8-1-2018

Privacy in Dynamical Systems and Networks: Anonymous Routing and Retail Competition

Omid Javidbakht
Lehigh University, omid.javidbakht@gmail.com

Privacy in Dynamical Systems and Networks: Anonymous Routing and Retail Competition

By

Omid Javidbakht

A dissertation
Presented to the Graduate and Research Committee
of Lehigh University
in Candidacy for the Degree of
Doctor of Philosophy
in
Electrical Engineering

August, 2018

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Date

Advisor

Accepted Date

Committee Members:

Prof. Parv Venkitasubramaniam
(Committee Chair)

Prof. Rick S. Blum

Prof. Daniel Conus

Prof. Alberto J. Lamadrid

Prof. Nader Motee

To my parents,

Akram and Reza

To my brother,

Farid

To my niece,

Hila

1 Acknowledgments

I have had the privilege of having many amazing people in my life that I believe without them, it would be impossible for me to be in the place I am today.

First and foremost, I would like to thank my PhD advisor professor Parv Venkitasubramaniam. I cannot explain it in words how great working with Parv was. He is an outstanding scholar who provides a great environment, and full support for his students to flourish. He has always been the greatest inspiration in my life. Without any doubts, he was the best supervisor, teacher, and mentor for me.

I would also like to thank my PhD committee members. I thank professor Rick S. Blum for teaching me the course Signal Detection and Estimation, and always being available to discuss about different topics including my research. He has a great personality and has always been an inspiration for me.

I thank professor Daniel Conus for teaching me courses Advance Probability, and Financial Calculus. He was one of the best teachers I have ever had and I truly enjoyed all his class sessions. I would like to emphasize here that the knowledge and passion, I earned at his classes were extremely helpful for me to understand Probability Theory and Stochastic Processes deeply.

I thank professor Alberto J. Lamadrid for collaborating with me in one of the most important works in my PhD titled "retail competition in privacy sensitive markets". He helped me to get a better understanding of Game Theory and through our collaboration, he was extremely helpful, patient, and always available to discuss the details.

I would like to thank professor Nader Motee for teaching me the course Convex Optimization. The knowledge I earned at his class was so helpful for me to investigate the tradeoffs between privacy and utilities in dynamical systems.

My sincere gratitude goes to National Science Foundation (NSF). My PhD research was generously supported by NSF under Grant CNS-1117701 and Grant CCF-1149495.

I would like to thank all the previous and current members of our research group and my labmates, Dr. Abhishek Mishra, Dr. Jiyun Yao, Dr. Anand Srinivas Guruswamy, Dr. Parth Pradhan, Dr. Basel Alnajjab, and Ruochi Zhang, for discussions on various research topics and presenting interesting papers that motivated me to look further into that direction.

I cannot express how lucky I am to have many great friends who were always there for me during happiness and difficulties. I would like to thank all my beloved friends specially Kia Khezeli, Kasra Ghaemi, Emre Akoz, Onur Babat, Patricia Castro de Aguiar, Reza Takapoui, Hossein Karkeh Abadi, Ali Makhdoumi, and Mehdi Yazdanpanah.

Last, but not least, I would like to thank my parents and my brother. I would have never been where I am today without their endless love and support which is why I dedicated this dissertation to them.

Contents

List of Tables

List of Figures

2 Abstract

Tradeoffs between privacy and utilities, and privacy preserving control mechanisms in dynamical systems and networks are studied in this dissertation. Despite security mechanisms and data encryption, these systems are still vulnerable to timing analysis, wherein an eavesdropper can use these observations to interpret the identity of individuals. Motivated by this vulnerability, the first three topics of this dissertation investigates privacy preserving mechanisms in dynamical systems and network. The last chapter studies the effect of privacy awareness of consumers on retail competition.

The first topic of this dissertation studies the tradeoff between delay and packet source anonymity in a network of mixes. The achievable anonymity is characterized analytically for a general multipath model, and it is shown that under light traffic conditions, there exists a unique single route strategy which achieves the optimal delay anonymity tradeoff. A low complexity algorithm is presented that derives the optimal routes to achieve a desired tradeoff. In the heavy traffic regime, it is shown that optimal anonymity is achieved for any allocation of rates across the different routes. Simulations on example networks are presented where it is shown that the optimal routes derived under light traffic performs quite well in general traffic regime.

Next, an analytical framework is presented to integrate and control the degree of link padding mechanisms in the functioning of anonymous relays such that a desired degree of source-destination pair anonymity is achieved from timing analysis without adding significant latency. In particular, the optimal choices of relays and the degree of link padding are investigated to characterize the best tradeoff between anonymity from timing analysis, as measured by Shannon entropy of source destination pairs, and the average latency. The optimization required for the best tradeoff is shown to require exponential complexity, and a sub optimal algorithm is presented that is shown numerically to perform close to the optimal, but only requires linear complexity. In addition, an incremental optimization is presented for a new user to be added optimally to an existing system without altering the prevalent routing scheme.

The third part of this dissertation studies the reward optimal decision making in Markov Decision Processes (MDPs) while protecting against inference of type of MDP. Against an adversary attempting to classify between two MDPs with identical state-action spaces but differing reward functions and transition probabilities, a joint policy design is studied for the pair of MDPs that maximize a weighted sum of infinite horizon discounted rewards. Specifically, the adversary observes the sequence of states with

the goal of identifying which of the two MDPs are in operation, while the controllers are designed such that an ϵ-differential privacy is guaranteed for the observed state transitions. It is demonstrated that a unique optimal weighted discounted reward exists for a fixed privacy parameter and the weighting factor. A value iteration method is proposed to determine the optimal reward and obtain the differentially private policies for the two MDPs. Convergence of the method is proved and the rate of convergence is characterized. A special application of this framework in routing where nodes serve as states is also studied in this section. Using differential privacy as a metric to quantify the privacy of the intended destination in networked data collections, optimal probabilistic routing schemes are investigated under unicast and multicast paradigms. It is shown that the optimal private unicast routing can be implemented in decentralized manner. Under a multicast paradigm, the optimal solution when overhead is weighted equal to the intended cost, the optimal solution is shown to be a variant of the Steiner tree problem. In general, it is proved that multicast private routing is an np-complete problem. Simulations and numerical results for both private unicast and multicast routing on random graphs are presented.

In the last section, the problem of coupon targeting competition between two retailers who sell the same product in a privacy sensitive market is considered. In particular, consumers purchasing decisions are influenced by product prices as well as prior privacy violations by retailers. A Hoteling line model is utilized to investigate the coupon targeting competition between the retailers. Within this framework, privacy sensitivity is modeled using a Markov chain, wherein consumers switch back and forth probabilistically between a privacy alerted state and privacy non-alerted state depending on whether or not they receive targeted coupons from a retailer. The competition between these two retailers at each segment of Hoteling line is modeled by a stochastic nonzero-sum game. In every segment of the Hoteling line, stationary equilibrium strategies of retailers that provide optimal discounted return over an infinite horizon is derived. It is demonstrated that segments in a privacy sensitive market are divided to three categories: 1) Segments not affected by privacy constraints. 2) Segments fully affected by privacy constraints. 3) Segments partially affected by privacy constraints. It is illustrated that in contrast to a price sensitive market, when privacy is a factor, consumers with weak brand loyalty can be driven away from the popular retailer because of a targeted coupon from that retailer. It is also proved that the popular retailer will be more conservative distributing targeted coupon to consumers with weak preference for him whilst the rival retailer will be more offensive on these consumers.

3 Introduction

Information security in dynamical systems and networks extends beyond the protection of communicated data; hiding the identities of parties is equally critical. Knowledge of individuals' identities in a network such as source-destination pairs and routes of information flow in networks which can be obtained fully or partially through eavesdropping in a network not only compromises user privacy, but also provides crucial information for an adversary to jam a particular flow, deploy black holes or launch other sophisticated attacks. One of the earliest uses of such analysis occurred in World War II [1], when the US Army established a Traffic Intelligence group (OP-G-20) on Corregidor island [2]. These traffic analysts, much before they broke the enemy cipher code, were able to use transmission timing to identify enemy chain of command and to a good extent, predict troop movements. Since the advent of the Internet, such retrieval of "networking information" through traffic analysis, and more specifically *transmission timing analysis*, has been a critical concern in the design and analysis of network protocols [3,4].

In this dissertation, we investigate the protection of the users' privacy in dynamical systems, and networks against an adversary who fully or partially observes the state of the system. We demonstrate that users can achieve privacy, however, they may receive lower utilities. In other words, we illustrate that privacy is achieved in cost of experinecing higher latency, achieving lower data rate, or receiving a lower reward in general framework. We derive the routing and control mechanisms for optimal tradeoffs between privacy measured by Shannon entropy [5] or differential privacy [6] and utilities in dynamical systems and networks. Specifically, we consider privacy preserving methodologies for three applications: 1) Packet source anonymity in mix networks. 2) Source-destination pair anonymity in networks 3) Markov Decision Processes (MDPs) under differential privacy constraints. While privacy preserving mechanisms and tradeoffs between privacy and utilities are well-studied in the literature, other related topics such as the influence of users' privacy awareness on other phenomena including retail competition require more attention. For example, privacy violations by an online social media or an online retailer can result in users' distrust which can drive users away to other social medias or retailers. The experiment by Tsai [7] is an evidence that consumers' privacy awareness has increased and consumers prefer to purchase from online retailers who protect their privacy. Motivated by privacy awareness of consumers, in the last chapter of this dissertation, we study the coupon targeting competition of retailers in a privacy sensitive market, where consumers may get privacy alerted and change their purchasing brands.

The first and the second topic of this dissertation study the routing and control mechanisms for the optimal tradeoff between latency and packet source anonymity or source-destination pairs anonymity in networks. The methodology to hide source identities from timing analysis was first investigated by David Chaum [8]. Chaum proposed the concept of mixes which are special proxy servers or routers that use layered encryption, random bit padding and packet shuffling (or batching) to provide anonymity. The encryption and bit-padding ensure that an eavesdropper monitoring the transmission links cannot use the contents or sizes of packets to matching an incoming packet to the mix with the corresponding outgoing packet from the mix. The packet shuffling reduces the correlation between the timing of incoming and outgoing packets. In practice, a network of such mixes are deployed and the packets from sources are routed through an arbitrary sequence of mixes prior to arriving at the destination. In popular anonymous systems, many of them deployed on the Internet, however, shuffling strategies are rarely used and the analysis of transmission times can still reveal to an adversary the identities of communicating parties and paths of data flow. In fact, a careful read of the disclaimers in the largest publicly deployed anonymity network, Tor, reveals an open admittance of vulnerability to timing analysis (see [9]). The primary reason for this vulnerability is that these systems impose tight latency constraints on the transmitted packets to satisfy Quality of Service (QoS) requirements and consequently measures to limit timing based inference such as mixing are not implemented under latency constraints. In general, modifications to timing through packet shuffling and link padding increase the latency of transmitted packets, and consequently, when packets are subjected to strict latency constraints, the abilities of mixes to shuffle are restrained, thereby reducing the achievable packet source anonymity or source-destination pair anonymity. Fundamentally, there is a tradeoff between the achievable anonymity and the allowed delay in data networks. In recent years, there has been significant progress towards the design of optimal mixing strategies and link padding mechanisms under such strict delay constraints [10–15]. These results primarily study the optimal design of packet shuffling and link padding for a single node. This work expands on that investigation to study the packet source and source-destination optimal anonymity latency tradeoff achievable in data networks with particular emphasis on the optimal routing through the network that maximizes a desired tradeoff.

In the first chapter, we investigate the problem of optimal routing to achieve tradeoff between packet source anonymity and latency in a network of mixes. Our approach relies on an information theoretic measure of anonymity, quantified using Shannon entropy of sources of packets arriving at destinations as observed by an omniscient eavesdropper. While the maximum achievable anonymity as a function of delay is still an open problem, we consider two extreme traffic rate regimes where the anonymity has been better investigated analytically - heavy traffic regime $\lambda \to \infty$ and the light traffic regime $\lambda \to 0$ to study the properties of optimal rate allocation in the multipath system. It is known that, when Shannon entropy is used to quantify the anonymity, in the heavy traffic regime, the anonymity of the individual mix approaches the prior entropy of arrival rates as $\lambda \to \infty$, and in the light traffic regime, the anonymity-delay tradeoff is linear and can be expressed using the light traffic derivative [16]. Using this entropy based metric, we demonstrate: 1) In the heavy traffic regime, the impact of rate allocation on the anonymity of the multipath system is negligible, or in other words, optimal routing in the heavy traffic regime can be designed based solely on traditional QoS considerations such as latency, throughput and congestion (which expectedly become critical in high rate regimes). 2) In the light traffic regime, we investigate the anonymity and delay as functions of rate allocation, topology of the network, and delay constraint of mixes. First, we show that to achieve the optimal tradeoff between anonymity and delay, single route solutions are optimal for each source. Based on this investigation, we propose a low complexity algorithm to determine the optimal route for each source. 3) Although the optimal rate allocation for medium (non extreme) traffic rates is theoretically an open problem, in our numerical results, we demonstrate that the light traffic optimal scheme outperforms other heuristic rate allocation schemes. 4) We also apply our results to a graphical model of practical anonymous systems (based on an abstraction of the popular Tor system) and demonstrate that the derived solution displays optimal scaling behavior as the network size increases.

The second topic of this dissertation studies the optimal relay selection and control of relay "operational modes" in an anonymous network. We consider a six relay subsystem abstraction based on the practical anonymous system Tor. This abstraction, although not without loss of generality, naturally follows from the present operation of the Tor network where each user chooses the sequence of three intermediate nodes based on bandwidth availability and delay-shortest path considerations. Another reason for this abstraction is the fact that not all users in an anonymous network have the same preference on delay and anonymity. By considering a subgroup of relays and optimizing their operation independently, that subgroup can cater to the subset of users with similar preferences for the levels of anonymity and delay. Considering six relay abstraction, our key contributions are summarized as follows. Using Shannon entropy as the metric for anonymity from timing analysis, we characterize the maximum possible anonymity as a function of the relay selection and *anonymization* parameters, and provide conditions on bandwidth under which this anonymity is achievable. When the bandwidth constraints are satisfied, the problem of optimal relay selection that maximizes a weighted combination of anonymity and delay is shown to be a computationally hard problem. In other words, we show that solving the resulting optimization problem requires exponential computation time $O(2^N)$, where N is the number of users. We therefore propose a sub-optimal heuristic based on Hill Climbing method which has linear complexity $O(N)$ and demonstrate that the achieved tradeoff for the proposed algorithm is close to optimal. In addition to the global optimization, we also present incremental optimization and discuss a decentralized scheme. We prove that incremental scheme always achieves the global optimal when maximum anonymity is desired.

The third section of this dissertation studies the design of control policies under differential privacy constraints. Markov decision processes (MDPs) are a discrete time mathematical framework for modeling decision making in dynamic systems. In a classical MDP, at each time step, the system is in some state s, and the controller decides on an action a. Given the current state s, and controller's action a, the controller receives a reward, and the state of the system transit to the next state according to a Markovian probability $P(s'|s, a)$, and the controller's goal is to maximize the total (discounted) reward over a finite or infinite horizon [17]. MDPs are widely used in cyber physical systems, finance, robotics, etc. Another important application of MDP is in reinforcement learning [18], where an agent interacts with an unknown environment towards maximizing some objective, and the underlying process is modeled as an MDP. The main difference between a classical MDP and reinforcement learning is that the latter does not assume the knowledge of the mathematical model of the MDP. In many applications of MDPs, the sequence of states (or some function of the states) are observable to eavesdroppers. For example, in a wireless network, an adversary can access length of packets [19], timing of packets transmitted [20], routes of packet flow over a network [21] and suchlike by eavesdropping. Using the observations, an adversary can infer about the nature of the MDPs, and consequently obtain sensitive information about the hyphenate decision-making. As machine learning algorithms continually improve the ability to identify personal preferences from seemingly unrelated data, it is critical that stochastic decision making processes be investigated from a privacy perspective which is the focus of this work. Motivated by this, we investigate the mathematical framework of Markov Decision Processes with the objective of limiting adversarial inference of a *type* of MDP. In particular, consider two MDPs with identical state-action spaces but differing reward and transition dynamics. For instance, these could represent user actions on a pair of websites. It is well known that sequence of click times or download sizes can reveal which websites are being accessed even if data transmitted is encrypted [22]. In this context, if the sequence of actions or response times were so designed to maximize user experience, then an eavesdropper can identify the website accessed by performing a hypothesis test on the observations. However, if the actions were so designed such that the observations from the pair of websites had near similar dynamics, then privacy of access can be preserved. In broader terms, for a pair of MDPs, if the policies were jointly designed such that the observed state dynamics for both MDPs were ϵ close to each other in a likelihood sense, then any hypothesis test between the MDPs would have very limited success. It is precisely the joint design of the policies for a pair of generic infinite horizon MDPs that we consider in this work such that a weighted sum of rewards of the two MDPs are maximized subject to an ϵ-differential privacy guarantee for the observed state dynamics. We provide a value iteration method to recursively derive the optimal rewards and the policies for the two MDPs that are differentially private at the desired ϵ level. The proposed method is shown to converge and the convergence rate of this method is proved to be equal to the discount factor. Further, in this section, we investigated an application of MDPs under privacy constraints in routing in networks, where nodes can be considered as states of the MDP. Specifically, the problem of destination privacy in networked data collection under constraints on routing overhead is studied, where, we propose an alternative approach wherein additional destinations are included in the path of transmission to create destination privacy for source packets. In particular, using differential privacy to quantify the privacy of the intended destination, we investigate optimal probabilistic routing for single source destination communication. We propose private routing schemes based on unicast and multicast routing. We demonstrate that the optimal solution of private unicast routing when overhead weighting factor is one is equivalent to the solution of the traveling salesman problem. However, for general overhead weighting factor, the optimal private unicast routing only allocates positive probabilities on $2^M - 2$ routes, where M is total number of destinations. Consequently, optimal routing can be derived by solving the resulting linear programming. When multicast routing is used to provide privacy to a single source-destination setup, we prove that the optimal solution is an np-complete problem. In particular, we demonstrate that the optimal solution of multicast routing when overhead weighting factor is one is equivalent to a Minimum Steiner Tree (MST) and for the general case, we prove that each source will allocate positive probabilities over $2^M - 2$ spanning trees.

In the final section of this dissertation, we study competitive coupon targeting between a pair of retailers when price and privacy are factors in the consumer decision making. We use the privacy sensitivity model as proposed by Sankar et al in [23], wherein consumers are assumed to exist in one of two states with respect to a retailer 1) Non-alerted state where consumers trust a retailer, and 2) Alerted state, where consumers are aware and wary by privacy violations by the retailer. Consumers switch between these states depending on whether they receive targeted coupons from a retailer. Following the coupon targeting model in a price sensitive market in [24], we assume that consumers are located on a Hoteling line such that the location of consumers on the line represents their preference for the retailers. We demonstrate that a privacy sensitive market is divided into 12 segments. Moreover, we derive the optimal stationary coupon targeting policies and discounted rewards for both retailers at each specific segment of the Hoteling line. We prove that consumers with weak preference for a retailer will change their purchasing brand if they notice their privacy is violated by the retailer. We also prove that at segments which adopts mixed strategies, the popular retailer has a less defensive strategy whilst the rival retailer has a more offensive targeting strategy as the discount factor increases. In other words, as the importance of future profit gets higher, the popular retailer will be more conservative about consumers with weak preference for him, because, these consumers are more likely to change their purchasing brand in the future, if they get alerted about this retailer. On the other hand, the rival retailer will be more aggressive to 1) get a higher share of market, 2) push the popular retailer to distribute targeted coupons. Eventually, we demonstrate that despite the price sensitive market, the rival retailer will have a non-negative discounted reward on the consumers with weak preference for the other retailer.

3.1 Related Works

Using Shannon entropy to quantify packet source anonymity, fundamental tradeoffs between delay and packet source anonymity were characterized in [11, 16]. The study of source anonymity in this work treats each packet as an independent entity, similar to the approaches in [16, 25, 26]. This applies to systems with short bursts of transmission such as email, browsing, texting etc. For heavy traffic applications such as peer-to-peer file sharing, multimedia transmission, the entire stream of packets needs to be considered together and individual packet shuffling techniques are no longer sufficient. For a deeper investigation into anonymity for long streams of packets in networks, refer to the work in [10, 27, 28]. Optimal single path routing to provide packet source anonymity has been a subject of analytical investigation in [29–31]. In these and other subsequent improvements, protocols that leverage randomness in routing to provide anonymity at the cost of higher end-to-end delay were studied. The analysis in [29–31], however, did not consider anonymity-delay characteristics of individual mixes or topological influence on anonymity. Since the original design by Chaum, shuffling strategies for mixes have been designed to optimize the tradeoff between local anonymity (secrecy of input-output pairing at a mix) and performance metrics such as delay [32, 33], memory [34], throughput [35] etc. These shuffling strategies study the protection of individual packets as opposed to long streams. Recent signal processing approaches [36,37] have demonstrated fundamental tradeoffs between delay and privacy in timing side channels as well. Protecting streams require the transmission of dummy packets, or in other words link padding, so as to make the outgoing streams from a mix indistinguishable to an external eavesdropper. The minimum rate of dummy packets required and the corresponding padding mechanism have been studied under different traffic and node parameters in [12, 35]. Several of these works consider Poisson arrival processes and derive the optimal strategies and rates. In the second section of this dissertation, we apply the dependent link padding strategies as derived in [12, 35], and use numerical simulations to obtain the corresponding dummy rates for practical heavy tailed traffic processes.

Theoretical analyses of optimal relay selection and control for anonymity are limited in the literature. In [35], the authors considered multi hop communication in adhoc wireless networks under the assumption that routes are fixed apriori and the key parameters to optimize were the modes of operation. By optimizing the selection of relay nodes that add the dummy packets, the authors demonstrated the tradeoff between the throughput and anonymity in the same system model using rate distortion tradeoff in Information Theory. From a practical standpoint, the relay selection or routing problem has been investigated to an extent in the Tor network under different adversarial conditions [38] and under different criteria such as bandwidth constraints[39,40], low latency[40], and autonomous system awareness[41], albeit without taking into consideration timing analysis. The work on Tor systems that is closest to the second topic of this work is [42], where the authors introduced a new Tor client named LASTor where they showed that LASTor can reduce latency in comparison with regular Tor clients by using an appropriate shortest path mechanism. Although, they investigated the delay anonymity tradeoff by doing simulations and showed the performance of their proposed LASTor, they did not consider operational control of relays to investigate the delay anonymity tradeoff.

The literature on privacy in routing is primarily focused on anonymous networks [8,43], where packet encryption and scheduling are used to provide anonymity. Probabilistic routing has been considered from a game theoretic perspective when an adversary has limited knowledge but is capable of intercepting routes [44]. To our best knowledge, there is no work in literature investigating probabilistic unicast and multicast routing to achieve specific degree of differential privacy. Differential privacy was introduced as a tool to provide privacy in data from learners and statisticians [6] and provides a point-wise measure on users privacy (without Bayesian assumptions). Using differential privacy as a metric to quantify privacy, we propose private unicast and multicast routing in data networks.

Algorithms for unicast routing for different applications in data networks have been presented in the literature [45–49], which are typically variants of shortest path algorithms with no additional constraints. Adding constraints such as delay increases the complexity of algorithms; for instance, the problem of unicast routing with cost constraints is an np-hard problem In [46, 47], authors proposed heuristic distributed algorithms for unicast routings under constraints on delay and path cost respectively.

Multicast routing is typically implemented by sending packets through a Steiner tree which spans all the destination nodes. Determining the Minimum Steiner Tree(MST) which has the minimum aggregated cost over all Steiner trees is known to be an np-complete problem [50]. There are some near optimal schemes for Minimum Steiner Tree problem which are run in polynomial time [51–55]. The problem of delay constrained multicast routing is well-studied in [55], where the authors demonstrated that the corresponding problem is np-complete and proposed a heuristic algorithm based on the KMB algorithm.

Tradeoffs between privacy and utility in dynamical and control systems are well-studied in the literature [56–60]. The problem of privacy utility tradeoffs has been explored in [57,58] using a notion the authors refer to as competitive privacy. In [59], the authors investigated filtering in a dynamical systems under differential privacy constraints, where they derived methods developed to approximate a given filter by a differentially private version, so that the distortion caused by the privacy mechanism is minimized. An overview of privacy in control and dynamical system is presented in [60], where two topics of applications of differential privacy in Kalman and general filters, and application of differential privacy to distributed optimization algorithms are studied. In [61], the authors proposed a privacy mechanisms such that at each time, the most accurate approximation of the system's state which preserves the privacy is published. In [62], an optimization framework is presented which solves constrained multi-agent optimization problems while keeping each agent's state differentially private. The authors demonstrated that under mild conditions each agent's optimization problem converges in mean-square to its unique solution while each agent's state is kept differentially private. MDPs under privacy constraints are also studied in the literature. In [56], the authors studied the tradeoff between system utility and achievable privacy in MDPs where privacy is measured by Shannon entropy. In their approach, they expressed the problem of MDP under privacy constraints as a Partially Observable Markov Decision Process (POMDP) with belief dependent rewards. In [63], the authors investigated a subset of decentralized MDPs, where the anonymity in interaction is specified within the joint reward and transition functions. In [64], privacy is modeled by beliefs in system's state, where the authors demonstrated that for MDPs and POMDPs, privacy verification can be computationally derived by solving a set of semi-definite programs and sum-of-squares programs, respectively.

Targeted coupon and advertisements in price sensitive market is well studied in literature [24,65–68]. In [65], targeted advertisement is studied against massive advertisement and it is shown that combination of massive and targeted advertisement can increases retailers profit and social welfare . In [66], the authors demonstrate that each retailer can increase its profit by targeting advertisement on consumers with higher preference for the retailer more than shoppers who may be attracted to the competition, or have weaker preference for the retailer. The problem of competitive one-to-one promotions is considered in [67], where the authors investigate the competition of two retailers in a market where each consumer is individually addressable, and retailers know each consumer's taste. They demonstrated that one-to-one promotion increases price discrimination and decreases the average price in market, and changes market share between two retailers. In [68], the authors investigated coupon targeting competition between two retailers under imperfect price information. Retailers can distribute either ordinary coupon, coupon advertising, or both at the same time. They show that price, promotional effort, and seller's profit is higher in the ordinary coupon equilibrium, compared to coupon advertising equilibrium.

One of the first works on economy of privacy was introduced by Varian [69], where he studied how one may define property rights in private information such that consumers may manage how their private information is shared with retailers. Acqusiti [70] studies the evolution of the economy analysis of privacy by discussing online and offline identities of individuals on ecommerce and their privacy concerns and economic implications. In [71], Acquisiti studies the incentive to participate in an anonymity system which protects identity and privacy. Tsai [7] studied the effect of online privacy information on purchasing behavior of consumers. Specifically, they design an experiment in which privacy policy information was clearly shown before the online purchase and observed that consumers tend to purchase from online retailers who better protect their privacy. In [72], the authors investigated the exchange between two principals who sequentially make contract with an agent, and they prove that based on some conditions, it is optimal if an upstream principle offers the agent full privacy. If any of these conditions is violated, then, disclosure of information may occur. In [73], the authors proved that it is profitable for retailers to offer different prices to consumers based on their purchasing history. Specifically, they considered a problem with a single profit maximizing retailer, and a rational consumer with a set of preferences on the prices offered for the good, as well as on the amount of private information provided. For example, a consumer could stop sharing private information using a number of alternatives including deleting the web browser cookie, changing the payment information (e.g., credit card), or using anonymous paying.

4 Packet Source Anonymity and Delay Tradeoff in Mix Networks: Optimal Routing

In this section, we investigate the protection the source identities of packets that flow through a network towards their intended destination, or in other words, enable anonymous communication over data networks.

The theme of our work can be understood by the routing problem in a simple network shown in Figure 1 where two sources S_1, S_2 transmit packets to the common destination D_1 through a network of three mixes M_1, M_2, M_3. The mixes have delay constraints d_1, d_2, d_3 respectively; in other words, mix M_i can delay a packet for no greater than d_i seconds. Without loss of generality, we assume $d_2 > d_1$. Larger the delay constraint, higher the uncertainty created by the shuffling strategy of an individual mix. Sources have fixed arrival rates, λ_1, λ_2 respectively, and choose to route a fraction of their packets through mix M_1 and the remainder through mix M_2. If both sources transmitted their entire traffic through M_1 their strategy would be delay optimal, but the anonymity achieved would be low since M_1 has limited delay to shuffle packets. If, instead they transmitted their packets all through M_2, the anonymity achieved would be higher but it would incur higher delay. Consequently, the right balance between anonymity and delay would depend on the proportions of each source's traffic transmitted through the two routes, and the strategies and delays of the individual mixes. The following questions that naturally arise in this setup form the basis of this work. 1)Given the topology and delay constraints, does multipath routing increase the anonymity? 2) If it increases anonymity, then, what is the optimal allocation of transmission rates on the different routes for each source destination pair that achieves a desired tradeoff? 3) How does this optimal tradeoff vary with the topology, traffic characteristics and delay parameters of the system?

Through this section, we study multipath routing to achieve optimal tradeoff between packet source anonymity and average latency in data networks. In section 4.1, we present the system model. In section 4.2, we investigate the problem of tradeoff in light traffic. Moreover, we propose a low complexity algorithm to determine optimal single path route four each user to achieve a certain degree of tradeoff. The routing problem in high traffic regime is studied in section 4.4. Finally, we present our simulation results for optimal packet source anonymity and latency tradeoff in section 4.5.

4.1 System Model

A mix network is denoted by a 3-tuple $\mathcal{N} = (G, D, \Lambda)$, where $G = (\mathcal{V}, \mathcal{E})$ is a directed network graph, $\mathcal{V}$ is the set of vertices representing network nodes and $\mathcal{E}$ is the set of edges denoting directed communication links. The set of nodes $\mathcal{V}$ is divided into three mutually exclusive sets: a. $\mathcal{S}$: set of sources. b. $\mathcal{M}$: set of mixes. c. $\mathcal{D}$: set of destinations. D is the set of delay constraints for the elements of set $\mathcal{M}$ and $\Lambda = \{\Lambda_{ij}, 1 \leq i \leq |\mathcal{S}|, 1 \leq j \leq |\mathcal{D}|\}$ is the set of arrival rates for the source-destination pairs. Each element Λ_{ij} denotes the total rate from the source S_i to the destination D_j. In order to study the system under high and low limiting traffic conditions, we parametrize the set Λ by a scalar λ, such that each $\Lambda_{ij} = \lambda R_{ij}$, and R_{ij} is kept constant as $\lambda \to 0$ or $\lambda \to \infty$. We describe the participants of the system in more detail below.

Source: Each source S_i transmits packets to each destination D_j according to an independent Poisson process of rate Λ_{ij}. Given the topology of the network, each source has a fixed and known set of routes to each destination through the mixes and our primary goal is to allocate the transmission rates across these routes to maximize anonymity. The set $\mathcal{P}(S_i, D_j)$ is the set of all the routes from source S_i to the destination D_j such that $P_k^{(i,j)} \in \mathcal{P}(S_i, D_j)$ is a directed walk on the graph G denoting the k^{th} route between source S_i and destination D_j. Specifically, we denote $P_k^{(i,j)} = (S_i, M_{P_k^{(i,j)}}, D_j)$, where $M_{P_k^{(i,j)}}$ is the sequence of mixes on this route. We assume that there are no cycles in any route. For example in Figure 1, $P_1^{(1,1)} = (S_1, M_{P_1^{(1,1)}}, R_1) \in \mathcal{P}(1,1)$, where $M_{P_1^{(1,1)}} = (M_1, M_5, M_{13}, M_{18})$. For every source-destination pair (S_i, D_j), we assume each packet is independently randomly chosen to be transmitted through a specific route in $\mathcal{P}(S_i, D_j)$. Consequently, the resulting set of point processes from source S_i to destination D_j will be independent stationary Poisson processes with rates $\{\lambda_{P_k^{(i,j)}}\}$ respectively.We parametrize each $\lambda_{P_k^{(i,j)}}$ by scalar λ such that $\lambda_{P_k^{(i,j)}} = \lambda r_{P_k^{(i,j)}}$, and $r_{P_k^{(i,j)}}$ is constant as $\lambda \to 0$ or $\lambda \to \infty$. For the pair (S_i, D_j), $\sum_{P_k^{(i,j)} \in \mathcal{P}(i,j)} \lambda_{P_k^{(i,j)}} = \Lambda_{ij}$

We note that the Poisson assumption of arrivals is a limiting one and has been used here due to its analytical tractability. Typical Internet traffic is better modeled using Markov modulated Poisson or Heavy tail distributions. We do expect, albeit without a formal proof, that the broad inferences from this work such as the optimality of single path routing in light traffic and the QoS preferential routing in heavy traffic would hold under other distributions as well.

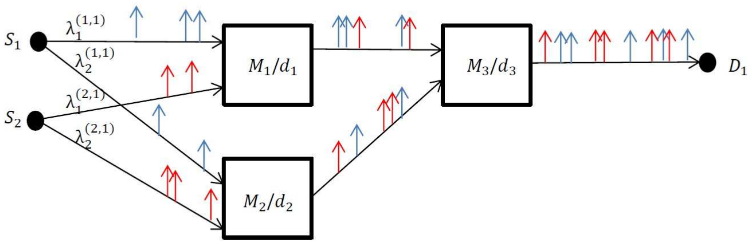


Figure 1: Example Network: S_1, S_2 are sources, M_1, M_2, M_3 are mixes, D_1 is the destination. The rate of packet arrivals allocated on a path S_i, M_k, M_3, D_1 is denoted as $\lambda_k^{(i,1)}$

Mix: Each mix M_i observes point processes on each of its incoming links, each process corresponds to the sequence of packets transmitted by the node originating the link. The sources, prior to transmitting packets to the mixes, employ layered encryption, which is described below:

> Let a source S transmit a message denoted by X to destination R through a sequence of mixes $M_1, \cdots, M_k$. There exists a public private key pair for every mix and the final destination. Let A_N denote the address of node N, and let $E_N(X)$ denote the ciphertext obtained by encrypting message X with the public key of node N. When source S wishes to transmit a message X to destination R through a sequence of mixes $M_1, \cdots, M_k$, it performs multiple layered encryption and generates the ciphertext:
>
> $$E_{M_1}(A_{M_2}, E_{M_2}(A_{M_3}, E_{M_3}(\cdots E_{M_k}(A_R, E_R(X)))) \cdots))$$
>
> which is transmitted to M_1. M_1 upon receiving uses its private key to decrypt the outermost message and determines the address of the subsequent node A_{M_2} and a ciphertext encrypted with the public key E_{M_2} which is then transmitted to M_2. M_2 subsequently decrypts the received message, obtains the address A_{M_3} of the succeeding node M_3 and transmits the E_{M_3} encrypted ciphertext to it. This repeated decryption and transmission continues in sequence until the R-encrypted message $E_R(X)$ reaches the destination node. When such a layered encryption scheme is utilized, each mix is only aware of the immediate preceding and succeeding node in the path of a packet.

Consequent to the layered encryption, the packets that depart from the mix are, from the perspective of an eavesdropper, content-wise not identifiable to a particular

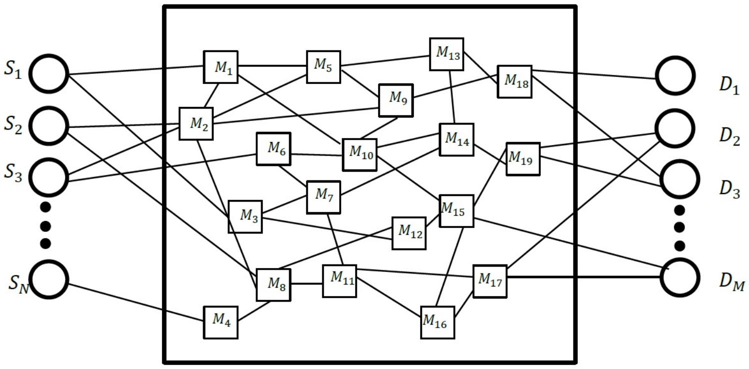


Figure 2: Example of System Model

incoming stream. Further, the layered encryption also ensures that the mix is unaware of the path of each arriving packet except for the immediate preceding and succeeding nodes. To prevent inference through transmission timing, every arriving packet can be delayed using a randomized strategy subject to the mix's maximum delay constraint d_i and transmitted on one of the outgoing streams of the mix based on the route which the packet belongs to. The mix can also transmit multiple packets in a batch where the order of packets in this batch is uniformly random. Let the set of all possible mixing strategies for the network of mixes $\mathcal{N}$ be denoted by $\Psi(\mathcal{N})$. In this work, we do not consider the specific design of mixing strategies to maximize anonymity. For a delay constrained mix, refer to [74] for the design of optimal mixing strategies. The focus of this work is on optimal routing and rate allocation by sources to maximize anonymity. For this purpose we consider specific mixing strategies that exhibit optimality properties under light traffic and heavy traffic conditions.

Eavesdropper: We consider an omniscient eavesdropper (Eve) who observes each individual point process in the network. Eve knows the topology of the network, the set of routes available to each source, the rate allocation across these routes and the strategy of each mix. Specifically, the reordering and batching strategy of every mix is known to Eve, *except* for the actual realization of the randomness used by the mixes, which is responsible for the uncertainty in her inference. Given the observations, Eve's goal is to determine the source of each packet arriving at the destination using her complete knowledge. Such an omniscient model is used to guarantee the provable degree of anonymity; in practice eavesdroppers, unless they own all network resources, will have access to lesser information and the results in this work are provably guaranteed to be achievable in that scenario.

Anonymity Definition

Each route $P_k^{(i,j)} \in \mathcal{P}(i,j)$(which is the k^{th} route between source S_i and destination D_j) contains an ordered sequence of mixes $M_{P_k^{(i,j)}}$. We define $d_{P_k^{(i,j)}} = \sum_{M_l \in M_{P_k^{(i,j)}}} d_{M_l}$ which denotes the maximum possible end to end delay experienced by a packet traversing this route. Let

$$d_{max} = \sup_{i,j,k} d_{P_k^{(i,j)}}$$

Any packet can experience a delay of at most d_{max} seconds in the mix network. Based on this fact, we divide the time horizon into non overlapping *cycles*. Each cycle begins with a packet arriving after an idle period of at least d_{max} seconds and ends when there has been no departure for at least d_{max} seconds. From the definition of d_{max}, all packets that arrive in a cycle will necessarily arrive at the destination before the cycle ends. This division of time into cycles is an analytical construct used to study the process in stationarity. Due to the strict delay constraints, the arrivals and departures in each cycle are independent across cycles. Furthermore, since the incoming processes are memoryless, we can study the expected anonymity achieved in a cycle instead of the entire time horizon of observation.

The complete observation and knowledge of Eve is denoted by Θ. Let $N(\Theta)$ denote the total number of packets in the cycle. We define the random variables $X_1, X_2, \cdots, X_{N(\Theta)}$ such that $X_k \in \{1, 2, \cdots, N\}$ denotes the source of the k_{th} packet which departs the mix network in that cycle. Conditioned on Θ, the knowledge of the mixing strategy results in a posterior joint distribution of $X_1, X_2, \cdots, X_{N(\Theta)}$ from the Eve's perspective, over the originating sources of departing packets in the cycle.

Let $\Gamma^{\psi}(\Theta)$ denote the Shannon entropy of this joint posterior distribution of $(X_1, X_2, \cdots,\ X_{N(\Theta)})$ when ψ is the set of mixing strategies used by mixes, then we define the anonymity as follows:

Definition 4.1 *The anonymity achieved by a mixing strategy $\psi \in \Psi(\mathcal{N})$ is defined as:*

$$\mathcal{A}_{\mathcal{N}}^{\psi}(\lambda) = \frac{\mathbb{E}(\Gamma^{\psi}(\Theta))}{\mathbb{E}(N(\Theta))} \tag{1}$$

The anonymity of the network, as expected, is a function of the mixing strategies, the source arrival rates, mix delay constraints and the rates allocated to multiple paths by the sources. We use Shannon entropy as our anonymity metric which has been used in many previous literature as it is tractable and has closed form solutions. The entropy measured has a physical connotation from the perspective of Eve: when the measure takes its minimum value (zero), Eve can perfectly determine the sources of packets at a destination. When the measure takes the maximum value (logarithm of number of sources), each packet is equally likely to belong to any one of the different sources, which is equivalent to having no information. In general, a key result in information theory, Fano's Inequality [5], proves that an observer's probability of error in decoding the sources of packets is lower bounded by the entropy of posterior random variables. We do note that entropy based measures have a weakness wherein they require a Bayesian framework and measure the stochastic average across the observations. As a result they are better used for a priori design of protocols.

In this work, we study anonymity in two traffic regimes, named light traffic and heavy traffic. In light traffic regime, we use light traffic derivative to investigate the optimal routing parameters for two reasons: the closed form characterization of the derivative which makes it amenable to optimization, and the fact that the light traffic derivative represents the sharpest gain in anonymity per unit traffic and consequently, the solution performs well at medium traffic rates as well. The light traffic derivative is defined as follows:

$$\Delta_0(\mathcal{M}) \geq \lim_{\lambda\to 0} \frac{d}{d\lambda}\mathcal{A}^{\psi}_{\mathcal{N}}(\lambda)$$

In heavy traffic regime, using anonymity definition in equation (1), we derive the anonymity achieved in a network of mixes as a linear function of anonymities of individual mixes.

