus Interferer Rate for Systems Using Code Switching and Static DS Codes

## 5.3 Defense against a Collision-Spoofing Interferer

The previous sections in this chapter consider a channel-selective interferer that focuses its attacks on success slots by attempting to degrade them into collisions. An alternate strategy the channel-selective interferer may pursue is to imitate collisions on hole slots. Instead of trying to appear as a legitimate user transmitting in the channel, the interferer may instead transmit an incoherent message with the same characteristics as a collision. When the interferer's transmission falls on a hole slot, the system has no way of knowing whether the channel output is from a genuine collision or a collision-spoofing interferer. Since the Rivest Algorithm increases its estimate $v$ of the number of packets in the system each time a time slot contains a collision, the collision-spoofing interferer will be able to trick the system into overestimating $v$. Since the transmission probability $q$ for all users is set as $1/v$, an overestimate of the number of packets

in the system will result in a transmission probability $q$ that is smaller than the optimal value. In turn, the smaller-than-optimal value of $q$ will result in a suppressed channel and lost throughput. Therefore, a means of mitigating a collision-spoofing interferer is of interest in order to ensure that the DS/ALOHA system achieves as high a throughput as possible.

An effective means of mitigating a collision-spoofing interferer is to implement a collision detection scheme for a system using code switching. Code switching allows the system to differentiate between a real collision, which will be present in the channel for the entire time slot period, and an imitated collision transmitted by the interferer, which will only be present in the channel intermittently during the time slot period because the interferer has to guess which DS codes the system is using. It is assumed that the system can perform a collision detection test on a per-symbol basis to determine whether the current time slot contains a hole or a genuine collision. If symbol periods are sampled from portions of the transmitted packet that use different DS codes, then each symbol will have an independent probability $\alpha$ of being affected by the channel-selective interferer. Therefore, if the length of the packet transmitted in each time slot is $L_p$ bits, and the DS code used by the channel is changed after every $N_B$ bit periods, then the maximum number of independent identically distributed (IID) symbol periods $N_{sym}$ the system can observe during a single time slot is:

$$N_{sym} = \left\lceil \frac{L_p}{N_B} \right\rceil \ , \tag{5.23}$$

where $\lceil L_p/N_B \rceil$ is the number of times the system changes its DS code during a single time slot. It is assumed that each collision detection test performed on the $N_{sym}$ symbol periods has a probability $P_d$ of correctly detecting a collision and a probability $P_f$ of mistakenly identifying a hole as a collision (a false

alarm). The total probability of a false alarm $P_{f,T}$ from error in the collision detection test and the collision-spoofing interferer, is then:

$$P_{f,T} = \alpha P_d + (1 - \alpha) P_f \quad , \tag{5.24}$$

where it is assumed that the collision detection test has the same probability $P_d$ of interpreting a transmission from the collision-spoofing interferer as a collision as it does of detecting a genuine collision. Note that the total probability of correctly detecting a collision is simply $P_d$ since it is assumed that the collision-spoofing interferer has no effect on a time slot where a genuine collision occurs. As long as $P_d$ is greater than $P_{f,T}$, the system is expected to see more of the $N_{sym}$ independent collision detection tests declare that a collision has occurred when a genuine collision occurs on the channel than when a collision-spoofing interferer is trying to generate a fake collision on a hole slot. Therefore, for $P_d > P_{f,T}$, the system can specify some threshold $\eta$ of collision detection tests that select a collision as having occurred that is more likely to be exceeded by a genuine collision than a fake collision.

The probability $P_D$ that a genuine collision is correctly detected by the system's $N_{sym}$ collision detection tests is equal to the probability that the number of collision detection tests that declare that a collision has occurred is greater than or equal to $\eta$ when a genuine collision occurs. Since the $N_{sym}$ collision detection tests are IID, the probability of correctly detecting a collision $P_D$ can be upper-bounded using the Chernoff Bound:

$$P_D \leq \left(1 - P_d + \frac{\eta - \eta P_d}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_d - \eta P_d}{\eta - \eta P_d}\right)^{\eta} \qquad for\ \eta > N_{sym} P_d \tag{5.25}$$

See Appendix D.3 for a derivation of this result. The probability $P_{FA}$ that the system generates a "false alarm" by interpreting a fake collision as a genuine collision is equal to the probability that the number of collision detection tests that declare that a collision has occurred is greater than or equal to $\eta$ during a hole slot. The probability of a false alarm $P_{FA}$ can be upper-bounded in a similar manner to $P_D$ using the Chernoff Bound:

$$P_{FA} \leq \left(1 - P_{f,T} + \frac{\eta - \eta P_{f,T}}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_{f,T} - \eta P_{f,T}}{\eta - \eta P_{f,T}}\right)^{\eta} \qquad for\ \eta > N_{sym} P_{f,T} \tag{5.26}$$

See Appendix D.3 for a derivation of this result. Given the results in (5.25) and (5.26), the tradeoff between the system's ability to detect genuine collisions and is susceptibility to collision-spoofing can be seen in the relationship of $P_D$ and $P_{FA}$ to $\eta$. Decreasing the threshold $\eta$ increases the probability of detecting genuine collisions $P_D$, but it also increases the probability of the system generating a false alarm $P_{FA}$ on hole slots. A plot of $P_D$ versus $P_{FA}$ for corresponding values of $\eta$, and different fractions of channels $\alpha$ affected by the collision-spoofing interferer, is given in Fig. 110.

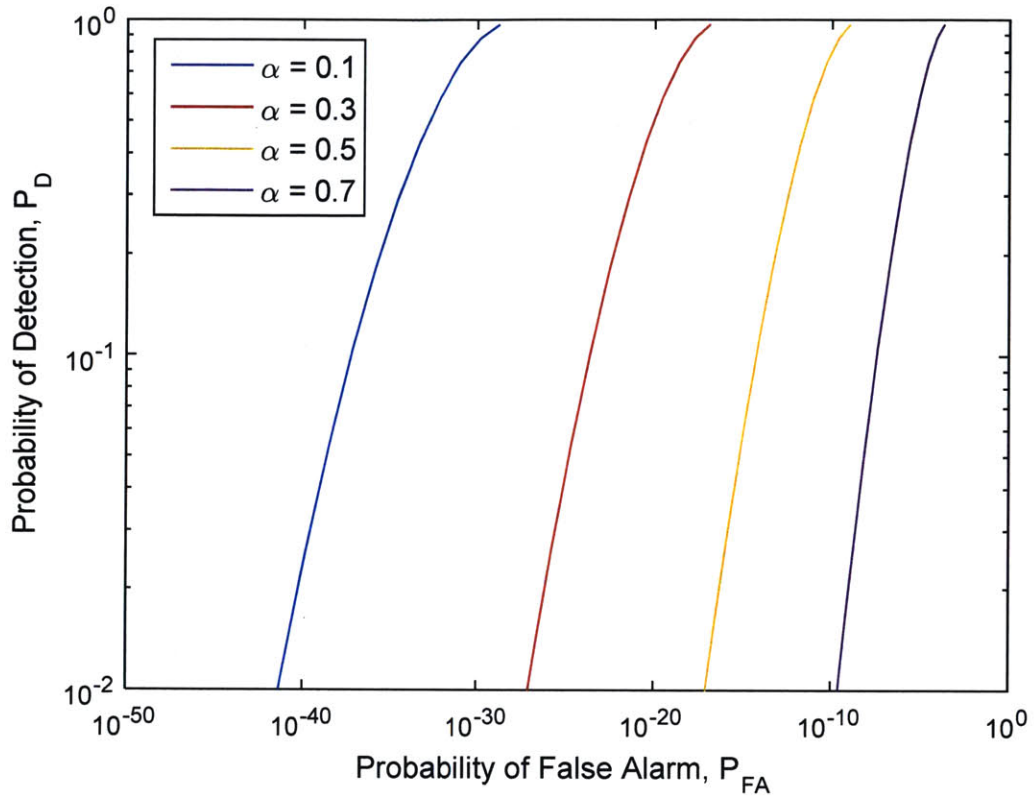


Fig. 110 Probability of Detection versus Probability of False Alarm for $N_{sys} = 100$, $P_D = 0.8$, $P_f = 0.2$

Note that the results in Fig. 110 are based on the assumptions that a 1,000 bit packet changes its codes every 10 bit periods (resulting in $N_{sys} = 100$ possible independent symbol period tests) and that a fairly accurate collision detection test is used with $P_d = 0.8$ and $P_f = 0.2$. We see from Fig. 110 that the system can achieve a high probability of detection (maximum in each case is $P_D = 0.9688$) with a relatively low probability of false alarm (worst case is $P_{FA} = 0.000207$ at $P_D = 0.9688$ for $\alpha = 0.7$). Thus, by performing $N_{sym}$ independent collision detection tests and specifying the appropriate threshold $\eta$, the system can accurately discriminate between genuine collisions and attempts by the collision-spoofing interferer to disguise hole slots as collisions. It should be noted that $P_D$ can be larger than 0.9688 since the threshold $\eta$ can be decreased below $N_{sym}P_d$ and $N_{sym}P_{f,T}$. However, the bounds developed in (5.25)

and (5.26) cannot be used in these cases because $\eta$ falls outside the range where the Chernoff Bound is defined.

## 5.4 Summary

This chapter explored possible attack strategies an adversary may use against the MAC layer of the DS/ALOHA system and developed techniques for mitigating their effectiveness. Section 5.1 analyzed the effectiveness of a channel-selective interferer in degrading the performance of the Rivest Algorithm and developed a modified algorithm to account for the interferer's behavior. The modified Rivest Algorithm was shown to have superior performance to the original Rivest Algorithm when an interferer is present in the channel. Next, Section 5.2 demonstrated that adding code switching to the channel can reduce the impact of a channel-selective interferer on the Rivest Algorithm. Pairing code switching with high rate coding was also shown to significantly improve the channel's maximum achievable throughput when an interferer is present. Finally, Section 5.3 introduced the concept of a collision-spoofing interferer and developed a strategy for protecting the channel from this form of interference by combing code switching with a method for detecting genuine collisions.

# Chapter 6

# Conclusion

Future SATCOM systems must be able to meet dynamic user traffic demands while operating in highly contested environments. For this reason, a dynamic random multiple-access scheme is needed that is both robust to intentional interference and has a low probability of intercept by an adversary. A system using a slotted ALOHA protocol and direct sequence spectrum spreading is one promising solution to the robust random multiple-access problem.

This thesis began with a description of the combined DS/ALOHA system in Chapter 2 that can support a large number of channels operating in the presence of a powerful transportable interferer. It was also shown in Chapter 3 that the DS/ALOHA system can respond to dynamic user traffic and can provide dual-class service to ensure that priority users are given preferential treatment. Chapter 4 analyzed several physical layer attack strategies available to the transportable interferer, and demonstrated that simple channel-hardening techniques such as repeat coding and DS code switching can effectively mitigate these attack vectors. A similar analysis of attack strategies against the MAC layer was made in Chapter 5, where repeat coding and code switching were once again shown to offer sufficient protection against these attacks.

As wireless communication technology continues to progress, so too will the capabilities of potential adversaries. Future work in dynamic and robust random multiple-access schemes for SATCOM

applications will have to consider the attack strategies available to more complex and powerful interference platforms. Attacks against higher network layers, such as the network and transport layers, will also have to be considered and will require effective mitigation techniques. As interference platforms become more complex, it will also be necessary to develop additional techniques to estimate their behavior including the power levels, waveforms, and frequency bands that are used in their attacks.

Future user demands will also drive design choices for SATCOM systems. As the number of terminals with SATCOM capabilities increases, the circuit-oriented architectures of existing systems will struggle to meet the increase in bursty user traffic. Thus, a random multiple-access mode will be of vital importance in future SATCOM systems in order to meet the highly dynamic traffic of future users. Future work in this area will better define the user requirements for SATCOM systems and distill them into various classes of service. Different multiple-access schemes can then be explored to determine the best scheme to support each class of service.

The development of the next generation of SATCOM systems requires a good understanding of the challenges and demands these systems will face during their lifetime. As advances in technology continue to change the environment in which these systems operate, it is essential that the design of these systems anticipates how such changes will affect their ability to meet user demands. Given the complexity of future threats, much work remains to ensure that these systems are protected against as many attack vectors as possible. This work has identified some of the challenges faced by future SATCOM systems, and the mitigation techniques explored here will hopefully serve as a foundation for future work to develop robust random multiple-access schemes.