For a single mix, the following result which was proved in Theorem 4 of [11] Characterizes the anonymity in the two extreme rate regime.

Theorem 4.1 *For a single mix ($\mathcal{M}_1$) with delay constraint d, serving two unequal rate sources, and a single destination, the light traffic derivative and the anonymity in high traffic are as follows:*

$$\lim_{\lambda\to 0} \frac{d}{d\lambda}\mathcal{A}^{\psi}_{\mathcal{M}_1}(\lambda) = \frac{2r_1r_2}{r_1+r_2}d \tag{2}$$

$$\lim_{\lambda\to \infty} \mathcal{A}^{\psi}_{\mathcal{M}_1}(\lambda) = h(\frac{r_1}{r_1+r_2}), \tag{3}$$

where $h(p)$ is entropy of a Bernoulli random variable with parameter p and $\lambda_1 = r_1\lambda$ and $\lambda_2 = r_2\lambda$ are rates of sources S_1 and S_2, respectively. As can be seen from the theorem, the optimal anonymity increases linearly with delay under light traffic, and approaches the maximum possible (prior entropy) in high traffic conditions. In this work we apply this single mix result in a network and derive the optimal routing parameters that maximize a weighted sum of network anonymity and average delay, which is described more formally below.

Delay: In our model, the average delay of network $\mathcal{N}$ as a linear function of routing parameters and each mix delay constraints is defined as follows:

$$\overline{D} = \frac{1}{\lambda_T} \sum_{u,v} \sum_{P_i^{(u,v)} \in \mathcal{P}(u,v)} \lambda_{P_i^{(u,v)}} d_{P_i^{(u,v)}}, \tag{4}$$

where $\lambda_T = \sum_{i,j} \Lambda_{ij}$.

Delay Anonymity Tradeoff: The primary challenge of this work is investigating the tradeoff between anonymity and delay. We model the preference of the network on delay and anonymity by the parameter $0 \leq \alpha \leq 1$ such that the objective is to maximize the weighted sum of delay and anonymity $\alpha\mathcal{A} - (1 - \alpha)\overline{D}$. As discussed in the example in Section 4.1, a longer path is likely to increase anonymity at higher delay whereas a shorter path can limit the delay with lower achieved anonymity. In the forthcoming sections, we study the optimal routing parameters that maximize this objective under the two extreme traffic conditions described earlier.

Using this model, in the subsequent section we will study the optimal multipath routing problem for two extreme traffic regimes. We demonstrate that in the light traffic regime, as $\lambda \to 0$, the maximization requires every source to transmit solely on a single path to each destination and we, consequently, provide a low complexity algorithm to determine the optimal path. We also prove that under heavy traffic conditions, where $\lambda \to \infty$, that maximum possible anonymity is achievable regardless of the routing parameters which means the network may choose the routing strategy based on minimizing delay alone. The analysis of each of these traffic regimes requires a corresponding characterization of anonymity in the network as a function of the topology, routing parameters and the mix delays, which forms the analytical basis for the optimization.

4.2 Optimal Routing in Light Traffic

In this section we consider the general network with N sources and M destinations such that the arrival rates for all source destination pairs are equal. The equality assumption is used merely to ease presentation. The results are imminently extendable to unequal rate models. More importantly, the key inferences derived continue to hold for the general model. Our approach is based on a specific mixing strategy proposed in [16,75]. The strategy was shown to be optimal in the light traffic regimes for individual mixes and linear cascade networks. According to this strategy (ψ_l), each mix M_i waits for an arrival after an idle period of at least d_{max} seconds. All the packets which arrive in d_i seconds following this arrival will be transmitted in a single batch at the end of d_i seconds. During the $(l_i - d_i)$ seconds following this batch transmission (l_i is the supremum of the sum of the delays in the route which include mix M_i and start from this mix), all the packets arrived to this mix will be transmitted without any delay. Upon completion of the l_i seconds, the mix resets and wait for a new arrival to restart this process.

This strategy, as shown in [16], obtains the optimal light traffic derivative in (2) for a single mix and linear cascade mix networks. In the following we study the derivative achieved by the strategy in a mix network as a function of the topology and multipath routing parameters.

4.2.1 Anonymity of a Mix Network in Light Traffic

In this section, we will see that the anonymity is a nonconvex function of the multipath routing parameters $\lambda_{P_k^{(i,j)}}$. The non convexity of the anonymity function would typically imply that we might need to apply approximation methods to efficiently compute the optimal parameters. However, as will be seen in the proof of Theorem 4.4, the quadratic form we derive for the optimal anonymity results in a unique optimal path for each source destination pair.

Prior to going through the anonymity of a general network, we present a simple example to develop the idea of anonymity in light traffic. Consider a network with two sources, two destinations and a single intermediate mix M_1. We assume a cycle with only two packets, wherein the first packet belongs to the route $P_1^{(1,1)}$ and the second one belongs to the route $P_1^{(2,2)}$. If these two packets depart from mix M_1 in a batch, then Eve will be confused between two pair of routes: 1) $P_1^{(1,1)}$ and $P_1^{(2,2)}$

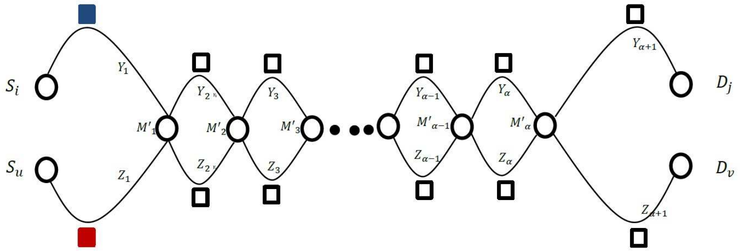


Figure 3: Mix Network in Lemma 4.2

2) $P_1^{(1,2)}$ and $P_1^{(2,1)}$. Thus, the anonymity achieved in this two packet cycle will be equal to:

$$\Gamma = h(\frac{\frac{\lambda_{P_1^{(1,1)}}}{\sum_{k,j}\lambda_{P_k(1,j)}}\frac{\lambda_{P_1^{(2,2)}}}{\sum_{k,j}\lambda_{P_k(2,j)}}}{\frac{\lambda_{P_1^{(1,1)}}}{\sum_{k,j}\lambda_{P_k(1,j)}}\frac{\lambda_{P_1^{(2,2)}}}{\sum_{k,j}\lambda_{P_k(2,j)}}+\frac{\lambda_{P_1^{(1,2)}}}{\sum_{k,j}\lambda_{P_k(1,j)}}\frac{\lambda_{P_1^{(2,1)}}}{\sum_{k,j}\lambda_{P_k(2,j)}}}), \tag{5}$$

where $h(p)$ is the Shannon entropy of Bernoulli random variable with parameter p. If the destinations of these two packets are identical, then the achievable entropy will be $h(0.5) = 1$. If the packets do not leave in a batch, then Eve can perfectly identify the source-destination pairs, thus achieving zero uncertainty.

Let's consider the following events in a general network defined with respect to the cycle initiated by a packet arriving at time 0 after a duration with no arrivals of length at least d_{max} seconds:

E^2 : There are exactly two packets in the cycle.

$E^a_{P_k^{(i,j)},P_l^{(u,v)}}$: There are two packets in the cycle one from route $P_k^{(i,j)} \in \mathcal{P}(i,j)$ and the other from $P_l^{(u,v)} \in \mathcal{P}(u,v)$and the first packet initiates the cycle.

$E_i^{\psi_l}$: is an indicator random variable defined for the specific two-packet cycle as:

$$E_i^{\psi_l} = \begin{cases} 1 & \text{if the two packets depart the } i^{th} \text{ mix common} \\ & \text{to both routers in a batch when the mixes} \\ & \text{use strategy } \psi_l \\ 0 & \text{otherwise} \end{cases}$$

Now, we define the variable $\Upsilon(i,j,k,u,v,l) = \mathbb{E}\{\Gamma^{\psi_l}|E^a_{P_k^{(i,j)},P_l^{(u,v)}}, E^2\}$ which is Eve's expected uncertainty in the case where there are two packets in the cycle; one packet on route $P_k^{(i,j)}$ and the other on route $P_u^{(v,l)}$, and the packet on route $P_k^{(i,j)}$ initiates the cycle.

When both packets in a two packet cycle arrive from the same source, the cycle has zero entropy, since the source of each packet is perfectly identifiable while the case where these two packets belongs to two different sources the achievable entropy should be calculated based on the posterior probabilities as follows:

A two packet cycle defined by an event $E^a_{P_k^{(i,j)},P_l^{(u,v)}}$ corresponds to a sub-network as shown in Figure 3 where there are two sources and two destinations and a set of intermediate mixes. We use $M' = (M'_1, M'_2, \ldots, M'_\alpha)$ to denote the ordered sequence of mixes where the two paths intersect. The walks $Y_1, \cdots, Y_{\alpha+1}$ and $Z_1, \cdots, Z_{\alpha+1}$ are each mutually exclusive sequences of mixes. There are therefore $2^{\alpha-1}$ possible routes from source S_i to destination D_j through the mixes $((Y_1$ or $Z_1)$, $M'_1, (Y_2$ or $Z_2)$, ..., $M'_\alpha, (Y_{\alpha+1}$ or $Z_{\alpha+1}))$. The following Lemma computes the average uncertainty achieved in such two packet cycles.

Lemma 4.2 *For a fixed routing parameters, the Eve's expected uncertainty in the network in Figure 3, where there are two packets in the cycle one from source S_i to destination D_j through the route $P_k^{(i,j)}$ and the second packet from source S_u to destination D_v through the route $P_l^{(u,v)}$ respectively is given by:*

$$\Upsilon(i,j,k,u,v,l) = \mathbb{E}\{\Gamma^{\psi_l} | E^a_{P_k^{(i,j)},P_l^{(u,v)}}, E^2\} =$$

$$\begin{cases} \sum_{(b_1,\cdots,b_\alpha)\neq(0,\cdots,0)} h(0.5) P\{E_1^{\psi_l} = b_1 \\ \quad ,\cdots, E_\alpha^{\psi_l} = b_\alpha | E^a_{P_k^{(i,j)},P_l^{(u,v)}}, E^2\} & \textit{if} \quad j = v \\ \sum_{(b_1,\cdots,b_\alpha)\neq(0,\cdots,0)} h(\frac{c_{ij}^{uv}}{c_{ij}^{uv}+c_{iv}^{uj}}) P\{E_1^{\psi_l} = b_1 \\ \quad ,\cdots, E_\alpha^{\psi_l} = b_\alpha | E^a_{P_k^{(i,j)},P_l^{(u,v)}}, E^2\} & \textit{if} \quad j \neq v \end{cases},$$

where c_{ij}^{uv} is the posterior probability that the packets from sources S_i and S_u arrive at destinations D_j and D_v respectively from Eve point of view given all the observations and knowledge of Eve.

Proof: Refer to [76] □.

Lemma 4.2 computes the achieved uncertainty for specific two packet cycles in the sub-network of Figure 3 as a function of routing parameters and the routes of the two packets. The expression in the lemma, although complicated, can be explained using a simple idea. If the two packets in a cycle leave any mix in a batch, then non-zero entropy is generated; this non-zero entropy is given by the $h(\cdot)$ term. This entropy term depends on the posterior probability of a given realization of the source destination pairing $(S_i, D_j), (S_u, D_v)$ given that the two packets departed in a batch from a particular mix. The actual computation of this probability depends on the exact realization of the routing parameters (a generalization of the expression in (5)

). However, as will be seen in the forthcoming analysis, this computation will be unnecessary since the optimal rate allocation results in single paths for the source destination pairs in which case, the posterior probability of a particular pairing is $\frac{1}{2}$.

In a general network, by identifying the set of mixes where packets are batched and the corresponding probabilities, the overall anonymity can be characterized, as in the following Theorem.

Theorem 4.3 *The light traffic derivative of Anonymity of a general mix network $\mathcal{N} = (\mathcal{G}, \mathcal{D}, \Lambda)$ is lower bounded by:*

$$\Delta_0(\mathcal{N}) \geq sd_{max} \sum_{i,j,k,u \neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T} \Upsilon(i,j,k,u,v,l), \tag{6}$$

where $\lambda_T = \sum_{i,j} \Lambda_{ij} = N\lambda$, $s = \frac{\lambda_T}{\lambda} = |\mathcal{S}| = N$, and $\Upsilon(i,j,k,u,v,l)$ is Eve's expected uncertainty in the event where there are two packets in the cycle; one packet on route $P_k^{(i,j)}$ and the other on route $P_u^{(v,l)}$.

Proof: For any strategy ψ, the anonymity is defined as follows:

$$\mathcal{A}_{\mathcal{M}}^{\psi}(\lambda) = \frac{\mathbb{E}(\Gamma^{\psi_l}(\Theta))}{\mathbb{E}(N(\Theta))} = \frac{\sum_{n=2}^{\infty} \mathbb{E}(\Gamma^{\psi_l}|N=n)\mathbb{P}(N=n)}{\mathbb{E}(N(\Theta))}, \tag{7}$$

where Θ is the total available information for Eve in the cycle begins from $t = 0$. For the light traffic derivative, it is easily seen that the cycles where $N > 2$ do not contribute to the light traffic derivative (as $\lambda \to 0$), only linear terms will have non zero contributions, and cycles with $N > 2$ necessarily contain $O(\lambda^2)$ factors by virtue of the Poisson process. Therefore, $\Delta_0(\mathcal{M})$ can be written as:

$$\Delta_0 \geq \lim_{\lambda \to 0} \frac{d}{d\lambda} \frac{\mathbb{E}\{\Gamma^{\psi_l}|N(\Theta) = 2\}\mathbb{P}\{N(\Theta) = 2\}}{\mathbb{E}\{N(\Theta)\}}$$

In order to find $\mathbb{E}\{\Gamma^{\psi_l}|N(\Theta) = 2\}$, we need to average Eve's uncertainty on all the possible pairs of routes $P_k^{(i,j)}$ and $P_l^{(u,v)}$. We can express $\mathbb{E}^0\{\Gamma^{\psi_l}|E^2\}$ as follows:

$$\Gamma = \mathbb{E}\{\Gamma^{\psi_l}|E^2\} = \sum_{i,j,k,u \neq i,v,l} \mathbb{P}\{E^a_{P_k^{(i,j)}, P_l^{(u,v)}}|E^2\}$$
$$\mathbb{E}\{\Gamma^{\psi_l}|E^a_{P_k^{(i,j)}, P_l^{(u,v)}}, E^2\}$$

$\mathbb{E}\{\Gamma^{\psi_l}|E^a_{P_k^{(i,j)}, P_l^{(u,v)}}, E^2\}$ is computed in Lemma 4.2, and

$$\mathbb{P}\{E^a_{P_k^{(i,j)}, P_l^{(u,v)}}|E^2\} = \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T}$$

Using the properties of Poisson processes, we can write

$$\begin{aligned}\mathbb{P}\{E^2\} &= (1-e^{-sd_{max}})e^{-sd_{max}} \\ \mathbb{E}\{N(\Theta)\} &= e^{sd_{max}}\end{aligned}$$

consequently,

$$\Delta_0(\mathcal{M}) \geq \lim_{\lambda\to 0}\frac{d}{d\lambda}\frac{\Gamma(1-e^{-sd_{max}})e^{-sd_{max}}}{e^{sd_{max}}} = sd_{max}\Gamma \tag{8}$$

□.

Theorem 3.2 provides the complete analytical characterization of the achievable light traffic anonymity as a function of the topology, routing parameters and the individual delay constraints of the mixes in the network. This anonymity is computed assuming that every mix uses the light traffic optimal strategy proposed in [16], and Eve is aware of the topology and the strategy of the mixes.

In the following Theorem, we show that the optimal routing parameters that maximizes the anonymity in Theorem 4.3 correspond to single path optimal solutions.

Theorem 4.4 *The solutions $\lambda^*_{P_k^{(i,j)}}$ which maximizes the total light traffic anonymity of any mix network that uses strategy ψ_l must necessarily be of the form:*

$$\forall i,j\exists k_{ij} \ s.t.\ \lambda^*_{P_{k_{ij}}^{(i,j)}} \neq 0, \lambda^*_{P_l^{(i,j)}} = 0, l \neq k_{ij} \tag{9}$$

Proof: There are three basic steps to proving the result of the theorem which are described as follows:

1. We compute an upper bound on the light traffic derivative using standard bounds on the binary entropy function. Lemma 4.5 demonstrates a property of the quadratic light traffic derivative form that enables the derivation of the upperbound and the resulting optimization.

2. We prove that the rate allocation parameters that optimize the upper bound have the single-path form stated in (9). This is shown in Lemma 4.6.

3. We then show that the optimal value for the upperbound is indeed an achievable light traffic derivative, thus proving the result of the Theorem.

1. Upper bound on light traffic derivative Note that the form of the light traffic derivative expression involves a quadratic functional of the routing parameters scaled by the probability of a particular event (that the two packets in the cycle depart in a batch at least once) in the corresponding two packet cycle. Before expressing the optimization problem and its solution, it is important to prove that for each pair of routes the event probability $P\{E_1^{\psi_l} = b_1, \cdots, E_\alpha^{\psi_l} = b_\alpha | E^a_{P_k^{(i,j)}, P_l^{(u,v)}}, E^2\}$ is independent of rate allocation parameters $\lambda_{P_k^{(i.j)}}$s in light traffic. This is shown in the following lemma.

Lemma 4.5 *For any pair of routes* $P_k^{(i,j)} \in \mathcal{P}(i,j)$ *and* $P_l^{(u,v)} \in \mathcal{P}(u,v)$*,* $P\{E_1^{\psi_l} = b_1, \cdots, E_\alpha^{\psi_l} = b_\alpha | E^a_{P_k^{(i,j)}, P_l^{(u,v)}}, E^2\}$ *is independent of rate allocation* $\lambda_{P_k^{(i,j)}}$*s and is only a function of the topology* $\mathcal{G}$ *and the delay constraints* D*, as* $\lambda \to 0$*.*

Proof: Refer to [76]. □.

It is evident from Theorem 4.3 that the anonymity is a nonconvex function of allocated rates. The general optimization problem we wish to study can be stated as follows.

$$\begin{aligned}
&\Phi : \max_{\{\lambda_{P_k^{(i,j)}}\}} \mathcal{A} = \\
&sd_{max} \sum_{i,j,k,u \neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T} \Upsilon(i,j,k,u,v,l) \\
&\text{subject to} : \forall i \in \{1, \cdots, N\}, j \in \{1, \cdots, M\} : \\
&\sum_k \lambda_{P_k^{(i,j)}} = \frac{\lambda}{M}, \lambda_{P_k^{(i,j)}} \geq 0 \qquad (10)
\end{aligned}$$

Let $q_{ijk,uvl}$ denote the probability that the two packets in the cycle depart in a batch from at least one common mix in the pair of routes $P_k^{(i,j)}$ and $P_l^{(u,v)}$:

$$\begin{aligned}
q_{ijk,uvl} \triangleq \sum_{(b_1,\cdots,b_\alpha) \neq (0,\cdots,0)} & P\{E_1^{\psi_l} = b_1, \cdots, E_\alpha^{\psi_l} = b_\alpha | \\
& E^a_{P_k^{(i,j)}, P_l^{(u,v)}}, E^2\} \qquad (11)
\end{aligned}$$

In order to solve this problem, we first compute an upper bound on $\mathcal{A}$, which uses the fact that the entropy terms $0 \leq h(\frac{c_{ij}^{uv}}{c_{ij}^{uv} + c_{iv}^{uj}}) \leq 1$ and $h(0.5) = 1$, and the fact that the probability $q_{ijk,uvl}$ is bounded as

$$0 \leq q_{ijk,uvl} \leq 1,$$

Consequently,

$$\begin{aligned}\mathcal{A} &= sd_{max} \sum_{i,j,k,u\neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T} \Upsilon(i,j,k,u,v,l) \\ &\leq sd_{max} \sum_{i,j,k,u\neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T} q_{ijk,uvl} \triangleq \mathcal{Q} \qquad (12)\end{aligned}$$

2. Optimizing the Upper bound

Lemma 4.6 *The solutions* $\lambda^*_{P_k^{(i,j)}}$ *to the optimization problem*

$$\begin{aligned}&\Psi : \max_{\{\lambda_{P_k^{(i,j)}}\}} \mathcal{Q} = sd_{max} \sum_{i,j,k,u\neq i,v,l} \frac{\lambda_{P_k^{(i,j)}}}{\lambda_T} \frac{\lambda_{P_l^{(u,v)}}}{\lambda_T} q_{ijk,uvl} \\ &\textit{subject to}: \forall i \in \{1, \cdots, N\}, j \in \{1, \cdots, M\}: \\ &\sum_k \lambda_{P_k^{(i,j)}} = \frac{\lambda}{M}, \lambda_{P_k^{(i,j)}} \geq 0\end{aligned}$$

must necessarily be of the form:

$$\forall i, j \exists k_{ij} \ \textit{s.t.} \ \lambda^*_{P_{k_{ij}}^{(i,j)}} = \frac{\lambda}{M}, \lambda^*_{P_l^{(i,j)}} = 0, l \neq k_{ij}$$

Proof: Due to Lemma 4.5, we know that $q_{ijk,uvl}$ is independent of $\lambda_{P_k^{(i,j)}}$. In the Hessian matrix of the function $\mathcal{Q}$, we can see that all the elements on the diagonal of the Hessian matrix are zero as $\forall i, j \text{and} k \ \frac{\partial^2 \mathcal{A}}{\partial \lambda^2_{P_k^{(i,j)}}} = 0$. This fact shows that the sum of the eigenvalues of this matrix should be zero. Consequently, all of them cannot be either positive or negative and this shows that the subspace where the gradient is zero, we will just have saddle points which cannot be the optimal solution and the maximum should exist in the boundary of the domain of rate allocation parameters. If, for any i, j, we choose set the $\lambda_{P_k^{(i,j)}} s$ to be binary (defining a boundary), our resulting domain would correspond to a subspace of functions which can be viewed as a boundary for the function $\mathcal{Q}$. With each subspace, if we set each $\lambda_{P_k^{(i,j)}}$ equal to zero individually again all the elements on the diagonal of the new Hessian matrix will be zero which shows that all the eigenvalues of the new Hessian matrix cannot have the same sign and the subspace where the gradient of new functions are zero cannot be optimal as it acts as a saddle point. We therefore ought to consider the new function's boundaries. Due to the quadratic nature of the anonymity function, this procedure when repeated is going to yield an identical conclusion and consequently, the only possible optimum points are the true *vertices* of the rate space where for each

$i \in \{S_1, S_2, ..., S_N\}$ and each $j \in \{D_1, D_2, ..., D_N\}$ only one the $\lambda_{P_k^{(i,j)}}s$ is nonzero and equal to $\frac{\lambda}{M}$. □

3. Equality of the optimal solution for the light traffic derivative and the upper bound Without loss of generality, for each source-destination pair (S_i, D_j), let the k_{ij}th route, denoted by $P_{k_{ij}}^{(i,j)}$, be the optimal route. Let the vector $\lambda_{opt} = (\lambda^*_{P_{k_{11}}^{(1,1)}}, ...\lambda^*_{P_{k_{1M}}^{(1,M)}}, \lambda^*_{P_{k_{21}}^{(2,1)}}, ...\lambda^*_{P_{k_{2M}}^{(2,M)}}, \cdots, \lambda^*_{P_{k_{N1}}^{(N,1)}}, ... \lambda^*_{P_{k_{NM}}^{(N,M)}})$ be the optimal solution of problem Ψ and $\mathcal{Q}^*$ be this optimal value. We know that

$$\max_{\lambda_{P_k^{(i,j)}}s} \mathcal{A} \leq \max_{\lambda_{P_k^{(i,j)}}s} \mathcal{Q} = \mathcal{Q}^* \tag{13}$$

As the optimal solution of Ψ yields single routes for a pair of packets one belonging to source destination pair (S_i, D_j) and the other belonging to (S_u, D_v) $h(\frac{c_{ij}^{uv}}{c_{ij}^{uv}+c_{iv}^{uj}}) = h(0.5) = 1$ as long as the two packets depart in a batch from at least one of the common mixes. Consequently, using Lemma 4.2 and Theorem 4.3, $\mathcal{A}(\lambda_{opt}) = \sum_{i,j,u\neq i,v} \frac{\lambda^*_{P_{k_{ij}}^{(i,j)}}}{\lambda_T} \frac{\lambda^*_{P_{k_{uv}}^{(u,v)}}}{\lambda_T} q_{ijk,uvl}$ which is equal to Q^*. Therefore, λ_{opt} is also the optimal solution of Φ and $\mathcal{A}^* = \mathcal{Q}^*$, which completes the proof of the theorem. □.

The proof of the theorem exposes an interesting artifact of the system: it does not matter how many mixes end up batching the packets in a cycle; as long as the packets are batched at least once, then maximum uncertainty can be achieved in light traffic cycles. Consequently, the single path solution is sufficient to maximize the overall anonymity. In the following section, we prove that the single path optimality extends to maximizing the weighted sum of delay and anonymity as well, and subsequently propose an algorithm to determine the optimal routes that achieve a desired tradeoff between anonymity and delay.

4.2.2 Delay Anonymity Tradeoff in Light Traffic

As mentioned in Section 4.1, the average end to end delay of network is a linear function of routing parameters $\lambda_{P_i^{(u,v)}}$ expressed as follows:

$$\overline{D} = \frac{1}{\lambda_T} \sum_{u,v} \sum_{P_i^{(u,v)} \in \mathcal{P}(u,v)} \lambda_{P_i^{(u,v)}} d_{P_i^{(u,v)}},$$

We model the network preference on anonymity and delay by the parameter $0 \leq \alpha \leq 1$. To express the delay anonymity tradeoff, we present the following optimization problem for a fixed α:

$$\begin{aligned} &\Omega: \max_{\{\lambda_{P_k^{(i,j)}}\}} \alpha\mathcal{A} - (1-\alpha)\overline{D} \\ &\text{subject to}: \forall i \in \{1, \cdots, N\}, j \in \{1, \cdots, M\}: \\ &\sum_k \lambda_{P_k^{(i,j)}} = \frac{\lambda}{M}, \lambda_{P_k^{(i,j)}} \geq 0 \end{aligned} \tag{14}$$

Corollary 4.6.1 *The optimal solution for problem Ω must necessarily be of the form:*

$$\forall i, j \exists k_{ij}^{\alpha} \ s.t. \ \lambda^*_{P^{(i,j)}_{k^{\alpha}_{ij}}} \neq 0, \lambda^*_{P^{(i,j)}_{l}} = 0, l \neq k^{\alpha}_{ij} \tag{15}$$

Proof:: As the average delay function is a linear function of rate allocation parameters, the above corollary naturally follows from the result of Theorem 4.4. □.

The above corollary extends the optimality of single path routing solutions to maximizing the weighted sum of anonymity and delay as well. We do note that this is a consequence of average delay being a linear functional of the parameters. It is conceivable that should another QoS criterion such as congestion be considered which is better influenced by multipath routing, then this optimality may not extend to those problems. In such scenarios, the result of Theorem 3.2 should be used in conjunction with the corresponding QoS metric to determine the optimal routing parameters.

Following Corollary 4.6.1, we propose a low complexity algorithm to determine the complete delay-anonymity tradeoff for any network of mixes.We know that for any weighting factor $0 \leq \alpha \leq 1$, the optimal routing yields single path route for each source destination pair. Let's consider the set of all such single path routing strategies $Q = \{(\mathcal{A}_1, \overline{D}_1), \cdots, (\mathcal{A}_{|Q|}, \overline{D}_{|Q|})\}$. $|Q|$ is the total number of such strategies. Each pair $(\mathcal{A}_u, \overline{D}_u)$ corresponds to a single path routing strategy, where for each $i \in \{1, 2, ..., N\}$ and $j \in \{1, 2, \cdots, M\}$, just one of the $\lambda^k_{P(i,j)}$ is nonzero. Without loss of generality we assume that these pairs are ordered such that their delays are increasing, so $\overline{D}_1$ is the minimum achievable end-to-end delay.

First, any pair $(\mathcal{A}_i, \overline{D}_i)$ such that $\exists u < i : \mathcal{A}_i < \mathcal{A}_u$ is removed from the set Q,as $\alpha\mathcal{A}_i - (1-\alpha)\overline{D}_i < \alpha\mathcal{A}_u - (1-\alpha)\overline{D}_u$ for any weighting factor $0 \leq \alpha \leq 1$. Each remaining pair $(\mathcal{A}_i, \overline{D}_i)$ corresponds to a line segment $(\mathcal{A}_i + \overline{D}_i)\alpha - \overline{D}_i$ as a function of α. Starting from $\alpha_0 = 0$, the pure delay optimal solution corresponds to the pair $(\mathcal{A}_1, \overline{D}_1)$ represents the optimal routing. This pair is recorded as $(\mathcal{A}_{0-opt}, \overline{D}_{0-opt})$. Then, algorithm finds the pair which intersect this line for smaller α compared to the other pairs and records this α as α_1, and this pair as $(\mathcal{A}_{1-opt}, \overline{D}_{1-opt})$. Then, at each step, algorithm continues to find the next line segment which intersects the current

Algorithm 1 Algorithm to find the optimal routing for each α

```
$u \leftarrow 1$
while $u < |Q|$
    $p = argmin\{j > u : A_j > A_u\}$
    $Q = Q/\{A_{u+1}, \cdots, A_{j-1}\}$
    $u \leftarrow p$
$i \leftarrow 0$
$u \leftarrow 1$
$(\mathcal{A}_{opt-i}, \overline{D}_{opt-i}) \leftarrow (\mathcal{A}_1, \overline{D}_1)$
while $u < |Q|$
    $p = argmin_{j>u}\{\frac{1}{1+\frac{A_j - A_u}{D_j - D_u}}\}$
    $\alpha_{i+1} = \frac{1}{1+\frac{A_p - A_u}{D_p - D_u}}$
    $i \leftarrow i + 1$
    $(\mathcal{A}_{opt-i}, \overline{D}_{opt-i}) \leftarrow (\mathcal{A}_p, \overline{D}_p)$
    $u \leftarrow p$
```

optimal segment for smaller α till it reaches $\alpha \geq 1$. At any step of algorithm, the pair $(\mathcal{A}_{i-opt}, \overline{D}_{i-opt})$ is recorded to be the optimal pair for the interval $[\alpha_i, \alpha_{i+1}]$. The following theorem demonstrates the optimality of Algorithm 1.

Theorem 4.7 *Algorithm 1 derives the optimal routing for any weighting factor α.*

Proof:: Let's assume for a weighting factor $\alpha_i \leq \alpha \leq \alpha_{i+1}$, there is a pair $(\mathcal{A}_t, \overline{D}_t)$ such that $\alpha\mathcal{A}_t - (1-\alpha)\overline{D}_t > \alpha\mathcal{A}_{opt-i} - (1-\alpha)\overline{D}_{opt-i}$, then $(\mathcal{A}_t, \overline{D}_t)$ should satisfy the following inequalities:

$$\begin{aligned} &\frac{1}{1+\frac{A_{opt-(i+1)} - A_{opt-i}}{D_{opt-(i+1)} - D_{opt-i}}} \geq \alpha \geq \\ &\frac{1}{1+\frac{A_t - A_{opt-i}}{D_t - D_{opt-i}}} \geq \frac{1}{1+\frac{A_{opt-i} - A_{opt-(i-1)}}{D_{opt-i} - D_{opt-(i-1)}}} \end{aligned} \tag{16}$$

which contradicts with the definition of $(\mathcal{A}_{opt-(i+1)}, \overline{D}_{opt-(i+1)})$ □.

It is noted that the optimal routing were derived assuming a specific mixing strategy described in [16]; the light traffic derivative for the strategy is known to be optimal for individual mixes and for a class of mix networks, referred to as mix cascades [16]. We therefore consider a general class of networks that are modeled after practical anonymous systems, and demonstrate that this lower bound has optimal scaling behavior with the size of the network. In practical anonymous systems, such as Tor [9] the network of intermediate nodes are divided into two groups, entry (or exit) nodes and transit nodes; each source (or destination) communicates with a single entry (or

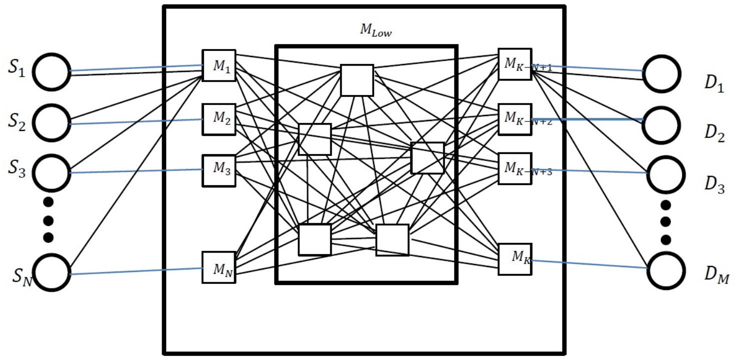


Figure 4: Complete graph mix network. The blue lines shows the worst connectivity between sources and mixes and destinations and mixes which achieves the lowerbound. The black lines shows one of the best possible connectivity which achieves the upperbound

exit) node, and the transit nodes typically form a complete graph. In the following, we use the previous results to derive the optimal scaling behavior of the light traffic anonymity for such networks.

4.3 Scaling Behavior of Complete Graphs

In this section, we consider a network modeled by a complete graph with K mix nodes, N source nodes, and T destination nodes. The set of mixes contain N entry mix nodes and T exit mix nodes such that all sources transmit only to entry nodes and destinations are directly accessible only from exit nodes. The K mixes nodes, however, form a complete graph. Each mix has an identical delay constraint d.

In the following theorem, we apply the results of the previous section to prove that the optimal anonymity for such complete mix networks scale as $O(NK)$. We show that for both upper bound and lower bound the mix network, the light traffic anonymity scales identically to a single mix with a delay constraint d_{max}, which can simulate any strategy of the original mix network.

Theorem 4.8 *The optimal light traffic derivative of anonymity of the complete mix network with N sources and T destinations in the light traffic regime is bounded from above and below as follows:*

$$d(N-1)(K-N-T) \leq \mathcal{A}_{\mathcal{M}_c} \leq d(N-1)K \tag{17}$$

Proof: We do not consider any specific set of routes between sources and destinations in the mix network. In order to provide a lower bound, we consider a scenario where each source and each destination has just one connection to separate entry and exit mixes respectively (Figure 4). Based on Theorem 4.4, for each source destination pair, it is sufficient to choose exactly one route to transmit packets. In order to maximize the light traffic derivative under this assumption, we let each source transmits its packets through the longest possible route. For example, source S_1 transmits the packets to destination D_1 through the route $(M_1, M_{N+1}, \cdots, M_{K-T}, M_{K-T+1})$. This cascade assumption would then imply that the sequence $(M_{N+1}, \cdots, M_{K-T}) = M_{Low}$ can be viewed as a single mix with the delay constraint equal to sum of all the mixes in it which is equal to $(K-T-N)d$. Using Theorem 4.3 for this system, the anonymity in light traffic can be proven to be lower bounded as

$$\mathcal{A} \geq NKdNT^2(N-1)\frac{\frac{\lambda}{T}}{N\lambda}\frac{\frac{\lambda}{T}}{N\lambda}\frac{(K+2-N-T)d}{Kd} = \\ d(N-1)(K-N-T) \tag{18}$$

The upper bound is obtained by replacing the network of mixes with a single mix having delay constraint $d_{max} = Kd$ such that all sources transmit to the mix and all destinations receive packets from the mix (Figure 4). That the anonymity of this system is an upper bound to the network of mixes comes from the fact that any strategy used by the network of mixes can be simulated by the enhanced single mix, and since Eve observing only one "super" mix has fewer observations, the anonymity achieved by the super mix is higher than that by the network of mixes. For such a system, the light traffic anonymity can easily be shown to be $d(N-1)K$. □.

4.4 Optimal Routing in Heavy Traffic

In this section, we will demonstrate that in the heavy traffic regime, as $\lambda \to \infty$, maximum anonymity is achievable regardless of the choice of routing parameters. Consequently, the derived rate allocation from the light traffic analysis would be suitable under heavy traffic conditions as well. An important step in the heavy traffic analysis required expressing the achievable anonymity of a general multiple-destination network as a linear combination of smaller sub-networks involving single mixes. This result, which is proven in Lemma 4.10, requires the definition of the intermediate anonymity achieved by an individual mix in the network.

Specifically, for a single mix M_i in the network $\mathcal{N}$, we define $\mathcal{A}^j_{M_i}$ to be the *intermediate* anonymity of packets on the j^{th} outgoing edge of mix M_i as follows:

$$\mathcal{A}^j_{M_i}(\lambda) = \lim_{\lambda \to \infty} \frac{H(X^{ij})}{N^{ij}}, \tag{19}$$

where $X^{ij} = (X_1^{ij}, \cdots, X_{N^{ij}}^{ij})$ and X_k^{ij} is the source of the k^{th} packet from Eve's perspective on the j^{th} outgoing edge and N^{ij} is number of packets on the jth outgoing edge.

In [75], we demonstrated that in the heavy traffic regime for a single destination network, the achieved anonymity is independent of the rate allocation thus allowing sources to optimize their multipath route selection based on other desired QoS metrics. In the following Theorem, we show the same fact holds for multiple destination networks as well. An important step in proving this result is the expression of the anonymity of the mix network as a linear functional of the intermediate anonymities given by (19).

Theorem 4.9 *If each mix utilizes an asymptotically optimal mixing strategy, then the maximum anonymity in a* **multiple destination mix network** *is achieved for any set of allocated rates as long as each destination node receives packets from a single mix.*

Proof: In order to prove this theorem, we first need to find the exact expression of high traffic anonymity in terms of the rate allocation parameters which is given by following lemma:

Lemma 4.10 *Anonymity of any arbitrary network in the high traffic rate regime is lower bounded by:*

$$\mathcal{A}_M(\lambda) \geq \sum_{i=1}^{|\mathcal{M}|} \sum_{j=1}^{\xi_i} \frac{w_{M_i}^j}{w} (\mathcal{A}_{M_i}^j -$$

$$\sum_{k=1}^{|\mathcal{S}|} \frac{\sum_{u=1}^{\zeta_i} w_{M_i u}^{jk}}{w_{M_i}^j} H(\frac{w_{M_i 1}^{jk}}{\sum_{u=1}^{\zeta_i} w_{M_i u}^{jk}}, \cdots, \frac{w_{M_i \zeta_i}^{jk}}{\sum_{u=1}^{\zeta_i} w_{M_i u}^{jk}})), \tag{20}$$

where w is the total rate of sources and $w_{M_i u}^{jk}$ is rate of packets from source S_k arriving on the u^{th} incoming edge to mix M_i and leaving mix M_i from the j^{th} outgoing edge. $w_{M_i}^j$ is the rate of packets on the jth outgoing edge of mix M_i. ζ_i is number of incoming edges of mix M_i and ξ_i is the number of outgoing edges of mix M_i.

Proof: Refer to [76]. □.

Lemma 4.10 expresses the anonymity achieved by the network of mixes as a weighted sum of the anonymity of each individual mix and the multipath rate allocation parameters. To prove the result of this theorem, we require that each mix achieves the maximum possible anonymity asymptotically. In other words, we must prove the existence of a mixing strategy ψ for any mix M_i in the system, such that if $w_{M_ix}^{jk}$ are the set of arrival rates to the mix, then the achieved anonymity is the optimal anonymity which is given by following equation.

$$\lim_{\lambda\to\infty} \mathcal{A}_M^{\psi}(\lambda) = \sum_{M_i\in\mathcal{F}} \sum_{j\in\mathcal{F}_i} \frac{w_{M_i}^j}{w} h(\frac{w_{M_ij}^1}{w_{M_i}^j}, \cdots, \frac{w_{M_ij}^N}{w_{M_i}^j}), \tag{21}$$

where $\mathcal{F}$ is the set of mixes which has at least one edge connected directly to one of the destinations and $\mathcal{F}_i$ is the set of outgoing edges of mix M_i which are connected to destinations. $w_{M_ij}^k$ is the rate of packets of source S_k on the j^{th} outgoing link of mix M_i. $w_{M_i}^j$ is the total rate of packets on j^{th} outgoing edge of mix M_i.

Existence of such a strategy has been shown in [16] and is a subject of a deeper investigation in [74], where the strategy with the best asymptotic convergence rate is presented. In so far as the discussion in this paper is concerned, consider the simple batching strategy of a mix M_i, wherein the mix batches all packets that arrive within periodic time intervals of d_i seconds. As $\lambda \to \infty$, the number of packets that arrive within any time period, say N_T would also increase towards infinity. According to the law of large numbers, the proportion of packets arriving on each link in this batch of packets would converge to the proportion of arrival rates from those respective links. By reordering the packets such that every possible ordering within a batch is uniformly random, the anonymity achieved will converge to the prior entropy given in inequality (20) as $\lambda \to \infty$. Given that each mix achieves the prior entropy as $\lambda \to \infty$ regardless of the nature of arrival processes, it remains to be seen that the anonymity of the network converges to the maximum possible regardless of the rate allocation; this can be shown by substituting the right-hand-side in (20) back into Lemma 4.10, so we get the optimal anonymity which is given in (21). $\square$.

As the optimal anonymity is achieved for any rate allocation in high traffic regime, the optimal delay anonymity region has one optimal point which is the delay optimal point. In a broader sense, the optimal routing problem can be designed based on other QoS criteria such as latency, throughput and congestion.

4.5 Simulations and Numerical Results

In this section, we present our simulation results on two example mix networks shown in Figures 1 and 5. We compare the anonymity optimal rate allocation to the other intuitive schemes. We see that the optimal routing derived in the light traffic regime also performs better when compared to other schemes in the regions where the traffic is neither heavy nor light. Finally, we present simulation results of the delay

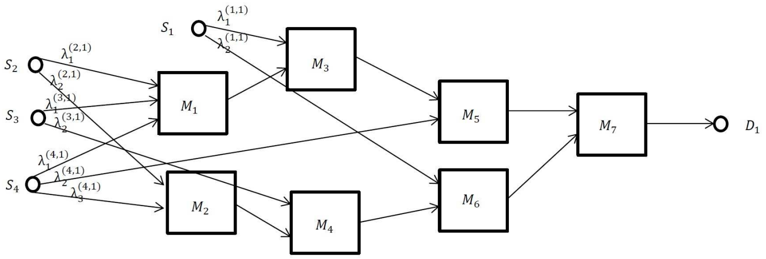


Figure 5: Mix network considered for the delay anonymity trade-off simulation

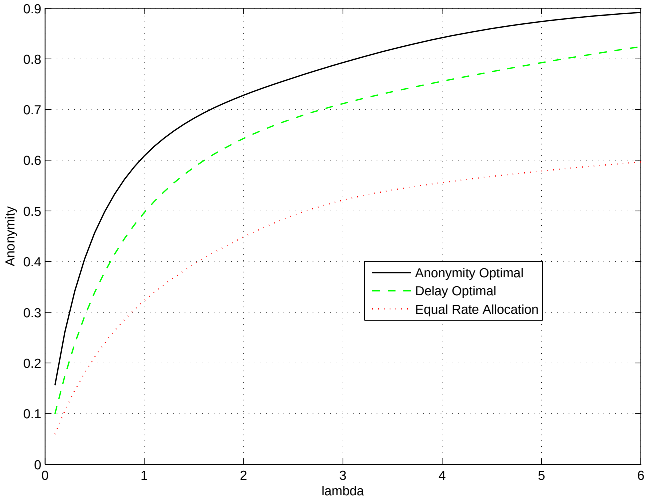


Figure 6: Comparing performance of optimal strategy in light traffic case to the other rate allocations

anonymity tradeoff for the mix network in Figure 5. In Figure 6, the anonymity achieved by the optimal light traffic based rate allocation for the 2 source network in Figure 1 is plotted as a function of general arrival rate λ, and the performance is compared to two intuitive rate allocation schemes, namely equal allocation and delay optimal allocation. In equal allocation, each source transmits half the traffic through mix M_1, and the other half through mix M_2, while in delay optimal allocation, each source transmits its traffic through the shortest path. In the simulation, the rate of S_2 was assumed to be twice that of S_1. For general traffic the optimal anonymity delay relationship is as yet an open problem, and any such optimization of rate allocation parameters would have to be performed using sub optimal strategies and analytically intractable expressions. An example strategy that is optimal under light traffic conditions and heavy traffic conditions but sub optimal for the general traffic

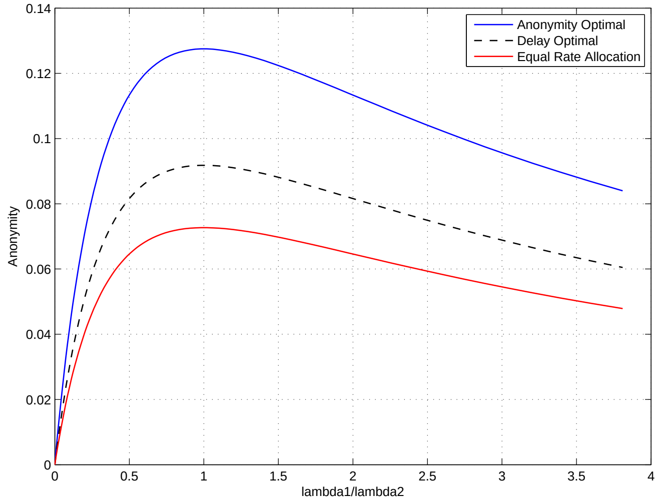


Figure 7: Anonymity versus $\frac{\lambda_1}{\lambda_2}$

would be that of a strategy that simply pools packets that arrives within the delay constraint and transmits a uniform random shuffle of a batch. Under our framework the anonymity can be computed as

$$\mathcal{A} = \sum_i \sum_j Pr\{i \text{ packets from } S_1 \text{ and } j \text{ packets from } S_2\}$$

$$Pr\{\text{leaving in a batch}\} \log_2 \begin{pmatrix} i+j \\ i \end{pmatrix} \qquad (22)$$

This strategy is used to characterize the anonymity for each set of routing parameters. From Theorem 4.9, we know that all of these allocations will achieve the maximum anonymity $h(\frac{1}{3})$as $\lambda \to \infty$. However, for the region where the traffic is neither heavy nor light, the optimal allocation we found using the light traffic derivative performs better than the intuitive schemes. This is not surprising, as the linear portion in the light traffic region provides the maximum gain per unit of rate increase. Consequently, the rise of the anonymity curve is best for the light traffic based optimal allocation. Since all allocations eventually converge to the maximum possible anonymity, the performance is expected to be better for a wide range of rates.

In Figure 7, we compared the achievable anonymity of delay optimal, anonymity optimal strategy, and equal rate allocation strategy for the network in Figure 1.

Figure 8 plots the anonymity-delay tradeoff for the network shown in Figure 5. There are four optimal strategy points here that each of them is optimal strategy for different ranges of α. Note that these points can be easily derived by the algorithm

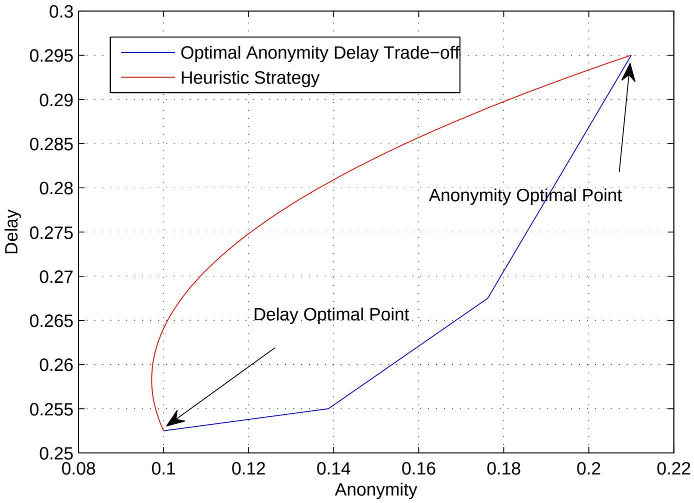


Figure 8: Delay Anonymity Trade-off in Mix Networks

presented in section 4.2.2. This tradeoff is compared to an intuitive linear allocation strategy wherein, for $\alpha = 0$, we use the optimal delay strategy and for $\alpha = 1$, we use the anonymity optimal strategy. As we increase α, we decrease the rate allocated to the delay optimal strategy and add it to anonymity optimal strategy until $\alpha = 1$ and at this point all the rate is allocated to the anonymity optimal strategy.

5 Relay Selection and Operation Control for Optimal Delay and Source-Destination Anonymity Tradeoff in Anonymous Networks

In this section, we provide an analytical framework to address source-destination pair anonymity and propose relay selection and operation methodologies that are resistant to timing analysis while satisfying low latency requirements.

In particular, we investigate the optimal relay selection and control of relay "operational modes" in an anonymous network. To understand "operational mode", consider the scenario depicted in Figure 10, where there are sources S_1 and S_2 transmitting to the destinations D_1 and D_2, respectively. In Figure 10a, the intermediate node follows the rule of First Come First Serve (FCFS) in which case an eavesdropper who observes the traffic in this network can identify the destination corresponding to each source. If, however, the intermediate node can delay the packets for upto d seconds, where d is greater than the interpacket timing on the high rate stream, then the relay can add dummy transmissions such that the output streams are indistinguishable to any eavesdropper (see Figure 10b). The optimal rate and mechanism to insert dummy packets to maintain this indistinguishability have been well studied in [12–15, 35]. Indeed it has been shown that if the incoming rates of the sources are made equal then the overhead dummy rate decreases inverse quadratically with the incoming traffic rate thus making it an effective mechanism for high rate traffic with limited bandwidth infringement. This technique however results in a linear scaling of dummy rate with the number of users accessing a relay and, when combined with the fact that it results in added delay, it has been largely ignored in practical anonymous systems.

In this section, we propose to alleviate these concerns by including two important choices in the implementation of such *dependent link padding*. First, we expand the ability of an intermediate relay to selectively introduce dummy transmissions to make a fraction of streams indistinguishable as opposed to introducing dummy transmissions on all outgoing streams. Second, in a virtual circuit, we enable the route selection mechanism for each source to determine if a particular relay should be adding dummy transmissions on its stream at all. Naturally, these choices are required to be made with the net goal of achieving the best possible anonymity whilst not introducing substantial latency. That is the primary theme of this section which is an investigation of the *optimal relay selection and control* for a sub-network ab-

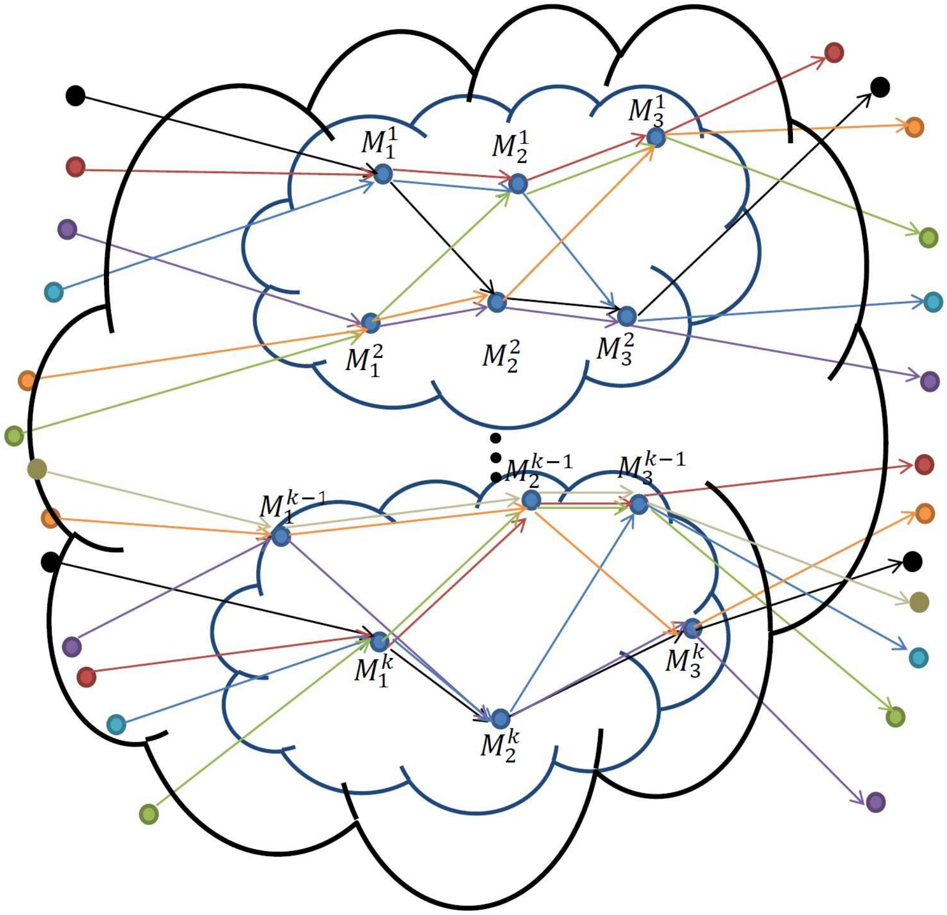
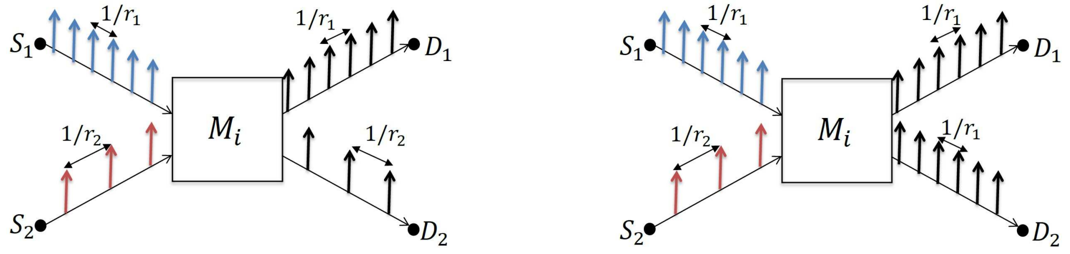


Figure 9: Six Relay System Abstraction.

straction as shown in Figure 9 which optimally trades off delay for anonymity. Using the developed methodology, protocol designers can choose a desirable operating point on this tradeoff curve.

Rest of this section is presented as follows: In section 5.1, we present the system model for anonymous system to provide source-destination anonymity. In section 5.2, we derive anonymity as function of rely selection and control mechanism parameters. Moreover, we provide sufficient conditions on this parameter such that optimal anonymity is provided. The problem of source-destination anonymity and delay tradeoff is investigated in section 5.3. Finally, we present the simulation results in section 5.4.



(a) Anonymous relay node in First Come First Serve (FCFS) mode (no anonymity)

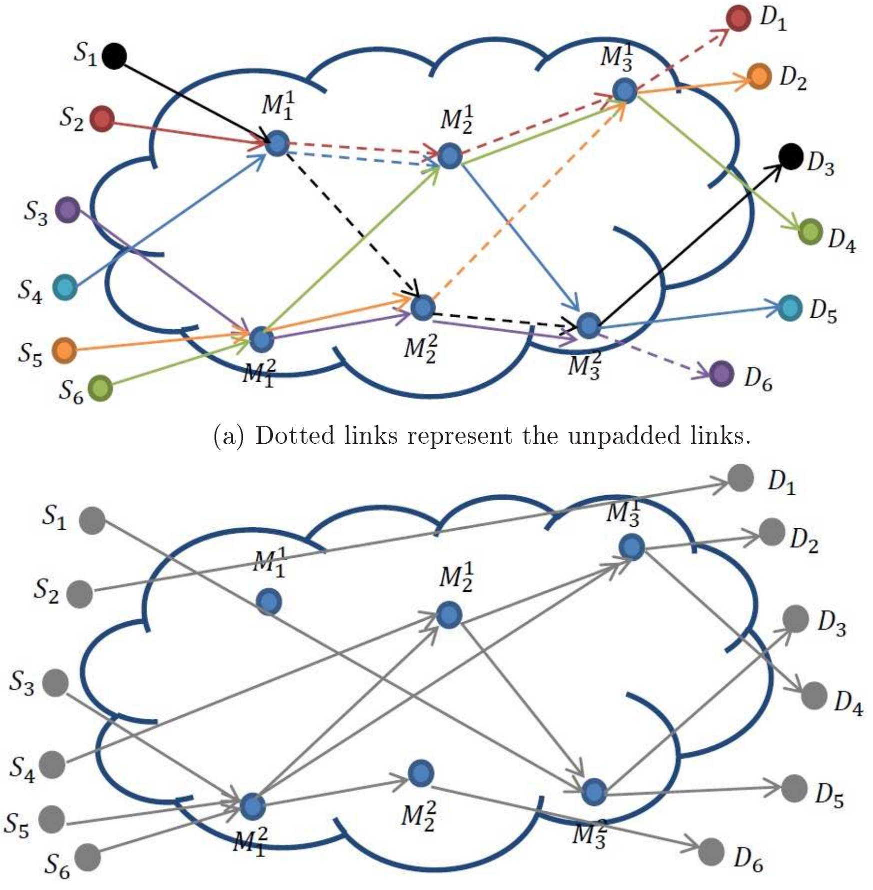
(b) Anonymous relay node in Anonymizing mode (maximum anonymity)

Figure 10: Standard and Anonymous Relays

5.1 System Model

The anonymous network abstraction contains six relay nodes which includes two entry guards, two intermediate relay nodes, and two exit guards. To emphasize that each of these six relay nodes are capable of adding dummy transmissions to boost anonymity, we shall often refer to them as *anonymous relays*. We assume that the users corresponding to each such group of six relays to have identical preferences for anonymity and delay. A large network can be viewed as containing hundreds of these groups of six. We focus our investigation on the anonymity in a single group. An example network with six relay nodes wherein each source chooses a sequence of three anonymous relay nodes (one each from the two entry guards, two intermediate relays and two exit guards) and is shown in Figure 11a. Our abstraction is defined formally as a 3-tuple $(\mathcal{G}, \Delta, \mathcal{B})$, where $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a directed graph with the set of nodes denoted by $\mathcal{V}$ and $\mathcal{E}$ the set of directed edges. $\mathcal{V} = \mathcal{S} \bigcup \mathcal{M} \bigcup \mathcal{D}$, where $\mathcal{S}$ is the set of source nodes, $\mathcal{D}$ the set of destination nodes, and $\mathcal{M}$ the set of six anonymous relays. We further refine $\mathcal{M} = \mathcal{M}_E \bigcup \mathcal{M}_M \bigcup \mathcal{M}_Q$, where $\mathcal{M}_E$ is the set of entry guard nodes, $\mathcal{M}_M$ is the set of intermediate relays, and $\mathcal{M}_Q$ is the set of exit guard nodes. The 3-tuple contains a set $\mathcal{B}$ of bandwidth constraints for each anonymous relay and a set Δ of delays associated with each edge.

Source: Each source $S_i \in \mathcal{S}$ transmits packets according to a stochastic process to a destination through a sequence of three anonymous relays- an entry guard from $\mathcal{M}_E$, an intermediate relay from $\mathcal{M}_M$ and an exit guard from $\mathcal{M}_Q$. Let r_i denote the packet arrival rate on the packet stream from source S_i. Each source has two key decisions to make. First, the source chooses the sequence of three anonymous relays; this choice is represented by the relay selection parameter $R_i = (X_{1i}, X_{2i}, X_{3i})$, where



(a) Dotted links represent the unpadded links.

(b) Unpadded outgoing links can be perfectly matched to their corresponding incoming link.

Figure 11: Link Padding.

$X_{1i} \in \mathcal{M}_E, X_{2i} \in \mathcal{M}_M$, and $X_{3i} \in \mathcal{M}_Q$. Second, the source chooses if it wishes its stream to be padded with dummy transmissions by each anonymous relay in effect controlling the operated mode of the relay partially. We denote this control action using the *anonymization parameter* $A_i = (I_{S_i,X_{1i}}, I_{S_i,X_{2i}}, I_{S_i,X_{3i}})$, where $I_{S_i,X_{ji}} = 1$ indicates that anonymous relay X_{ji} should add dummy transmissions to the stream from source S_i, and $I_{S_i,X_{ji}} = 0$ indicates that the relay X_{ji} would transmit packets from S_i on a FCFS basis without any link padding thus allowing an eavesdropper to match the outgoing stream with its corresponding incoming stream. Note that although the intended data rate for source S_i is r_i, the choice of anonymization parameter could result in an overhead dummy rate which we denote by $r_{Du}^{S_i}$.

Anonymous relay: Each anonymous relay will be denoted by M_j^i, where $j = 1, 2, 3$ denotes respectively the entry guard, intermediate relay, and exit guard. Each anonymous relay M_j^i has a delay constraint $d_{M_j^i}$, and bandwidth $\mathcal{B}_{M_j^i}$. The aggregate incoming packet rate to the anonymous relay node M_j^i cannot exceed $\mathcal{B}_{M_j^i}$. If there are totally n incoming streams to the anonymous relay M_j^i, where k incoming streams have requested their streams not to be padded by that relay and $n-k$ incoming streams have requested to be anonymized through padding by setting $I_{S_u,M_j^i}=1$, then the anonymous relay will transmit the packets of the k incoming streams on FCFS basis without any delay or padding. Packets from the remaining $n-k$ incoming streams can be delayed by the anonymous relay node for a maximum of $d_{M_j^i}$ seconds. So that outgoing stream of those $n-k$ sources are indistinguishable. This waiting period allows the anonymous relay to accumulate packets from the $n-k$ streams, such that one packet from each of these streams can be transmitted at the same time in a batch on their corresponding outgoing edge. Note that if there is no packet from some of these streams in this period the relay will transmit a dummy packet on the corresponding outgoing edges so that all $n-k$ outgoing streams have identical timing. This is the essence of dependent link padding which is known to be optimal under delay constraints. This ensures that from Eve's perspective, the outgoing streams (that have been padded) cannot be uniquely associated to the correct incoming stream from the timing. Dependent link padding, while not in use in real systems due to concerns about bandwidth consumption, is essential to thwart timing analysis. In this work, by imposing tight latency constraints and controlling the number of stream padded at each relay, we alleviate these concerns.

Eavesdropper: For purposes of this work, we consider an omniscient eavesdropper (Eve) who observes the transmission timing on every communication link in the network. Eve knows the topology of the network and the link padding strategy of the anonymous relays. Eve's goal is to use this timing information to determine accurately the pairs of source-destination (S_i, D_j) who are communicating. We note that Eve is a specific type of adversary– a passive one– and is not the only type of adversary in an anonymous system. That being said, the objective of this paper is to understand the optimal tradeoff between anonymity and delay under a timing analysis attack, and other mechanisms to thwart active adversaries can be built in conjunction with the framework delineated here.

Quantifying Anonymity from Timing: We use Shannon conditional entropy to quantify anonymity from timing analysis– in particular to measure the uncertainty in the source-destination pairing from the perspective of Eve. We define random variables $X_1, X_2, \cdots, X_N$ where random variable X_i denotes the destination node for packets from source S_i. We denote the complete observation and knowledge of the Eve by Θ. Conditioned on Θ, $(X_1, X_2, \cdots, X_N)$ follows a posterior joint distribution induced by the choices of relay selection and anonymization parameters. Let $\Psi(\mathcal{M})$ denote the set of all possible relay selection and anonymization strategies.

Definition 5.1 *The anonymity achieved by a specific strategy* $\psi \in \Psi(\mathcal{M})$ *is defined as:*

$$\mathcal{A}_\psi = \frac{H(X_1, \cdots, X_N|\Theta)}{\log N!}, \tag{23}$$

where for any pair of random vectors $\mathbf{X}, \mathbf{Y}$, $H(\mathbf{X}|\mathbf{Y})$ is the conditional entropy.

Shannon conditional entropy was proposed as a measure of anonymity in [77]. Since then, it has been used to design optimal mixing strategies [78–80] and characterize fundamental relationships between anonymity and network resources [35,81,82]. In an $N-$source, $N-$destination system, the total number of permutations of source-destination pairings possible is $N!$, and for any strategy ψ, the uncertainty $H(X_1, \cdots, X_N|\Theta) \leq \log N!$ [83]. This maximum is achieved, if from Eve's perspective, every source is equally likely to be communicating with each destination. Likewise, an uncertainty $H(X_1, \cdots, X_N|\Theta) = 0$ indicates that Eve can perfectly identify the destination corresponding to each source. As per equation (23), the normalized anonymity is bounded as $0 \leq \mathcal{A} \leq 1$. In general, Eve's probability of error in identifying source destination pairs increases with $\mathcal{A}$ (see Fano's inequality, [83]) which provides the tangible connection between the metric and the "action" of the adversary.

Delay: In our model, there are two sources of latency:
1) Transmission delay that occurs on each link represented by $d_{X,Y}$ where $(X,Y) \in \mathcal{E}$ which is the delay incurred by each packet on its transmission from node X to node Y.
2) Delay incurred by packets at an anonymous relay M_j^i, denoted by $d_{M_j^i}$, should the source of the packets choose to have its stream padded by relay M_j^i. The average delay for the network abstraction can be expressed as linear function of the relay selection and anonymization parameters:

$$\begin{aligned}\bar{\mathcal{D}} = \frac{1}{r_{\mathrm{tot}}} \sum_{\mathrm{S_i} \in \mathcal{S}} r_{\mathrm{i}}(d_{\mathrm{S_i},\mathrm{R_i}(1)} + I_{\mathrm{S_i},\mathrm{R_i}(1)} d_{\mathrm{R_i}(1)} + d_{\mathrm{R_i}(1),\mathrm{R_i}(2)} + \\ I_{\mathrm{S_i},\mathrm{R_i}(2)} d_{\mathrm{R_i}(2)} + d_{\mathrm{R_i}(2),\mathrm{R_i}(3)} + I_{\mathrm{S_i},\mathrm{R_i}(3)} d_{\mathrm{R_i}(3)} + d_{\mathrm{R_i}(3),\mathrm{D_i}}),\end{aligned} \tag{24}$$

where $r_{tot} = \sum_i r_i$.

Delay Anonymity Tradeoff: The primary challenge we investigate in this work is the tradeoff between anonymity and latency. That such a tradeoff exists is amply evident from the the single anonymous relay system discussed in the introduction (see Figure 1). In the six relay abstraction we consider, this tradeoff is a function of the choices made by the sources. Although each source is liable to have an individual preference for the degree to which performance can be traded for anonymity, in our work, we assume all the users in a single abstraction have similar preferences for the operating point on the tradeoff curve. We model this preference using a weighting parameter $0 \leq \alpha \leq 1$, where the sources desire to maximize the weighted sum $\alpha\mathcal{A} - (1-\alpha)\bar{\mathcal{D}}$. An α close to zero would indicate that the sources desire less latency, whereas an α close to 1 would indicate that they desire high anonymity. Our goal is to study the *joint optimization* of the relay selection parameters $\{R_i\}$ and the anonymization parameters $\{A_i\}$ such that this weighted sum is maximized for any chosen α.

A summary of notations in this paper is presented in Table1.

5.2 Anonymity Optimal Relay Selection

For fixed relay selection parameters $\{R_i\}$ and anonymization parameters $\{A_i\}$, the network may be represented as shown in Figure 11a, where dotted edges represent links which are not padded with dummy transmissions and solid edges represent padded links. If an incoming traffic stream is not padded, Eve can identify the corresponding outgoing edge using timing analysis. In contrast, if at least two incoming links are padded, then the corresponding outgoing edges will have identical timing patterns and are thus indisinguishable to Eve. Each of these padded outgoing links will have an identical packet rate equal to the maximum incoming rate amongst the corresponding incoming links; whereas the rate of unpadded links will remain unchanged. Since an unpadded outgoing link can be matched to an incoming link perfectly and incurs no overhead, removing the dotted links and connecting them to the subsequent anonymous relay on their path will not change the analysis of anonymity and dummy rate in the network (See Figure 11b). Therefore, it is sufficient to merely consider the anonymized links in the network's graph (See Figure 12).

For a given choice of relay selection and anonymization parameters, we define three sets of counting variables. $l_{M_j^{i_1},M_j^{i_2}}$ denotes the number of padded links from the anonymous relay $M_j^{i_1}$ to the anonymous relay $M_j^{i_2}$, l_{s,M_j^i} denote the number of sources requesting the anonymous relay M_j^i to be the first anonymous relay on its route which anonymize their streams by padding, and the variable $l_{M_j^i,d}$ denotes the number of padded links from the anonymous relay M_j^i to the destinations which are not padded any further downstream. These parameters are defined mathematically as follows:

$$
\begin{aligned}
& l_{s,d} = \sum_u \mathbf{1}(A_u = (0,0,0)) \\
& l_{sM_j^i} = \sum_{u:R_u(j)=M_j^i} \mathbf{1}(A_u(j) = 1, k < j : A_u(k) = 0) \\
& l_{M_j^i,d} = \sum_{u:R_u(j)=M_j^i} \mathbf{1}(A_u(j) = 1, k > j : A_u(k) = 0) \\
& l_{M_j^i,M_v^l} = \sum_{u:R_u(j)=M_j^i,R_u(v)=M_v^l} \mathbf{1}(A_u(j) = A_u(v) = 1, \\
& j < k < v : A_u(k) = 0)
\end{aligned}
$$

where $\mathbf{1}$ is the indicator function ($\mathbf{1}(\sigma) = 1$ if σ is TRUE and 0 otherwise). Since padding a set of incoming streams results in the corresponding outgoing streams to have identical timing patterns, the anonymity achieved by a particular choice of relay selection and anonymization parameters can be expressed as a function of the counting variables defined above.

We note that, only a subset of possible choices of relay selection and anonymization parameters are feasible, owing to the bandwidth constraints at the anonymous relays. Prior to characterizing the achieved anonymity, we shall derive the necessary conditions for the relay selection and anonymization parameters to satisfy each anonymous relay's bandwidth constraint and subsequently characterize the anonymity for feasible parameters. We define the variables $r_{M_j^i}$ to be the rate of packets on each of the links padded by the anonymous relay M_j^i derived as follows:

$$
\begin{aligned}
r_{M_j^i} = \max\{ & \max_{l=1,2,k<j} \{ r_{M_k^l} \mathbf{1}(l_{M_k^l,M_j^u} \neq 0)\}, \\
& \max_{S_i:k<j:A_i(k)=0,R_i(j)=M_j^u} \{r_i\}\}
\end{aligned}
$$

The above rate is characterized assuming that the transmission of dummy packets is merely due to the incoming rates of packet streams being different. In general there is an additional overhead that is inverse quadratically related to the maximum incoming rate which is not explicitly considered for the mathematical portions, but is used in the numerical sections. This difference is shown in Figure 13, where we considered a single anonymous relay and four packet streams which have heavy tail

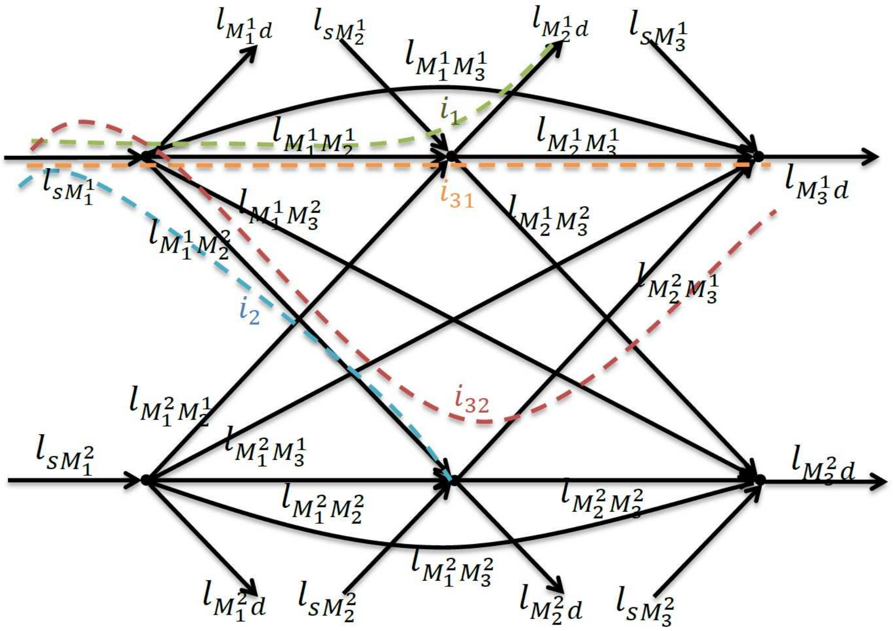


Figure 12: The networks graph after removing the unpadded outgoing links. (The dashed lines represents the variables defined in Lemma 5.1)

traffic distribution. The rate of dummy transmission required for the streams are shown as function of the anonymous relay's allowable delay. As is observable, as long as the allowed delay at the relay exceeds a certain threshold this additional overhead is negligible. Assuming the allowable delay is in the negligible overhead region, we can express the rate of dummy transmissions padded for each source as:

$$r_{Du}^{S_i} = \max_j \{r_{R_i(j)} \mathbf{1}(A_i(j) \neq 0)\} - r_i \tag{25}$$

The bandwidth constraint of each anonymous relay $M_j^u \in \mathcal{M}$ will restrict the relay selection and anonymization parameters:

$$\sum_{\mathrm{S_i:R_i(j)=M_j^u}} \mathbf{1}(k < j : \mathrm{A_i}(k) = 0) r_{\mathrm{i}} + \sum_{\mathrm{l,k<j}} r_{\mathrm{M_k^l}} l_{\mathrm{M_k^l,M_j^u}} \leq \mathcal{B}_{\mathrm{M_j^u}}$$

In the rest of this paper, we denote the relay selection parameters $\{R_i\}$ and anonymization parameter$\{A_i\}$ feasible if they satisfy the bandwidth constraints.

Assuming the relay selection and anonymization parameters satisfy the bandwidth constraints, computation of the achieved anonymity requires a counting of all possible source destination pairings that could result in the observed set of packet streams from Eve's perspective. Considering the network shown in Figure 12 where all the links are padded, we are interested to find the destinations D_js that a specific source S_i may

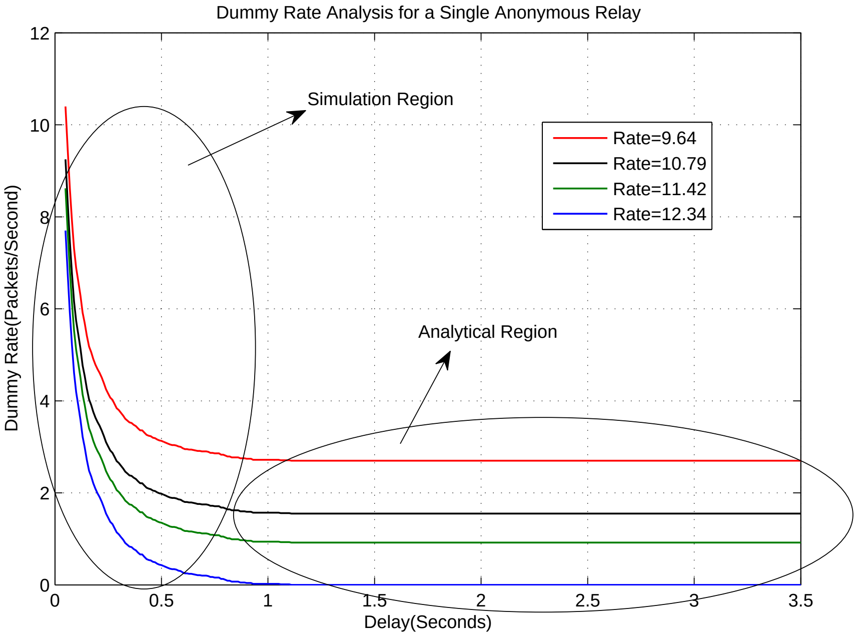


Figure 13: Dummy rate for a single anonymous relay where there are four incoming streams modeled by heavy tail traffic.

communicate with. Let's consider three different cases for source S_i: 1) If source S_i enters the network using the anonymous relay M_3^1, then it is surely communicating with one of the destinations connected to M_3^1. 2) If source S_i enters the network using the anonymous relay M_2^1, then it is surely communicating with one of the destinations connected to M_2^1 or M_3^1 or M_3^2. 3) If source S_i enters the network using the anonymous relay M_1^1, then it cannot communicate with the destinations connected to the anonymous relay M_1^2.

Thus, we consider six sets of sources: $l_{s,M_1^1}, l_{s,M_1^2}, \cdots, l_{s,M_3^2}$, where all the source belonging to any of these sets can communicate with the same set of destinations discussed above. In order to count all the possible communicating source- destination pairs, we need to exhaustively delineate the viable cases by every source. Considering l_{s,M_1^1} sources connected to the anonymous relay M_1^1, we have $l_{M_1^1,d}$ out of l_{s,M_1^1}sources which communicate with the destinations directly connected to M_1^1, we may have i_1 sources which communicate with the destinations directly connected to M_2^1, i_2 sources communicate with the destinations directly connected to M_2^2, $i_{31}+i_{32}+l_{M_1^1,M_3^1}$ sources which communicate with the destinations connected to M_3^1 (i_{31} sources through the path (M_1^1, M_2^1, M_3^1), i_{32} sources through the path (M_1^1, M_2^2, M_3^1), and $l_{M_1^1,M_3^1}$ through the path (M_1^1, M_3^1)), and the rest of sources will communicate with the destinations connected to M_3^2. We also define the variables j_1, j_2, j_{31}, j_{32} for the sources belong to l_{s,M_1^2} in the same way. Once these variables are fixed, the number of sources from the other four sets communicating with each set of destinations is known. For example, number of sources from the set l_{s,M_2^1} communicating with the destinations connected to M_2^1 will be $l_{M_2^1,d} - i_1 - i_2$. We note that the quantities $i_1, i_2, \cdots$ will be restricted by some of the graphs structure parameters. For instance i_1 can not exceed $\min\{l_{M_1^1,M_2^1}, l_{M_2^1,d}\}$. Through an exhaustive counting of all scenarios and considering the constraints on the variables $i_1, i_2, \cdots$, the achieved anonymity as a function of variables $l_{X,Y}$ is expressed in the following lemma:

Lemma 5.1 *For a fixed feasible set of route selection parameters $\{R_i\}$ and anonymization parameters $\{A_i\}$, the achieved anonymity can be expressed as follows:*

$$\begin{aligned}
&\mathcal{A} = \frac{\log(C \prod_{i=1}^{2} \prod_{j=1}^{3} l_{M_i^j,d}!)}{\log(N!)}, \ \textit{where} \\
&C = \sum_{\substack{\zeta_{i_1} \le i_1 \le \epsilon_{i_1}, \\ \zeta_{i_2} \le i_2 \le \epsilon_{i_2}}} \sum_{\substack{\zeta_{i_{31}} \le i_{31} \le \epsilon_{i_{31}}, \\ \zeta_{i_{32}} \le i_{32} \le \epsilon_{i_{32}}}} \sum_{\substack{\zeta_{j_1} \le j_1 \le \epsilon_{j_1}, \\ \zeta_{j_2} \le j_2 \le \epsilon_{j_2}}} \sum_{\substack{\zeta_{j_{31}} \le j_{31} \le \epsilon_{j_{31}}, \\ \zeta_{j_{32}} \le j_{32} \le \epsilon_{j_{32}}}} \\
&\frac{1}{Norm(i_{31}, i_{32})} \left(\begin{array}{c} l_{S,M_1^1} \\ l_{M_1^1,D}, i_1, i_2, i_{31} + i_{32} + l_{M_1^1,M_3^1} \end{array} \right) \\
&\frac{1}{Norm(j_{31}, j_{32})} \left(\begin{array}{c} l_{S,M_1^2} \\ l_{M_1^2,D}, j_1, j_2, j_{31} + j_{32} + l_{M_1^2,M_3^1} \end{array} \right) \\
&\left(\begin{array}{c} l_{S,M_2^1} \\ l_{M_2^1,D} - i_1 - j_1, l_{M_2^1,M_3^1} - i_{31} - j_{31} \end{array} \right) \\
&\left(\begin{array}{c} l_{S,M_2^2} \\ l_{M_2^2,D} - i_2 - j_2, l_{M_2^2,M_3^1} - i_{32} - j_{32} \end{array} \right),
\end{aligned} \tag{26}$$

where $\epsilon_{i_1}, \zeta_{i_1}$ denotes the maximum and minimum number of sources connected directly to M_1^1 (l_{S,M_M^1}) which can communicate with the destinations connected to M_2^1 $(l_{M_2^1,D})$, and so on (the boundaries and constant are specified in the appendix) and $Norm()$ is a normalization constant.

Proof: In order to find the anonymity we need to count all the possible pairs of source-destination which may communicate. For this purpose, we will count all the cases which may occur to each group of l_{s,M_i^j}. We divide the source of group $l_{M_1^1}$ to 5 groups:1) $l_{M_1^1,d}$ communicating with the destinations $l_{M_1^1,d}$. 2) i_1 communicating with the destinations $l_{M_2^1,d}$. 3) i_2 communicating with the destinations $l_{M_2^2,d}$. 4)

$i_{31}+i_{32}+l_{M_1^1,M_3^1}$ communicating with the destinations $l_{M_3^1,d}$. 5) The rest of sources $l_{s,M_1^1}-l_{M_1^1,d}-i_1-i_2-i_{31}-i_{32}-l_{M_1^1,M_3^1}$ are communicating with $l_{M_3^2,d}$.
j_1, j_2, j_{13}, andj_{23} are also defined in the same manner. Once all of these quantities are fixed. The number of sources which may communicate from l_{s,M_2^1} or l_{s,M_2^2} to the other sets of destinations are identified. For example number of sources from l_{s,M_2^1} to $l_{M_2^1,d}$ will be equal to $l_{M_2^1,d}-i_1-j_1$. Considering the constraint on each of the quantities i_1, i_2, i_{31}, i_{32} and $j_1, j_2, j_{31}+j_{32}$, we can count all the possible pair of source-destination which may communicate. However, we should notice that there are cases where $i_{31}+i_{32}+l_{M_1^1,M_3^1}$ and $j_{31}+j_{32}+l_{M_1^2,M_3^1}$ are fixed and counted several times in our summation. Thus, by defining the $Norm$ function which counts this redundancy for the fixed $i_{31}+i_{32}+l_{M_1^1,M_3^1}$ and $j_{31}+j_{32}+l_{M_1^2,M_3^1}$, we eliminate the redundant cases. $\square$.