# Appendix A

# Derivations for Equations in Chapter 2

## A.1 Physical Parameter Calculations for Section 2.1.3

The EIRP of the transmitter is simply the transmitter power $P_{TX}$ multiplied by the gain of its antenna $G_{TX}$:

$$E_{TX} = P_{TX} G_{TX} \quad ,$$

where $P_{TX}$ has been specified as 10 watts and $G_{TX}$ has the following form for and antenna beam width of 10 degrees [16]:

$$G_{TX} = \frac{4\pi}{beam\ width^2} = \frac{4\pi}{\left(10^o \times \frac{\pi\ rad}{180^o}\right)^2} \approx 412$$

Therefore:

$$E_{TX} = 4120\ watts$$

For a receiver antenna with a diameter of 10 meters [16]:

$$G_{RX} = \frac{\pi^2 d_{RX}^2 e_{RX}}{\lambda_c^2} \quad ,$$

where $d_{RX}$ is the receiver antenna diameter (3 meters), $e_{RX}$ is the receiver antenna efficiency (conservative estimate of 0.7 is used), and $\lambda_c$ is the wavelength of the center frequency of the band being used. For a center frequency of 44.5 GHz, $\lambda_c$ is:

$$\lambda_c = \frac{2.9979 \times 10^8\ m/s}{44.5\ GHz} \approx 0.006737\ meters$$

Therefore:

$$G_{RX} = 1{,}369{,}958$$

The path loss is:

$$F_p = \left(\frac{\lambda_c}{4\pi L}\right)^2 ,$$

where $L$ is the signal path distance in meters which is 35,786,000 meters for a geosynchronous orbit. At this distance the path loss is:

$$F_p \approx 2.2443 \times 10^{-22}$$

The data signal bandwidth $W_d$ is simply the spread signal bandwidth $W_{ss}$ divided by the processing gain and varies with the number of shift registers used $n_s$:

$$W_d = \frac{W_{ss}}{2^{n_s} - 1}$$

The noise power spectral density $N_0$ is [19]:

$$N_0 = kTF_{sys} \quad ,$$

where $k$ is the Boltzmann constant ($1.3806 \times 10^{-23}\ W/K \cdot Hz$), $T$ is the receiver antenna temperature in Kelvin, and $F_{sys}$ is the system loss of the receiver which is assumed to be 2 dB. The receiver temperature can be determined by solving for the value of $T$ that satisfies the thermal equilibrium equation [20]:

$$q_{in} = q_{out} \quad ,$$

where $q_{in}$ is the heat energy per unit time (in watts) absorbed by the receiver and $q_{out}$ is the heat energy per unit time (in watts) emitted by the receiver [20]. An expression for $q_{in}$ is [20]:

$$q_{in} = \alpha_{sat} A_{RX}(1358 + 237 + 30\ W/m^2) \quad ,$$

where $\alpha_{sat}$ is the thermal absorptivity of the receiver, $A_{RX}$ is the area of the receiver, and 1625 $W/m^2$ is the total thermal energy per unit time per square meter that is input to the receiver from solar radiation (1358 $W/m^2$), earth shine (237 $W/m^2$), and albedo (30 $W/m^2$) [20]. An expression for $q_{out}$ is [20]:

$$q_{out} = \sigma_{SB} \varepsilon_{sat} A_{RX} T^4 \quad ,$$

where $\sigma_{SB}$ is the Stefan-Boltzmann constant ($5.67 \times 10^{-8}\ W/m^2 \cdot K^4$) and $\varepsilon_{sat}$ is the thermal emissivity of the receiver [20]. Substituting the expressions for $q_{in}$ and $q_{out}$ into the thermal equilibrium equation and solving for $T$ yields:

$$T = \left(\frac{\alpha_{sat}(1625\,W/m^2)}{\sigma_{SB}\varepsilon_{sat}}\right)^{1/4}$$

Note that this result is independent of $A_{RX}$ since it is assumed that the same receiver area is absorbing and emitting thermal energy. From [19] a common choice for satellite coatings is white paint coating which has a thermal absorptivity of $\alpha_{sat} = 0.21$ and a thermal emissivity of $\varepsilon_{sat} = 0.9$. Substituting these values into the expression above results in a receiver temperature of $T = 285.96\,K$. Substituting this value into the expression for noise power spectral density yields:

$$N_0 \approx 6.25 \times 10^{-21}\,W/Hz$$

## A.2 Supporting Calculations for Section 2.1.4.2

For a 100 Giga-sample per second input, a real-valued FFT is performed over the frequency range of 0 to 50 GHz. FFT bins must be no smaller than the data signal bandwidth of interest in order to ensure reliable detection and require two points per bin. The number of FFT points $N_{FFT}$ required is then:

$$N_{FFT} = \frac{50\,GHz}{2.4\frac{kHz}{bin}} \times \frac{2\,points}{bin} \approx 4.17 \times 10^7$$

However, for a split-radix FFT $N_{FFT}$ must be a power of 2. The closest power of 2 is $N_{FFT} = 2^{26} \approx 6.71 \times 10^7$. The number of flops required for a $N_{FFT}$ point FFT is [12]:

$$N_{flop} = 4 \cdot N_{FFT}\log_2(N_{FFT}) - 6 \cdot N_{FFT} + 8$$

Assuming that each flop of the FFT requires a flop of overhead, $N_{flop}$ becomes:

$$N_{flop} = 8 \cdot N_{FFT} \log_2(N_{FFT}) - 12 \cdot N_{FFT} + 16$$

Therefore, for $N_{FFT} = 2^{26}$ the number of flops required is 13.154 Giga-flops.

# Appendix B

## Derivations for Equations in Chapter 3

## B.1 Derivation of Expected Delay for Section 3.1.1

For a packet to be successfully transmitted it must first pass its transmission test and then transmit on a where no other users transmit. Given a number of packets waiting for transmission $N$, the time a packet spends in the ALOHA channel $T_w$ is expressed as:

$$T_w = (N_A + N_{RTT})N_{TX}L_pT_b \quad ,$$

where $N_A$ is random variable modelling the number of ALOHA slots required for a user to pass its test to transmit with probability $q$, $N_{RTT}$ is the number of slots in a single round trip time, $N_{TX}$ is a random variable modelling the number of attempted transmissions required to successfully transmit the packet, $L_p$ is the packet length in bits, and $T_b$ is the data bit period. The expression $(N_A + N_{RTT})$ models the aggregate number of ALOHA slots per attempted transmission of a packet since the user takes $N_A$ slots to attempt a transmission and then must wait $N_{RTT}$ slots for feedback. The expression $L_pT_b$ models the amount of time occupied by a single ALOHA slot. Assuming that the random variables $N_A$ and $N_{TX}$ are independent, the expected value of $T_w$ is then:

$$E[T_w] = E\left[(N_A + N_{RTT})N_{TX}L_pT_b\right] = (E[N_A] + N_{RTT})E[N_{TX}]L_pT_b$$