The anonymity characterized in Lemma 5.1 is at most equal to 1 which occurs when given an observation of the timing processes on all the links, every source destination pairing is equally likely. We find conditions on the choices of parameters $\{R_i\}$ and $\{A_i\}$ such that this maximum anonymity is achieved. Note that it is not sufficient merely for all relays to pad all outgoing streams to achieve maximum anonymity. For instance, if half the sources choose a particular sequence of relays, and the remaining choose a mutually exclusive sequence, then the achieved anonymity would be at most $\frac{1}{2}$.

Theorem 5.2 *The feasible relay selection parameters* $\{R_i\}$ *and anonymization parameters* $\{A_i\}$ *yields in optimal anonymity if they satisfy the following conditions:*

$$\begin{aligned}
&\mathcal{C}_1 : \forall X \in \mathcal{M}_{\mathrm{E}}, \forall Y \in \mathcal{M}_{\mathrm{Q}} : l_{\mathrm{X,d}} = l_{\mathrm{s,Y}} = l_{\mathrm{X,Y}} = l_{\mathrm{s,d}} = 0\\
&\mathcal{C}_2 : \forall Z, Z' \in \mathcal{M}_{\mathrm{M}} : \mathbf{1}(l_{\mathrm{s,Z}} \neq 0, l_{\mathrm{Z',d}} \neq 0) = 0\\
&\mathcal{C}_3 : \forall Z \in \mathcal{M}_{\mathrm{M}} : l_{\mathrm{Z,M_3^1}}, l_{\mathrm{Z,d}} \leq\\
&l_{\mathrm{M_1^1,Z}} + l_{\mathrm{M_1^2,Z}}, l_{\mathrm{M_1^1,Z}} + l_{\mathrm{s,Z}}, l_{\mathrm{M_1^2,Z}} + l_{\mathrm{s,Z}}
\end{aligned} \tag{27}$$

Proof: We need to find sufficient conditions such that all $N!$ possible communicating pairs of source-destination $\{(S_i, D_j)\}$ are possible in Eve's perspective which are derived as:
-Condition $\mathcal{C}_1$: It is straightforward that $l_{s,d}$ should be zero, otherwise Eve can ascertain the destination of these sources perfectly and the maximum number of possible communicating pairs will be less than $(N-l_{s,d})!$ which does not yield optimal anonymity. If $l_{M_1^1,d} \neq 0$, Eve can ascertain that the sources which use M_1^2 as their

entry guard and request it to anonymize their stream will not communicate with the destinations directly connected to M_1^1(in the graph shown in Figure 12). If $l_{s,M_3^i} \neq 0$, Eve can ascertain that these sources will communicate with destinations connected to M_3^i. If $l_{M_1^i,M_3^j} \neq 0$, then, Eve can infer that there are $l_{M_1^i,M_3^j}$ of sources which use M_1^i as entry guard that will communicate with the destinations connected to M_3^j.
-Condition $\mathcal{C}_2$: If $l_{s,M_2^1} \neq 0, l_{M_2^2,d} \neq 0$, then Eve ascertains that that the source belongs to l_{s,M_2^1} will not communicate with the destinations connected directly to $M_2^2(l_{M_2^2,d})$.
-Condition $\mathcal{C}_3$ is obtained by applying the Chu-Vandermonde identity assuming conditions $\mathcal{C}_1$, and $\mathcal{C}_2$ hold. $\square$.

Theorem 1 gives sufficient conditions to achieve maximum anonymity. As can be observed from the conditions, in order to achieve maximum anonymity, it is not necessary for all sources to request all the three anonymous relays in its route sequence to pad their streams. Nevertheless, the anonymity is achieved at the cost of additional delay. Any choice of parameters that satisfy these conditions would maximize the weighted reward $\alpha\mathcal{A} - (1-\alpha)\bar{\mathcal{D}}$ merely for $\alpha = 1$.

5.3 Delay Anonymity Trade-off

That a tradeoff exists between the achieved anonymity and the delay caused by intermediate nodes padding the streams is easy to understand. Although, it may not seem straightforward, there is also a tradeoff between the achieved anonymity and the latency caused by the transmission delay between the nodes. For example, consider a network with four sources where each source chooses its relay selection parameters based on the minimum latency caused by the delay between the nodes and all anonymization parameters are set $(1,1,1)$. Assume that due to bandwidth constraints, each anonymous relay can serve no more than two streams. Then, without loss of generality,we may assume $R_1 = R_2 = (M_1^1, M_2^1,\ M_3^1)$ and $R_3 = R_4 = (M_1^2, M_2^2, M_3^2)$. Such choice of relay selection and anonymization parameters yields minimum latency caused by the delays between the nodes, and anonymity equal to $\frac{\log(2!*2!)}{\log(4!)}$ which is far less than the optimal anonymity. If the network is willing to increase the latency by changing the parameters of sources S_2 and S_3 to $R_2 = (M_1^1, M_2^2, M_3^1)$, and $R_3 = (M_1^2, M_2^1, M_3^1)$, respectively, which yields in higher latency, the optimal anonymity will be achieved.

In the six relay abstraction, the average delay of the network was defined in equation (24) as a linear function of relay selection and anonymization parameters. As mentioned in Section 5.1, we model the preference of all the sources on the delay anonymity tradeoff curve by the weighting parameter $0 \leq \alpha \leq 1$. In order to find the optimal trade off between anonymity and the average delay we need to find the relay node selection and control which maximizes the weighted sum of anonymity and delay which is $\alpha\mathcal{A} - (1-\alpha)\bar{\mathcal{D}}$. This can be expressed as the following integer programming problem:

$$\Phi : \max_{(R_1,\cdots,R_N,A_1,\cdots,A_N)} \alpha\mathcal{A} - (1-\alpha)\bar{\mathcal{D}}, \tag{28}$$

where $\{A_i\}$ and $\{R_i\}$ are feasible solutions. Note that the integer programming problem as stated above with a non-convex metric is $np-$hard and in order to find the optimal anonymity delay tradeoff region, a computational solver needs to search among all feasible parameters which yields in $O(2^N)$ search points. This is impractical particularly if the algorithm would have to be implemented in real time. We therefore present a suboptimal heuristic which requires only $O(N)$ search points to characterize the delay anonymity tradeoff region (which sweeps across the domain of α from 0 to 1).

5.3.1 Suboptimal Delay Anonymity Region

The main idea behind the suboptimal algorithm to compute the delay-anonymity tradeoff is as follows. Assume all the anonymization parameters are zero, i.e. $\forall S_i \in \mathcal{S} : A_i = (0,0,0)$. For each source S_i, we have the sequence $(d_i^1, R_i^1), (d_i^2, R_i^2), \cdots, (d_i^8, R_i^8)$ which are the sorted delays of each routes for the source S_i such that d_i^1 is the least delay for source S_i and R_i^1 is the relay selection parameter for source S_i which has the delay d_i^1 (We note that d_i^j is the latency caused by the transmission time between nodes and does not include the delay by the intermediate nodes). The route selection $R_i = R_i^1$ and anonymization parameter $A_i = (0,0,0)$ yields in the delay optimal point $\mathcal{A}_0^* = 0, \bar{\mathcal{D}}_0^*$. The algorithm works by incrementally altering the relay selection parameters from this minimum delay setup until the maximum possible anonymity is achieved. Specifically, at each iteration, the algorithm searches for a change in either an element of a source anonymization parameter or changing the route of one of the sources which yields in the least increase in delay. If this least increase is accomplished through a change in an anonymization parameter, then the resulting increased anonymity and delay are recorded, and the algorithm moves to the subsequent iteration. If instead, the least delay increase is an outcome of a route change, the algorithm verifies if indeed the anonymity has increased. If so, then the values and parameters are recorded. If not, then this selection is discarded and the algorithm moves on to the choice that results in the next lowest delay increase to repeat this process. Thus the algorithm, at every successful iteration records a choice of parameters $R_1, \cdots, R_N$, and $A_1, \cdots, A_N$, and the corresponding anonymity and average delay $\mathcal{A}(R_1, \cdots, R_N, A_1, \cdots, A_N)$, and $\bar{\mathcal{D}}(R_1, \cdots, R_N, A_1, \cdots, A_N)$, respectively. The set of these recorded pairs delineates the complete tradeoff (suboptimal). At every iteration, since only one parameter is changed, the complexity is linear in the number of nodes ($O(N)$ per point on the tradeoff. In the following we provide a bound on the difference between the optimal and suboptimal tradeoffs and in Section 5.4 we demonstrate numerically that the performance of this algorithm is close to that of the exponential complexity optimal search.

Algorithm 2 Suboptimal Algorithm for delay anonymity region

```
1:  For i=1:N
2:      $R_i \leftarrow R_i^1, A_i = (0, 0, 0)$
3:  Endfor
4:  $Z' = sort(r_1, r_2, \cdots, r_N)$, $Z = [Z' \; Z' \; Z']$, $U = 0$, $q = 1$
5:  $F = \{R_1^1, \cdots, R_1^8, \cdots, R_N^1, \cdots, R_N^8\}$
6:  $\mathcal{A}^U \leftarrow \mathcal{A}(R_1, \cdots, R_N, A)$, $\bar{\mathcal{D}}^U \leftarrow \bar{\mathcal{D}}(R_1, \cdots, R_N, A)$
7:  $j, o = argmin_{R_i^k \in F}\{r_i(d(R_i^k) - d(R_i))\}$
8:  If $d_M Z(q) < r_j(d(R_j^o) - d(R_j))$ and $q \leq 3N$
9:      $A_i(\lceil \frac{q}{N} \rceil) = 1$,
10:     $\mathcal{A}^U \leftarrow \mathcal{A}(R_1, \cdots, R_N, A)$, $\bar{\mathcal{D}}^U \leftarrow \bar{\mathcal{D}}(R_1, \cdots, R_N, A)$
11:     U=U+1, q=q+1, go to 6.
12: Elseif $\mathcal{A}(R_1, \cdots R_j^o, \cdots, R_N, A) > \mathcal{A}(R_1, \cdots, R_N, A)$
13:     $F = F/R_j^o$, $R_j \leftarrow R_j^o$
14:     $\mathcal{A}^U \leftarrow \mathcal{A}(R_1, \cdots, R_N, A), \bar{\mathcal{D}}^U \leftarrow \bar{\mathcal{D}}(R_1, \cdots, R_N, A)$
15:     U=U+1, go to 6
16: Elseif $F \neq \emptyset$
17:     $F = F/R_j$, go to 6
18: Endif
```

Let the delay constraint of each anonymous relay be d, and B be the maximum number of streams that can be served by a single relay. Then, the following theorem provides an upper bound on the performance loss due to suboptimality. Note that these assumptions are for the sake of presentation simplicity and the bound can be easily derived for the general case.

Theorem 5.3 *If $\mathcal{A}^*(\alpha)$ and $\bar{\mathcal{D}}^*(\alpha)$ are the optimal anonymity and average delay for weighting factor α, then, suboptimal algorithm $(\mathcal{A}^{sub}(\alpha), \bar{\mathcal{D}}^{sub}(\alpha))$ ensures the perfor-*

mance bounded as follows:

$$[\alpha\mathcal{A}^*(\alpha) - (1-\alpha)\bar{\mathcal{D}}^*(\alpha)] - [\alpha\mathcal{A}^{sub}(\alpha) - \\ (1-\alpha)\bar{\mathcal{D}}^{sub}(\alpha)] \leq \frac{\log(N)}{\log(N!)} + \frac{\frac{\delta}{d}}{1+\frac{1}{3(1-B/N)d}}, \tag{29}$$

where $\delta = \max_{1\leq k\leq N, 1\leq j\leq 7}\{d_k^{j+1} - d_k^j\}$.

Proof: Let's define $a(i) = \frac{\log(i!)}{\log(N!)}$. The following lemma presents the minimum number of padded links required to achieve anonymity $a(i)$.

Lemma 5.4 *The minimum number of padded links required in order to achieve anonymity $a(i)$ is*

$$m(i) = \begin{cases} i & \text{if} \quad i \leq B \\ i + 3(i-B) & \text{if} \quad i > B \end{cases}$$

Proof: If $i \leq B$, one anonymous relay can perform link padding for all i sources. When $i > B$, if the network served only i source-destination pairs, then the conditions in Theorem 1 for maximum anonymity reduce to the expression in the Lemma. When the number of source-destination pairs is increased to N, this expression would serve as a lower bound on the number of padded links. □.

For a fixed α, there exists i such that $a(i) \leq \mathcal{A}^*(\alpha) \leq a(i+1)$. By using the result of Lemma 2, it is straightforward to check that:

$$\bar{\mathcal{D}}^*(\alpha) \geq \frac{m(i)d}{N} + \bar{\mathcal{D}}_0^* \triangleq \bar{\mathcal{D}}(i) \tag{30}$$

where $\mathcal{D}_0^*$ is the delay of the shortest path in the algorithm. 1)If $i \leq B$, then, suboptimal algorithm changes at most $B - N/2$ routes and pads $m(i)$ links to achieve $\mathcal{A}^{sub}(\alpha) = a(i)$ and

$$\bar{\mathcal{D}}^{sub}(\alpha) \leq \bar{\mathcal{D}}(i) + \frac{(B-\frac{N}{2})\delta}{N} \tag{31}$$

Using inequalities (30) and (31),

$$\alpha[\mathcal{A}^*(\alpha) - \mathcal{A}^{sub}(\alpha)] \leq \alpha[\frac{\log((i+1)!)}{\log(N!)} - \frac{\log(i!)}{\log(N!)}] \leq \\ \frac{\log(N)}{\log(N!)}, \quad \bar{\mathcal{D}}^*(\alpha) - \bar{\mathcal{D}}^{sub}(\alpha) \geq \frac{(B-\frac{N}{2})\delta}{N} \tag{32}$$

2)If $i > B$, suboptimal algorithm changes at most $3(i-B)$ routes and pads exactly $m(i)$ links to achieve $\mathcal{A}^{sub}(\alpha) = a(i)$ and

$$\bar{\mathcal{D}}^{sub}(\alpha) \leq \bar{\mathcal{D}}(i) + \frac{3(i-B)\delta}{N} \tag{33}$$

Using inequalities (30) and (33),

$$\begin{aligned}\alpha[\mathcal{A}^*(\alpha) - \mathcal{A}^{sub}(\alpha)] &\leq \frac{\log(N)}{\log(N!)} \\ \bar{\mathcal{D}}^*(\alpha) - \bar{\mathcal{D}}^{sub}(\alpha) &\geq \frac{3(i-B)\delta}{N} \end{aligned} \tag{34}$$

Moreover, using the fact that $\alpha\mathcal{A}^*(\alpha) - (1-\alpha)\bar{\mathcal{D}}^*(\alpha) > -(1-\alpha)\bar{\mathcal{D}}_0^*$ and $\mathcal{A}^* \leq 1$, we can upper bound $1-\alpha$ as:

$$1 - \alpha \leq \frac{1}{1 + (\bar{\mathcal{D}}^* - \bar{\mathcal{D}}_0^*)} \leq \frac{1}{1 + \frac{m(i)d}{N}} \tag{35}$$

Combining (32), (34), and(35) provides the bound. □.

The performance of suboptimal algorithm improves as B increases which is intuitive as for larger B, number of changes in routes decreases. For example, if $B = N$, suboptimal algorithm just needs to change at most $N/2$ routes such that all N sources are using at least one common anonymous relay and this relay is the only relay performs link padding.

5.3.2 Incremental Optimization

The algorithms described thus far are joint optimization schemes where relay selection and control parameters are chosen for all sources together. In practice, users arbitrarily join the system, and consequently, we propose an incremental mechanism that merely requires each arriving source to obtain numerical information from routers to compute the optimal route and anonymization parameters. We will show that if an existing system is anonymity optimal then a new arriving user can maintain that optimality. We assume the new user wants to join the system, has the equal (or agreeably close to) preference parameter α to its own. To minimize the bandwidth draw of dependent link padding, it is beneficial if users in this network have data rates that are close to each other, thus limiting network congestion. For a new user who wishes to join the network, the following incremental optimization needs to be solved to find his optimal parameters assuming the choices for the existing nodes are undisturbed.

Assume we have the system with N users and for a specific $0 \leq \alpha \leq 1$, the value of the optimal incremental optimization are $\mathcal{A}_N^{inc}$ and $\bar{\mathcal{D}}_N^{inc}$ and the solution is denoted by R_i^{Ninc}. When the new user is added, we want to maximize the value of

$\alpha\mathcal{A}^{inc}_{N+1}-(1-\alpha)\bar{\mathcal{D}}^{inc}_{N+1}$. We therefore express the new optimization problem as follows:

$$\begin{aligned}&\Gamma : \max_{R_{N+1}} \alpha\mathcal{A}^{inc}_{N+1} - (1-\alpha)\bar{\mathcal{D}}^{inc}_{N+1}\\ &\text{Subject to: } \forall 1 \le i \le N : R_i = R_i^{Ninc}, A_i = A_i^{Ninc}\end{aligned}$$

This is a simple integer programming problem due to the division of the whole systems into sub-systems and the search is over 16 possible solutions and identifying the choice that maximizes $\alpha\mathcal{A}^{inc}_{N+1} - (1-\alpha)\bar{\mathcal{D}}^{inc}_{N+1}$. Thus, whenever a new user wants to enter the network $\mathcal{A}^{inc}_{N+1} - (1-\alpha)\bar{\mathcal{D}}^{inc}_{N+1}$ is computed for each of the possible routes and anonymization parameter, and then the route corresponding to the maximum value is selected. Although an incremental optimization to add a user to an optimal system need not be a jointly optimal solution for all users, in the following Lemma, we show that in the maximum anonymity scenario, where $\alpha = 1$, incremental optimization will always yield in the jointly optimal solution.

Lemma 5.5 *If $\alpha = 1$, and the existing route selection for the existing users is anonymity optimal, then the incremental optimization will also yield in an anonymity optimal solution for all $N+1$ users.*

Proof: As $\alpha = 1$ and delay is not the preference, we assume all the current sources and the new source has anonymization parameter equal to $(1,1,1)$. If $\mathcal{A}^{inc}_N = 1$ holds, based on Theorem 1, we have $l_{M_1^1,M_2^1}(N)$, $l_{M_1^2,M_2^1}(N) \ge l_{M_2^1,M_3^1}(N)$, and $l_{M_1^1,M_2^2}(N)$, $l_{M_1^2,M_2^2}(N) \ge l_{M_2^2,M_3^1}(N)$. If these inequalities are strict, then adding the new route to any eight candidates yields in optimal anonymity, as all the $\{l_{X,Y}(N+1)\}$ will satisfy the conditions of Theorem 1. If at least one of these inequalities holds with equality, then adding the new user to the route for which equality holds again satisfies the new inequalities of Theorem 5.2, while also satisfying the bandwidth constraint as it is added to the route which has lighter traffic. Let's assume both of them hold with equality, ie $l_{M_1^1,M_2^1}(N) = l_{M_1^2,M_2^1}(N) = l_{M_2^1,M_3^1}(N) = x$, then the new route can be added to the route M_1^1, M_2^1, M_3^2 or M_1^2, M_2^1, M_3^2, then the new parameters will again satisfy the condition of Theorem 1, and it will also satisfies the bandwidth constraint as it is added to the route which have lighter traffic. The same scenario can be applied for the case where all the four inequalities hold with equality. Consequently, we can always add the new users route in a way that ensures $\mathcal{A}^{inc}_{N+1} = 1$ □.

5.4 Numerical Results and Simulations

In our simulations, using the model proposed in [84], we simulated users' streams by heavy tailed distributed traffic. Even though the analytical results thus far assume that the delay constraint does not cause overhead, in our numerical simulations we compute the true rate of dummy transmissions required for heavy tailed distributed traffic.

Specifically, using the heavy tail traffic model, we simulated the network consisting six anonymous relays, six sources with average rate of 10 packets/second for all the feasible sets of anonymization and relay selection parameters in time period of $[0, 100]$ seconds. We assumed each anonymous relay has delay constraint equal to 0.3 seconds (to be in quadratic region) and bandwidth constraint equal to 36 packets/seconds. The dummy rate, average packet delay(caused by anonymous relays), and anonymity is plotted for all the feasible solutions in Figure 14. The simulation starts with zero anonymization parameters which yields in zero anonymity, dummy rate, and average delay. Each jump in the plot shows a change in anonymization parameters, and the swings in each of these regions are caused by changing the relay selection parameters.

While theorem 5.3 ensures that the performance of suboptimal algorithm in the six relay abstraction model is bounded by (29), in Figure 15, we simulated our suboptimal algorithm on a more general network which consists eight anonymous relays and six pairs of source-destination. Each source may choose any multihop path to communicate its desired destination and it will decide whether any of the anonymous relays on this path will perform link padding or not. We note that the complexity of optimal delay anonymity tradeoff in such a network is $O((|\mathcal{M}|!)^N 2^{N|\mathcal{M}|})$. Unlike the six relay abstraction, for general networks, a "closed form" expression for the anonymity is not likely to exist. The achieved anonymity can, however, be derived using recursion from N pairs of source-destination to $N-1$ pairs. As it is evident in Figure 15, the delay gap between the optimal solution and suboptimal solution for a fixed anonymity value is negligible.

Next, we compared the performance of suboptimal solution of problem Φ with the solution of the incremental optimization problem while number of sources are increased from 10 to 19. For the incremental solution, we start with the suboptimal solution for 10 sources, then, any new sources will choose it's relay selection and anonymization parameters to solve the optimization problem Γ. As it is shown in Figure 16, the gap between the curves decreases as α increases and for $\alpha = 1$, both

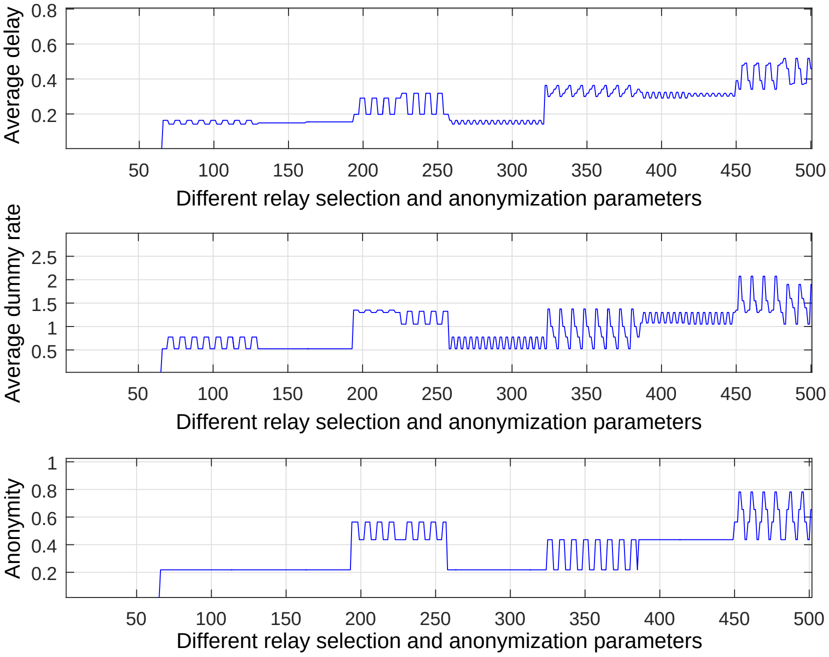


Figure 14: Anonymity, average delay, and average dummy of six relay network for different relay selection and anonimization parameters considering heavy tail traffic for users.

the curves achieves the optimal anonymity.

N	# source-destination pairs	$\mathcal{B}_{M_j^i}$	bandwidth constraint of M_j^i	r_i	arrival rate of S_i	$\bar{\mathcal{D}}$	average delay of network
$\mathcal{V}$	set of nodes	R_i	relay selection parameter of S_i	r_{tot}	$\sum_{i=1}^{N} r_i$	$l_{X,Y}$	# of padded links from X to Y
$\mathcal{E}$	set of edges	A_i	anonymization parameter of S_i	$d_{M_j^i}$	delay constraint of M_j^i	d_i^j	transmission delay of R_i^j
$\mathcal{S}$	set of sources	X_i	r.v denotes destination of S_i	$\mathcal{M}$	set of anonymous relays	$\mathcal{D}$	set of destinations
Θ	complete observation and knowledge of Eve	X_{ij}	jth anonymous relay on S_i's route	S_{Du}^i	overhead dummy rate of S_i	$r_{M_j^i}$	packet rate on padded links of M_j^i
$\mathcal{M}_E$, $\mathcal{M}_M$, $\mathcal{M}_Q$	set of entry guards, intermediate nodes, and exit guards	I_{S_i}, $\mathrm{X_{ij}}$	anonymization parameter corresponding to jth anonymous relay on S_i's route	$d_{X,Y}$	transmission delay from X to Y	R_i^j	relay selection parameter of S_i yields jth shortest path

Table 1: Notation table

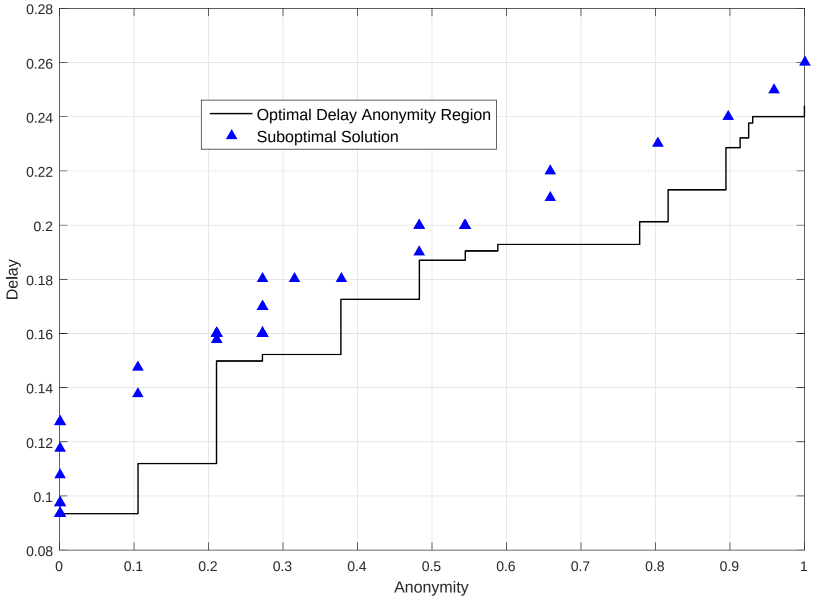


Figure 15: Delay anonymity region for a network consisting 6 pairs of source-destinations and 8 anonymous relays.

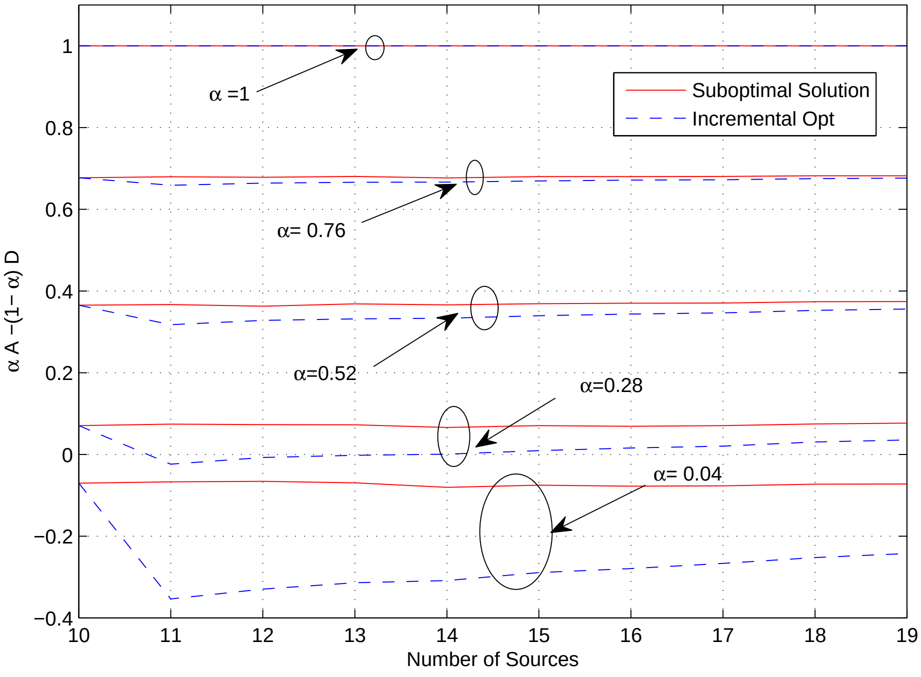


Figure 16: Comparing performance of suboptimal solution and incremental optimization solution.

6 Differential Privacy in Dynamical Systems and Networks

In this chapter, we study the design of control policies under differential privacy constraints. Differential privacy was introduced as a tool to provide privacy in data from learners and statisticians [85] provides a point-wise measure on users privacy (without Bayesian assumptions). In particular to providing point-wise privacy, differential privacy is also immune against any side information that an adversary may have. Using the notation of differential privacy, and for a fix privacy parameter, we aim to design optimal control policies which achieves the weighted sum of maximum rewards. In the first section of this chapter, we study differential privacy preserving policies for Markov Decision Processes. In the second section, we consider an application of this framework in routing, where nodes serve as states of the dynamical system.

6.1 Inference Resistant Policy Design for Markov Decision Processes

Markov decision processes (MDPs) are a discrete time mathematical framework for modeling decision making in dynamic systems. In a classical MDP, at each time step, the system is in some state s, and the controller decides on an action a. Given the current state s, and controller's action a, the controller receives a reward, and the state of the system transit to the next state according to a Markovian probability $P(s'|s,a)$, and the controller's goal is to maximize the total (discounted) reward over a finite or infinite horizon [17]. MDPs are widely used in cyber physical systems, finance, robotics, etc. Another important application of MDP is in reinforcement learning [18], where an agent interacts with an unknown environment towards maximizing some objective, and the underlying process is modeled as an MDP. The main difference between a classical MDP and reinforcement learning is that the latter does not assume the knowledge of the mathematical model of the MDP. In many applications of MDPs, the sequence of states (or some function of the states) are observable to eavesdroppers. For example, in a wireless network, an adversary can access length of packets [19], timing of packets transmitted [20], routes of packet flow over a network [21] and suchlike by eavesdropping. Using the observations, an adversary can infer about the nature of the MDPs, and consequently obtain sensitive information about the decision making entity. As machine learning algorithms continually improve the ability to identify personal preferences from seemingly unrelated data, it is critical that stochastic decision making processes be investigated from a privacy perspective which is the focus of this work.

In this work, we investigate the mathematical framework of Markov Decision Processes with the objective of limiting adversarial inference of a *type* of MDP. In particular, as shown in Figure 17, consider two MDPs with identical state-action spaces but differing reward and transition dynamics. For instance, these could represent user actions on a pair of websites. It is well known that sequence of click times or download sizes can reveal which websites are being accessed even if data transmitted is encrypted [22]. In this context, if the sequence of actions or response times were so designed to maximize user experience, then an eavesdropper can identify the website accessed by performing a hypothesis test on the observations. However, if the actions were so designed such that the observations from the pair of websites had near similar dynamics, then privacy of access can be preserved. In broader terms, for a pair of MDPs, if the policies were jointly designed such that the observed state dynamics for both MDPs were ϵ close to each other in a likelihood sense, then any hypothesis test between the MDPs would have very limited success. It is precisely the joint design of the policies for a pair of generic infinite horizon MDPs that we consider in this work such that a weighted sum of rewards of the two MDPs are maximized subject to an ϵ-differential privacy guarantee for the observed state dynamics.

Further, we provide a value iteration method to recursively derive the optimal rewards and the policies for the two MDPs that are differentially private at the desired ϵ level. The proposed method is shown to converge and the convergence rate of this method is proved to be equal to the discount factor.

6.1.1 System Model

In this work, we consider the inference resistant control of two Markov Decision Processes, $\mathcal{M}_1$ and $\mathcal{M}_2$. Each MDP $\mathcal{M}_i$ is represented by a 5-tuple $\mathcal{M}_i = (\mathcal{S}, \mathcal{A}, r_i, P_i, \beta)$, where $\mathcal{S} = \{1, 2, \cdots, n\}$ is the set of states and $\mathcal{A}$ is the set of actions, and $0 \leq \beta < 1$ is the discount factor, all identical for both MDPs. Each $r_i : \mathcal{S} \times \mathcal{A} \to \mathbb{R}$ denotes the reward function wherein $r_i(s, a)$ is the immediate reward received when the controller for MDP $\mathcal{M}_i$ chooses action a in state s. P_i represents the set of transition probabilities for MDP $\mathcal{M}_i$ such that $P_i(s'|s, a)$ is the probability that the state of MDP $\mathcal{M}_i$ transit to state s', given the current state is s, and the controller i takes action a. Let's denote the space of all policies for MDP $\mathcal{M}_i$ by Π_i, such that for a policy $\pi_i = \{\pi_i^0, \pi_i^1, \cdots\} \in \Pi_i$, $\pi_i^t(a|s)$ represents the probability of taking action a by

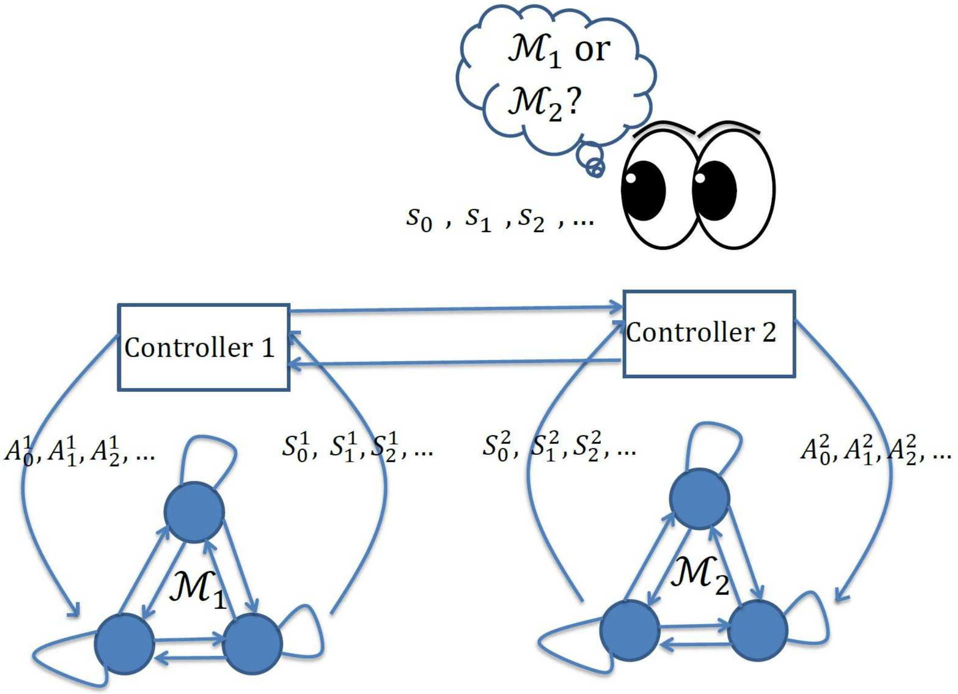

$\mathcal{M}_1$ or
$\mathcal{M}_2$?
s_0 , s_1 , s_2 , …
Controller 1
Controller 2
$A_0^1, A_1^1, A_2^1, \ldots$
$S_0^1,\ S_1^1, S_2^1, \ldots$
$S_0^2,\ S_1^2, S_2^2, \ldots$
$A_0^2, A_1^2, A_2^2, \ldots$
$\mathcal{M}_1$
$\mathcal{M}_2$

Figure 17: In our system model, there are two MDPs with the same state and action spaces and different transition probabilities and rewards. There is an adversary who observes a sequence of states from one of the MDPs and aims to identify which MDP the sequence belongs to.

controller i at time t, given the current state is s. We also denote the space of joint policies of MDPs $\mathcal{M}_1$ and $\mathcal{M}_2$, by Π, where $\Pi = \Pi_1 \times \Pi_2$.

In a stochastic control problem, in general, policies may be dependent on all the history of previous states, and actions. However, in MDPs, because of their Markovian property, it is shown that the optimal policies are just dependent on the current state.

For MDP $\mathcal{M}_i$, if controller i has the policy π_i, given the initial state is s, the discounted reward will be as follows:

$$V_i^{\pi_i}(s) = \sum_{t=0}^{\infty} \beta^t \mathbb{E}_{\pi_i}\{r_i(S_t^i, A_t^i)|S_0^i = s\}, \tag{36}$$

In a classical MDP, a controller by choosing a policy makes a sequence of decisions to maximize his discounted reward expressed in equation (36). For each standalone MDP, it is known that optimal policy is stationary and deterministic, in other words, the optimal policy is a sequence of identical deterministic mapping from state to action space. If privacy was not a concern, then, each MDP could be solved independently and the optimal stationary policy and discounted reward for each standalone MDP can be derived by methods such as value iteration, policy iteration, or linear programming [17]. However, in the presence of an adversary who is trying to identify the MDP, two controllers cooperate to hide their identity to the adversary while maximizing a weighted sum of their discounted rewards.

Before, we move forward with the rest of our system model and the technical results, we need to define the adversary, and his knowledge.

- **Adversary**: We consider a passive adversary who is aware of the state space, action space, transition probabilities and rewards of both MDPs. At any given time, the adversary observes a sequence of states for one of the MDPs and his goal is to identify which MDP it belongs to. In fact, the adversary maps the sequence of states to one of two hypotheses:

$$\mathcal{H}_1: \text{ The observed state sequence belongs to } \mathcal{M}_1$$
$$\mathcal{H}_2: \text{ The observed state sequence belongs to } \mathcal{M}_2$$

This is a classical hypothesis testing problem, where it is known that the optimal strategy for adversary is to implement a likelihood ratio detector [86]. For example, if the adversary observes a sequence of states $s_0, s_1, \cdots, s_T$, then, he computes the following log-likelihood ratio and decides on each hypothesis based on the log-likelihood ratio:

$$\begin{aligned}
&\frac{1}{T} l(s_0, s_1, \cdots, s_T) = \frac{1}{T} \log \frac{Pr(s_0, s_1, \cdots, s_T | \mathcal{M}_1)}{Pr(s_0, s_1, \cdots, s_T | \mathcal{M}_2)} = \\
&\frac{1}{T} \log \frac{\mu_{1,0}^{\pi_1}(s_0) \prod_{t=0}^{T-1} p_{1,t}^{\pi_1}(s_{t+1}|s_t)}{\mu_{2,0}^{\pi_2}(s_0) \prod_{t=0}^{T-1} p_{2,t}^{\pi_2}(s_{t+1}|s_t)} \\
&\frac{1}{T} [\log \frac{\mu_{1,0}^{\pi_1}(s_0)}{\mu_{2,0}^{\pi_2}(s_0)} + \sum_{t=0}^{T-1} \log \frac{p_{1,t}^{\pi_1}(s_{t+1}|s_t)}{p_{2,t}^{\pi_2}(s_{t+1}|s_t)}] \overset{\mathcal{H}_1 \mathcal{H}_2}{\geq <} 0, \qquad (37)
\end{aligned}$$

where $\mu_{i,t}^{\pi_i}(s)$ is the stationary distribution of state s, and $p_{i,t}^{\pi_i}(s'|s)$ is the probability of transiting from state s to state s' at time t, given the policy π_i is applied by the ith controller. $p_{i,t}^{\pi_i}(s'|s)$ and $\mu_i^{\pi_i}(s)$ can be derived as follows:

$$\forall s, s' \in \mathcal{S},\ i = 1, 2:\ p_{i,t}^{\pi_i}(s'|s) = \sum_a \pi_i^t(a|s) P_i(s'|s, a)$$
$$\forall s' \in \mathcal{S},\ i = 1, 2: \mu_{i,t}^{\pi_i}(s') = \sum_s \mu_{i,t}^{\pi_i}(s) p_{i,t}^{\pi_i}(s'|s) \qquad (38)$$

If $l(.) \geq 0$, then, the optimal detector accepts $\mathcal{H}_1$, else it accepts $\mathcal{H}_2$. By taking the limit on equation (37), when $T \to \infty$, we have:

$$\lim_{T\to\infty} \frac{1}{T} l(s_0, s_1, \cdots, s_T) = \sum_{(s,s')} \mu(s) \log \frac{p_1^{\pi_1}(s'|s)}{p_2^{\pi_2}(s'|s)}, \tag{39}$$

where $\mu(s)$ represents the stationary distribution of state s under the true hypothesis. Note that $\mu(s)$ is function of π_1 or π_2, depending on the true hypothesis. The above equation implies that $\lim_{T\to\infty} \frac{1}{T} l(s_0, s_1, \cdots, s_T)$ is a convex combination of the terms $\log \frac{p_1^{\pi_1}(s'|s)}{p_2^{\pi_2}(s'|s)}$. Therefore, if for each pair of (s, s') and $\epsilon \geq 0$, we guarantee $-\epsilon \leq \log \frac{p_1^{\pi_1}(s'|s)}{p_2^{\pi_2}(s'|s)} \leq \epsilon$, it is assured that $-\epsilon \leq \lim_{T\to\infty} \frac{1}{T} l(s_0, s_1, \cdots, s_T) \leq \epsilon$ which implies the notion of ϵ-differential privacy for the normalized log likelihood between pair of MDPs. In effect, by choosing an appropriate ϵ, the optimal adversarial inference can be made as challenging as desired. In other words, if the ϵ-differential privacy is guaranteed for all transition probabilities $(p_1^{\pi_1}(s'|s), p_2^{\pi_2}(s'|s))$, then, ϵ-differential privacy is guaranteed against the adversary who uses the optimum likelihood ratio detector.