The random variable $N_A$ is geometrically distributed with parameter $q = 1/v$ and mean $v$. The random variable $N_{TX}$ is also geometrically distributed with a parameter $P_{N-1}$ which is equal to the probability that the other $N - 1$ users do not transmit on a given slot. This probability can be expressed as:

$$P_{N-1} = \left(\frac{1}{v}\right)^{N-1}$$

Which converges to $e^{-1}$ for sufficiently large $N$ (assuming that $v \approx N$). Since delay is primarily of interest to the when it is long, it is reasonable to assume that $N$ is sufficiently large to yield $P_{N-1} \approx e^{-1}$. The random variable $N_{TX}$ is then geometrically distributed with parameter $e^{-1}$ and mean $e$. Substituting the mean values of $N_A$ and $N_{TX}$ into the previous expression for $E[T_w]$ yields:

$$E[T_w] = e(v + N_{RTT})L_p T_b$$

## B.2 Derivation of Expected Delay for Section 3.1.2

The expected delay for the continuous transmission attempt scheme can be derived in a similar manner to the expected delay for the wait-for-feedback scheme with the following modification:

$$T_w = (N_A N_{TX} + N_{RTT})L_p T_b \quad ,$$

where only $N_A$ is multiplied by $N_{TX}$ since users do not wait for feedback before attempting retransmission, but won't know if a particular retransmission was successful until $N_{RTT}$ slot later. Following the same logic from Appendix B.1, the expected delay is now:

$$E[T_w] = (e \cdot v + N_{RTT})L_p T_b$$

## B.3 Derivation of Expected Delay for Section 3.3.4

For the packet from a strict time deadline user to be transmitted successfully, one of the repeated transmissions of the packet must occur on a hole slot. The time a packet from a strict time deadline user spends in the ALOHA channel $T_w$ can be expressed as:

$$T_w = (N_S + N_{RTT}N_{TX})L_pT_b \quad ,$$

where $N_{TX}$ is a random variable modelling the number of repeated transmission attempts, each with $N_{Rep}$ repeated transmissions, required for a successful transmission of the time deadline packet. The variables $N_{TX}$, $L_p$, and $T_b$ are treated as constants representing the number of ALOHA slots in a RTT, the packet length in bits, and the data bit period, respectively. Note that the expression above is similar to the equation from Appendix B.1 except that the random variable $N_A$ is replaced by the random variable $N_S$ modelling the number of repeated transmissions that occur before the first successful transmission of the time deadline packet, given that a successful transmission occurred within the $N_{Rep}$ repeated transmissions. The expected delay $E[T_w]$ is then:

$$E[T_w] = E\left[(N_S + N_{RTT}N_{TX})L_pT_b\right] = (E[N_S] + N_{RTT}E[N_{TX}])L_pT_b \quad ,$$

where it is assumed that the random variables $N_S$ and $N_{TX}$ are independent. The random variable $N_{TX}$ has a geometric distribution with parameter $p$ equal to the probability that a single set of $N_{Rep}$ transmissions results in at least one successful transmission of the packet. The parameter $p$ has the form:

$$p = 1 - Pr\{no\ successes\} = 1 - (1 - e^{-1})^{N_{Rep}} \quad ,$$

where it is assumed from [4] that the probability of a hole is $e^{-1}$ and therefore the probability of all of the repeated transmissions occurring on slots other than holes is $(1-e^{-1})^{N_{Rep}}$. Since the expectation of a geometric distribution with parameter $p$ is equal to $p^{-1}$, the expected value of $N_{TX}$ is:

$$E[N_{TX}] = \frac{1}{1-(1-e^{-1})^{N_{Rep}}}$$

Therefore, the final form of $E[T_w]$ is:

$$E[T_w] = \left(E[N_S] + \frac{N_{RTT}}{1-(1-e^{-1})^{N_{Rep}}}\right) L_p T_b$$

The number of transmissions required for a successful transmission conditioned on a success occurring within the $N_{Rep}$ transmissions of a single attempt $N_S$ has the following truncated and scaled geometric distribution:

$$p_{N_S}(n_s) = \begin{cases} \dfrac{e^{-1}(1-e^{-1})^{n_s-1}}{1-(1-e^{-1})^{N_{Rep}}} \ , & for\ n_s = 1, 2, \dots, N_{Rep} \\ 0 \ , & otherwise \end{cases}$$

The expected value of $N_S$ is then:

$$E[N_S] = \sum_{n_s=1}^{N_{Rep}} n_s\, p_{N_S}(n_s) = \frac{1}{1-(1-e^{-1})^{N_{Rep}}} \cdot \sum_{n_s=1}^{N_{Rep}} n_s \cdot e^{-1}(1-e^{-1})^{n_s-1}$$

Simplifying the expression above:

$$E[N_S] = \frac{1}{1-(1-e^{-1})^{N_{Rep}}} \cdot \frac{1 - N_{Rep}e^{-1}(1-e^{-1})^{N_{Rep}} - (1-e^{-1})^{N_{Rep}}}{e^{-1}}$$

Combining the quotients results in the final form:

$$E[N_S] = \frac{1 - N_{Rep}e^{-1}(1-e^{-1})^{N_{Rep}} - (1-e^{-1})^{N_{Rep}}}{e^{-1} - e^{-1}(1-e^{-1})^{N_{Rep}}}$$

The expected delay for the other users when a user with a strict time deadline is present on the channel has the familiar form from Appendix B.1:

$$E[T_w] = E\left[(N_A + N_{RTT})N_{TX}L_pT_b\right] = (E[N_A] + N_{RTT})E[N_{TX}]L_pT_b \quad ,$$

where $E[N_A]$ is again equal to $v$. The number of transmission attempts required $N_{TX}$ is now geometrically distributed with parameter $p$ equal to:

$$p = P_{N-2}P_{clear} \quad ,$$

where $P_{N-2}$ is the probability that the other $N-2$ users do not transmit on the ALOHA slot during which a transmission attempt occurs and $P_{clear}$ is the probability that the time deadline user is not performing a repeated transmission on the slot. Note that these probabilities are independent. Following a similar justification to Appendix B.1, the value of $P_{N-2}$ is approximated as $e^{-1}$. The probability $P_{clear}$ is approximated as the average fraction of ALOHA slots that remain clear of time deadline user transmissions in a single RTT. Note that it is assumed that only one time deadline packet is present during each RTT. The value of $P_{clear}$ is then approximated as:

$$P_{clear} = \frac{N_{RTT} - N_{Rep}}{N_{RTT}}$$

Therefore, since the expected value of the geometric distribution for $N_{TX}$ is equal to $p^{-1}$, the expression for $E[N_{TX}]$ is:

$$E[N_{TX}] = e \cdot \left( \frac{N_{RTT}}{N_{RTT} - N_{Rep}} \right)$$

Substituting the expressions for $E[N_A]$ and $E[N_{TX}]$ into the expression for $E[T_w]$ leads to the final form:

$$E[T_w] = \frac{e \cdot N_{RTT}(v + N_{RTT}) L_p T_b}{N_{RTT} - N_{Rep}}$$

# Appendix C

# Derivations for Equations in Chapter 4

## C.1 SNR Derivations for Section 4.1.1

The signal-to-noise ratio is essentially a ratio of received signal power to received noise and interference power. In its most basic form, the SNR in the presence of an interferer is then:

$$SNR = \frac{E_{TX} G_{RX} F_p}{E_I G_{RX} F_p + N_0 W_d} \quad ,$$

where it is assumed that the interferer's signal is additive with the ambient channel noise. Note that signals from the user and interferer are able to take advantage of the receiver antenna's gain $G_{RX}$ while the ambient noise is not. Additionally, the user and interferer's signals suffer attenuation due to path loss $F_p$ while the ambient noise does not. The expression above does not account for power advantages provided to the user through the use of antenna nulling spectrum spreading. When both antenna nulling and a spread spectrum technique such as DS spreading is introduced, the broadband interferer's power is further attenuated by a factor equal to $G_p G_n$ of the system resulting in the expression:

$$SNR = \frac{E_{TX} G_{RX} F_p}{E_I G_{RX} F_p G_p^{-1} G_n^{-1} + N_0 W_d}$$

Using the expression above as a starting point, the SNR for the downlink of the SATCOM system acting as a relay can be developed by noting that modifications must be made to $E_{TX}$ and $E_I$ to model the power robbing that occurs on the uplink. Both $E_{TX}$ and $E_I$ must be converted to a fraction of the EIRP available for transmission by the satellite $E_{sat}$ which is proportional to the strength of the signals received by the satellite on its uplink. The total signal strength observed $P_{Total}$ by the uplink channel of the satellite is simply the sum of the power from user signals and the interferer signal:

$$P_{Total} = (1 - e^{-1})N_C E_{TX} G_{RX} F_p + E_I G_{RX} F_p G_n^{-1} \quad ,$$

where it is assumed that $(1 - e^{-1})$ of the channels will have signals on them with a transmitted EIRP of $E_{TX}$ at any given time. This assumption is based on the fact that the probability of a success or collision occurring on an ALOHA slot is $1 - e^{-1}$ when the ALOHA channel is operating at full capacity [4]. Note that the processing gain does not affect the interferer's ability to siphon power from the downlink since no signal processing is performed. The fraction of $E_{sat}$ that is devoted to the interferer's signal $r_I$ is given by the following expression:

$$r_I = \frac{E_I G_{RX} F_p G_n^{-1}}{(1 - e^{-1})N_C E_{TX} G_{RX} F_p + E_I G_{RX} F_p G_n^{-1}}$$

Which simplifies to:

$$r_I = \frac{E_I G_n^{-1}}{(1 - e^{-1})N_C E_{TX} + E_I G_n^{-1}}$$

Similarly, the fraction of $E_{sat}$ devoted to signals from legitimate users $r_U$ has the following form:

$$r_U = \frac{(1-e^{-1})N_C E_{TX}}{(1-e^{-1})N_C E_{TX} + E_I G_n^{-1}}$$

Using the expressions for $r_I$ and $r_U$ the previous expression for SNR can be modified to incorporate the effect of power robbing by noting that $E_{TX} = [E_{sat} r_U]/[(1-e^{-1})N_C]$ and $E_I = E_{sat} r_I$. The additional term of $(1-e^{-1})N_C$ in the expression for $E_{TX}$ is used to take into account that the total power available for signals from legitimate users must be divided among all active channels. The expression for the SNR for the downlink case is then:

$$SNR = \frac{\frac{E_{sat} r_U}{(1-e^{-1})N_C} G_{RX} F_p}{E_{sat} r_I G_{RX} F_p G_p^{-1} G_n^{-1} + N_0 W_d}$$

Substituting in using the expressions for $r_I$ and $r_U$ yields:

$$SNR = \frac{\frac{E_{sat}}{(1-e^{-1})N_C}\left(\frac{(1-e^{-1})N_C E_{TX}}{(1-e^{-1})N_C E_{TX} + E_I G_n^{-1}}\right) G_{RX} F_p}{E_{sat}\left(\frac{E_I G_n^{-1}}{(1-e^{-1})N_C E_{TX} + E_I G_n^{-1}}\right) G_{RX} F_p G_p^{-1} G_n^{-1} + N_0 W_d}$$

Some simplifying of the expression above leads to the final form:

$$SNR_{DR} = \frac{E_{sat}\left(\frac{E_{TX}}{(1-e^{-1})E_{TX} N_C + G_n^{-1} E_I}\right) G_{RX} F_P}{E_{sat}\left(\frac{G_n^{-1} E_I}{(1-e^{-1})E_{TX} N_C + G_n^{-1} E_I}\right) G_{RX} F_P G_p^{-1} + N_0 W_d}$$

The SNR for the uplink of the system using onboard signal processing has the same form as the generic expression for SNR developed previously in this section since power robbing does not occur in this scheme. Therefore, $SNR_{UP}$ has the following form:

$$SNR_{UP} = \frac{E_{TX} G_{RX} F_p}{E_I G_{RX} F_p G_p^{-1} G_n^{-1} + N_0 W_d}$$

The SNR for the downlink of the onboard processing scheme is derived from the generic SNR case by noting that there is on interferer signal present on the downlink due to the signal processing performed on the uplink. This leads to the expression:

$$SNR = \frac{E_{TX} G_{RX} F_p}{N_0 W_d}$$

However, the transmitted downlink power per user signal is no longer $E_{TX}$, but is rather $E_{sat}$ divided equally among the $(1 - e^{-1})N_C$ channels that are expected to be active at any given time. Therefore, the final expression for $SNR_{DP}$ is:

$$SNR_{DP} = \frac{E_{sat} G_{RX} F_p}{(1 - e^{-1}) N_C \, N_0 W_d}$$

## C.2 Derivation of Limit for Section 4.1.2

In order to derive $I/S_{Req}$ for the power-limited case, it is first necessary to understand how it is derived in the generic case. Assuming that ambient noise power is negligible compared to the interferer's power, the expression for $E_b/N_T$ in the generic case is:

$$E_b/N_T = \frac{G_n E_{TX} F_p G_{RX}/W_d}{E_I F_p G_{RX}/W_{ss}} \quad ,$$

where the interferer must spread its power over $W_{ss}$ while the user can spread its power over the narrower band $W_d$. Simplifying and rearranging the equation above yields:

$$E_I/E_{TX} = G_n \cdot \frac{W_{ss}/W_d}{E_b/N_T}$$

Noting that $I/S_{Req}$ is equivalent to $E_I/E_{TX}$:

$$I/S_{Req} = G_n \cdot \frac{W_{ss}/W_d}{E_b/N_T}$$

A similar method can be employed to determine $I/S_{Rob}$. Letting $N_T = N_I + N_0$, where $N_I$ is the power spectral density of the broadband interferer in watts per hertz, the expression for $E_b/N_T$ for the power robbing case is:

$$E_b/N_T = \frac{\left(\frac{E_{sat}}{(1-e^{-1})N_C}\right)\left(\frac{(1-e^{-1})N_C E_{TX}}{(1-e^{-1})N_C E_{TX} + E_I G_n^{-1}}\right)\left(\frac{F_p G_{RX}}{W_d}\right)}{N_0 + E_{sat}\left(\frac{E_I G_n^{-1}}{(1-e^{-1})N_C E_{TX} + E_I G_n^{-1}}\right)\left(\frac{F_p G_{RX}}{W_{ss}}\right)} \quad ,$$

where the satellite downlink EIRP that is allocated to user signals is assumed to be evenly split among the $(1-e^{-1})N_C$ channels expected to be active. Note that the principle change between the expression for $E_b/N_T$ above and the expression for the generic case is that $E_{TX}$ and $E_I$ have been replaced by the portion of $E_{sat}$ that is allocated to each signal type. Simplifying the expression above yields:

$$E_b/N_T = \frac{E_{TX}W_{ss}}{\frac{N_0 W_d W_{ss}\left((1-e^{-1})N_C E_{TX} + E_I G_n^{-1}\right)}{E_{sat}F_p G_{RX}} + E_I G_n^{-1} W_d}$$