- **ϵ-Differential Private Policies**: The structure of adversary which was explained in the previous section motivates us to use differential privacy to guarantee that two MDPs will not be detectable to the adversary. Thus, in order to guarantee the privacy, we need to assure that at anytime the transition probabilities between states for both MDPs are ϵ-differentially private. We note that transition probabilities are sufficient statistics for the adversarial detection problem. Particularly, perturbation bounds in [87] can be used to guarantee differential privacy on stationary distribution, given that transition probabilities are differentially private.

  The following defines what makes a pair of policies for the two MDPs ϵ-differential private.

Definition 6.1 *For a fixed $\epsilon \geq 0$, and transition probabilities P_1 and P_2, we call the set $\Pi_{\epsilon,P_1,P_2} \subset \Pi$, the set of all ϵ-differential private policies, if for all pairs of policies $(\pi_1, \pi_2) \in \Pi_{\epsilon,P_1,P_2}$, the following conditions hold:*

$$\forall s, s' \in \mathcal{S} \text{ and } t = 0, 1, \cdots : e^{-\epsilon} \leq \frac{p_{1,t}^{\pi_1}(s'|s)}{p_{2,t}^{\pi_2}(s'|s)} \leq e^{\epsilon}$$

Moreover, we call any pair of policies (π_1, π_2), pair of ϵ-differential private policies if $(\pi_1, \pi_2) \in \Pi_{\epsilon,P_1,P_2}$.

Similar to a classical MDP, the discounted reward of MDP $\mathcal{M}_i$ for a fixed policy π_i, given the initial state is s is denoted by $V_i^{\pi_i}(s)$, and can be derived by equation (36). Through this paper, we may also consider the vector of discounted rewards as $\mathbf{V}_i^{\pi_i} = (V_i^{\pi_i}(1), \cdots, V_i^{\pi_i}(n))^T$. In a differentially private setting, the controllers cooperate to maximize a weighted sum of their discounted rewards while preserving the differential privacy constraints. In other words, we aim to derive pair of ϵ-differential privacy (π_1, π_2) which maximizes the following discounted reward:

$$Q(s) = \lambda V_1^{\pi_1}(s) + (1-\lambda) V_2^{\pi_2}(s), \tag{40}$$

where $0 \leq \lambda \leq 1$ is the weighting factor and $(\pi_1, \pi_2) \in \Pi_{\epsilon, P_1, P_2}$. In other words, the optimal weighted discounted reward denoted by $Q^*_{\epsilon,\lambda}$ satisfies the following:

$$\begin{aligned} \forall s \in \mathcal{S}:\ Q^*_{\epsilon,\lambda}(s) = \lambda V^*_{1,\epsilon,\lambda}(s) + (1-\lambda) V^*_{2,\epsilon,\lambda}(s) = \\ \max_{(\pi_1,\pi_2)\in(\Pi\times\Pi)_{\epsilon,P_1,P_2}} \lambda V_1^{\pi_1}(s) + (1-\lambda) V_2^{\pi_2}(s) \end{aligned} \tag{41}$$

6.1.2 MDPs under ϵ-Differential Privacy

In this section, we propose an iterative method to derive the optimal weighted sum of discounted rewards and optimal ϵ-differentially private policies. First, we introduce the mapping $T_{\epsilon,\lambda} : \mathbb{R}^{2n} \rightarrow \mathbb{R}^{2n}$, and prove that by applying mapping $T_{\epsilon,\lambda}$ successively on any arbitrary vector in the space of $\mathbb{R}^{2n}$, the optimal discounted rewards can be derived.

Let's consider two arbitrary vectors $\mathbf{V}_1 = (V_1(1), \cdots, V_1(n))^T$ and $\mathbf{V}_2 = (V_2(1), \cdots, V_2(n))^T$. We define the mapping $T_{\epsilon,\lambda}$ such that for $(\mathbf{V}_1^{new}, \mathbf{V}_2^{new}) = T_{\epsilon,\lambda}\ (\mathbf{V}_1, \mathbf{V}_2)$, we have:

$$V_i^{new}(s) = \sum_a q_i^*(a|s)[r_i(s,a) + \beta \sum_{s'} P_i(s'|s,a) V_i(s')]$$

where (q_1^*, q_2^*) is the maximizer of the following linear programming:

$$\begin{aligned} &\Psi:\ \max_{q_1,q_2} \lambda \sum_a q_1(a|s)[r_1(s,a) + \beta \sum_{s'} P_1(s'|s,a) V_1(s')] \\ &+(1-\lambda) \sum_a q_2(a|s)[r_2(s,a) + \beta \sum_{s'} P_2(s'|s,a) V_2(s')] \\ &\text{subject to:} \\ &\forall s, s' \in \mathcal{S}:\ e^{-\epsilon} \leq \frac{\sum_a q_1(a|s) P_1(s'|s,a)}{\sum_a q_2(a|s) P_2(s'|s,a)} \leq e^{\epsilon} \\ &\forall s \in \mathcal{S}:\ \sum_a q_1(a|s) = \sum_a q_2(a|s) = 1, \end{aligned} \tag{42}$$

We also define the weighted addition operator $A_\lambda : \mathbb{R}^{2n} \to \mathbb{R}^n$ such that for $\mathbf{Q} = (Q(1), \cdots, Q(n))^T = A_\lambda(\mathbf{V}_1, \mathbf{V}_2)$, we have: $\forall s \in \mathcal{S} : Q(s) = \lambda V_1(s) + (1-\lambda)V_2(s)$.

In the following theorem, we prove that for any arbitrary vectors $\mathbf{V}_1$ and $\mathbf{V}_2$, the sequence $\mathbf{Q}_K = A_\lambda(T^K_{\epsilon,\lambda}(\mathbf{V}_1, \mathbf{V}_2))$ converges to the optimal weighted sum of discounted rewards. Moreover, pair of optimal discounted rewards $(\mathbf{V}^*_{1,\epsilon,\lambda}, \mathbf{V}^*_{2,\epsilon,\lambda})$ satisfies a fixed point equation which is similar to Bellman equation.

Theorem 6.1 *The following statements hold:*

1. $\exists \mathbf{V}^*_{1,\epsilon,\lambda}, \mathbf{V}^*_{2,\epsilon,\lambda} \in \mathbb{R}^n$ *such that* $\mathbf{Q}^*_{\epsilon,\lambda} = A_\lambda(\mathbf{V}^*_{1,\epsilon,\lambda}, \mathbf{V}^*_{2,\epsilon,\lambda}) = A_\lambda T_{\epsilon,\lambda}(\mathbf{V}^*_{1,\epsilon,\lambda}, \mathbf{V}^*_{2,\epsilon,\lambda})$.

2. $\forall \mathbf{V}_1, \mathbf{V}_2 \in \mathbb{R}^n : \ \mathbf{Q}^*_{\epsilon,\lambda} = \lim_{K\to\infty} A_\lambda(T^K_{\epsilon,\lambda}(\mathbf{V}_1, \mathbf{V}_2))$

3. $\mathbf{Q}^*_{\epsilon,\lambda}$ *is unique.*

Proof: Before proving the theorem, in the following lemma, we demonstrate that mapping $T_{\epsilon,\lambda}$ is monotone. This result while being straightforward, is very critical for understanding the fixed point equations and proof of Theorem 6.1.

Lemma 6.2 *Consider two vectors* $\mathbf{V} = (\mathbf{V}_1, \mathbf{V}_2)$ *and* $\mathbf{V}' = (\mathbf{V}'_1, \mathbf{V}'_2)$ *such that* $A_\lambda(\mathbf{V}_1, \mathbf{V}_2) \leq A_\lambda(\mathbf{V}'_1, \mathbf{V}'_2)$. *In other words, for each* $s \in \mathcal{S}$, *we have* $\lambda V_1(s) + (1-\lambda)V_2(s) \leq \lambda V'_1(s) + (1-\lambda)V'_2(s)$. *Then, for any* $K > 0$, *we have* $A_\lambda T^K_{\epsilon,\lambda}(\mathbf{V}_1, \mathbf{V}_2) \leq A_\lambda T^K_{\epsilon,\lambda}(\mathbf{V}'_1, \mathbf{V}'_2)$.

Proof: $A_\lambda T^K_{\epsilon,\lambda}(\mathbf{V}_1, \mathbf{V}_2)$ derives the optimal weighted sum of discounted rewards of K finite horizon problem with terminating rewards $\lambda V_1(s) + (1-\lambda)V_2(s)$. It is straightforward that as terminating rewards increases in all states, the discounted reward of K finite horizon problem increases as well. □.

We start by proving the second argument. First, we prove that the sequence $\mathbf{Q}_K$ defined by $\mathbf{Q}_K = A_\lambda(T^K_{\epsilon,\lambda}(\mathbf{V}_1, \mathbf{V}_2))$ is a Cauchy sequence. In other words, we need to demonstrate that for each $\mu > 0$ there exists a positive integer K_μ such that for each $k_1, k_2 \geq K_\mu$, we have $||\mathbf{Q}_{k_1} - \mathbf{Q}_{k_2}||_\infty \leq \mu$, where $||\mathbf{Q}_{k_1} - \mathbf{Q}_{k_2}||_\infty = \max_s |Q_{k_1}(s) - Q_{k_2}(s)|$. For a given pair of ϵ-differential private policies $\pi_1 = \{\pi_1^0, \pi_1^1, \cdots\}$, and $\pi_2 = \{\pi_2^0, \pi_2^1, \cdots\}$, and fixed K, we can split the rewards of ith MDP to two parts as follows:

$$V_i^{\pi_i}(s) = \sum_{t=0}^{K-1} \beta^t \mathbb{E}_{\pi_i}\{r_i(S_t^i, A_t^i)|S_0^i = s\} +$$
$$\sum_{t=K}^{\infty} \beta^t \mathbb{E}_{\pi_i}\{r_i(S_t^i, A_t^i)|S_0^i = s\} \tag{43}$$

Considering that rewards are bounded, i.e. $\max_{i,s,a}|r_i(s,a)| \le R$, we have:

$$|\sum_{t=K}^{\infty}\beta^t\mathbb{E}_{\pi_i}\{r_i(S_t^i,A_t^i)|S_0^i=s\}| \le \frac{\beta^K R}{1-\beta} \tag{44}$$

By combining equation (43) and inequality (44), we can derive the following:

$$\begin{aligned}
&\lambda V_1^{\pi_1}(s)+(1-\lambda)V_2^{\pi_2}(s)-\frac{\beta^K R}{1-\beta} \le \\
&\lambda\sum_{t=0}^{K-1}\beta^t\mathbb{E}_{\pi_1}\{r_1(S_t^1,A_t^1)|S_0^1=s\}+ \\
&(1-\lambda)\sum_{t=0}^{K}\beta^t\mathbb{E}_{\pi_2}\{r_2(S_t^2,A_t^2)|S_0^2=s\} \\
&\le \lambda V_1^{\pi_1}(s)+(1-\lambda)V_2^{\pi_2}(s)+\frac{\beta^K R}{1-\beta}
\end{aligned}$$

By taking maximum over all ϵ-differential private policies on all sides of above inequality, we have:

$$\begin{aligned}
&\lambda\mathbf{V}^*_{1,\epsilon,\lambda}+(1-\lambda)\mathbf{V}^*_{2,\epsilon,\lambda}-\beta^K L \le A_\lambda T^K_{\epsilon,\lambda}(\mathbf{V}_1,\mathbf{V}_2) \\
&\le \lambda\mathbf{V}^*_{1,\epsilon,\lambda}+(1-\lambda)\mathbf{V}^*_{2,\epsilon,\lambda}+\beta^K L,
\end{aligned} \tag{45}$$

where $L=(||\mathbf{Q}_0||_\infty+\frac{R}{1-\beta})$ and $||\mathbf{Q}_0||_\infty=\max_s\{\lambda V_1(s)+(1-\lambda)V_2(s)\}$. In other words, we have $||A_\lambda T^K_{\epsilon,\lambda}(\mathbf{V}_1,\mathbf{V}_2)-\mathbf{Q}^*_{\lambda,\epsilon}||_\infty \le \beta^K L$. Using triangle inequality, we have: $||A_\lambda T^{k_1}_{\epsilon,\lambda}(\mathbf{V}_1,\mathbf{V}_2)-A_\lambda T^{k_2}_{\epsilon,\lambda}(\mathbf{V}_1,\mathbf{V}_2)||_\infty \le 2\beta^{\min(k_1,k_2)}L$. Therefore, for any $k_1,k_2 \ge N_\mu=\lceil\log_\beta\frac{\mu}{2L}\rceil$, we have $||\mathbf{Q}_{k_1}-\mathbf{Q}_{k_2}||_\infty \le \mu$ which proves that the sequence $\mathbf{Q}_k$ is a Cauchy sequence.

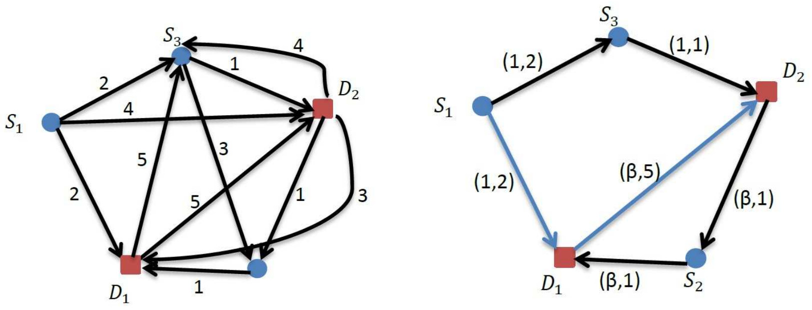
Now, we can take limit on all sides of equation (45), when $K\to\infty$. Consequently, we have $\lim_{K\to\infty} A_\lambda T^K_{\epsilon,\lambda}$ $(\mathbf{V}_1,\ \mathbf{V}_2)=Q^*$. Moreover, it is evident from equation (45) that the convergence rate of Q_K is equal to the discount factor β.

Now, we can apply mapping $T_{\epsilon,\lambda}$ on all sides of equation (45) and using the monotonicity of $T_{\epsilon,\lambda}$ we have:

$$\begin{aligned}
&A_\lambda T_{\epsilon,\lambda}(\mathbf{V}^*_{1,\epsilon,\lambda},\mathbf{V}^*_{2,\epsilon,\lambda})-\beta^{K+1}L \le A_\lambda T^{K+1}_{\epsilon,\lambda}(\mathbf{V}_1,\mathbf{V}_2) \\
&\le A_\lambda T_{\epsilon,\lambda}(\mathbf{V}^*_{1,\epsilon,\lambda},\mathbf{V}^*_{2,\epsilon,\lambda})+\beta^{K+1}L,
\end{aligned} \tag{46}$$

Now, by taking the limit when $K\to\infty$, combined with the fact that $\lim_{K\to\infty} A_\lambda T^{K+1}_{\epsilon,\lambda}$ $(\mathbf{V}_1,\ \mathbf{V}_2)=\mathbf{Q}^*_{\epsilon,\lambda}$, we conclude that $\mathbf{Q}^*_{\epsilon,\lambda}=A_\lambda(\mathbf{V}^*_{1,\epsilon,\lambda},\ \mathbf{V}^*_{2,\epsilon,\lambda})=A_\lambda T_{\epsilon,\lambda}$ $(\mathbf{V}^*_{1,\epsilon,\lambda},$ $\mathbf{V}^*_{2,\epsilon,\lambda})$. $\square$.

As a result of Theorem 6.1, we can derive the optimal stationary policies which is presented in the following lemma.



(a) A graph with 3 source nodes and 2 destination nodes.

(b) Two private routes are shown by black and blue arrows.

Figure 18: Private Routes in Networked Data Collection.

Corollary 6.2.1 *The pair of stationary ϵ-differential policies (π_1^*, π_2^*), where $\pi_1^* = \{q_1^*, q_1^*, \cdots\}$, and $\pi_2^* = \{q_2^*, q_2^*, \cdots\}$ is optimal if (q_1^*, q_2^*) are the policies which solves the following:*

$$A_\lambda(\mathbf{V}_{1,\epsilon,\lambda}^*, \mathbf{V}_{2,\epsilon,\lambda}^*) = A_\lambda T_{\epsilon,\lambda}(\mathbf{V}_{1,\epsilon,\lambda}^*, \mathbf{V}_{2,\epsilon,\lambda}^*) \tag{47}$$

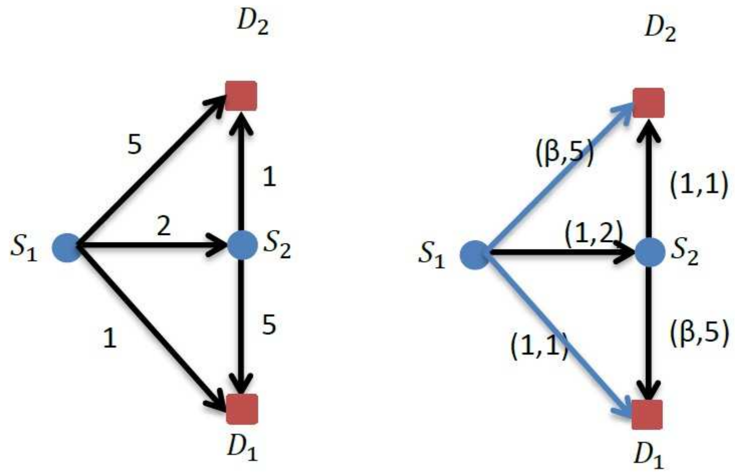
Using the results of theorem 6.1 and Corollary 6.2.1, we can solve for the optimal ϵ-differential private policies for any pair of finite state MDPs, for any weighted rewards. In particular, by starting from an arbitrary vectors $(\mathbf{V}_1, \mathbf{V}_2)$, and successively applying the mapping $T_{\epsilon,\lambda}$, the optimal discounted rewards, and subsequently, the optimal stationary ϵ-differential private policies can be derived.

6.2 Differential Privacy in Networked Data Collection

In this section, we study the problem of unicast and multicast routing in networks under differential privacy constraints. We explain our approach using a couple of examples. Consider the graph shown in figure 18a. There are some routes from the source node S_1 to the destination node D_2 including the shortest path between these two nodes which travels through S_3. If S_1 transmits packets through any of these routes to D_2, an eavesdropper observing this route can identify the destination of each packet departing source node S_1. If there is overhead routing, privacy may be achieved, albeit it results in higher cost. For example, if the intended destination is D_2, the packet may continue traveling to D_1 as well. In this case, the eavesdropper will be uncertain about the intended destination. In figure 18b, two such routes are shown. The cost of the route till the packet arrives it's intended destination may have higher priority to the cost of the rest of route. For example, if the cost is representing latency, the source will desire less latency to it's intended destination than the other one. Consequently, we assume the cost of a route is simply sum of the costs associated with each edge till the packet arrives it's intended destination, added with sum of the weighted costs associated with the other edges on the route. This weighting factor is denoted by $0 \leq \beta \leq 1$. For example the route shown by black edges will have cost $3 + 2\beta$ if the intended destination is D_2, and cost 5 for the case that the intended destination is D_1. Note that the route represented by black edges has the minimum cost over all such routes if the intended destination is D_2. Similarly, the route represented by blue edges has the minimum cost over all such routes if the intended destination is D_1. If source node S_1 always chooses the black route if D_2 is intended and blue route if D_1 is intended, no privacy will be provided, as an eavesdropper can identify the intended destination, based on her knowledge and observation. Consequently, in order to achieve some degree of privacy, the source should choose a probability distribution over all such routes which travels through all destination nodes. As multicast routing is a scheme to transmit overhead to other destinations as well, it can also be used to provide privacy for the single intended destination case. For example, in figure 19a, a graph with two source nodes and two destination nodes are represented and two private spanning tree are shown by blue and black arrows. The tree represented by black arrows minimizes the total cost for the case when D_1 is the intended destination and the route represented by blue arrows minimizes the cost for the case when D_2 is the intended destination. Similar to private unicast routing, for the sake of privacy, source S_1 can choose a probability distribution over all such spanning trees such that the weighted cost is minimized subject to the privacy requirements..

6.2.1 System Model

We model the network by a graph $G = (V, E)$, where $V = \mathcal{S} \bigcup \mathcal{D}$ is the set of vertices, and E is the set of directed edges. The set V is union of two sets: $\mathcal{S} = \{S_1, \cdots, S_N\}$ which is set of source nodes, and $\mathcal{D} = \{D_1, \cdots, D_M\}$ which is set of destination nodes. We assume that the set $\mathcal{D}$ is given; in a broader context, the source needs to decide the grouping of destinations that would balance the overhead costs with the desire for privacy. Each edge $(i, j) \in E$ of the network corresponds to a cost $c_{i,j}$. If privacy was not a consideration, each source would find the shortest path (minimum total cost of edges) to each destination and transmit packets through the respective paths. To provide privacy, we propose that a packet which departs source S_i to any destination



(a) A graph with 2 source nodes and 2 destination nodes.

(b) Two private spanning tree are shown by black and blue arrows.

Figure 19: Private Spanning Trees.

$D_j \in \mathcal{D}$ will *necessarily* travel through all other destinations in $\mathcal{D}$ as well. Intuitively, as the number of spanned destinations increases eavesdropper's uncertainty about the intended destination will increase, albeit in cost of higher average cost.

- **Unicast Private Routing**: Let's denote the set of private routes for a source $S_i \in \mathcal{S}$ by $\mathcal{R}_{S_i}$ which is the set of all the routes in the graph that start at node S_i and contains all nodes in $\mathcal{D}$. A private route $r \in \mathcal{R}_{S_i}$ can be expressed as a sequence of nodes $r = (S_i, M^r_{S_i,D_{j^r_1}}, D_{j^r_1}, M^r_{D_{j^r_1},D_{j^r_2}}, D_{j^r_2}, \cdots D_{j^r_M})$, where $M^r_{X,Y}$ is the sequence of source nodes between node X and node Y in route r. For example, in Figure 20 where there are two destinations D_1 and D_2, a route $r \in \mathcal{R}_{S_1}$ is shown by a red curve which can be written as $r = (S_1, S_4, D_2, S_2, S_4, S_7, D_1)$. Note that in this case $M^r_{S_1,D_2} = (S_4)$, $M^r_{D_2,D_1} = (S_2, S_4, S_7)$, $D_{j^r_1} = D_2$, and $D_{j^r_2} = D_1$. The corresponding cost of private route r if the intended destination is D_j is equal to:

$$\forall r \in \mathcal{R}_i, \forall D_j \in \mathcal{D} : C(r, D_j, \beta) = \sum_{n=1}^{k:r(k+1)=D_j} c_{r(n),r(n+1)} + \beta \sum_{n=k+1}^{l(r)-1} c_{r(n),r(n+1)}, \tag{48}$$

where $l(r)$ is the length of route $r, r(n)$ is the nth node in route r, and $0 \leq \beta \leq 1$ is the weighting factor. Equation (48) has two parts: the first sum reflects the cost till the packet arrives to it's intended destination and the second sum

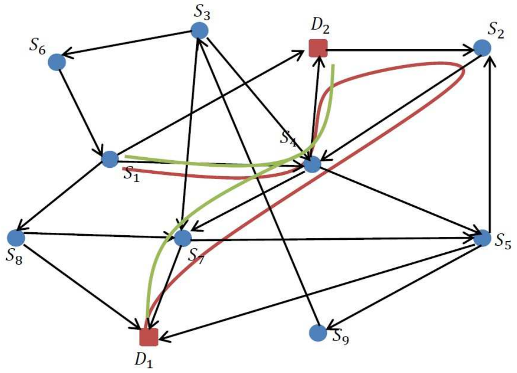


Figure 20: A private route $r \in \mathcal{R}_{S_1}$ is shown by the red curve and a private spanning tree $t \in T_{S_1}$ is shown by the green curve.

reflects the weighted cost for the rest of the route. The β factor quantifies the degree of importance accorded to the overhead beyond achieving the intended target.

We assume each source $S_i \in \mathcal{S}$ communicates with all nodes $D_j \in \mathcal{D}$. To effectively balance privacy with total cost, node S_i chooses a probability distribution $\mathcal{P}_{S_i}^{D_j} = \{P_{S_i}^{D_j}(r) | \sum_{r \in \mathcal{R}_{S_i}} P_{S_i}^{D_j}(r) = 1\}$ on the set of private routes $\mathcal{R}_{S_i}$ to communicate with node D_j. If the source chooses probability distribution $P_{S_i}^{D_j}$, then, the expected cost will be as follows:

$$\mathcal{C}(S_i, D_j, \beta) = \sum_{r \in \mathcal{R}_{S_i}} P_{S_i}^{D_j}(r) C(r, D_j, \beta) \tag{49}$$

The goal of unicast private routing scheme is minimizing $\sum_{D_j} \mathcal{C}(S_i, D_j, \beta)$ while satisfying $\epsilon-$differential privacy conditions, which will be explained in definition 6.2.

- **Multicast Private Routing**: Multicast routing is primary used to transmit a packet to a group of destinations. In the context of this paper, multicast routing by virtue of the multitude of destinations can be used to provide destination privacy, ie we use multicast to privatize unicast routing. For source S_i to multicast to all nodes in $\mathcal{D}$, the packets would be transmitted on a tree which spans $\mathcal{D} \bigcup \{S_i\}$, in other words, the Steiner Tree. The Minimum Steiner Tree (MST) is defined as the Steiner Tree which has the minimum total cost.

  For a source S_i, we define T_{S_i} as the set of all the trees in the graph G which span all the elements of $\{S_i\} \bigcup \mathcal{D}$ (We will call these trees as private spanning trees). The overhead weighted cost of a private spanning tree will be different for the different intended destination. For a private spanning tree $t \in T_{S_i}$, in order to define the cost $W(t, D_j, \beta)$ which is the cost of private tree t when the node D_j is the intended destination for this packet, we need to identify the unique path $t(S_i, D_j)$ in tree t which travels from node S_i to node D_j. For example, in Figure 20, a private spanning tree t for source S_1 is shown by the green curve. In this case, $t = \{(S_1, S_4), (S_4, D_2), (S_4, S_7), (S_7, D_1)\}$, $t(S_1, D_1) = \{(S_1, S_4), (S_4, S_7), (S_7, D_1)\}$, and $t(S_1, D_2) = \{(S_1, S_4), (S_4, D_2)\}$.

Considering a tree $t \in T_{S_i}$, the cost $l(t, D_j)$ will be defined as follows:

$$\begin{aligned} &\forall t \in T_{S_i}, \forall D_j \in \mathcal{D} : W(t, D_j, \beta) = \\ &\sum_{(u,v) \in t(S_i, D_j)} c_{u,v} + \beta \sum_{(u,v) \in T/t(S_i, D_j)} c_{u,v}, \end{aligned} \tag{50}$$

where $0 \leq \beta \leq 1$. Note that equation (50) has two parts: the first sum which has weighting factor one is the path that packet will travel to it's intended destination, and the second sum which has weighting factor β for the edges not included on this path.

In order to effectively balance privacy with costs, we add randomness in the choice of private spanning trees. Source S_i chooses a probability distribution $\mathcal{P}_{T_{S_i}}^{D_j} = \{P_{T_{S_i}}^{D_j}(t) | \sum_{t \in T_{S_i}} P_{T_{S_i}}^{D_j} = 1\}$ over the set of private spanning trees. For a specific probability distribution $P_{T_{S_i}}^{D_j}$, the expected cost will be as follows:

$$\mathcal{W}(S_i, D_j, \beta) = \sum_{t \in T_{S_i}} P_{T_{S_i}}^{D_j} W(t, D_j, \beta) \tag{51}$$

The main goal of private multicast routing is minimizing $\sum_{D_j} \mathcal{W}(S_i, D_j, \beta)$ while providing $\epsilon-$ differential privacy which we define in the following.

- **Differential Private Routing**:

  Eavesdropper (Eve): We consider an omniscient eavesdropper (Eve) who observes the traffic in the network. Eve knows all the information of the network including identity of nodes, costs of each edge, set of private routes, and set private spanning trees. In particular, Eve knows the probability distribution that each source chooses on it's private routes, ie Eve knows all $\{P_{S_i}^{D_j}\}$ and $\{P_{T_{S_i}}^{D_j}\}$. Eve's goal is identifying the destination node for a specific packet which departs source S_i. By observing the route a packet travels, Eve decides on the destination of this packet. In this work, we use the differential privacy to quantify the destination privacy. Based on the definition of differential, conditioned on the fact that Eve observes the private route r or private spanning tree t, the $\epsilon-$differential private routing for unicast and multicast routing scheme will be defined as follows:

Definition 6.2 ($\epsilon-$Differential Unicast Private Routing) *We say that a route probability distribution $\{P_{S_i}^{D_j}\}$ for the $3-$tuple $(G, \mathcal{S}, \mathcal{D})$ is $\epsilon-$differential private if:*

$$\forall S_i \in \mathcal{S}, \forall r \in \mathcal{R}_{S_i}, \forall D_k, D_j \in \mathcal{D} : \frac{P_{S_i}^{D_j}(r)}{P_{S_i}^{D_k}(r)} \leq e^{\epsilon} \tag{52}$$

Definition 6.3 ($\epsilon-$Differential Multicast Private Routing) *We say that a spanning tree probability distribution $\{P_{T_{S_i}}^{D_j}\}$ for the $3-$tuple $(G, \mathcal{S}, \mathcal{D})$ is $\epsilon-$differential private if:*

$$\forall S_i \in \mathcal{S}, \forall t \in T_{S_i}, \forall D_k, D_j \in \mathcal{D} : \frac{P_{T_{S_i}}^{D_j}(t)}{P_{T_{S_i}}^{D_k}(t)} \leq e^{\epsilon} \tag{53}$$

We note that the above follows the standard definition of differential privacy (as applied in the context of a dataset). In the broader context of the problem, however, the choice and size of the set $\mathcal{D}$ brings an added dimension to the privacy notion in routing. In the rest of this article, we investigate the optimal routing which minimizes the aggregated unicast cost ($\sum_{D_j \in \mathcal{D}} \mathcal{C}(S_i, D_j, \beta)$) for a specific source S_i and minimizing the aggregated multicast cost ($\sum_{D_j \in \mathcal{D}} \mathcal{W}(S_i, D_j, \beta)$) while satisfying the conditions defined in definitions 6.2, and 6.3, respectively.

6.2.2 Private Unicast Routing

In this section, our goal is to optimize the probability distributions $\{P_{S_i}^{D_j}\}$ such that the total average cost is minimized while satisfying differential privacy conditions. In other words, for each source node S_i our objective is to solve the following optimization problem:

$$\begin{aligned}
&\Phi : \min_{P_{S_i}^{D_1},\cdots,P_{S_i}^{D_M}} \sum_{D_j \in \mathcal{D}} \sum_{r \in \mathcal{R}_{S_i}} P_{S_i}^{D_j}(r) C(r, D_j, \beta) \\
&\text{Subject to :} \forall D_j \in \mathcal{D} : \sum_{r \in \mathcal{R}_{S_i}} P_{S_i}^{D_1}(r) = 1 \\
&\forall r \in \mathcal{R}_{S_i}, \forall D_k, D_j \in \mathcal{D} : \frac{P_{S_i}^{D_j}(r)}{P_{S_i}^{D_k}(r)} \leq e^{\epsilon} \qquad (54)
\end{aligned}$$

First, we consider solving this problem for the equal weighting parameter case where $\beta = 1$. In the following theorem, we prove that the optimal solution of problem Φ where $\beta = 1$, is identical to the optimal solution of traveling sales man problem.

Theorem 6.3 *Optimal unicast private routing for the case of equal weighting parameter ($\beta = 1$) yields*

$$\forall D_j \in \mathcal{D} : P_{S_i}^{D_j}(r^*_{TSM}) = 1,$$

where $r^*_{TSM} \in \mathcal{R}_{S_i}$ is the optimal route for traveling sales man problem where the starting node is S_i and the sales man should visit all the nodes in $\mathcal{D}$.

Proof: r^*_{TSM} satisfies the following inequality:

$$\forall D_j \in \mathcal{D}, \forall r \in \mathcal{R}_{S_i} : C(r^*_{TSM}, D_j, 1) \leq C(r, D_j, 1)$$

The immediate consequence of above inequality is that for a specific destination node D_j, $C(r^*_{TSM}, D_j, 1)$ will be smaller than any convex combination of $C(r, D_j, 1)$. Thus,

$$\begin{aligned}
&MC(r^*_{TSM}, D_j, 1) \leq \\
&\min_{P_{S_i}^{D_1},\cdots,P_{S_i}^{D_M}} \sum_{D_j \in \mathcal{D}} \sum_{r \in \mathcal{R}_{S_i}} P_{S_i}^{D_j}(r) C(r, D_j, \beta) \qquad (55)
\end{aligned}$$

and the condition of theorem presents a feasible solution which achieves this lower-bound and this completes the proof. □.

We note that the optimal unicast routing in the case of $\beta = 1$ yields the highest degree of privacy which is $0-$differential privacy. While the optimal unicast private routing for $\beta = 1$ yields a single route, the following theorem proves that the optimal unicast private routing for the case $0 \leq \beta < 1$ allocates nonzero probabilities on $2^M - 2$ different routes. Let's define the set of private route $\mathcal{R}^{SH}$ to be the set of all the private routes which includes the shortest path from the source node S_i to a destination node D_j and then the shortest path from the destination node D_j to the destination node D_u, and so on such that all the destination nodes are included on the route. There are $M!$ such routes and the following theorem proves that there are only $2^M - 2$ private routes between the elements of $\mathcal{R}^{SH}$ which have nonzero probability for the optimal unciast routing. Before going through the theorem, we introduce vector $\bar{C}(r, \beta)$ such that the m_{th} element of this vector is $C(r, D_m, \beta)$.

Theorem 6.4 *Optimal unicast private routing for the case of $0 \leq \beta < 1$ yields nonzero probability allocation only over all the routes $r^* \in \mathcal{R}^* \subset \mathcal{R}^{SH}$. Moreover each $r^* \in \mathcal{R}^*$ is the unique solution of following optimization problem*

$$\min_{t \in \mathcal{R}_{S_i}} \mathcal{E}^T \bar{C}(t, \beta), \tag{56}$$

where $\mathcal{E}_{1\times|\mathcal{D}|}$ is a vector such that each elements of it is either 1 or e^{ϵ} excluding two cases of $\bar{\mathbf{1}}_{1\times|\mathcal{D}|}$ and $e\bar{\mathbf{1}}_{1\times|\mathcal{D}|}$, where $\bar{\mathbf{1}}_{1\times|\mathcal{D}|}$ is the vector with all elements equal to one.

Proof: Considering the dual optimization problem of Φ and Complementary Slackness, we will prove this theorem. For a specific private route r, we have $M \times (M-1)$ inequality constraints which indicate privacy constraints. For each route r, we may have two scenarios: 1)$\forall D_j \in \mathcal{D}$, we have $P_{S_i}^{D_j}(r) = 0$. 2)$\forall D_j \in \mathcal{D}$, we have $P_{T_{S_i}}^{D_j}(r) \neq 0$ and they satisfy privacy inequality constraints. Moreover, Complementary Slackness forces $P_{T_{S_i}}^{D_j}(r)$ to satisfy the following conditions:

$$\begin{aligned} &\exists D_j, D_k \in \mathcal{D} : P_{S_i}^{D_j}(r) = e^{\epsilon} P_{S_i}^{D_k}(r) \\ &\forall D_u \neq D_k, D_j : P_{S_i}^{D_u}(r) = P_{S_i}^{D_j}(r) \text{ or } P_{S_i}^{D_u}(r) = P_{S_i}^{D_k}(r) \end{aligned} \tag{57}$$

Considering the conditions expressed in (57), we can set the routes which have nonzero probabilities to $2^M - 2$ groups and it is straightforward to check for each of these groups just one of them which is the solution of optimization problem expressed in (56) will have nonzero probability. It is also straightforward to check that for each vector $\mathcal{E}$ the solution of (56) is an element of $\mathcal{R}^{SH}$. Consequently, $\mathcal{R}^* \subset \mathcal{R}^{SH}$ □.

By the result of theorem 6.4, each node will use Dijkstra's algorithm to find the elements of the set $\mathcal{R}^{SH}$ and then by performing a simple search, one can find the elements of the set $\mathcal{R}^*$ and subsequently solve the corresponding linear programming problem.

6.2.3 Private Multicast Routing

In this section, we consider the problem of multicast routing for privacy in graph G. As we discussed in section 6.2.1, multicast routing can be used to provide destination privacy. However, the overhead weighted cost for different intended destination will be different and each source will choose a probability distribution over all it's private spanning trees. The optimal multicast routing scheme can be found by solving the following optimization problem:

$$\begin{aligned} &\Psi : \min_{P_{T_{S_i}}^{D_1},\cdots,P_{T_{S_i}}^{D_M}} \sum_{D_j \in \mathcal{D}} \sum_{t \in T_{S_i}} P_{T_{S_i}}^{D_j}(t) L(t, D_j, \beta) \\ &\textbf{Subject to:} \forall D_j \in \mathcal{D} : \sum_{t \in T_{S_i}} P_{T_{S_i}}^{D_j}(t) = 1 \\ &\forall t \in T_{S_i}, \forall D_j, D_k \in \mathcal{D} : \frac{P_{T_{S_i}}^{D_j}(t)}{P_{T_{S_i}}^{D_k}(t)} \leq e^{\epsilon} \end{aligned} \tag{58}$$

Similar to unicast private routing, we first consider the case of equal weighting factor ($\beta = 1$). In the following theorem, we prove that the optimal multicast routing for privacy when $\beta = 1$ is identical to the solution of the Minimum Steiner Tree (MST) problem:

Theorem 6.5 *Optimal multicast private routing for the case of equal weighting (*$\beta =$ 1*) yields*

$$\forall D_j \in \mathcal{D} : P_{T_{S_i}}^{D_j}(t^*_{MST}) = 1, \tag{59}$$

where t^*_{MST} *is the Minimum Steiner Tree which spans all the elements of* $\{S_i\} \bigcup \mathcal{D}$.

Proof: by the definition of MST, we know that $\forall D_j \in \mathcal{D}$ and $\forall t \in T_{S_i}$, we have $W(t^*_{MST}, D_j, 1) \leq W(t, D_j, 1)$. Consequently, $W(t^*_{MST}, D_j, 1)$ is less than any convex combination of $W(t, D_j, 1)$ and we have

$$\begin{aligned} &MW(t^*_{MST}, D_j, 1) \leq \\ &\min_{P_{T_{S_i}}^{D_1},\cdots,P_{T_{S_i}}^{D_M}} \sum_{D_j \in \mathcal{D}} \sum_{t \in T_{S_i}} P_{T_{S_i}}^{D_j} W(t, D_j, 1) \end{aligned} \tag{60}$$

and the conditions in the theorem presents a feasible solution which achieves this lowerbound. □.

Note that the solution of theorem 6.5 yields the highest degree of privacy which is $0-$differential privacy. Prior to investigating the solution when $0 < \beta < 1$, let's consider the optimal multicast routing when $\beta = 0$. It is straightforward to prove that the optimal multicast routing with $\epsilon-$differential privacy when $\beta = 0$, is achieved by always transmitting through a tree which has it's root at S_i and there is an individual route from S_i to each destination D_j which is the shortest path from the node S_i to the node D_j.

For notation convenience, we define the vector $\bar{W}(t, \beta)$ such that the m_{th} element of this vector is $W(t, D_m, \beta)$. The following theorem proves that the optimal multicast routing for privacy in graph $G = (V, E)$ when $0 < \beta < 1$, allocates nonzero probability $P_{T_{S_i}}^{D_j}(t)$ only over $2^M - 2$ trees, where M is the number of destination nodes.

Theorem 6.6 *The optimal Solution of Ψ yields on allocation of nonzero $P_{T_{S_i}}^{D_j}(t)$ over the set T^* such that $|T^*| = 2^M - 2$ and elements of this set are the solution of the following problem:*

$$\min_{t \in T_{S_i}} \mathcal{E}^T \bar{W}(t, \beta), \tag{61}$$

where $\mathcal{E}_{1\times|\mathcal{D}|}$ is a vector such that each elements of it are either 1 or e^{ϵ} excluding two cases of $\bar{\mathbf{1}}_{1\times|\mathcal{D}|}$ and $e\bar{\mathbf{1}}_{1\times|\mathcal{D}|}$.

Proof: Similar to proof of Theorem 6.4 . □.

Note that there is no polynomial time solution to find the elements of T^*, because the problem is np-complete. In our simulation, we find the suboptimal solution of this problem using KMB algorithms. We construct the KMB complete graph over the nodes $\{S_i\} \bigcup \mathcal{D}$ such that the edge between each pair of nodes in the new complete graph is the shortest path between those node in the original graph and then, we look for the solutions of (61) between the spanning trees of this new subgraph. In the next step, we solve the corresponding linear programming over these spanning trees.