Rearranging:

$$E_{TX}W_{ss} = \frac{N_0 W_d W_{ss}\left((1-e^{-1})N_C E_{TX} + E_I G_n^{-1}\right)(E_b/N_T)}{E_{sat}F_p G_{RX}} + E_I G_n^{-1} W_d (E_b/N_T)$$

$$E_{TX}\left[W_{ss} - \frac{N_0 W_d W_{ss}(1-e^{-1})N_C(E_b/N_T)}{E_{sat}F_p G_{RX}}\right] = E_I\left[\frac{N_0 W_d W_{ss} G_n^{-1}(E_b/N_T)}{E_{sat}F_p G_{RX}} + G_n^{-1} W_d (E_b/N_T)\right]$$

$$E_I/E_{TX} = \frac{W_{ss}\left[E_{sat}F_p G_{RX} - (1-e^{-1})N_C W_d N_0 (E_b/N_T)\right]}{G_n^{-1}(E_b/N_T)W_{ss}W_d N_0 + G_n^{-1}(E_b/N_T)W_d E_{sat}F_p G_{RX}}$$

Noting that $I/S_{Rob}$ is equivalent to $E_I/E_{TX}$:

$$I/S_{Rob} = \frac{W_{ss}\left[E_{sat}F_p G_{RX} - (1-e^{-1})N_C W_d N_0 (E_b/N_T)\right]}{G_n^{-1}(E_b/N_T)W_{ss}W_d N_0 + G_n^{-1}(E_b/N_T)W_d E_{sat}F_p G_{RX}}$$

The limiting value $I/S_{Limit}$ can be expressed as:

$$I/S_{Limit} = \lim_{W_{ss}\to\infty} I/S_{Rob} = \lim_{W_{ss}\to\infty} \frac{W_{ss}\left[E_{sat}F_p G_{RX} - (1-e^{-1})N_C W_d N_0 (E_b/N_T)\right]}{G_n^{-1}(E_b/N_T)W_{ss}W_d N_0 + G_n^{-1}(E_b/N_T)W_d E_{sat}F_p G_{RX}}$$

The numerator and denominator of the expression above both approach infinity in the limit, necessitating the application of L'Hospital's Rule:

$$I/S_{Limit} = \lim_{W_{ss}\to\infty} \frac{E_{sat}F_pG_{RX} - (1-e^{-1})N_CW_dN_0(E_b/N_T)}{G_n^{-1}(E_b/N_T)W_dN_0}$$

Simplifying and rearranging:

$$I/S_{Limit} = \frac{E_{sat}F_pG_{RX}}{G_n^{-1}(E_b/N_T)N_0W_d} - \frac{(1-e^{-1})N_CN_0W_d(E_b/N_T)}{G_n^{-1}(E_b/N_T)N_0W_d}$$

$$I/S_{Limit} = \frac{G_nE_{sat}F_pG_{RX}}{(E_b/N_T)N_0W_d} - G_n(1-e^{-1})N_C$$

# Appendix D

# Derivations for Equations in Chapter 5

## D.1 Derivations of Results for Section 5.1.2

The unnormalized distribution of $N$ given that a hole is observed is:

$$P_v(n) \cdot H_q(n) = \frac{v^n e^{-v}}{n!} \cdot (1-q)^n$$

Letting $w = 1 - q$, and multiplying the right hand side of the equation above by $e^{-vw}/e^{-v(1-q)}$ yields:

$$P_v(n) \cdot H_q(n) = \frac{(vw)^n e^{-vw}}{n!} \cdot e^{-v+v(1-q)}$$

Noting that $(vw)^n e^{-vw}/n!$ is a Poisson distribution with mean $vw$, which will be written as $P_{vw}(n)$, the expression above can be simplified to:

$$P_v(n) \cdot H_q(n) = e^{-vq} \cdot P_{vw}(n)$$

The unnormalized distribution of $N$ given that a success is observed is:

$$P_v(n) \cdot S_q(n) = \frac{v^n e^{-v}}{n!} \cdot (1-\alpha) \binom{n}{1} q(1-q)^{n-1}$$

Letting $w = 1 - q$, and multiplying the right hand side of the equation above by $e^{-vw}/e^{-v(1-q)}$ yields:

$$P_v(n) \cdot S_q(n) = \frac{(vw)^{n-1}e^{-vw}}{(n-1)!} \cdot (1-\alpha)vq \cdot e^{-v+v(1-q)}$$

Noting that $(vw)^{n-1}e^{-vw}/(n-1)!$ is a Poisson distribution with mean $vw$, which will be written as $P_{vw}(n-1)$, the expression above can be simplified to:

$$P_v(n) \cdot S_q(n) = (1-\alpha)vq \cdot e^{-vq} \cdot P_{vw}(n-1)$$

Since the only possible outcomes for each slot are a hole, succession, or collision, the unnormalized distribution of $N$ given that a collision is observed is simply:

$$P_v(n) \cdot C_q(n) = P_v(n) \cdot \left[1 - H_q(n) - S_q(n)\right]$$

Given that the number of packets in the system is approximated as a Poisson distribution with mean $v$, the number of transmitted packets in a time slot $N_{TS}$ is also Poisson-distributed with mean $vq$. The distribution of the number transmitted packets in a time slot $P_{vq}(n_{TS})$ is used to normalize the conditional distributions of $N$ developed in this section to achieve the final conditional distributions. The final distribution of $N$ given that a hole is observed is:

$$P_{N|H}(n) = \frac{e^{-vq} \cdot P_{vw}(n)}{P_{vq}(0)} = \frac{e^{-vq} \cdot P_{vw}(n)}{e^{-vq}}$$

Simplifying the expression above yields:

$$P_{N|H}(n) = P_{vw}(n)$$

The final distribution of $N$ given that a success is observed is:

$$P_{N|S}(n) = \frac{(1-\alpha)vq \cdot e^{-vq} \cdot P_{vw}(n-1)}{(1-\alpha)P_{vq}(1)} = \frac{vq \cdot e^{-vq} \cdot P_{vw}(n-1)}{vq \cdot e^{-vq}}$$

Simplifying the expression above yields:

$$P_{N|S}(n) = P_{vw}(n-1)$$

The final distribution of $N$ given that a collision is observed is:

$$P_{N|C}(n) = \frac{P_v(n) \cdot \left[1 - H_q(n) - S_q(n)\right]}{1 - P_{vq}(0) - P_{vq}(1)} = \frac{P_v(n) \cdot \left[1 - H_q(n) - S_q(n)\right]}{1 - e^{-vq} - (1-\alpha)vq \cdot e^{-vq}}$$

The expectation of the final distribution of $N$ given that a collision is observed is:

$$E[N|C] = \sum_{i=1}^{\infty} \frac{i \cdot P_v(i) \cdot \left[1 - H_q(i) - S_q(i)\right]}{1 - e^{-vq} - (1-\alpha)vq \cdot e^{-vq}} = \frac{\sum_{i=1}^{\infty} i \cdot \frac{v^i e^{-v}}{i!} \cdot \left[1 - (1-q)^i - (1-\alpha)(1-q)^{i-1}\right]}{1 - e^{-vq} - (1-\alpha)vq \cdot e^{-vq}}$$

Simplifying:

$$E[N|C] = \frac{v \cdot e^{-vq}(\alpha + e^{vq} + q - 2)}{e^{-vq}(e^{vq} - 1 - (1-\alpha)vq)} = \frac{v(\alpha + e^{vq} + q - 2)}{e^{vq} - 1 - (1-\alpha)vq}$$

Assuming that $q = 1/v$ and that $v \geq 1$:

$$E[N|C] = \frac{v\alpha + ve + vq - 2v}{e - 1 - (1 - \alpha)} = \frac{v(e - 2 + \alpha) + 1}{e - 2 + \alpha}$$

Simplifying:

$$E[N|C] = v + \frac{1}{e - 2 + \alpha}$$

## D.2 Optimization for Section 5.1.3

The probability of observing $N_\alpha$ time slots with transmissions for the interferer out of $N_h$ time slots is:

$$P_{N_\alpha|N_h \cap \alpha}(n_\alpha) = \binom{N_h}{n_\alpha} \alpha^{n_\alpha}(1 - \alpha)^{N_h - n_\alpha}$$

The maximum likelihood hypothesis test selects the value $\alpha$ that maximizes the probability described above. Differentiating with respect to $\alpha$ yields:

$$\frac{d}{d\alpha} P_{N_\alpha|N_h \cap \alpha}(n_\alpha) = \binom{N_h}{n_\alpha} [\alpha^{n_\alpha}(n_\alpha - N_h)(1 - \alpha)^{N_h - n_\alpha - 1} + n_\alpha \alpha^{n_\alpha - 1}(1 - \alpha)^{N_h - n_\alpha}]$$

Optimizing:

$$\frac{d}{d\alpha} P_{N_\alpha|N_h \cap \alpha}(n_\alpha) = 0 = \binom{N_h}{n_\alpha} [\alpha^{n_\alpha}(n_\alpha - N_h)(1 - \alpha)^{N_h - n_\alpha - 1} + n_\alpha \alpha^{n_\alpha - 1}(1 - \alpha)^{N_h - n_\alpha}]$$

$$0 = \alpha^{n_\alpha}(n_\alpha - N_h)(1 - \alpha)^{N_h - n_\alpha - 1} + n_\alpha \alpha^{n_\alpha - 1}(1 - \alpha)^{N_h - n_\alpha}$$

$$0 = \alpha(n_\alpha - N_h) + n_\alpha(1 - \alpha)$$

$$0 = \alpha n_\alpha - \alpha N_h + n_\alpha - \alpha n_\alpha$$

$$\alpha N_h = n_\alpha$$

$$\alpha = n_\alpha / N_h$$

Therefore, choosing $\hat{\alpha} = N_\alpha / N_h$ maximizes the probability of choosing the correct value of $\alpha$.

## D.3 Derivation of Chernoff Bound for Section 5.3

Let $Z_i$ be a binary random variable modelling the outcome of the i[th] collision detection test. The conditional distributions of $Z_i$ are then:

$$Z_i|collision = \begin{cases} 1, & w.p. \ P_d \\ 0, & w.p. \ 1 - P_d \end{cases}$$

$$Z_i|hole = \begin{cases} 1, & w.p. \ P_{f,T} \\ 0, & w.p. \ 1 - P_{f,T} \end{cases}$$

The aggregate outcome on the $N_{sym}$ independent collision detection tests can then be modelled as a random variable $S_N$ with the form:

$$S_N = \sum_{i=1}^{N_{sym}} Z_i$$

The probability of the system detecting a genuine collision $P_D$, given the threshold value $\eta$, is then:

$$P_D = Pr\{S_N \geq \eta | collision\}$$

Similarly, the probability of the system generating a false alarm $P_{FA}$ (declaring a hole slot a collision) is:

$$P_{FA} = Pr\{S_N \geq \eta | hole\}$$

Since $S_N$ is the sum of IID random variables, it can be upper-bounded using the Chernoff Bound [21]:

$$Pr\{S_N \geq \eta\} \leq exp\left[N_{sym}\left(\gamma_Z(r) - r\frac{\eta}{N_{sym}}\right)\right] \qquad for\, r \geq 0, r \in I(Z) \ ,$$

where $\gamma_Z(r)$ is the natural logarithm of the moment generating function of $Z_i$ and $I(Z)$ is the interval over which the moment generating function of $Z_i$ exists [21]. Since $Z_i$ is a binary random variable [21]:

$$\gamma_Z(r) = ln(1 - p + pe^r) \ ,$$

where $p$ is the probability that $Z_i = 1$. Minimizing $\gamma_Z(r) - r\eta/N_{sym}$ to obtain the tightest upper bound on $P_D$ and $P_{FA}$:

$$\frac{d}{dr}\left(\gamma_Z(r) - r\frac{\eta}{N_{sym}}\right) = \frac{pe^r}{1 - p + pe^r} - \frac{\eta}{N_{sym}} = 0$$

$$pe^r = \frac{\eta}{N_{sym}}(1 - p + pe^r)$$

$$\left(\frac{pN_{sym} - \eta p}{N_{sym}}\right)e^r = \frac{\eta - \eta p}{N_{sym}}$$

$$r^* = ln\left(\frac{\eta - \eta p}{pN_{sym} - \eta p}\right)$$

Since $r \geq 0$ and $ln(x) \geq 0$ for $x \geq 1$, the following condition is placed on $\eta$:

$$\frac{\eta - \eta p}{pN_{sym} - \eta p} \geq 1$$

$$\eta - \eta p \geq pN_{sym} - \eta p$$

$$\eta \geq pN_{sym}$$

Substituting $r^*$ into the bound on $S_N$:

$$Pr\{S_N \geq \eta\} \leq exp\left[N_{sym}\left(ln\left(1 - p + p \cdot exp\left[ln\left(\frac{\eta - \eta p}{pN_{sym} - \eta p}\right)\right]\right) - \frac{\eta}{N_{sym}} ln\left(\frac{\eta - \eta p}{pN_{sym} - \eta p}\right)\right)\right]$$