The following theorem proves that finding the optimal private multicast routing for the case of $0 < \beta \leq 1$ is NP-Complete.

Theorem 6.7 *Given a graph $G = (V, E)$, the problem of private multicast routing from a source node $S_i \in V$ which spans all the elements of $\mathcal{D} \subset V$ and minimizes the cost defined in equation (50) is an NP-Complete problem.*

Proof: we will prove that the solution of optimization problem expressed in (61) is NP-Complete which will be sufficient for the whole problem. The problem is NP, as a non-deterministic guess can list a set of edges and in polynomial time, it is possible to check:1)These edges form a tree.2)The tree spans all the elements of $\{S_i\} \bigcup \mathcal{D}$. The problem is NP-hard as the solution of optimization problem expressed in (61) for the case of $\beta = 1$ yields Minimum Steiner Tree. Consequently, the problem is NP-Complete. □.

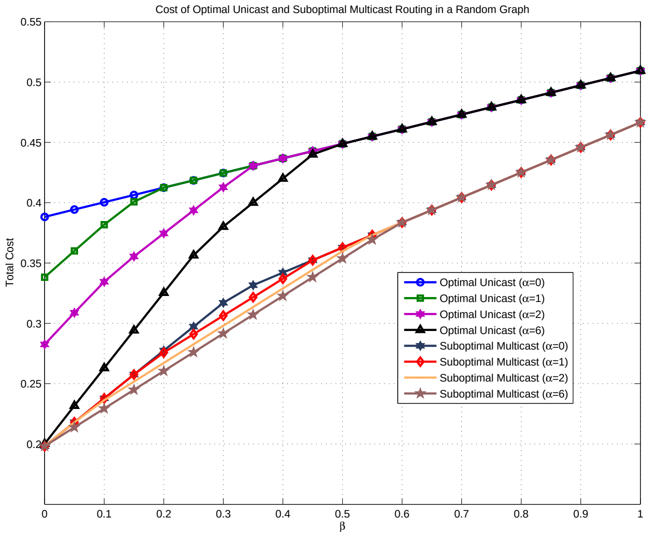


Figure 21: Cost of optimal unicast and suboptimal multicast routing as a function of β for different amount of ϵ in a complete random graph.

6.2.4 Simulations and Numerical Results

In our first simulation, we considered a network modeled by a complete random graph which consists of 12 source nodes and 3 destination nodes. The cost of each edge is a uniform random variable $U[0,1]$ and total cost curves are derived for different ϵs for optimal private unicast and suboptimal multicast routing. It is seen that the total cost increases as ϵ decreases for both schemes which is intuitive as higher ϵ yields lower degree of privacy, consequently, sources are allowed to allocate higher probabilities on the paths (or spanning trees) with lower cost. Another interesting fact is that all the usnicast routing curves merge each other for higher βs, which is also intuitive as it was seen for $\beta = 1$, optimal routing was independent of ϵ. Multicast routing cost merges for both $\beta = 0$ and $\beta = 1$ as we proved that for these cases optimal routing is independent of ϵ. In the second simulation, we plotted the average cost for specific amount of ϵ, and β as a function of number of source nodes in the graph while there are three destination nodes. For each n, the simulation was run over 1000 random graph of size $n + 3$, and the average is plotted. It is known that the average cost of the shortest path, and the minimum steiner tree converge asymptotically as the size of the complete graph grows. The figure demonstrates the convergence of optimal differntially private paths and trees as well.

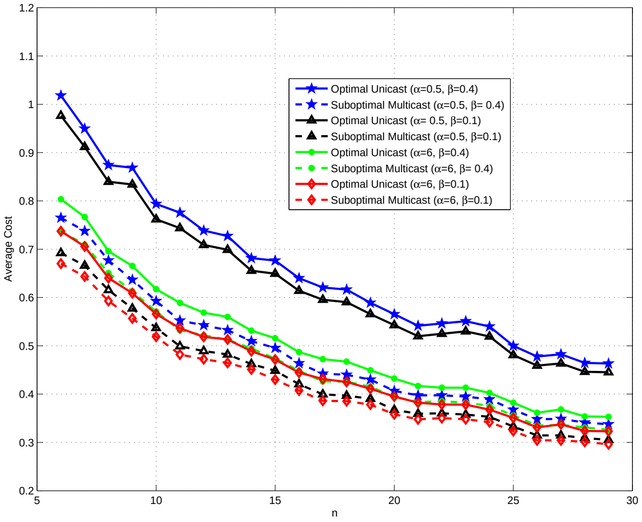


Figure 22: The average total cost for different amount of ϵ, and β as a function of network size.

7 Coupon Targeting Competition in a Privacy Sensitive Market

In the era of massive data collection, retailers collect and utilize private information about consumers by analyzing their purchasing history, trading private data, tracking Cookies, and similar strategies. Using this data, retailers can predict consumers taste, preference and the amount of money they are willing to spend on any given product [88]. Consequently, a retailer may offer lower prices to price sensitive consumers whilst consumers with less price sensitivity who are loyal to the retailer will be offered higher prices. Offering different prices to consumers based on their loyalty and price sensitivity increases retailers profits and results in price discrimination [89–91].

Retailers may prefer to compete for price sensitive consumers by offering targeted coupons instead of lowering their prices, as coupon targeting engenders market segmentation, whereas decreasing prices does not [24]. It is also well understood that targeted coupons and other innovative coupon strategies increase the revenue of retailers [92, 93], and results in price discrimination [73, 94, 95]. Coupons are, of course, ultimately beneficial to the consumers owing to price reduction and minimizing the need to "shop around" for merchandise.

Coupons targeted at specific custom areas based on their preferences, however, engender a fundamental violation of individual privacy. Preference for a particular product, or a class of products, can often lead to sensitive information revealed to retailers. A noteworthy example is when the father of a teen inadvertently discovered his daughter's pregnancy due to a targeted coupon from Target [96]. Knowledge of privacy violations can make consumers stop purchasing from specific retailers, or at the very least, decrease the consumer loyalty towards the retailer [23]. It is also shown in [7] that consumers are more willing to purchase from online retailers who protect their privacy. In effect, price sensitivity and brand loyalty alone do not dictate consumer purchasing decisions, and impact of privacy violation ought to be considered in retailer decisions to send targeted coupons. It is this privacy aware decision process that this article aims to shed light upon. More specifically, we study competitive coupon targeting between a pair of retailers when price and privacy are explicitly considered as factors in the consumer decision making.

In this section, we use the privacy sensitivity model as proposed by Sankar et al in [23], wherein consumers are assumed to exist in one of two states with respect to a retailer 1) Non-alerted state where consumers trust a retailer, and 2) Alerted state, where consumers are aware and wary of privacy violations by the retailer. Consumers switch between these states depending on whether they receive targeted coupons from a retailer. The switching is modeled probabilistically using Markov chains; a consumer in a non-alerted state switches to an alerted state with a fixed probability if s/he receives a targeted coupon, and a consumer in an alerted state switches back with some fixed probability if s/he does not receive a targeted coupon.

Following the coupon targeting model in a price sensitive market in [24], we assume that consumers are located on a Hotelling line such that the location of consumers on the line represents their preference for the retailers. It is known that the Hotelling line in a price sensitive market is divided into four segments which are shown in Figure 23. The competition between retailers in a price sensitivity market at each segment is modeled by a static bimatrix game. However, in a privacy sensitive market, static games cannot capture the profit of retailers, as they need to consider both immediate reward and the impact of their action on futures rewards. For example, a retailer may receive some profit by sending a targeted coupon to a consumer, but as a consequence of sending the targeted coupon, the consumer may get privacy alerted about the retailer and stop purchasing from this retailer in the future. Thus, we model the competition of retailers in a privacy sensitive market using nonzero-sum stochastic games. Note that in [23] the interaction between a single retailer and a single consumer using Markov Decision Processes with a similar setting is investigated.

In this work, we demonstrate that a privacy sensitive market is divided into 12 segments. Moreover, we derive the optimal stationary coupon targeting policies and discounted rewards for both retailers at each specific segment of the Hotelling line. We prove that consumers with weak preference for a retailer will change their purchasing brand if they notice their privacy is violated by the retailer. We also prove that at segments which adopts mixed strategies, the popular retailer has a less defensive strategy whilst the rival retailer has a more offensive targeting strategy as the discount factor increases. In other words, as the importance of future profit gets higher, the popular retailer will be more conservative about consumers with weak preference for it, because, these consumers are more likely to change their purchasing brand in the future, if they get alerted about this retailer. On the other hand, the rival retailer will be more aggressive to 1) get a higher share of market, 2) push the popular retailer to distribute targeted coupons. Eventually, we demonstrate that despite the price sensitive market, the rival retailer will have a non-negative discounted reward on the consumers with weak preference for the incumbent retailer.

In order to model a privacy sensitive market, we need to adopt a measure for privacy in our model. There are several popular approaches to quantify privacy in literature. Information theoretic metrics such as Shannon entropy [97], or min-entropy [98] which are based on Bayesian assumptions about prior probabilities. Although information theoretic measures are tractable and concave, they measure average privacy. Statisticians use differential privacy as a tool to measure point-wise privacy (no Bayesian assumption) in data collection [85]. While quantitative measures of privacy allows one to include privacy as a tangible commodity, in the context of consumer markets, we need a mechanism to study user behavior in response to privacy violations. The approach proposed in [23] provides this mechanism, and we adopt it in the context of market competition. In this approach, instead of measuring privacy, we are looking at privacy violation as an action-reaction phenomenon, and using probabilistic models for that investigation. Such phenomenon is modeled by a Markov Chain (MC) with two states of privacy (alerted and non-alerted) for a specific consumer, representing the status of the consumer about a specific retailer.

The primary goal of this section is to investigate market behavior when consumers' purchasing decisions are impacted by price differences and privacy violations. Through this investigation, several questions arise: (1) What is the market segmentation in a privacy sensitive market? (2) How does the privacy-sensitivity affect retailers' profit? (3) What are the optimal targeted coupon strategy of retailers in each segment of a Hotelling line? (4) How does the discounting factor for future profits influence retailer decision making? (5) What are the long term consumer purchasing patterns and optimal strategies for consumers in a privacy sensitive market?

7.1 Overview of Coupon Targeting Problem in a Price Sensitive Market

In this section, we survey the model and main results in classical coupon targeting competition between two retailers in a price sensitive market. In the coupon targeting competition problem studied in [24], there are two retailers A, and B selling a commodity product, with different brands associated to each retailer, a fixed price P, and a marginal cost c. Retailers may distribute targeted coupons to specific consumers with discount value d and the marginal cost of distributing a coupon for each retailer, denoted by $z > 0$. Consumers are distributed uniformly on the line segment $[0, 1]$ while each retailer is located at one edge of this line, i.e., retailer A is located on $x = 0$ and retailer B is located at $x = 1$. The location of consumers reflects their loyalty to each brand and affect their purchasing decision. For example, consumers who are located closer to retailer A are more willing to buy this product from retailer A. However, if they get a targeted coupon from retailer B, they may purchase from retailer B. In [24], the influence of loyalty on purchasing decisions is modeled using a transportation cost t. If V is the common reservation price for each consumer, then, a consumer located at $x = X$ is willing to pay $V - tX$ for brand A and $V - t(1 - X)$ for brand B. It is assumed that V is large enough such that each consumer will purchase this product. Under this model, the market was shown to be divided into four segments defined as follows: (See Figure 23)

- Consumers loyal to retailer A: these consumers would purchase from retailer A regardless of whether they receive coupons from either retailer. Consequently the location of such a consumer satisfies: $P + tX \leq P - d + t(1 - X)$, in other word, these consumers are located in the interval $[0, X_A]$ where:

$$X_A = \frac{-d + t}{2t} \tag{62}$$

- Consumers with weak preference for retailer A: Consider a marginal consumer located at $x = \hat{X}$ who is indifferent if s/he does not have targeted coupon from both retailer or s/he has targeted coupon from both retailers. Such a consumer is located at $\hat{X} = \frac{1}{2}$. The consumers in the interval $[X_A, \hat{X}]$ are called consumers with weak preference for retailer A. These consumers purchase from retailer B if they have a targeted coupon from B and they do not have a targeted coupon from retailer A. Otherwise, they will purchase from retailer A.

- Similarly, consumers loyal to retailer B are located in the interval $[X_B, 1]$ and consumers with weak preference for retailer B are located in the interval $[\hat{X}, X_B]$, where $X_B = \frac{d+t}{2t}$.

These segments are shown in Figure 23 for symmetric cost parameters for both retailers. We note that the location of a consumer indicates her/his loyalty and preference for retailers, and parameter $t > 0$ represents price sensitivity of the market. For example, if $t \to 0$, then, the market will be divided into two segments, each representing consumers with weak preference for one of the retailers. Such a market represents the highest price sensitivity degree, as all the consumers change their purchasing brand if they are offered a targeted coupon from the rival retailer. On the other hand, if $t \to \infty$, the market is divided into two segments such that consumers at each segment

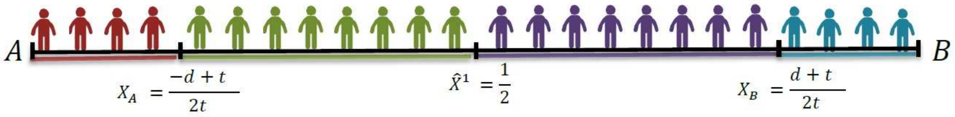


Figure 23: Market Segmentation in a Price Sensitive Market.

have strong preference for one of the retailers, representing a market with no price sensitivity, i.e., all consumers will purchase from their favorite retailer.

The equilibrium and optimal strategy of retailers at each segments is derived in [24] and we review these results in the following theorem.

Theorem 7.1 *Denote by p_i the probability associated to retailer A sending targeted coupons to consumers in ith segment, and denote by q_i the probability associated to retailer B sending targeted coupons to consumers in the ith segment. According to [24], the optimal strategies for an one-step game between retailer A and B in each segments are as follows:*

$$p = [p_1,\ p_2,\ p_3,\ p_4] = [0,\ \frac{P-c-d-z}{P-c-d},\ \frac{d+z}{P-c},\ 0]$$
$$q = [q_1,\ q_2,\ q_3,\ q_4] = [0,\ \frac{d+z}{P-c},\ \frac{P-c-d-z}{P-c-d},\ 0]$$

And the reward of each retailer at the equilibrium are as follows:

$$V_A = [P-c,\ P-c-d-z,\ 0,\ 0]$$
$$V_B = [0,\ 0,\ P-c-d-z,\ P-c]$$

The results in Theorem 7.1 are intuitive, as in segment 1, none of the retailers are willing to distribute targeted coupon between the consumers, as they cannot increase their reward by doing so. However, the bimatrix game in segment 2 which is shown in table 2 adopts a mixed strategy at the equilibrium point. In this segment, if both retailers do not distribute targeted coupons, retailer A receives the maximum possible reward, $P-c$ and retailer B receives 0 reward. However, retailer B can improve their reward by distributing a targeted coupon. In this case retailer B receives $P-c-d-z$ and retailer A receives zero. On the other hand, retailer A can again increase their reward by distributing a targeted coupon. Consequently, the bimatrix game in this segment is similar to prisoner's dilemma. In this segment, retailer A has a defensive strategy and tries to encourage the consumers with weak preference towards retailer

V_A, V_B	Targeting	Not Targeting
Targeting	$P-c-d-z, -z$	$P-c-d-z, 0$
Not Targeting	$0, P-c-d-z$	$P-c, 0$

Table 2: Bimatrix Game in Segment $\mathcal{S}_2$

A to maintain their loyalty, whereas retailer B has an offensive strategy and tries to increase its market share by offering them targeted coupons.

Subsequently, we adapt this Hotelling line model to study coupon targeting when consumers include privacy violations as a factor in their decision making which we model as an increase in transportation costs under an alerted state.

7.2 System Model

In the basic Hotelling line model [24] described previously, the bimatrix games were static and resulted in simple mixed strategy equilibria. In a privacy sensitive market, however, the competition is played out over the entire time horizon, since retailers sending coupons not only need to worry about immediate profits but also privacy related consequences in subsequent time steps as well. Privacy sensitivity, as mentioned earlier, is modeled as in [23], wherein consumers exist in one of two states with respect to each retailer: alerted or non-alerted. Consequently, consumers exist in one of four possible groups $\{S, S^B, S^A, S^{AB}\}$explained in the following paragraph. We model the impact of privacy using a differential in the transportation costs. In particular, a consumer alerted about retailer A would incur a higher transportation cost t_A from that retailer as opposed to a transportation cost $t_{NA} < t_A$ were s/he is not alert about that retailer. (Note that the subscripts "A", and "NA" stand for "Alerted", and "Non-Alerted", respectively.) When applying this notion to the Hotelling line model, four different Hotelling lines arise, one for each group.

- S: Consumers in this group are in non-alerted state about both retailers. Consequently, the transportation cost for both retailers will be t_{NA}. Assuming symmetric conditions, the marginal consumers for this group are located at

$$X_A^1 = \frac{-d + t_{NA}}{2t_{NA}}, \; \hat{X}^1 = \frac{1}{2}, \; X_B^1 = \frac{d + t_{NA}}{2t_{NA}}, \tag{63}$$

  We assume all the consumers start in this group at the beginning of the game.

- S^B: Consumers in this group are in the non-alerted state about retailer A and in the alerted state about retailer B. Consequently, the transportation cost for retailer A and B will be t_{NA}, and t_A, respectively. The marginal consumers in this group are located at:

$$X_A^2 = \frac{-d + t_A}{t_{NA} + t_A},\ \hat{X}^2 = \frac{t_A}{t_{NA} + t_A},\ X_B^2 = \frac{d + t_A}{t_{NA} + t_A}, \tag{64}$$

- S^A: Consumers in this group are in the alerted state about retailer A and in the non-alerted state about retailer B. Consequently, the transportation cost for retailer A and B will be t_A, and t_{NA}, respectively. The marginal consumers in this group are located at

$$X_A^3 = \frac{-d + t_{NA}}{t_{NA} + t_A},\ \hat{X}^3 = \frac{t_{NA}}{t_{NA} + t_A},\ X_B^3 = \frac{d + t_{NA}}{t_{NA} + t_A}, \tag{65}$$

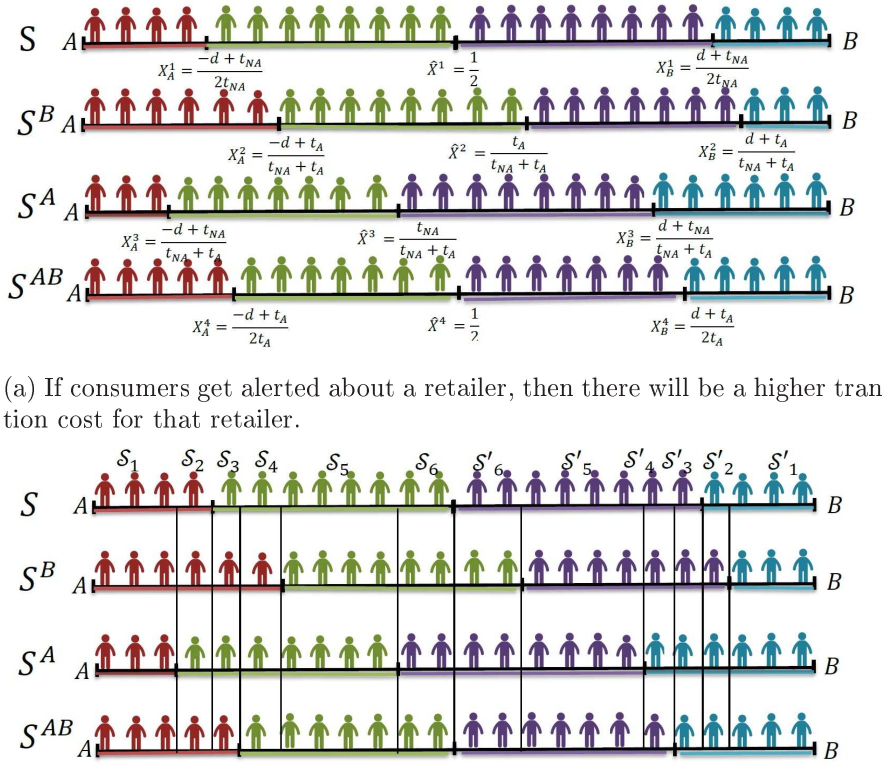
- S^{AB}: Consumers in this group are in alerted state about both retailers. Consequently, the transportation cost for both retailer will be t_A. The marginal consumers in this group are located at

$$X_A^4 = \frac{-d + t_A}{2t_A},\ \hat{X}^4 = \frac{1}{2},\ X_B^4 = \frac{d + t_A}{2t_A}, \tag{66}$$

The two dimensional nature of the privacy sensitive market results in a market segmentation with 12 segments as shown in Figure 24. Due to identical marginal costs, these are composed of two symmetric groups of 6 segments each. Note that for any i, the segment $\mathcal{S}_i'$ is symmetric with respect to the segment $\mathcal{S}_i$ and therefore it is sufficient to investigate the segments $\mathcal{S}_i$ for all i.

Consumers in a specific segment may move from one group to the other group within the same segment. However, they will not move from one segment to another. Consequently, the stochastic game at each segment is independent of other segments. Each retailer aims to maximize its discounted reward over an infinite horizon at each segment. As discussed before, each retailer may get a higher immediate reward by distributing a targeted coupon at a specific group of a segment. However, consumers may get alerted about this retailer and switch to the other retailer. Consequently, retailers' actions at the current time will influence both their immediate reward and future reward. This interaction between retailers and consumers in a specific segment of the Hotelling line is modeled by a nonzero stochastic game.

We model the stochastic game at segment $\mathcal{S}_i$ as a tuple $(\mathcal{S}, \mathcal{A}_A, \mathcal{A}_B, P, r_A, r_B, \beta)$, where $\mathcal{S}$ is the set of states such that $\alpha = [\alpha_S, \alpha_{S^B}, \alpha_{S^A}, \alpha_{S^{AB}}] \in \mathcal{S}$ represents the



S
A
B
$X_A^1 = \frac{-d + t_{NA}}{2t_{NA}}$
$\hat{X}^1 = \frac{1}{2}$
$X_B^1 = \frac{d + t_{NA}}{2t_{NA}}$
S^B
$X_A^2 = \frac{-d + t_A}{t_{NA} + t_A}$
$\hat{X}^2 = \frac{t_A}{t_{NA} + t_A}$
$X_B^2 = \frac{d + t_A}{t_{NA} + t_A}$
S^A
$X_A^3 = \frac{-d + t_{NA}}{t_{NA} + t_A}$
$\hat{X}^3 = \frac{t_{NA}}{t_{NA} + t_A}$
$X_B^3 = \frac{d + t_{NA}}{t_{NA} + t_A}$
S^{AB}
$X_A^4 = \frac{-d + t_A}{2t_A}$
$\hat{X}^4 = \frac{1}{2}$
$X_B^4 = \frac{d + t_A}{2t_A}$
$\mathcal{S}_1$ $\mathcal{S}_2$ $\mathcal{S}_3$ $\mathcal{S}_4$ $\mathcal{S}_5$ $\mathcal{S}_6$ $\mathcal{S}'_6$ $\mathcal{S}'_5$ $\mathcal{S}'_4$ $\mathcal{S}'_3$ $\mathcal{S}'_2$ $\mathcal{S}'_1$

(a) If consumers get alerted about a retailer, then there will be a higher transportation cost for that retailer.

(b) Market segmentation of a privacy-sensitive market. Note that the segment $\mathcal{S}'_i$ is symmetric to $\mathcal{S}_i$

Figure 24: Market Segmentation in a Privacy Sensitive Market

distribution of consumers at segment $\mathcal{S}_i$ over the four groups identified above. $\mathcal{A}_A$ and $\mathcal{A}_B$ are the set of actions for retailers A, and B, respectively. Each player may either send a targeted coupon to consumers in each group of the segment or not. Consequently, $\mathcal{A}_A = \mathcal{A}_B = \{T, UT\}$, where T denotes sending a targeted coupon and UT represents not sending a targeted coupon. At time t, if the current state is α_t, and player A, and B choose the actions a_A, and a_B, respectively, player A and B will receive a corresponding immediate reward of $r_A(\alpha_t, a_A, a_B)$ and $r_B(\alpha_t, a_A, a_B)$. Following this, the state of the game will transient to α_{t+1} with probability $P(\alpha_{t+1}|\alpha_t, a_A, a_B)$. The discount factor of the stochastic game is $0 \leq \beta < 1$.

Following the model in [23], we assume that a single consumer can be in a state $s \in \{A, NA\}$ about retailer X. If retailer X takes the action a_X, then the next state will be s' with probability $P_{a_x}(s'|s)$. The matrix P_{a_x} for each action $a_x \in \{T, UT\}$ is defined as follows:

$$P_T = \begin{pmatrix} \lambda_N & 1-\lambda_N \\ 0 & 1 \end{pmatrix}, \; P_{UT} = \begin{pmatrix} 1 & 0 \\ 1-\lambda_A & \lambda_A \end{pmatrix}, \tag{67}$$

where the first row and column correspond to the non-alerted state, and the second row and column correspond to the alerted state. Here, $1-\lambda_N$ represents the probability that a non-alerted consumer gets alerted if s/he receives a targeted coupon, and $1-\lambda_A$ represents the probability that an alerted consumer transients to the non-alerted state if s/he does not receive a targeted coupon. Note that if a consumer is alerted and s/he receives a targeted coupon, s/he will remain in the alerted state. Similarly, if a consumer in the non-alerted does not receive targeted coupon from the retailer, s/he will remain in the non-alerted state. λ_N and λ_A represents the privacy sensitivity of the market. For example, a market with no privacy concern can be modeled by $\lambda_N = 1$ and $\lambda_A = 0$, and a full privacy sensitive market can be modeled by $\lambda_N = 0$ and $\lambda_A = 1$. Note that $\frac{t_{NA}}{t_A}$ represents the effect of getting privacy alerted on purchasing decision of consumers.

The matrix defined by $P = P_{a_A} \otimes P_{a_B}$, where $\otimes$ represents the Kronecker product, captures the 4×4 transition matrix of our game. If the current state of the game is α_t and player A and B take actions a_A and a_B, respectively, the next state of the game will be α_{t+1} which is derived as follows:

$$\alpha_{t+1} = \alpha_t(P_{a_A} \otimes P_{a_B}), \tag{68}$$

The set of stationary policies of player X is denoted by Π_X such that a policy $\pi_X \in \Pi_X$ identifies a probability distribution on the action set of the player at a specific state. For example, $\pi_X(\alpha) = [\pi_X^S(\alpha), \pi_X^{S^B}(\alpha), \pi_X^{S^A}(\alpha), \pi_X^{S^{AB}}(\alpha)]$ denotes the policy of retailer X, and $\pi_X^s(\alpha)$ represent the probability that retailer X will distribute a targeted coupon to the consumer in group s when the current state of the game is α. Note that throughout this work, we use $\pi_X^s(\alpha, T)$ and $\pi_X^s(\alpha)$ interchangeably and we use $\pi_X^s(\alpha, UT)$ and $1-\pi_X^s(\alpha)$ interchangeably. If player A and B fix their policies π_A and π_B, respectively, the total reward of each of the players is as follows:

$$V_A^{\pi_A,\pi_B} = \sum_{t=0}^{\infty} \beta^t \mathbb{E}_{\pi_A,\pi_B}(r_A(S_t, A_{A,t}, A_{B,t}))$$
$$V_B^{\pi_A,\pi_B} = \sum_{t=0}^{\infty} \beta^t \mathbb{E}_{\pi_A,\pi_B}(r_B(S_t, A_{A,t}, A_{B,t}))$$

Definition 7.1 *The policies π_A^* and π_B^* results in an equilibrium if and only if the following holds:*

$$\begin{aligned} &\forall \pi_A \in \Pi_A : V_A^{\pi_A^*, \pi_B^*} \geq V_A^{\pi_A, \pi_B^*} \\ &\forall \pi_B \in \Pi_B : V_B^{\pi_A^*, \pi_B^*} \geq V_B^{\pi_A^*, \pi_B} \end{aligned} \tag{69}$$

So far, we have assumed that the state space of our non-zero sum stochastic game is continuous and represents the distribution of consumers over the identified four groups. However, in the following lemma, we prove that the optimal policy of each retailer in both finite and infinite horizon games is independent of the consumers' distributions. In other word, it is sufficient to restrict the state space of the game to four states, such that each group denotes a state of our non-zero sum game.

Lemma 7.2 *The optimal policy of retailers in the non-zero sum stochastic game at each segment is independent of the consumers' distribution over four groups and it is sufficient to consider $\mathcal{S} = \{S, S^B, S^A, S^{AB}\}$ as the state space .*

Proof: First, we prove the lemma by induction for the finite horizon case. Specifically, we prove that if Lemma holds for the case where N horizons left, it will also hold for $N+1$ horizon. The results hold for all Ns including $N \to \infty$. For proof's detail, refer to section 7.5.1. □.

Lemma 7.2 implies that consumers move between the four groups and not as fractions in groups. Moreover, it is sufficient to consider a state space including just these four groups, i.e. $\mathcal{S} = \{S, S^B, S^A, S^{AB}\}$. In the rest of this paper, we maintain the same notation introduced so far. However, instead of α_t, we use the notation $s_t \in \{S, S^B, S^A, S^{AB}\}$ which represents the state. For example, $V_{A,N}^{\pi_A, \pi_B}(S^{AB})$ represents the total discounted reward of retailer A, when N periods are left, retailer A, and B have policies π_A and π_B, respectively, and the initial state of the game is S^{AB}. Refer to table 3 for a complete explanation of the notation.

While the equilibrium of a finite-horizon non-zero sum stochastic game has non-stationary policies, the infinite horizon competition has an equilibrium in stationary policies space [99, 100]. If player A and B fix stationary policies π_A and π_B, respectively, the infinite horizon reward of each player is as follows:

$$V_A^{\pi_A,\pi_B} = \sum_{t=0}^{\infty} \beta^t \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} diag(\pi_A(a_1), \pi_B(a_2))(P_{a_1} \otimes P_{a_2}) r_A(a_1, a_2)$$

$$V_B^{\pi_A,\pi_B} = \sum_{t=0}^{\infty} \beta^t \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} diag(\pi_A(a_1), \pi_B(a_2))(P_{a_1} \otimes P_{a_2}) r_B(a_1, a_2),$$

where $diag(x, y)$ is an $n \times n$ diagonal matrix such that the element on (i, i) is the product of the ith element of vector x and the ith element of vector y and the rest of the elements of this matrix will be zero and $V_X^{\pi_A,\pi_B} = [V_X^{\pi_A,\pi_B}(S)$, $V_X^{\pi_A,\pi_B}(S^B)$, $V_X^{\pi_A,\pi_B}(S^A)$, $V_X^{\pi_A,\pi_B}(S^{AB})]^T$. On the other hand, we can also rewrite the discounted reward using Bellman Equations:

$$\forall s \in \mathcal{S} : V_A^{\pi_A,\pi_B}(s) = \underbrace{r^A(s, \pi_A, \pi_B)}_{immediate\ reward} \underbrace{+\beta \sum_{s' \in \mathcal{S}} P(s'|s, \pi_A, \pi_B) r(s', \pi_A, \pi_B)}_{reward\ to\ go}$$

The above equation implies that the total discounted reward of each firm contains two parts: 1) Immediate reward 2) Reward to go, where both parts depend on the current state and both retailers' policies.

7.3 Retailers Competition at each Segment

In this section, we study the equilibrium of competition at each segment of the Hotelling line and discuss how privacy constraints effects the policy and discounted reward of each retailer at each segment. Segments on Hotelling line of a privacy sensitive market can be categorized to three: 1) Segments not affected by privacy constraints. 2) Segments fully affected by privacy constraints. 3) Segments partially affected by privacy constraints. In following sections, we study each of these categories:

7.3.1 Segments not Affected by Privacy Constraints

In this section, we study the coupon targeting competition at segments $\mathcal{S}_1$ and $\mathcal{S}_5$, where the competition is not affected by the privacy sensitivity of the market. The primary reason that these segments are not affected by privacy sensitivity of the market is that in these segments, consumers at all four groups have the same preference on retailers.

1. **Coupon Targeting Competition in Segment** $\mathcal{S}_1$: In segment $\mathcal{S}_1$, at all four groups, consumers have strong preference on retailer A and they will purchase

Symbol	Meaning	Symbol	Meaning
$X_A^i, \hat{X}^i, X_B^i$	marginal consumers at group i	$\otimes$	kronecker product
$\mathcal{S}_i$	segment i	$[T]_{i,j}$	element on ith row and jth column of matrix T
$\mathcal{S}$	state space	P	transition matrix
$\mathcal{A}_X$	action space for player X	$r_X(s, a_A, a_B)$	immediate reward of player X if the current state is s and player A, and B take actions a_A and a_B, respectively
Π_X	set of stationary policies of player X	β	discount factor
α_j	proportion of consumers at group j	$\pi_X(s)$	probability that retailer X sends targeted coupon to consumers at group s
λ_N	probability that a non-alerted consumer remains non-alerted if s/he receives a targeted coupon	$\pi_X(s, A)$	probability of retailer X taking action A to consumers at group s
λ_A	probability that an alerted consumer stays alerted if s/he does not receive a targeted coupon	$V_X^{\pi_A, \pi_B}(s)$	reward of retailer X if retailer A and B have policies π_A, π_B, respectively and the current state is s.
$V_X^*(s)$	optimal reward of retailer X if the initial state of game is s	V_X^*	vector of optimal reward of retailer X in infinite non-zero sum game

Table 3: Table of Notations

from retailer A in all circumstances. The consumers in segment $\mathcal{S}_1$ have **privacy independent strong preference** for retailer A and even if they notice privacy violation by retailer A (or retailer B), they will still purchase from A. It is straightforward to check that in all four groups of segment $\mathcal{S}_1$, none of the retailers is willing to distribute targeted coupon, as, by doing so, they cannot they cannot increase their rewards, i.e., $\pi_A^* = [0, 0, 0, 0]$ and $\pi_B^* = [0, 0, 0, 0]$. Consequently, the optimal discounted reward of retailer A and B in the infinite horizon non-zero sum stochastic game of segment $\mathcal{S}_1$ will be as follows:

$$V_A^* = [\frac{(P-c)}{1-\beta}, \frac{(P-c)}{1-\beta}, \frac{(P-c)}{1-\beta}, \frac{(P-c)}{1-\beta}] \tag{70}$$

$$V_B^* = [0, 0, 0, 0] \tag{71}$$

2. **Coupon Targeting Competition in Segment** $\mathcal{S}_5$: Similar to segment $\mathcal{S}_1$, consumers at all four groups of segment $\mathcal{S}_5$ have similar preference for retailer B. In other words, consumers at this segment have **privacy independent weak preference** for retailer A, meaning even if they get privacy alerted about retailer A (or retailer B), they purchase from B if they only have targeted coupon from retailer B. The following theorem derives the optimal policies and discounted rewards of retailers at segment $\mathcal{S}_5$.

Theorem 7.3 *The optimal discounted reward of retailer A and B in the infinite horizon non-zero sum stochastic game of segment $\mathcal{S}_5$ will be as follows:*

$$V_A^* = [\frac{(P-c-d-z)}{1-\beta}, \frac{(P-c-d-z)}{1-\beta}, \frac{(P-c-d-z)}{1-\beta}, \frac{(P-c-d-z)}{1-\beta}],\ V_B^* = [0, 0, 0, 0] \tag{72}$$

Moreover, the optimal policies of retailer A and B will be $\pi_A^* = [\frac{P-c-d-z}{P-c-d}, \frac{P-c-d-z}{P-c-d}, \frac{P-c-d-z}{P-c-d}, \frac{P-c-d-z}{P-c-d}]$ *and* $\pi_B^* = [\frac{d+z}{P-c}, \frac{d+z}{P-c}, \frac{d+z}{P-c}, \frac{d+z}{P-c}]$

Proof: Refer to section 7.5.2. □.

The result of Theorem 7.3 are intuitive as consumers' purchasing behavior will be the same in all states. In other words, in this segment whether consumers are privacy alerted or non-alerted about either of the retailers, they will have a weak preference for retailer A. That being said privacy violation by retailers will not effect consumers' purchasing decision in segment $\mathcal{S}_5$.

$V_A(S), V_B(S)$	Targeting	Not Targeting
Targeting	$P-c-d-z+\beta V_A(S), -z$	$P-c-d-z+\beta V_A(S), 0$
Not Targeting	$\beta V_A(S), P-c-d-z$	$P-c+\beta V_A(S), 0$

Table 4: Bimatrix game for infinite horizon game in segment $\mathcal{S}_5$ at state S. Note that the bimatrix game at states S^B, S^A, and S^{AB} will be completely similar.

7.3.2 Segments Fully Affected by Privacy Constraints

In this section, we study the equilibrium of nonzero-sum stochastic games at segments $\mathcal{S}_2, \mathcal{S}_4$, and $\mathcal{S}_6$, where both optimal policies and discounted rewards of retailers are affected by privacy parameters. It is shown that in segments $\mathcal{S}_2$, and $\mathcal{S}_4$, retailer B receives zero discounted reward, however, in segment $\mathcal{S}_6$, retailer B has nonzero reward. In other words, in a privacy sensitive market, consumers who initially had a weak preference on the popular (here retailer A) will be driven away to the rival retailer (here retailer B), if they notice that their privacy is violated by the popular retailer.

1. **Coupon Targeting Competition in Segment** $\mathcal{S}_2$: Segment $\mathcal{S}_2$ is the first segment, where privacy awareness effects popular retailer's profit. In this segment, if consumers are privacy alerted just about retailer A, i.e. if they are at group S^A, they have weak preference on retailer A. Otherwise, they have strong preference about retailer A. It is straightforward to check that both retailers are not willing to distribute targeted coupon at groups S, S^B, S^{AB}. However, in group S^A, both retailers have mixed strategy. The following presents the optimal policies and discounted rewards at this segment.

   Theorem 7.4 *The optimal policies of retailer A, and B in segment $\mathcal{S}_2$ are as follows:*

   $$\pi_A^* = [0,\ 0, \frac{P-c-d-z}{P-c-d}, 0]$$
   $$\pi_B^* = [0,\ 0, \frac{(d+Z)+\beta(1-\lambda_A)\Delta}{(P-c)+\beta(1-\lambda_A)(1-\lambda_N)\frac{1-\beta\lambda_A}{1-\beta\lambda_A^2}\Delta}, 0] \tag{73}$$

   Moreover, the discounted rewards of retailer A, and retailer B are as follows:

   $$V_A^*(S) = V_A^*(S^B) = \frac{P-c}{1-\beta} \tag{74}$$
   $$V_A^*(S^A) = \frac{P-c}{1-\beta} - \Delta,\ V_A^*(S^{AB}) = \frac{P-c}{1-\beta} - \beta\lambda_A(1-\lambda_A)\Delta$$
   $$V_B^*(S) = 0,\ V_B^*(S^B) = 0,\ V_B^*(S^A) = 0,\ V_B^*(S^{AB}) = 0, \tag{75}$$

where $\Delta = \frac{(d+z)}{(1-\beta)+\beta\frac{(1-\lambda_N)\lambda_A(1-\beta\lambda_A)}{1-\beta\lambda_A^2}}$.

Proof: proof of this theorem is similar to the proof of Theorem 7.5. $\square$.

If $\lambda_A \neq 1$, it is straightforward to check that the stationary distribution at this segment is unique and all the consumers will eventually be in group S. This is intuitive as in group S, none of the retailers is distributing targeted coupons. Thus, consumers in this group remain in this group. For $\lambda_A \neq 1$, there is a nonzero probability of transiting from other groups to group S. Therefore, group S is the only terminating state in the Markov Chain (MC), while there is nonzero probabilities of transiting from other groups to group S which proves the claim. The interesting result of this claim is that for the case $\beta \to 1$, where the discounted rewards converges to the average reward, the discounted reward of retailer A at all group converges to $\frac{P-c}{1-\beta}$. Consequently, for the case, where $\beta \to 1$, the privacy sensitivity of the market does not influence any of the retailers.

2. **Coupon Targeting Competition in Segment $\mathcal{S}_4$**: In segment $\mathcal{S}_4$, at groups S, S^A, and S^{AB}, retailer B has an offensive strategies and tries to persuade the consumers with a weak preference for retailer A to purchase from him. However, retailer B will not distribute a targeted coupon to consumers in group S^B, where consumers are alerted about this retailer. This is intuitive as consumers in group S^B will purchase from retailer A in all circumstances. Thus, retailer B tries to gain back the trust of consumers in this group by not distributing a targeted coupon to them.

   In order to derive the optimal discounted rewards and stationary policies in this segment, we solve the fixed point equations. Note that the fixed point equations are derived by finding the unique stationary policies which solves the bimatrix games shown in tables 5, 6, 7 ,8.

   In the following theorem, we prove that reward of retailer B in infinite horizon game at all states will be zero. Moreover, retailer A will have an optimal policy of independent of discount factor β.