Simplifying:

$$Pr\{S_N \geq \eta\} \leq exp\left[N_{sym} ln\left(1 - p + \frac{\eta - \eta p}{N_{sym} - \eta}\right) - \eta \cdot ln\left(\frac{\eta - \eta p}{pN_{sym} - \eta p}\right)\right]$$

$$Pr\{S_N \geq \eta\} \leq exp\left[ln\left\{\left(1 - p + \frac{\eta - \eta p}{N_{sym} - \eta}\right)^{N_{sym}}\right\} + ln\left\{\left(\frac{pN_{sym} - \eta p}{\eta - \eta p}\right)^{\eta}\right\}\right]$$

$$Pr\{S_N \geq \eta\} \leq exp\left[ln\left\{\left(1 - p + \frac{\eta - \eta p}{N_{sym} - \eta}\right)^{N_{sym}}\right\}\right] exp\left[ln\left\{\left(\frac{pN_{sym} - \eta p}{\eta - \eta p}\right)^{\eta}\right\}\right]$$

$$Pr\{S_N \geq \eta\} \leq \left(1 - p + \frac{\eta - \eta p}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{pN_{sym} - \eta p}{\eta - \eta p}\right)^{\eta}$$

Noting that $p = P_d$ given a genuine collision and $p = P_{f,T}$ given a hole, $P_D$ and $P_{FA}$ can be expressed as:

$$P_D = Pr\{S_N \geq \eta | collision\} \leq \left(1 - P_d + \frac{\eta - \eta P_d}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_d - \eta P_d}{\eta - \eta P_d}\right)^{\eta}$$

$$P_D \leq \left(1 - P_d + \frac{\eta - \eta P_d}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_d - \eta P_d}{\eta - \eta P_d}\right)^{\eta} \quad for\ \eta \geq P_d N_{sym}$$

$$P_{FA} = Pr\{S_N \geq \eta | hole\} \leq \left(1 - P_{f,T} + \frac{\eta - \eta P_{f,T}}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_{f,T} - \eta P_{f,T}}{\eta - \eta P_{f,T}}\right)^{\eta}$$

$$P_{FA} \leq \left(1 - P_{f,T} + \frac{\eta - \eta P_{f,T}}{N_{sym} - \eta}\right)^{N_{sym}} \left(\frac{N_{sym} P_{f,T} - \eta P_{f,T}}{\eta - \eta P_{f,T}}\right)^{\eta} \quad for\ \eta \geq P_{f,T} N_{sym}$$

# Bibliography


[1] A. Tellis, Statement to the House, Committee on Armed Services. *China's Counterspace Programs - Only More Bad News,* Hearing, January 28, 2014.

[2] Defense Science Board Task Force on Achieving Ineroperability in a Net-Centric Environment, "Creating an Assured Joint DoD and Interagency Interoperable Net-Centric Enterprise," Office of the Under Secretary for Defense for Acquisition, Technology, and Logisitics, Washington D.C., 2009.

[3] J. Chapin and V. Chan, "Architecture Concepts for a Future Heterogeneous, Survivable Tactical Internet," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, San Diego, 2013.

[4] R. Rivest, "Network Control by Bayesian Broadcast," *IEEE Trans. Inf. Theory,* vol. 33, no. 3, pp. 323-328, 1987.

[5] R. Pickholtz, D. Schilling and L. Milstein, "Theory of Spread-Spectrum Communications - A Tutorial," *IEEE Trans. Commun.,* vol. 30, no. 5, pp. 855-884, 1982.

[6] M. Simon, J. Omura, R. Scholtz and B. Levitt, Spread Spectrum Communications Handbook, New York: McGraw-Hill, 2002.

[7] J. Stine and D. Portigal, "An Introduction to Spectrum Management," MITRE, 2004.

[8] D. Bertsekas and R. Gallager, "Slotted Aloha," in *Data Networks*, Englewood Cliffs, Prentice Hall, 1992, pp. 277-286.

[9] R. Gallager, Principles of Digital Communication, New York: Cambridge University Press, 2008.

[10] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," *IEEE Trans. Inf. Theory,* vol. 13, no. 4, pp. 619-621, 1967.

[11] Fujitsu, "56 GSa/s 8-bit Analog-to-Digital Converter," 2010. [Online]. Available: http://www.fujitsu.com/emea/news/pr/fseu-en_20100913-978.html. [Accessed 18 January 2016].

[12] H. Sorensen, M. Heideman and C. Burrus, "On Computing the Split-Radix FFT," *IEEE Trans. Acoust., Speech, Signal Process.,* vol. 34, no. 1, pp. 152-156, 1986.

[13] Intel, "Intel® Core i7-900 Desktop Processor Extreme Edition Series," 2011. [Online]. Available: http://download.intel.com/support/processors/corei7ee/sb/core_i7-900_d_x.pdf. [Accessed 18 January 2016].

[14] Xicom Technology, "500W Ka-Band Antenna Mount High Power Amplifiers," 2011. [Online]. Available: http://www.xicomtech.com/products/documents/XTD-500Ka-KaL%20Rev%2010.pdf. [Accessed 18 January 2016].

[15] Teledyne MEC, "TWT Performance Fundamentals," 2014. [Online]. Available: http://www.teledyne-mec.com/products/technical_description.aspx. [Accessed 18 January 2016].

[16] University of Hawai'i, "Antenna Introduction/Basics," [Online]. Available: http://www.phys.hawaii.edu/~anita/new/papers/militaryHandbook/antennas.pdf. [Accessed 16 January 2016].

[17] L. Liu, "Simulation and Analysis of Slotted Aloha on Long-Delay Channel Under Variable Packet Arrival Rate," Internal Report, 2015.

[18] J. Tsitsiklis, "Analysis of a Multiaccess Control Scheme," *IEEE Trans. Autom. Control,* vol. 32, no. 11, pp. 1017-1020, 1987.

[19] W. Imbriale, S. Gao and L. Boccia, Space Antenna Handbook, Hoboken: Wiley, 2012.

[20] J. Sellers, Understanding Space: An Introduction to Astronautics, New York: McGraw-Hill, 2006.

[21] R. Gallager, "Chernoff Bounds," in *Stochastic Processes Theory for Applications*, Cambridge, Cambridge University Press, 2013, pp. 33-36.