   Theorem 7.5 *The optimal policy of retailer A in segment $\mathcal{S}_4$ is independent of the discount factor β and is as follows:*

$$\pi_A^* = [\frac{P-c-d-z}{P-c-d},\ 0, \frac{P-c-d-z}{P-c-d}, \frac{P-c-d-z}{P-c-d}] \tag{76}$$

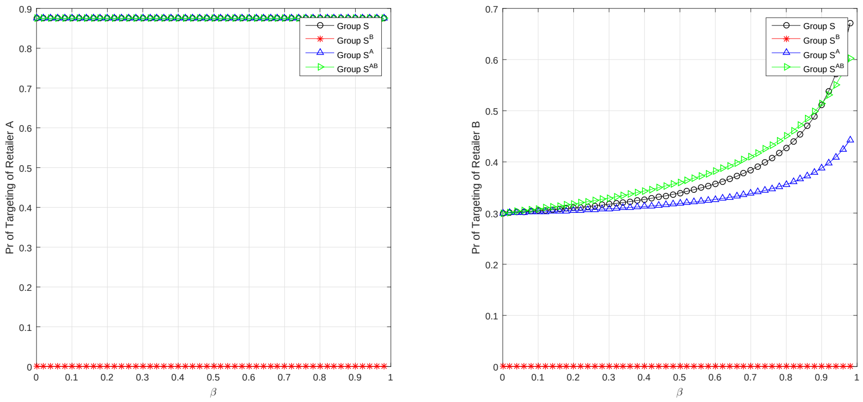


Figure 25: Optimal policies of retailer A and retailer B in segment $\mathcal{S}_4$

Moreover, the discounted rewards of retailer A, and retailer B are given by:

$$V_A^*(S) = \frac{\beta(1-\lambda_N)}{(1-\beta)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(P-c) -$$

$$\frac{(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(P-c-d-z) \tag{77}$$

$$V_A^*(S^B) = \frac{[(1-\beta\lambda_A)(1-\beta\lambda_N)+\beta^2(1-\lambda_N)(\lambda_N-\lambda_A)]}{(1-\beta)(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(P-c) -$$

$$\frac{\beta(1-\lambda_A)(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta)(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(P-c-d-z) \tag{78}$$

$$V_A^*(S^A) = \frac{P-c-d-z}{1-\beta} \tag{79}$$

$$V_A^*(S^{AB}) = \frac{P-c-d-z}{1-\beta}$$

$$V_B^*(S) = 0,\ V_B^*(S^B) = 0,\ V_B^*(S^A) = 0,\ V_B^*(S^{AB}) = 0 \tag{80}$$

Proof: In order to derive the optimal policy of retailer A, and the discounted reward of B, we use backward induction. Next, we derive the optimal discounted reward of retailer A in two steps: First, we prove that the optimal discounted reward at group S^A, and S^{AB} are independent of λ_A and λ_N, and we derive these discounted rewards. Then, we will derive the optimal discounted reward of retailer A by solving the fixed point equations at group S, and S^B. For proof's detail refer to section 7.5.3. □.

As a direct result of Theorem 7.5, the optimal policy of firm B in segment $\mathcal{S}_4$ can be derived, which is presented in section 7.5.4.

3. **Coupon Targeting Competition in segment $\mathcal{S}_6$:** Despite the first five

$V_A^*(S), V_B^*(S)$	Targeting	Not Targeting
Targeting	$P - c - d - z + \beta(\lambda_N^2 V_A^*(S) + \lambda_N(1-\lambda_N)(V_A^*(S^B) + V_A^*(S^A)) + (1-\lambda_N)^2 V_A^*(S^{AB})), -z$	$P-c-d-z+\beta(\lambda_N V_A^*(S) + (1-\lambda_N)V_A^*(S^A)), 0$
Not Targeting	$\beta(\lambda_N V_A^*(S) + (1-\lambda_N)V_A^*(S^B)), P-c-d-z$	$P-c+\beta V_A^*(S), 0$

Table 5: Bimatrix Game of Segment $\mathcal{S}_4$ in Group S.

$V_A^*(S^B), V_B^*(S^B)$	Targeting	Not Targeting
Targeting	$P-c-d-z+\beta(\lambda_N V_A^*(S^B)+(1-\lambda_N)V_A^*(S^{AB})), -z$	$P-c-d-z+\beta(\lambda_N(1-\lambda_A)V_A^*(S)+\lambda_A\lambda_N V_A^*(S^B)+(1-\lambda_A)(1-\lambda_N)V_A^*(S^A)+\lambda_A(1-\lambda_N)V_A^*(S^{AB})), 0$
Not Targeting	$P-c+\beta V_A^*(S^B), -z$	$P-c+\beta(\lambda_A V_A^*(S^B)+(1-\lambda_A)V_A^*(S)), 0$

Table 6: Bimatrix Game of Segment $\mathcal{S}_4$ in Group S^B.

$V_A^*(S^A), V_B^*(S^A)$	Targeting	Not Targeting
Targeting	$P-c-d-z+\beta(\lambda_N V_A^*(S^A)+(1-\lambda_N)V_A^*(S^{AB})), -z$	$P-c-d-z+\beta V_A^*(S^A), 0$
Not Targeting	$\beta((1-\lambda_A)\lambda_N V_A^*(S)+(1-\lambda_A)(1-\lambda_N)V_A^*(S^B)+\lambda_A\lambda_N V_A^*(S^A)+\lambda_A(1-\lambda_N)V_A^*(S^{AB})), P-c-d-z$	$P-c+\beta(\lambda_A V_A^*(S^A)+(1-\lambda_A)V_A^*(S)), 0$

Table 7: Bimatrix Game of Segment $\mathcal{S}_4$ in Group S^A.

$V_A^*(S^{AB}), V_B^*(S^{AB})$	Targeting	Not Targeting
Targeting	$P-c-d-z+\beta V_A^*(S^{AB}), -z$	$P-c-d-z+\beta((1-\lambda_A)V_A^*(S^A)+\lambda_A V_A^*(S^{AB})), 0$
Not Targeting	$\beta((1-\lambda_A)V_A^*(S^B)+\lambda_A V_A^*(S^{AB})), P-c-d-z$	$P-c+\beta((1-\lambda_A)^2 V_A^*(S)+\lambda_A(1-\lambda_A)(V_A^*(S^B)+V_A^*(S^A))+\lambda_A^2 V_A^*(S^{AB})), 0$

Table 8: Bimatrix Game of Segment $\mathcal{S}_4$ in Group S^{AB}.

segments, segment $\mathcal{S}_6$ is the only segment in which retailer B has a nonzero reward at the equilibrium. The primary reason for this is that if consumers in this segment get alerted just about firm A (Group S^A), then they will have a weak preference for firm B. In other words, consumers in Group S^A will purchase from firm A only if they have a targeted coupon from firm A and they do not

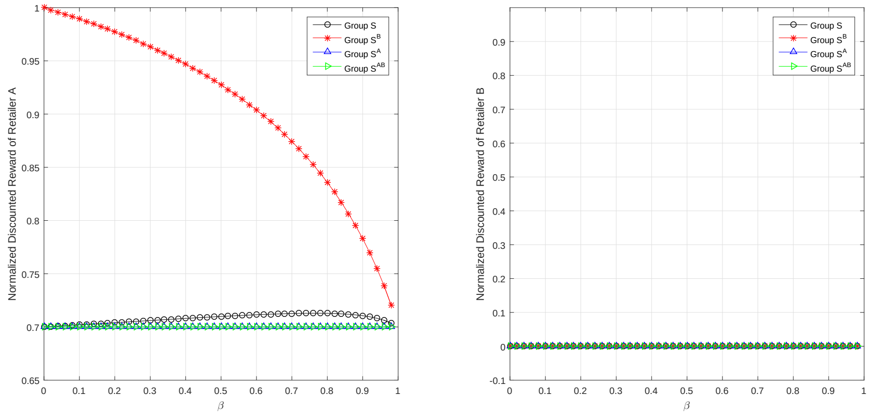


Figure 26: Optimal normalized discounted rewards of retailer A and retailer B in segment $\mathcal{S}_4$

have a targeted coupon from firm B. Consequently, in this segment, retailer A has less defensive strategy and is less likely to distribute a targeted coupon whilst retailer B is more offensive to get a higher share of the market as well as pushing retailer A to distribute targeted coupon.

In order to find the equilibrium of the stochastic game in this segment, we need to solve the fixed point games represented in tables 9, 10, 11, and 12. In the equilibrium point of the game, each retailer is indifferent between sending or not sending a targeted coupon at each state (or group). For example in state S, retailer A is indifferent between sending or not sending a targeted coupon, i.e., its reward when it sends a targeted coupon to consumers in this group should be equal to to his reward if it does not send a targeted coupon to consumers in this group. Consequently,

$$\begin{aligned}&\pi_B^*(S)(P-c-d-z+\beta(\lambda_N^2 V_A^*(S)+\lambda_N(1-\lambda_N)(V_A^*(S^B)+V_A^*(S^A))+\\&(1-\lambda_N)^2 V_A^*(S^{AB})))+(1-\pi_B^*(S))(P-c-d-z+\beta(\lambda_N V_A^*(S)+\\&(1-\lambda_N)V_A^*(S^A)))=\pi_B^*(S)(\beta(\lambda_N V_A^*(S)+(1-\lambda_N)V_A^*(S^B)))\\&+(1-\pi_B^*(S))(P-c+\beta V_A^*(S))\end{aligned} \tag{81}$$

which results in the following:

$$\pi_B^*(S)=\frac{d+z+\beta(1-\lambda_N)(V_A^*(S)-V_A^*(S^A))}{P-c+\beta(1-\lambda_N)^2(V_A^*(S)-V_A^*(S^A)+V_A^*(S^{AB})-V_A^*(S^B))} \tag{82}$$

Similarly, we can find the optimal policies of retailers A and B, which are presented in section 7.5.5.

$V_A^*(S), V_B^*(S)$	Targeting	Not Targeting
Targeting	$P - c - d - z + \beta(\lambda_N^2 V_A^*(S) + \lambda_N(1 - \lambda_N)(V_A^*(S^B) + V_A^*(S^A)) + (1 - \lambda_N)^2 V_A^*(S^{AB})), -z + \beta(\lambda_N^2 V_B^*(S) + \lambda_N(1 - \lambda_N)(V_B^*(S^B) + V_B^*(S^A)) + (1 - \lambda_N)^2 V_B^*(S^{AB}))$	$P - c - d - z + \beta(\lambda_N V_A^*(S) + (1 - \lambda_N)V_A^*(S^A)), \beta(\lambda_N V_B^*(S) + (1 - \lambda_N)V_B^*(S^A))$
Not Targeting	$\beta(\lambda_N V_A^*(S) + (1 - \lambda_N)V_A^*(S^B)), P - c - d - z + \beta(\lambda_N V_B^*(S) + (1 - \lambda_N)V_B^*(S^B))$	$P - c + \beta V_A^*(S), \beta V_B^*(S)$

Table 9: Bimatrix Game of Segment $\mathcal{S}_6$ in Group S

$V_A^*(S^B), V_B^*(S^B)$	Targeting	Not Targeting
Targeting	$P - c - d - z + \beta(\lambda_N V_A^*(S^B) + (1 - \lambda_N)V_A^*(S^{AB})), -z + \beta(\lambda_N V_B^*(S^B) + (1 - \lambda_N)V_B^*(S^{AB}))$	$P - c - d - z + \beta(\lambda_N(1 - \lambda_A)V_A^*(S) + \lambda_A\lambda_N V_A^*(S^B) + (1 - \lambda_A)(1 - \lambda_N)V_A^*(S^A) + \lambda_A(1 - \lambda_N)V_A^*(S^{AB})), \beta(\lambda_N(1 - \lambda_A)V_B^*(S) + \lambda_A\lambda_N V_B^*(S^B) + (1 - \lambda_A)(1 - \lambda_N)V_B^*(S^A) + \lambda_A(1 - \lambda_N)V_B^*(S^{AB}))$
Not Targeting	$\beta V_A^*(S^B), P - c - d - z + \beta V_B^*(S^B)$	$P - c + \beta(\lambda_A V_A^*(S^B) + (1 - \lambda_A)V_A^*(S)), +\beta(\lambda_A V_B^*(S^B) + (1 - \lambda_A)V_B^*(S))$

Table 10: Bimatrix Game of Segment $\mathcal{S}_6$ in Group S^B

$V_A^*(S^A), V_B^*(S^A)$	Targeting	Not Targeting
Targeting	$-z + \beta(\lambda_N V_A^*(S^A) + (1 - \lambda_N)V_A^*(S^{AB})), P - c - d - z + \beta(\lambda_N V_B^*(S^A) + (1 - \lambda_N)V_B^*(S^{AB}))$	$P - c - d - z + \beta V_A^*(S^A), \beta V_B^*(S^A)$
Not Targeting	$\beta((1 - \lambda_A)\lambda_N V_A^*(S) + (1 - \lambda_A)(1 - \lambda_N)V_A^*(S^B) + \lambda_A\lambda_N V_A^*(S^A) + \lambda_A(1 - \lambda_N)V_A^*(S^{AB})), P - c - d - z + \beta((1 - \lambda_A)\lambda_N V_B^*(S) + (1 - \lambda_A)(1 - \lambda_N)V_B^*(S^B) + \lambda_A\lambda_N V_B^*(S^A) + \lambda_A(1 - \lambda_N)V_B^*(S^{AB})$	$\beta(\lambda_A V_A^*(S^A) + (1 - \lambda_A)V_A^*(S)), P - c + \beta(\lambda_A V_B^*(S^A) + (1 - \lambda_A)V_B^*(S))$

Table 11: Bimatrix Game of Segment $\mathcal{S}_6$ in Group S^A.

$V_A^*(S^{AB}), V_B^*(S^{AB})$	Targeting	Not Targeting
Targeting	$P-c-d-z+\beta V_A^*(S^{AB}), -z+\beta V_B^*(S^{AB})$	$P-c-d-z+\beta((1-\lambda_A)V_A^*(S^A)+\lambda_A V_A^*(S^{AB})), \beta((1-\lambda_A)V_B^*(S^A)+\lambda_A V_B^*(S^{AB}))$
Not Targeting	$\beta((1-\lambda_A)V_A^*(S^B)+\lambda_A V_A^*(S^{AB})), P-c-d-z+\beta((1-\lambda_A)V_B^*(S^B)+\lambda_A V_B^*(S^{AB}))$	$P-c+\beta((1-\lambda_A)^2V_A^*(S)+\lambda_A(1-\lambda_A)(V_A^*(S^B)+V_A^*(S^A))+\lambda_A^2V_A^*(S^{AB})), \beta((1-\lambda_A)^2V_B^*(S)+\lambda_A(1-\lambda_A)(V_B^*(S^B)+V_B^*(S^A))+\lambda_A^2V_B^*(S^{AB}))$

Table 12: Bimatrix Game of Segment $\mathcal{S}_6$ in Group S^{AB}.

One may solve for optimal discounted reward and optimal policies by substituting equations (82)-(98) in the bimatrix game at each state and solve the resulting system of degree 2 polynomial equations using Puiseux series or the Grobner basis methods [101]. The alternative choice is using nonlinear programming to solve for the equilibrium of the stochastic game in this segment [99].

In the following Theorem, we prove that the linear approximations of stationary policies in the form of $\pi_A^*(i) \approx f_0^i + \beta f_1^i$ presented in Appendix 7.5.6) achieves an ϵ-equilibrium for the non-zero sum stochastic game in segment $\mathcal{S}_6$.

Theorem 7.6 *The linear approximation of optimal stationary policies of the retailers forms an ϵ-equilibrium for the non-zero sum stochastic game in segment $\mathcal{S}_6$, where $\epsilon \leq$* $\frac{4\beta^2(P-c-d-z)\max\{2\lambda_N(1-\lambda_N)^3,(1-\lambda_N)^3(1-\lambda_A+\lambda_N),\lambda_A^2(1-\lambda_A),2\lambda_A(1-\lambda_A)^3\}}{1-\beta}$

Proof: Refer to section 7.5.7. □.

7.3.3 Segments Partially Affected by Privacy Constraints

In this section, we study the equilibrium of the competition in segment $\mathcal{S}_3$. In this segment, the optimal policies of both retailers are independent of the discount factor β, and the privacy sensitivity parameters λ_A and λ_N. However, the discounted rewards of retailer A are affected by these parameters.

1. **Coupon Targeting Competition in Segment $\mathcal{S}_3$**: In segment $\mathcal{S}_3$, if consumers are in the non-alerted state about retailer B, they have weak preference

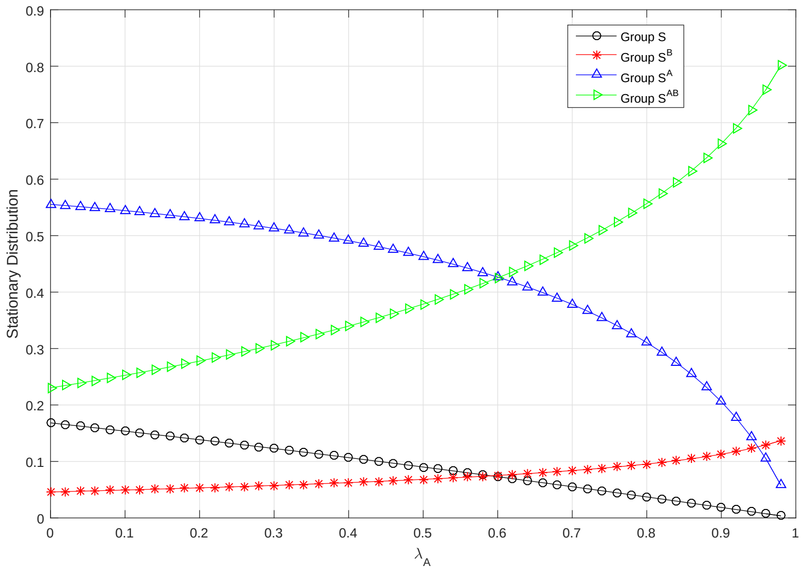


Figure 27: Stationary distribution of stochastic game at $\mathcal{S}_4$ for different λ_A. Note that as λ_A increases which means alerted consumers are less likely to transit to non-alerted state, all consumers end up being at group S^{AB}.

for retailer A. Otherwise, they have strong preference for retailer A. In other words, in this segment, if consumers get alerted about retailer B, they will purchase from retailer A in all circumstances.

Following the result of theorem 7.1, it is known that in a one-step game (one period), retailer B has a reward equal to zero at all the states (groups). Moreover, at the (Nash) equilibrium of a one-step game, none of the retailers are willing to distribute a targeted coupon in states S^B, and S^{AB}. However, retailer A, and B distribute targeted coupons over the consumers at states S, and S^A with probability $\frac{P-c-d-z}{P-c-d}$, and $\frac{d+z}{P-c}$, respectively. In the following theorem, we prove that the above results hold for the infinite horizon stochastic game at segment $\mathcal{S}_3$. We note that the infinite horizon stochastic game can be solved by finding the equilibrium of four bimatrix game for each state. The bimatrix game for state S is represented in table 13 and 14. In these tables, each element includes two parts: 1) instantaneous reward and 2) discounted reward to go. For example, if both retailers distribute targeted coupon over consumers in group S. Retailer A receives an instantaneous reward $P-c-d-z$ and discounted reward to go $\beta \sum_{s \in \mathcal{S}} P(s|S,T,T)V_A(s)$.

$V_A(S)$	Targeting	Not Targeting
Targeting	$(P - c - d - z) + \beta\sum_{s\in\mathcal{S}} P(s\|S,T,T)V_A(s)$	$(P - c - d - z) + \beta\sum_{s\in\mathcal{S}} P(s\|S,T,UT)V_A(s)$
Not Targeting	$\beta\sum_{s\in\mathcal{S}} P(s\|S,UT,T)V_A(s)$	$(P - c) + \beta\sum_{s\in\mathcal{S}} P(s\|S,UT,UT)V_A(s)$

Table 13: Reward of retailer A in the bimatrix game of segment $\mathcal{S}_3$ in state S (group S). The reward includes two parts: 1)an instantaneous reward 2) a reward to go. For example, if both retailers distribute a targeted coupon over consumers in group 1. Retailer A receives an instantaneous reward $P-c-d-z$ and a discounted reward to go $\beta\sum_{s\in\mathcal{S}} P(s|S,T,T)V_A(s)$. Rows, and columns corresponds to actions of retailer A, and retailer B, respectively.

$V_B(S)$	Targeting	Not Targeting
Targeting	$-z + \beta\sum_{s\in\mathcal{S}} P(s\|S,T,T)V_B(s)$	$\beta\sum_{s\in\mathcal{S}} P(s\|S,T,UT)V_B(s)$
Not Targeting	$(P - c - d - z) + \beta\sum_{s\in\mathcal{S}} P(s\|S,UT,T)V_B(s)$	$\beta\sum_{s\in\mathcal{S}} P(s\|S,UT,UT)V_B(s)$

Table 14: Reward of retailer B in the bimatrix game of segment $\mathcal{S}_3$ in state S (group S).

Theorem 7.7 *The optimal policy of each retailer in the infinite horizon game in segment $\mathcal{S}_3$ will be as follows:*

$$\pi_A^* = [\frac{P-c-d-z}{P-c-d},\ 0, \frac{P-c-d-z}{P-c-d},\ 0]$$
$$\pi_B^* = [\frac{d+z}{P-c},\ 0, \frac{d+z}{P-c},\ 0] \tag{83}$$

Moreover, the discounted reward of retailer B, in this case will be zero, ie for $i = 1, \cdots, 4 : V_B^*(i) = 0$

Proof: We prove this theorem by induction, i.e., we prove that if the results hold for the case of a finite horizon with N horizons left, it will also hold for the case where $N+1$ horizons are left. For details of proof refer to section 7.5.8$\square$.

7.4 Numerical Results

In this section, we present our numerical result for segments $\mathcal{S}_4$ and $\mathcal{S}_6$. In our numerical results, we derived optimal policies and discounted rewards by value evaluation and policy iteration method. All the numerical results are derived with parameters: $P = 1, c = 0, d = 0.2, z = 0.1, \lambda_N = 1/3$, and $\lambda_A = 2/3$. In Figure 25, we present the optimal policies of each retailer in segment $\mathcal{S}_4$ as a function of β. Figure 25 shows

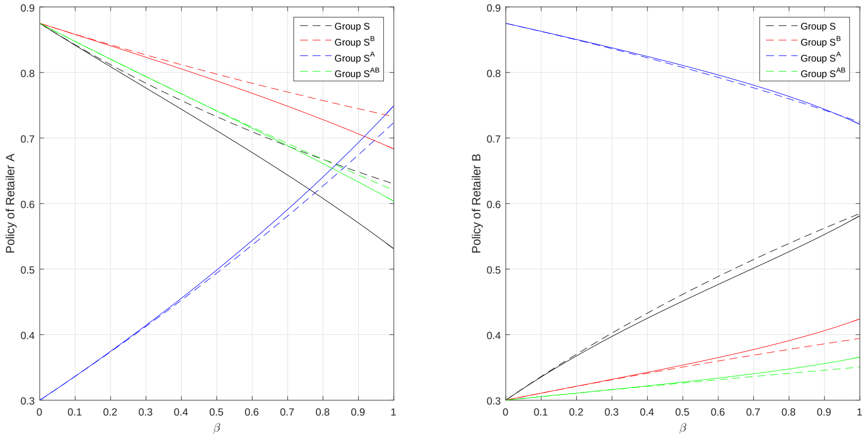


Figure 28: Optimal policies of retailer A and retailer B in segment $\mathcal{S}_6$ are shown by solid lines while the linear approximations are shown by dotted lines.

that the optimal policy of retailer A is independent of β. The optimal discounted rewards of retailer A and retailer B in segment $\mathcal{S}_4$ are shown in figure 26, where it shows that retailer B has reward equal to zero for all values of β. Moreover, we show that $V_A^*(S^B) \geq V_A^*(S) \geq V_A^*(S^A) = V_A^*(S^{AB})$ holds for all the values of β. In figure 27, we present the stationary distribution of consumers on four groups of segment $\mathcal{S}_4$ as a function of λ_A. As $\lambda_A \rightarrow 1$, all consumers go to group S^{AB}. The reason for this is that as λ_A increases, privacy alerted consumers are less likely to transit to a non-alerted state. Therefore, in the Markov Chain of this game at the equilibrium, state S^{AB} is the terminating state, whereas there is a nonzero probability to transit from other groups to S^{AB}. Consequently, at the stationary distribution, all consumers will be at S^{AB}, in other words, S^{AB} is an absorbing state.

In figure 28, we present the optimal policies for both retailers, shown as solid lines. This is derived by policy iteration. The dotted lines represents the linear approximation of policies derived by Taylor expansion around $\beta = 0$. In figure 29, we compare the performance of optimal and suboptimal policies in terms of the discounted rewards of retailers.

In Figure 30, we present the policies of retailers in segment $\mathcal{S}_6$ as function of λ_A. In group S, retailer A becomes more conservative as λ_A increases which is intuitive as it knows that if consumers get alerted about it, retailer A is less likely gain back their trust. In group S^A, as λ_A increases, retailer A's probability of sending a targeted coupon increases. The primary reason for this phenomenon is that retailer B is

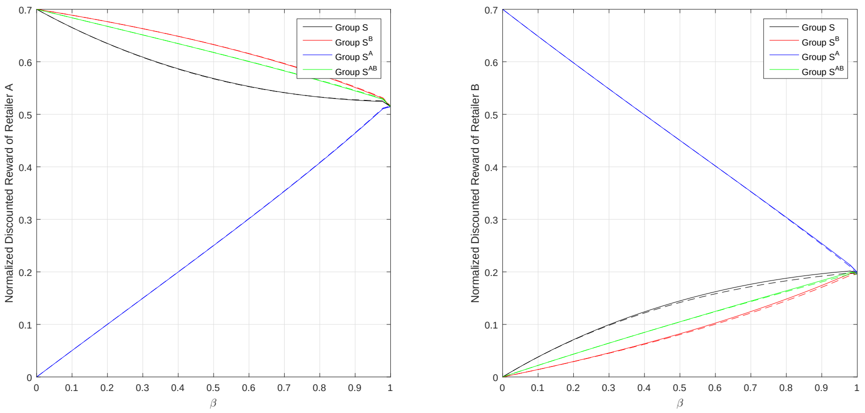


Figure 29: Optimal normalized discounted rewards of retailer A and retailer B in segment $\mathcal{S}_6$ (solid lines) and the suboptimal rewards by linear approximations (dotted lines). As it is seen the difference is negligible.

"pushing" retailer A to send a targeted coupon by being more offensive.

In Figure 33, the discounted reward of retailers are plotted as a function of λ_N. As λ_N increases, i.e., the degree of privacy sensitivity of the market decreases, the reward of firm B decreases which proves the fact that privacy sensitivity of the market is in favor of the rival retailer.

7.5 Proofs

Through proofs of some of the theorems in this section, we can solve the competition for the finite horizon case and then, using these results, we prove the desired results for the infinite case. In this appendix, $V^*_{X,N}(s)$ denotes the optimal discounted reward of player X where N periods are left. $\pi_{X,N}$ denotes the policy of player X where N periods are left (Note that this policy is a function of N and is not necessarily stationary). $V^{\pi_A;\pi_B}_{X,N}(s)$ denotes the discounted reward of player X, when the current state of the game is s, N periods are left, and player A and B have policies π_A and π_B, respectively.

7.5.1 Proof of Lemma 7.2

We prove this fact by induction. Let's first consider the finite horizon problem. Let's consider two states $\alpha = [\alpha_S, \alpha_{S^B}, \alpha_{S^A}, \alpha_{S^{AB}}]$ and $\alpha' = [\alpha'_S, \alpha'_{S^B}, \alpha'_{S^A}, \alpha'_{S^{AB}}]$. We will prove that optimal action probabilities for the retailers in state α are indeed optimal in state α' as well. Let's assume that $(\pi^*_A(\alpha), \pi^*_B(\alpha))$, and $(\pi^*_A(\alpha'), \pi^*_B(\alpha'))$ are the

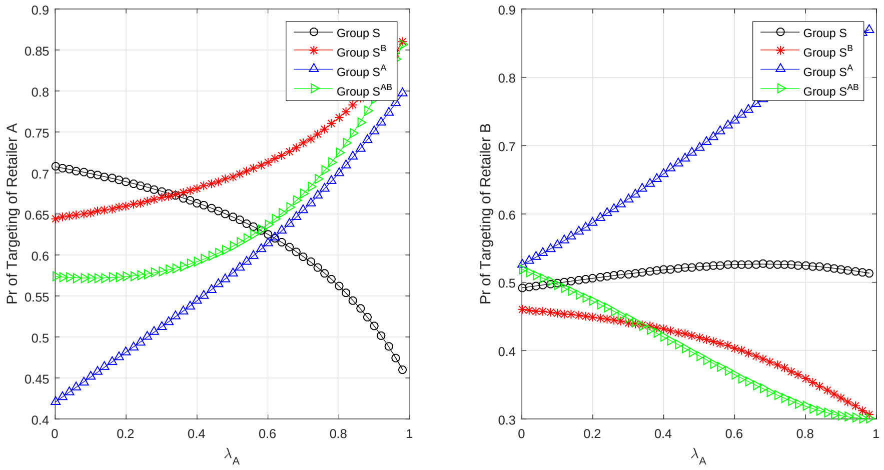


Figure 30: Policy of retailers as a function of λ_A ins segment $\mathcal{S}_6$. Note that $\beta = 0.9$.

optimal pair of action probabilities for α and α', respectively. The terminating reward of each of the players at group j will be as follows:

$$V^*_{A,0}(\alpha) = \sum_{i \in \mathcal{S}} \alpha_i \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*i}_{A,0}(\alpha, a_1)\pi^{*i}_{B,0}(\alpha, a_2) r_A(i, a_1, a_2)$$

$$V^*_{B,0}(\alpha) = \sum_{i \in \mathcal{S}} \alpha_i \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*i}_{A,0}(\alpha, a_1)\pi^{*i}_{B,0}(\alpha, a_2) r_B(i, a_1, a_2)$$

Let's assume player A changes his action probabilities in group S to $\pi^{*S}_A(\alpha')$. As $(\pi^*_A(\alpha), \pi^*_B(\alpha))$ is the optimal action probabilities for state α, the following holds:

$$\begin{aligned} &\sum_{i \in \mathcal{S}} \alpha_i \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \alpha_i \pi^{*i}_{A0}(\alpha, a_1)\pi^{*i}_{B0}(\alpha, a_2) r_A(i, a_1, a_2) \geq \\ &\alpha_1 \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*i}_{A0}(\alpha', a_1)\pi^{*s}_{B0}(\alpha, a_2) r_A(1, a_1, a_2) + \\ &\sum_{i \in \mathcal{S}-\{S\}} \alpha_i \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*i}_{A0}(\alpha, a_1)\pi^{*i}_{B0}(\alpha, a_2) r_A(i, a_1, a_2) \end{aligned}$$

Consequently, we have

$$\begin{aligned} &\alpha_1 \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*S}_{A0}(\alpha, a_1)\pi^{*S}_{B0}(\alpha, a_2) r_A(1, a_1, a_2) \geq \\ &\alpha_1 \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*S}_{A0}(\alpha', a_1)\pi^{*S}_{B0}(\alpha, a_2) r_A(1, a_1, a_2) \end{aligned}$$

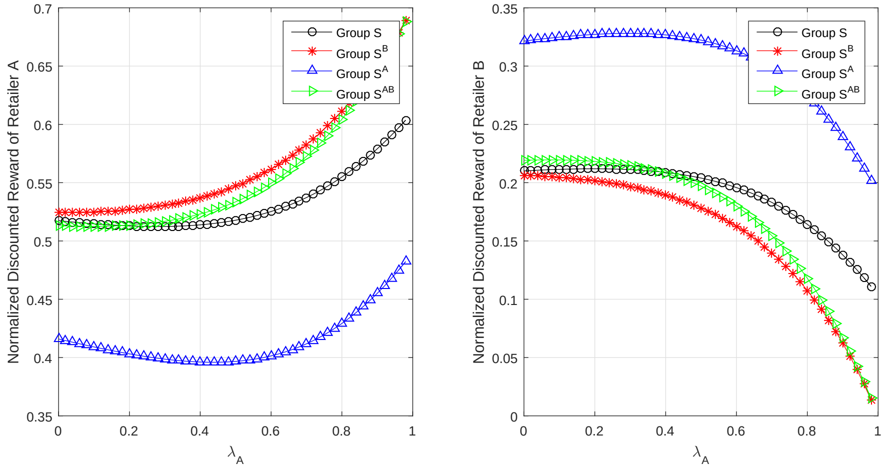


Figure 31: Discounted rewards of retailers as a function of λ_A ins segment $\mathcal{S}_6$. Note that $\beta = 0.9$.

which results in:

$$\begin{aligned} &\alpha'_1 \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*S}_{A0}(\alpha, a_1)\pi^{*S}_{B0}(\alpha, a_2) r_A(1, a_1, a_2) \geq \\ &\alpha'_1 \sum_{a_1 \in \{T,NT\}} \sum_{a_2 \in \{T,NT\}} \pi^{*S}_{A0}(\alpha', a_1)\pi^{*S}_{B0}(\alpha, a_2) r_A(1, a_1, a_2) \end{aligned} \tag{84}$$

By applying the same procedures for other groups and player 2, it is straightforward to show that the following holds:

$$\begin{aligned} V_{A,0}^{(\pi^*_A(\alpha), \pi^*_B(\alpha))}(\alpha') \geq V_{A,0}^{(\pi^*_A(\alpha'), \pi^*_B(\alpha))}(\alpha') \\ V_{B,0}^{(\pi^*_A(\alpha), \pi^*_B(\alpha))}(\alpha') \geq V_{B,0}^{(\pi^*_A(\alpha), \pi^*_B(\alpha'))}(\alpha') \end{aligned}$$

The immediate result of above equations is that $(\pi^*_A(\alpha), \pi^*_B(\alpha))$ derives equilibrium for the state α'. Now, let's consider that for $N-1$, the optimal action probabilities of retailers are independent of α and have the following structures:

$$\begin{aligned} V^*_{A,N-1}(\alpha) = [\alpha_S, \alpha_{S^B}, \alpha_{S^A}, \alpha_{S^{AB}}]^T \begin{pmatrix} f_1(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ f_2(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ f_3(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ f_4(\pi^*_A(\alpha), \pi^*_B(\alpha)) \end{pmatrix} \\ V^*_{B,N-1}(\alpha) = [\alpha_S, \alpha_{S^B}, \alpha_{S^A}, \alpha_{S^{AB}}]^T \begin{pmatrix} g_1(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ g_2(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ g_3(\pi^*_A(\alpha), \pi^*_B(\alpha)) \\ g_4(\pi^*_A(\alpha), \pi^*_B(\alpha)) \end{pmatrix} \end{aligned} \tag{85}$$

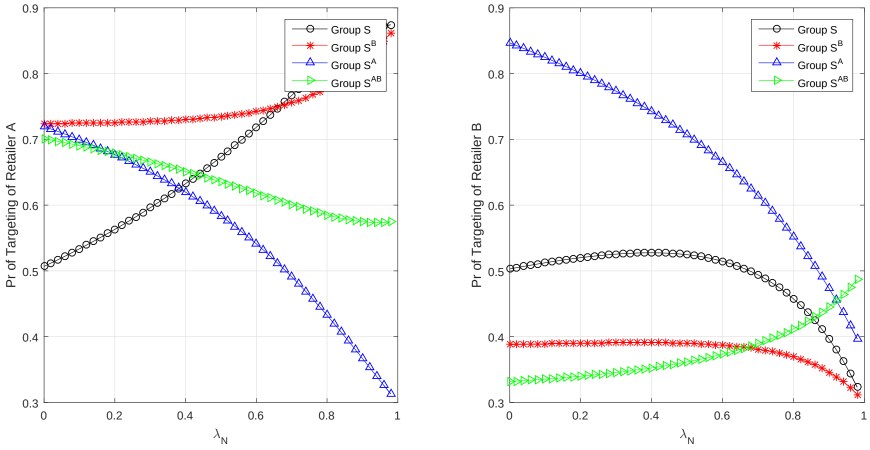


Figure 32: Policy of retailers as a function of λ_N ins segment $\mathcal{S}_6$. Note that $\beta = 0.9$.

Then, by induction, we will prove the same properties holds for the N period problem. The optimal reward of retailer A if N time steps are remaining will be as follows:

$$V^*_{A,N}(\alpha) = \sum_{i\in\mathcal{S}} \alpha_i \sum_{a_1\in\{T,NT\}} \sum_{a_2\in\{T,NT\}} \pi^{*i}_{A0}(\alpha,a_1)\pi^{*i}_{B0}(\alpha,a_2)(r_A(i,a_1,a_2) + \sum_{k=1}^{4}[P_{a_1}\otimes P_{a_2}]_{i,k} f_i(\pi^*_A(\alpha),\pi^*_B(\alpha))),$$

where $[T]_{j,k}$ is the element on the jth row and kth column of matrix T.
Let's assume that player A changes his action probabilities in group one to $\pi^{*1}_{A,N}(\alpha')$ and then, the following will be derived:

$$\alpha'_1 \sum_{a_1\in\{T,NT\}} \sum_{a_2\in\{T,NT\}} \pi^{*S}_{A,N-1}(\alpha,a_1)\pi^{*S}_{B,N-1}(\alpha,a_2)(r_A(i,a_1,a_2) + \sum_{k=1}^{4} [P_{a_1}\otimes P_{a_2}]_{i,k} f_i(\pi^*_A(\alpha),\pi^*_B(\alpha))) \geq \alpha'_1 \sum_{a_1\in\{T,NT\}} \sum_{a_2\in\{T,NT\}} \pi^{*S}_{A,N-1}(\alpha',a_1) \pi^{*S}_{B,N-1}(\alpha,a_2)(r_A(i,a_1,a_2) + \sum_{k=1}^{4}[P_{a_1}\otimes P_{a_2}]_{i,k} f_i(\pi^*_A(\alpha),\pi^*_B(\alpha))),$$

By applying the same procedure for each group and player B, It is straightforward to check that $(\pi^*_{A,N}(\alpha),\pi^*_{B,N}(\alpha))$ is an equilibrium for state α'. $\square$.

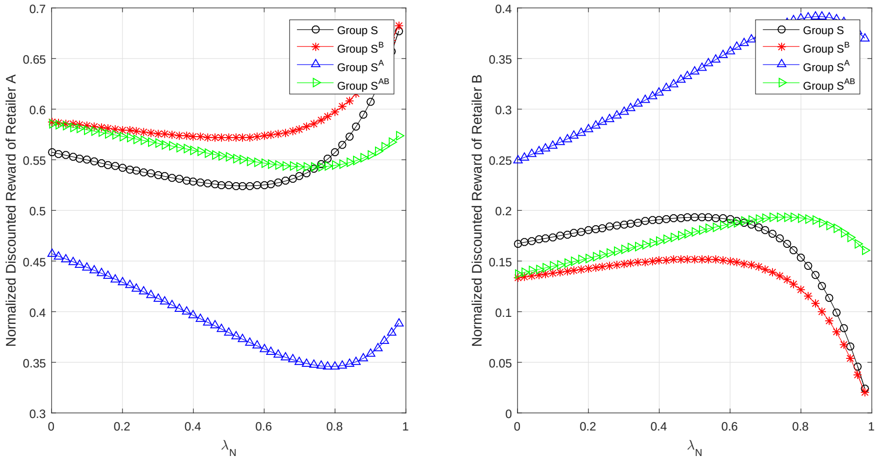


Figure 33: Discounted rewards of retailers as a function of λ_N ins segment $\mathcal{S}_6$. Note that $\beta = 0.9$.

7.5.2 Proof of Theorem 7.3

Let's start with the finite horizon case. We claim that for $N-$period finite horizon game, the reward and policies of retailer A, and B will be as follows:

$$\begin{aligned}
V^*_{A,N} &= [(P-c-d-z)\frac{1-\beta^{N+1}}{1-\beta}), \cdots, (P-c-d-z)\frac{1-\beta^{N+1}}{1-\beta})] \\
V^*_{B,N} &= [0, \cdots, 0] \\
\pi^*_{A,N} &= [\frac{P-c-d-z}{P-c-d}, \cdots, \frac{P-c-d-z}{P-c-d}] \\
\pi^*_{B,N} &= [\frac{d+z}{P-c-d-z}, \cdots, \frac{d+z}{P-c-d-z}]
\end{aligned} \tag{86}$$

It is straightforward to check that above condition holds for the terminating state, where $N = 0$. We will prove that if the above policies are optimal for the case where $N-1$ periods are left, it will also be optimal for $N-$period horizon case. The bimatrix game when N periods are left is the same in all four groups and is shown in table 4. In the equilibrium point, the optimal policy of retailer A is achieved when it is indifferent between sending and not sending a targeted coupon. Consequently,

$$\begin{aligned}
&\pi^*_{B,N}(i)(P-c-d-z+\beta(P-c-d-z)\frac{1-\beta^N}{1-\beta}) + (1-\pi^*_{B,N}(i))(P-c-d-z \\
&+\beta(P-c-d-z)\frac{1-\beta^N}{1-\beta}) = \pi^*_{B,N}(i)(\beta(P-c-d-z)\frac{1-\beta^N}{1-\beta}) + \\
&(1-\pi^*_{B,N}(i))(P-c+\beta(P-c-d-z)\frac{1-\beta^N}{1-\beta})
\end{aligned} \tag{87}$$

$V_B(S)$	Targeting	Not Targeting
Targeting	$-z + \beta \times 0$	$0 + \beta \times 0$
Not Targeting	$P - c - d - z + \beta \times 0$	$0 + \beta \times 0$

Table 15: Bimatrix Game of Segment $\mathcal{S}_4$ in Groups S, S^A, and S^{AB}. (Finite Horizon)

which results in $\pi^*_{B,N} = \frac{d+z}{P-c-d-z}$. Similarly, at the equilibrium point retailer B is indifferent between sending and not sending targeted coupon results in the following equilibrium condition:

$$\pi^*_{A,N}(i)(-z) + (1 - \pi^*_{A,N}(i))(P - c - d - z) = 0 \tag{88}$$

Thus, the optimal policy of retailer B is $\pi^*_{A,N}(i) = \frac{P-c-d-z}{P-c-d}$. By substituting $\pi^*_{A,N}(i)$ and $\pi^*_{B,N}(i)$ in the bimatrix game rewards, the desired result for discounted rewards $V^*_{A,N}$ and $V^*_{B,N}$ is derived. □.

7.5.3 Proof of Theorem 7.5

First, let's derive the optimal policy of retailer A, and optimal discounted reward of retailer B using backward induction. Considering the finite horizon game, at the terminating step, it is straightforward to check that retailer B has zero reward in all states. Moreover, at the terminating step, retailer A does not distribute targeted coupons in state S^B and distributes targeted coupons in the other states with probability $\frac{P-c-d-z}{P-c-d}$. Now, if we assume that these conditions hold for the game when $N-1$ horizons are left, we just need to prove the same conditions hold for the case where N horizons are left. The rewards of retailer B in group S, S^A, and S^{AB} is shown in table 15. Solving the bimatrix game for N horizon problem results in mix policy of retailer A equal to $\frac{P-c-d-z}{P-c-d}$ for states $\{S, S^A, S^{AB}\}$ which is derived by neutrality of retailer B on sending or not sending targeted coupon. The reward of retailer B in group S^B is represented in table 16. In this group, both the retailers are not willing to distribute targeted coupon as they cannot improve their reward by changing their strategies. Thus, in group S^B of segment $\mathcal{S}_4$, none of the retailers distributes targeted coupons. By substituting the derived policies of retailers and the fact that at equilibrium of this game player B will be in different of sending or not sending targeted coupon, we derive that retailer B has zero reward for N horizon stochastic game. As the results holds for all N, it also holds for infinite case, where $N \to \infty$.

Now, let's prove the rest of theorem in two steps:

$V_B^2(S^B)$	Targeting	Not Targeting
Targeting	$-z + \beta \times 0$	$0 + \beta \times 0$
Not Targeting	$-z + \beta \times 0$	$0 + \beta \times 0$

Table 16: Bimatrix Game of Segment $\mathcal{S}_4$ in Group S^B. (Finite Horizon)

1. Optimal discounted reward at group S^A and S^{AB} Let's assume that $V_A^*(S^A)$ and $V_A^*(S^{AB})$ are independent of λ_A and λ_N. Let's consider the fixed point equation for group S^{AB} when $\lambda_N = \lambda_A = 1$. As in the equilibrium point, the reward of retailer A at first row and second row of bimatrix game represented in table 8 are equivalent, the following holds:

$$V_A^*(S^{AB}) = \pi_B^*(S^{AB})(P - c - d - z + \beta V_A^*(S^{AB})) +$$
$$(1 - \pi_B^*(S^{AB}))(P - c - d - z + \beta V_A^*(S^{AB})) \tag{89}$$

which results in $V_A^*(S^{AB}) = \frac{P-c-d-z}{1-\beta}$. Similarly, we can write the fixed point equation for group S^A, and considering the fact that at equilibrium point reward of first row and second row of bimatrix game represented at table 7, the following holds:

$$V_A^*(S^A) = \pi_B^*(S^A)(P - c - d - z + \beta V_A^*(S^A)) +$$
$$(1 - \pi_B^*(S^A))(P - c - d - z + \beta V_A^*(S^A)) \tag{90}$$

which results in $V_A^*(S^A) = \frac{P-c-d-z}{1-\beta}$. Now, we prove our primary assumption that $V_A^*(S^A)$ and $V_A^*(S^{AB})$ are independent of λ_A and λ_N holds and the derived discounted reward for group S^A and S^{AB} satisfy fixed point equation of both groups for any λ_A and λ_N. The following are fixed point equations for group S^A and S^{AB}.

$$V_A^*(S^A) = \pi_B^*(S^A)(P - c - d - z + \beta(\lambda_N V_A^*(S^A) + (1 - \lambda_N)V_A^*(S^{AB}))) +$$
$$(1 - \pi_B^*(S^A))(P - c - d - z + \beta V_A^*(S^A)) \tag{91}$$
$$V_A^*(S^{AB}) = \pi_B^*(S^{AB})(P - c - d - z + \beta V_A^*(S^{AB})) +$$
$$(1 - \pi_B^*(S^{AB}))(P - c - d - z + \beta(\lambda_A V_A^*(S^{AB}) + (1 - \lambda_A)V_A^*(S^A))) \tag{92}$$

It is straightforward to check that the above equations hold if $V_A^*(S^A) = V_A^*(S^{AB}) = \frac{P-c-d-z}{1-\beta}$. Thus, our assumption is verified.

2. Optimal discounted reward at group S and S^B Now, let's consider the fixed point equation at group S^B, where both retailers have pure stationary policies

$\pi^*_A(S^B) = \pi^*_B(S^B) = 0$. Fixed point equation of group S^B result in following:

$$V^*_A(S^B) = P - c + \beta(\lambda_A V^*_A(S^B) + (1 - \lambda_A)V^*_A(S)) \tag{93}$$

Consequently,

$$V^*_A(S^B) = \frac{P - c}{1 - \beta\lambda_A} + \frac{\beta(1 - \lambda_A)}{1 - \beta\lambda_A} V^*_A(S) \tag{94}$$

The fixed point equation of group S is as follows:

$$V^*_A(S) = \pi^*_B(S)(\beta(\lambda_N V^*_A(S) + (1 - \lambda_N)V^*_A(S^B))) + (1 - \pi^*_B(S))(P - c + \beta V^*_A(S)) \tag{95}$$

By rearranging equation (95) and using equation (94), we will have the following equation:

$$\pi^*_B(S) = \frac{(d + z) + [\frac{-\beta(d+z)(1-\lambda_N)-(P-c-d-z)(1-\beta\lambda_A)}{\beta-\beta\lambda_N-1+\beta\lambda_A} + \frac{(1-\beta)(1-\beta\lambda_A)}{\beta-\beta\lambda_N-1+\beta\lambda_A} V^*_A(S)]}{(P - c) + (1 - \beta\lambda_A)\frac{\lambda_N(1-\beta)+\beta(1-\lambda_A)}{\beta(1-\lambda_N)-(1-\beta\lambda_A)} V^*_A(S)} \tag{96}$$

Combining equations (96),(**??**) and $V^*_A(S^A) = V^*_A(S^{AB}) = \frac{P-c-d-z}{1-\beta}$, we have the following:

$$V^*_A(S) = \frac{\beta(1 - \beta)(1 - \lambda_N)}{(1 - \beta)[(1 - \beta\lambda_A)(1 - \beta\lambda_N) - \beta^2(1 - \lambda_N)^2]}(P - c) - \\ \frac{(1 - \beta\lambda_N)[\beta(1 - \lambda_N) - (1 - \beta\lambda_A)]}{(1 - \beta)[(1 - \beta\lambda_A)(1 - \beta\lambda_N) - \beta^2(1 - \lambda_N)^2]}(P - c - d - z)$$

And substituting the above in (94), we have

$$V^*_A(S^B) = \frac{(1 - \beta)[(1 - \beta\lambda_A)(1 - \beta\lambda_N) + \beta^2(1 - \lambda_N)(\lambda_N - \lambda_A)]}{(1 - \beta)(1 - \beta\lambda_A)[(1 - \beta\lambda_A)(1 - \beta\lambda_N) - \beta^2(1 - \lambda_N)^2]}(P - c) - \\ \frac{\beta(1 - \lambda_A)(1 - \beta\lambda_N)[\beta(1 - \lambda_N) - (1 - \beta\lambda_A)]}{(1 - \beta)(1 - \beta\lambda_A)[(1 - \beta\lambda_A)(1 - \beta\lambda_N) - \beta^2(1 - \lambda_N)^2]}(P - c - d - z) \tag{97}$$

□.

7.5.4 Optimal Policies of Firm B in Segment $\mathcal{S}_4$

Corollary 7.7.1 *The optimal policy of retailer B in segment $\mathcal{S}_4$ will be as follows:*

$$\pi_B^*(S) = \frac{(d+z) + \beta^2 \frac{(1-\lambda_N)^2}{[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)}{(P-c) + \beta \frac{(1-\lambda_N)^2(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)}$$

$$\pi_B^*(S^B) = 0$$

$$\pi_B^*(S^A) = \frac{(d+z) + \beta^2 \frac{(1-\lambda_A)(1-\lambda_N)}{[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)}{(P-c) + \beta \frac{(1-\lambda_A)(1-\lambda_N)(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)}$$

$$\pi_B^*(S^{AB}) = \frac{(d+z) + [\beta^2 \frac{(1-\lambda_A)^2(1-\lambda_N)}{[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}}{(P-c) + \beta \frac{(1-\lambda_A)^2(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)} +$$

$$\frac{\beta \frac{(1-\lambda_A)\lambda_A^2(1-\beta\lambda_N))}{[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}](d+z)}{(P-c) + \beta \frac{(1-\lambda_A)^2(1-\beta\lambda_N)[\beta(1-\lambda_N)-(1-\beta\lambda_A)]}{(1-\beta\lambda_A)[(1-\beta\lambda_A)(1-\beta\lambda_N)-\beta^2(1-\lambda_N)^2]}(d+z)}$$

Proof: The results of corollary are direct results of Theorem 7.5. □.

7.5.5 Optimal Policies of Retailers in Segment $\mathcal{S}_6$

$$\pi_A^*(S) = \frac{P-c-d-z+\beta(1-\lambda_N)(V_B^*(S^B)-V_B^*(S))}{P-c-d+\beta(1-\lambda_N)^2(V_B^*(S^B)-V_B^*(S)+V_B^{*3}-V_B^*(S^{AB}))}$$

$$\pi_B^*(S^B) = \frac{d+z+\beta(1-\lambda_N)(1-\lambda_A)(V_A^*(S)-V_A^*(S^A))}{P-c+\beta(1-\lambda_N)(1-\lambda_A)(V_A^*(S)-V_A^*(S^A)+V_A^*(S^{AB})-V_A^*(S^B))}$$

$$+\frac{\beta(1-\lambda_N)\lambda_A(V_A^*(S^B)-V_A^*(S^{AB}))}{P-c+\beta(1-\lambda_N)(1-\lambda_A)(V_A^*(S)-V_A^*(S^A)+V_A^*(S^{AB})-V_A^*(S^B))}$$

$$\pi_A^*(S^B) = \frac{P-c-d-z+\beta(1-\lambda_A)(V_B^*(S)-V_B^*(S^B))}{P-c-d+\beta(1-\lambda_N)(1-\lambda_A)(V_B^*(S^B)-V_B^*(S)+V_B^*(S^A)-V_B^*(S^{AB}))}$$

$$\pi_B^*(S^A) = \frac{P-c-d-z+\beta(1-\lambda_A)(V_A^*(S^A)-V_A^*(S))}{P-c-d+\beta(1-\lambda_N)(1-\lambda_A)(V_A^*(S^A)-V_A^*(S)+V_A^*(S^B)-V_A^*(S^{AB}))}$$

$$\pi_A^*(S^A) = \frac{d+z+\beta(1-\lambda_N)(1-\lambda_A)(V_B^*(S)-V_B^*(S^B))}{P-c+\beta(1-\lambda_N)(1-\lambda_A)(V_B^*(S)-V_B^*(S^B)+V_B^*(S^{AB})-V_A^*(S^A))}$$

$$+\frac{\beta(1-\lambda_N)\lambda_A(V_B^*(S^A)-V_B^*(S^{AB}))}{P-c+\beta(1-\lambda_N)(1-\lambda_A)(V_B^*(S)-V_B^*(S^B)+V_B^*(S^{AB})-V_A^*(S^A))}$$

$$\pi_B^*(S^{AB}) = \frac{d+z+\beta(1-\lambda_A)^2(V_A^*(S)-V_A^*(S^A))}{P-c+\beta(1-\lambda_A)^2(V_A^*(S)-V_A^*(S^A)+V_A^*(S^{AB})-V_A^*(S^B))}$$

$$+\frac{\beta(1-\lambda_A)\lambda_A(V_A^*(S^B)-V_A^*(S^{AB}))}{P-c+\beta(1-\lambda_A)^2(V_A^*(S)-V_A^*(S^A)+V_A^*(S^{AB})-V_A^*(S^B))}$$

$$\pi_A^*(S^{AB}) = \frac{P-c-d-z+\beta(1-\lambda_A)^2(V_B^*(S^B)-V_B^*(S))}{P-c-d+\beta(1-\lambda_A)^2(V_B^*(S^B)-V_B^*(S)+V_B^*(S^A)-V_B^*(S^{AB}))}$$

$$+\frac{\beta\lambda_A(1-\lambda_A)(V_B^*(S^{AB})-V_B^*(S^A))}{P-c-d+\beta(1-\lambda_A)^2(V_B^*(S^B)-V_B^*(S)+V_B^*(S^A)-V_B^*(S^{AB}))}$$

7.5.6 Linear Approximation of Policies in $\mathcal{S}_6$

$$
\begin{aligned}
& f^S = f_0^S + \beta f_0^S = \frac{P-c-d-z}{P-c-d} - \beta \frac{(P-c-d-z)^2(1-\lambda_N)^2}{(P-c-d)^2} \\
& g^S = g_0^S + \beta g_1^S = \frac{d+z}{P-c} + \beta \frac{(P-c-d-z)(1-\lambda_N)(P-c-d-z+\lambda_N(d+z))}{(P-c)^2} \\
& f^{S^B} = f_0^{S^B} + \beta f_1^{S^B} = \frac{P-c-d-z}{P-c-d} - \beta \frac{(P-c-d-z)^2(1-\lambda_N)(1-\lambda_A)}{(P-c-d)^2} \\
& g^{S^B} = g_0^{S^B} + \beta g_1^{S^B} = \frac{d+z}{P-c} + \beta \frac{(P-c-d-z)^2(1-\lambda_N)(1-\lambda_A)}{(P-c)^2} \\
& f^{S^A} = f_0^{S^A} + \beta f_1^{S^A} = \frac{d+z}{P-c} + \\
& \beta \frac{(P-c-d-z)(1-\lambda_N)(\lambda_A(P-c-d-z)+(d+z))}{(P-c)^2} \\
& g^{S^A} = g_0^{S^A} + \beta g_1^{S^A} = \frac{P-c-d-z}{P-c-d} - \\
& \beta \frac{(P-c-d-z)(1-\lambda_A)(z+\lambda_N(P-c-d-z))}{(P-c-d)^2} \\
& f^{S^{AB}} = f_0^{S^{AB}} + \beta f_1^{S^{AB}} = \frac{P-c-d-z}{P-c-d} - \\
& \beta \frac{(P-c-d-z)(1-\lambda_A)(P-c-d-z+z\lambda_A)}{(P-c-d)^2} \\
& g^{S^{AB}} = g_0^{S^{AB}} + \beta g_1^{S^{AB}} = \frac{d+z}{P-c} + \beta \frac{(P-c-d-z)^2(1-\lambda_A)^2}{(P-c)^2}
\end{aligned}
\tag{98}
$$

7.5.7 Proof of Theorem 7.6

Consider the 16-dimensional vector defined as follows:

$$z = (V_A, V_B, \pi_A, \pi_B), \tag{99}$$

where $V_A = (V_A(S), \cdots, V_A(S^{AB}))$, $V_B = (V_B(S), \cdots, V_B(S^{AB}))$, $\pi_A = (\pi_A(S), \cdots, \pi_A(S^{AB}))$, $\pi_B = (\pi_B(S), \cdots, \pi_B(S^{AB}))$. Then, the equilibrium of non-zero sum stochastic game at segment $\mathcal{S}_6$ can be found by solving the following nonlinear programming:

$$\Psi : \min f(z) = \sum_{X \in \{A,B\}} \mathbf{1}^T (V_X - r_X(\pi_A, \pi_B) - \beta P(\pi_A, \pi_B) V_X)$$

subject to:

$$\forall s \in \mathcal{S} : R_A(s) \begin{pmatrix} \pi_B(s) \\ 1-\pi_B(s) \end{pmatrix} + \beta T(s, V_A) \begin{pmatrix} \pi_B(s) \\ 1-\pi_B(s) \end{pmatrix} \leq V_A^s \mathbf{1_2}$$

$$\forall s \in \mathcal{S} : \begin{pmatrix} \pi_A(s) & 1-\pi_A(s) \end{pmatrix} R_B(s) + \beta \begin{pmatrix} \pi_A(s) & 1-\pi_A(s) \end{pmatrix} T(s, V_B) \leq V_B^s \mathbf{1_2^T}$$

where $\forall X \in \{A, B\} : R_X(s) = [r_X(s, a^A, a^B)]_{a^A, a^B}$ and $T(s, V_X)$s are 2×2 matrices such that the elements of each matrix is the same as reward to go of bimatrix games of tables 9 10 11 12. For example, $T(S, V_A)$ will be as follows:

$$T(S, V_A) =$$
$$\begin{pmatrix} (\lambda_N^2 V_A(S) + \lambda_N(1-\lambda_N)(V_A(S^B) + V_A(S^A)) + (1-\lambda_N)^2 V_A(S^{AB})) & (\lambda_N V_A(S) + (1-\lambda_N) V_A(S^A)) \\ (\lambda_N V_A(S) + (1-\lambda_N) V_A(S^B)) & V_A(S) \end{pmatrix}$$

The solution of nonlinear optimization problem Ψ is the equilibrium of the non-zero sum stochastic game of segment $\mathcal{S}_6$ [99]. Moreover, at the optimum solution z^*, $f(z^*) = 0$ and all the inequalities in nonlinear optimization problem Ψ hold with equality.

In order to prove this theorem, we first refer to the follwoing result from [99].

Corollary 7.7.2 *Let $\hat{z}$ be a feasible solution for problem Ψ, then, the $(\hat{\pi_A}, \hat{\pi_B})$ of $\hat{z}$ forms an ϵ-equilibrium with $\epsilon \leq \frac{f(\hat{z})}{1-\beta}$*

By fixing the policies by the linear approximations given in equations (98), the nonlinear optimization problem Ψ will be transformed to the following linear programming:

$$\Phi : \min_{V_A, V_B} \kappa(z) = \sum_{X \in \{A,B\}} \mathbf{1}^T (V_X - r_X(f, g) - \beta P(f, g) V_X)$$

subject to:

$$\forall s \in \mathcal{S} : R_A(s) \begin{pmatrix} g^s \\ 1 - g^s \end{pmatrix} + \beta T(s, V_A) \begin{pmatrix} g^s \\ 1 - g^s \end{pmatrix} \leq V_A^s \mathbf{1_2} \tag{100}$$

$$\forall s \in \mathcal{S} : \begin{pmatrix} f^s) & 1 - f^s \end{pmatrix} R_B(s) + \beta \begin{pmatrix} f^s & 1 - f^s \end{pmatrix} T(s, V_B) \leq V_B^s \mathbf{1_2^T}, \tag{101}$$

where $f = (f^S, \cdots, f^{S^{AB}})$ and $g = (g^S, \cdots, g^{S^{AB}})^T$. This optimization problem has 16 linear constraints such that each pair involves one column or one row of bimatrix game at each state. For example constraint $R_A(S) \begin{pmatrix} g^S \\ 1 - g^S \end{pmatrix}$ $+\beta T(S, V_A)$ $\begin{pmatrix} g^S \\ 1 - g^S \end{pmatrix} \leq V_A(S) \mathbf{1_2}$ includes two constraints corresponding the rows of bimatrix game at state 1. By substituting $R_A(S)$ and $T(S, V_A)$, inequalities simplify to the followings:

$$F_1^S(V_A, V_B, f, g) = (P - c - d - z) + V_A(S)(\beta\lambda_N^2 g^1 + \beta\lambda_N(1 - g^S) - 1)$$
$$+ V_A(S^B)(\beta\lambda_N(1 - \lambda_N) g^1) +$$
$$V_A(S^A)(\beta\lambda_N(1 - \lambda_N) g^S + \beta(1 - \lambda_N(1 - g^S))) + V_A(S^{AB})\beta(1 - \lambda_N)^2 \leq 0$$
$$F_2^S(V_A, V_B, f, g) = (1 - g^S)(P - c) + V_A(S)(\beta\lambda_N g^1 + \beta(1 - g^S) - 1) +$$
$$V_A(S^B)(\beta(1 - \lambda_N) g^S) \leq 0$$

We not that the objective function of Φ can be written in terms of F_i^j as follows:

$$\kappa(z) = -\sum_{i\in\mathcal{S}}(f^i F_1^i + (1-f^i)F_2^i) - \sum_{i\in\mathcal{S}}(g^i G_1^i + (1-g^i)G_2^i) \tag{102}$$

By deriving the dual of linear programming Φ, and considering complementary slackness, one can check that one of the pairs of inequalities F_1^i or F_2^i should hold with equality while the other one will be hold with strict inequality. It can be shown that there exists a threshold β_{10} such that for $\beta < \beta_{10}$, the first inequality of state 1 holds with equality and the second one holds with strict inequality, i.e, $F_1^S = 0$ and $F_2^S < 0$. By multiplying F_1^S with λ_N and subtracting $F_1^S * \lambda_N$ from F_2^S (note that $F_1^S * \lambda_N = 0$), and using the fact that $V_A(S), \cdots, V_A(S^{AB}) < \frac{P-c-d-z}{1-\beta}$, we can bound $F_2^S \times (1-f^S)$ as follows:

$$-F_2^S \times (1-f^S) < 2\beta^2\lambda_N(1-\lambda_N)^3(P-c-d-z) \tag{103}$$

By performing the same procedure for other states and retailer B, and for different amount of β (note that for $\beta \geq \beta_{10}$, the second inequality will hold with equality and first one with strict inequality), one can verify that:

$$\begin{aligned}&\kappa(z) < \frac{4\beta^2(P-c-d-z)}{1-\beta}\\ &\max\{2\lambda_N(1-\lambda_N)^3, (1-\lambda_N)^3(1-\lambda_A+\lambda_N), \lambda_A^2(1-\lambda_A), 2\lambda_A(1-\lambda_A)^3\}\end{aligned}$$

□.

7.5.8 Proof of Theorem 7.7

We prove this theorem by induction on remaining time steps. The solution to the game played in the final period should be identical to the one step described in Section 7.1, expressed as follows:

$$\begin{aligned}\pi^*_{A,0} &= [\frac{P-c-d-z}{P-c-d},\ 0, \frac{P-c-d-z}{P-c-d},\ 0]\\ \pi^*_{B,0} &= [\frac{d+z}{P-c},\ 0, \frac{d+z}{P-c},\ 0]\end{aligned} \tag{104}$$

Moreover, the discounted reward of retailer B is zero in the final period. Now, we prove that if the conditions of the theorem hold for N-1 steps remaining, it should hold of N steps remain as well. At the equilibrium of the game, retailer A will be indifferent between sending or not sending targeted coupon, i.e. the rewards for sending and not sending targeted coupon should be equal. Consequently,

$$\pi^*_{B,N}(S,T)[(P-c-d-z)+\beta\sum_{s\in\mathcal{S}}P(s|S,T,T)V^*_{A,N-1}(s)]+(1-$$
$$\pi^*_{B,N-1}(S,T)[(P-c-d-z)+\beta\sum_{s\in\mathcal{S}}P(s|S,T,UT)V^*_{A,N-1}(s)]=\pi^*_{B,N}(S,T)[$$
$$\beta\sum_{s\in\mathcal{S}}P(s|S,UT,T)V^*_{A,N-1}(s)](1-\pi^*_{B,N-1}(S,T)[(P-c)+\beta$$
$$\sum_{s\in\mathcal{S}}P(s|S,UT,UT)V^*_{A,N-1}(s)]$$

We note that $V^*_{A,N-1}(S)=V^*_{A,N-1}(S^A)$ and $V^*_{A,N-1}(S^B)=V^*_{A,N-1}(S^{AB})$. Similarly, retailer B will be indifferent between sending and not sending targeted coupon which results in the following

$$\pi^*_{A,N}(S,T)(-z)+(1-\pi^*_{A,N}(S,T))[(P-c-d-z)]=$$
$$\pi^*_{A,N}(S,T)(0)+(1-\pi^*_{A,N}(S,T)(0)$$

Solving equations in (105) and (105) derives the optimal policies of both retailers:

$$\pi^*_{B,N}(S,T)=\frac{d+z}{P-c},\quad \text{and,}\,\pi^*_{A,N}(S,T)=\frac{P-c-d-z}{P-c-d} \tag{105}$$

It is straightforward to check that the same policies holds at state S^A, in the equilibrium point. However, in S^B and S^{AB}, the equilibrium results in pure strategy of not distributing coupons. The proof i s completed by verifying that $V_{B,N}(s)=0$ by substituting $\pi^*_{A,N}$ and $\pi^*_{B,N}$ in the corresponding bimatrix game. □.

8 Conclusion and Future Works

In this dissertation, we investigated privacy preserving mechanisms and tradeoffs between privacy and utilities in dynamical systems and networks. We studied three topics of packet source anonymity in mix networks, source-destination anonymity in Tor like networks, and differential privacy in stochastic control and routing.

In the first topic, we considered the problem of optimal routing in mix network. Our approach used extreme traffic conditions to derive key inferences about routing to maximize the delay anonymity tradeoff. Delay is a specific utility criterion that is impacted by mixing strategies for anonymity. One of the main reasons for using delay as a utility criterion is that, in commercial anonymous systems, strategies such as mixing are not considered primarily due to increased delay. The analysis presented in this dissertation is a first step to alleviating that concern and providing a mechanism to include shuffling and batching strategies whilst maintaining latency constraints. Other utilities such as Memory utilization, fairness, congestion are also impacted to a certain extent, and we believe that the formal approach we presented here can be expanded to study those relationships as well.

In the second topic, we presented a relay selection and control framework to thwart an omniscient eavesdropper who uses timing analysis to reveal the source-destination pairs communicating in an anonymous network. The omniscient eavesdropper as modeled in this work is admittedly a conservative assumption and would likely apply to powerful organizations such as nation states. Practical eavesdroppers would likely monitor a fraction of the links. The performance of our algorithms are guaranteed against such an eavesdropper as well but may not be optimal. While the work proposed here focuses on a specific topological structure, our analytical approach can be extended to other topologies as well albeit with higher computational complexity. For instance, in a network with $|\mathcal{M}_E|$ entry guards, $|\mathcal{M}_M|$ intermediate nodes, and $|\mathcal{M}_Q|$ exit guards, the anonymity calculation will require $|\mathcal{M}_E|(|\mathcal{M}_M|+|\mathcal{M}_M|\times(|\mathcal{M}_Q|-1))$ variables and summations.

In the third topic of this dissertation, we studied the problem of control policy design for Markov Decision Processes (MDPs) under differential privacy constraints. The key takeaway from the work is the proposed value iteration methodology that derived optimal inference resistant policies for a pair of MDPs. Our approach is easily extended to more than two hypotheses. The choice of ϵ is a key design aspect which should depend on the perceived length of time the system is likely to be monitored by the adversary. Setting epsilon to zero would guarantee perfect privacy in that the observed state dynamics would be identical for both MDPs, albeit at a significant cost in total rewards obtained. We also studied an application of the proposed framework in routing problems in data collection networks. The key assumption in the problem of routing under differential constraints was knowledge of the set D which is the set of destinations chosen to provide privacy. In a broader context, the choice of the set alongside the optimization in this work would provide a comprehensive solution to private routing. An interesting direction moving forward would be to apply this idea in the context of reinforcement learning wherein the agent has to explore and exploit to maximize his reward with the added caveat that an adversary is unable to identify the type of MDP.

In the last topic of this dissertation, we studied the effect of consumers' privacy awareness in retail competition. Specifically, we studied the competition between two retailers who sell the same product with the same price and marginal cost in a privacy sensitive market. We modeled a privacy sensitive market by a Hoteling line where consumers switch between alerted and non-alerted states about each retailer. We derived optimal policies of each retailer at each segment of Hoteling line by solving the fixed point equations of non-zero sum stochastic games at each segment. We demonstrated that despite price sensitive market, in a privacy sensitive market, the popular retailer will be more conservative sending targeted coupons to consumers with weak preference for him, as they may notice privacy violations by this retailer and stop purchasing from him. We proved that privacy sensitivity of the market is in the favor of rival retailer, in other words, as the popular retailer is less defensive, the rival retailer can increase his profit by being more offensive.

We propose investigating targeting coupon for asymmetric prices and coupon values for each retailer. Moreover, one may consider a two steps competition where in the first step of the game, each retailer sets his price an coupon value and in the second step of the game, there is an infinite horizon competition between the retailers. Another interesting work will be the one where each retailer can change their prices and coupon value. However, such a competition will be more complicated as it will constantly change the market segmentation.

References

[1] N. West, *The SIGINT Secrets: The Signal Intelligence War: 1900 to Today*. New York: William Morrow, 1988.

[2] U. S. Navy, "Military Study Communication Intelligence Research Activities," Tech. Rep. SRH-151, RG 457, June 1937.

[3] A. Back, U. Moller, and A. Stiglic, "Traffic analysis attacks and trade-offs in anonymity providing systems," in *Proceedings of 4th International Information Hiding Workshop*, Pittsburg, PA, April 2001.

[4] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues and open problems," in *Designing Privacy Enhancing Technologies: Proceedings of International Workshop on Design Issues in Anonymity and Unobservability*, ser. LNCS, H. Federrath, Ed., vol. 2009. Springer-Verlag, 2001, pp. 10–29. [Online]. Available: citeseer.ist.psu.edu/454354.html

[5] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[6] C. Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 338–340.

[7] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, vol. 22, no. 2, pp. 254–268, 2011.

[8] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981.

[9] "The TOR Project: Anonymity Online," Feb, `http://www.torproject.org`.

[10] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2770–2784, June 2008.

[11] P. Venkitasubramaniam and V. Anantharam, "On the anonymity of chaum mixes," in *2008 Proc. International Symposium on Information Theory*, Toronto, Canada, July 2008.

[12] W. Wang, M. Motani, and V. Srinivasan, “Dependent link padding algorithms for low latency anonymity systems,” in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 323–332.

[13] S. Yu, G. Zhao, W. Dou, and S. James, “Predicted packet padding for anonymous web browsing against traffic analysis attacks,” *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 4, pp. 1381–1393, 2012.

[14] J. Feigenbaum, A. Johnson, and P. Syverson, “Preventing active timing attacks in low-latency anonymous communication,” in *Privacy Enhancing Technologies*. Springer, 2010, pp. 166–183.

[15] C. Diaz, S. J. Murdoch, and C. Troncoso, “Impact of network topology on anonymity and overhead in low-latency anonymity networks,” in *Privacy Enhancing Technologies*. Springer, 2010, pp. 184–201.

[16] P. Venkitasubramaniam and V. Anantharam, “Anonymity of Mix Networks under Light Traffic Conditions,” in *Proceedings of the 36th Allerton Conf. on Communications, Control, and Computing*, Monticello, IL, October 2008.

[17] D. P. Bertsekas, D. P. Bertsekas, D. P. Bertsekas, and D. P. Bertsekas, *Dynamic programming and optimal control*. Athena Scientific Belmont, MA, 1995, vol. 1, no. 2.

[18] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. MIT press Cambridge, 1998, vol. 1, no. 1.

[19] M. Liberatore and B. N. Levine, “Inferring the source of encrypted http connections,” in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 255–263.

[20] D. X. Song, D. Wagner, and X. Tian, “Timing analysis of keystrokes and timing attacks on ssh.” in *USENIX Security Symposium*, vol. 2001, 2001.

[21] J.-F. Raymond, “Traffic analysis: Protocols, attacks, design issues, and open problems,” in *Designing Privacy Enhancing Technologies*. Springer, 2001, pp. 10–29.

[22] A. Bortz and D. Boneh, “Exposing private information by timing web applications,” in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 621–628.

[23] C. Huang, L. Sankar, and A. D. Sarwate, “Designing incentive schemes for privacy-sensitive users,” *arXiv preprint arXiv:1508.01818*, 2015.

[24] G. Shaffer and Z. J. Zhang, “Competitive coupon targeting,” *Marketing Science*, vol. 14, no. 4, pp. 395–416, 1995.

[25] C. Díaz, S. Seys, J. Claessens, and B. Preneel, “Towards measuring anonymity,” in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, R. Dingledine and P. Syverson, Eds. Springer-Verlag, LNCS 2482, April 2002.

[26] A. Serjantov and G. Danezis, “Towards an information theoretic metric for anonymity,” in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, R. Dingledine and P. Syverson, Eds. Springer-Verlag, LNCS 2482, April 2002.

[27] B.Radosavljevic and B. Hajek, “Hiding traffic flow in communication networks,” in *Military Communications Conference*, 1992.

[28] S. Jiang, N. H. Vaidya, and W. Zhao, “Routing in packet radio networks to prevent traffic analysis,” in *IEEE Workshop on Information Assurance and Security*, West Point, NY, June 2000, pp. 96–102.

[29] B. Zhu, Z. Wan, M. S. Kankanhalli, F. Bao, and R. H. Deng, “Anonymous secure routing in mobile ad-hoc networks,” in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 2004, pp. 102–108.

[30] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, “Sdar: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks,” in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 2004, pp. 618–624.

[31] S. Seys and B. Preneel, “Arm: Anonymous routing protocol for mobile ad hoc networks,” *International Journal of Wireless and Mobile Computing*, vol. 3, no. 3, pp. 145–155, 2009.

[32] G. Danezis, “The traffic analysis of continuous-time mixes,” in *Privacy Enhancing Technologies*. Springer, 2005, pp. 35–50.

[33] P. Venkitasubramaniam and V. Anantharam, “On the anonymity of chaum mixes,” in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*. IEEE, 2008, pp. 534–538.

[34] C. Diaz and B. Preneel, "Reasoning about the anonymity provided by pool mixes that generate dummy traffic," in *Information Hiding*. Springer, 2005, pp. 309–325.

[35] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2770–2784, 2008.

[36] S. Kadloor, X. Gong, N. Kiyavash, and P. Venkitasubramaniam, "Designing router scheduling policies: A privacy perspective," *Signal Processing, IEEE Transactions on*, vol. 60, no. 4, pp. 2001–2012, 2012.

[37] S. Kadloor and N. Kiyavash, "Delay optimal policies offer very little privacy," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2454–2462.

[38] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users get routed: Traffic correlation on tor by realistic adversaries," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 337–348.

[39] T. Wang, K. Bauer, C. Forero, and I. Goldberg, "Congestion-aware path selection for tor," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 98–113.

[40] F. Chen and J. Pasquale, "Toward improving path selection in tor," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[41] M. Edman and P. Syverson, "As-awareness in tor path selection," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 380–389.

[42] M. Akhoondi, C. Yu, and H. V. Madhyastha, "Lastor: A low-latency as-aware tor client," in *Security and Privacy (SP), 2012 IEEE Symposium on*. IEEE, 2012, pp. 476–490.

[43] O. Javidbakht and P. Venkitasubramaniam, "Rate allocation for multihop routing in anonymous networking," in *Information Sciences and Systems (CISS), 2014 48th Annual Conference on*. IEEE, 2014, pp. 1–6.

[44] S. Bohacek, J. P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing security via stochastic routing," in *Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference on.* IEEE, 2002, pp. 58–62.

[45] E. W. Dijkstra, "A note on two problems in connexion with graphs," *Numerische mathematik*, vol. 1, no. 1, pp. 269–271, 1959.

[46] D. S. Reeves and H. F. Salama, "A distributed algorithm for delay-constrained unicast routing," *IEEE/ACM Transactions on Networking (TON)*, vol. 8, no. 2, pp. 239–250, 2000.

[47] G. Xue, "Minimum-cost qos multicast and unicast routing in communication networks," *Communications, IEEE Transactions on*, vol. 51, no. 5, pp. 817–824, 2003.

[48] P. M. Merlin and A. Segall, "A failsafe distributed routing protocol," *Communications, IEEE Transactions on*, vol. 27, no. 9, pp. 1280–1287, 1979.

[49] J. M. Jaffe and F. H. Moss, "A responsive distributed routing algorithm for computer networks," *Communications, IEEE Transactions on*, vol. 30, no. 7, pp. 1758–1762, 1982.

[50] M. R. Garey and D. S. Johnson, "Computers and intractability: a guide to the theory of np-completeness. 1979," *San Francisco, LA: Freeman*, 1979.

[51] L. Kou, G. Markowsky, and L. Berman, "A fast algorithm for steiner trees," *Acta informatica*, vol. 15, no. 2, pp. 141–145, 1981.

[52] B. M. Waxman, "Routing of multipoint connections," *Selected Areas in Communications, IEEE Journal on*, vol. 6, no. 9, pp. 1617–1622, 1988.

[53] J.-M. Ho, G. Vijayan, and C.-K. Wong, "New algorithms for the rectilinear steiner tree problem," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 9, no. 2, pp. 185–193, 1990.

[54] X. Lin and L. M. Ni, "Multicast communication in multicomputer networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 4, no. 10, pp. 1105–1117, 1993.

[55] V. P. Kompella, J. C. Pasquale, and G. C. Polyzos, "Multicasting for multimedia applications," in *INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE.* IEEE, 1992, pp. 2078–2085.

[56] P. Venkitasubramaniam, "Privacy in stochastic control: A markov decision process perspective," in *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on.* IEEE, 2013, pp. 381–388.

[57] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on.* IEEE, 2011, pp. 220–225.

[58] E. V. Belmega, L. Sankar, and H. V. Poor, "Repeated games for privacy-aware distributed state estimation in interconnected networks," in *Network Games, Control and Optimization (NetGCooP), 2012 6th International Conference on.* IEEE, 2012, pp. 64–68.

[59] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[60] S. Han and G. J. Pappas, "Privacy in control and dynamical systems," *Annual Review of Control, Robotics, and Autonomous Systems*, no. 0, 2018.

[61] F. Koufogiannis and G. J. Pappas, "Differential privacy for dynamical sensitive data," in *Decision and Control (CDC), 2017 IEEE 56th Annual Conference on.* IEEE, 2017, pp. 1118–1125.

[62] M. Hale and M. Egerstedty, "Differentially private cloud-based multi-agent optimization with constraints," in *American Control Conference (ACC), 2015.* IEEE, 2015, pp. 1235–1240.

[63] P. Varakantham, Y. Adulyasak, and P. Jaillet, "Decentralized stochastic planning with anonymity in interactions." in *AAAI*, 2014, pp. 2505–2512.

[64] M. Ahmadi, B. Wu, H. Lin, and U. Topcu, "Privacy verification in pomdps via barrier certificates," *arXiv preprint arXiv:1804.03810*, 2018.

[65] L. Esteban and J. M. Hernández, "Endogenous direct advertising and price competition," *Journal of Economics*, vol. 112, no. 3, pp. 225–251, 2014.

[66] G. Iyer, D. Soberman, and J. M. Villas-Boas, "The targeting of advertising," *Marketing Science*, vol. 24, no. 3, pp. 461–476, 2005.

[67] G. Shaffer and Z. J. Zhang, "Competitive one-to-one promotions," *Management Science*, vol. 48, no. 9, pp. 1143–1160, 2002.

[68] J. L. Moraga-González and E. Petrakis, "Coupon advertising under imperfect price information," *Journal of Economics & Management Strategy*, vol. 8, no. 4, pp. 523–544, 1999.

[69] H. R. Varian, "Economic aspects of personal privacy," *Privacy and Self-regulation in the Information Age*, 1996.

[70] A. Acquisti, "Privacy and security of personal information," in *Economics of Information Security.* Springer, 2004, pp. 179–186.

[71] A. Acquisti, R. Dingledine, and P. Syverson, "On the economics of anonymity," in *International Conference on Financial Cryptography.* Springer, 2003, pp. 84–102.

[72] G. Calzolari and A. Pavan, "On the optimality of privacy in sequential contracting," *Journal of Economic theory*, vol. 130, no. 1, pp. 168–204, 2006.

[73] A. Acquisti and H. R. Varian, "Conditioning prices on purchase history," *Marketing Science*, vol. 24, no. 3, pp. 367–381, 2005.

[74] P. Venkitasubramaniam, "Optimal Anonymity of Mix Networks under Delay Constraints: An Information Theoretic Perspective," Jan. 2013, http://www.lehigh.edu/∼pav309/VenkTRAnonymityDelay.pdf.

[75] O. Javidbakht and P. Venkitasubramaniam, "Rate Allocation for Multihop Routing in Anonymous Networks," in *Proceedings of the 48th CISS Conf. on Information Sciences and Systems*, Princeton, NJ, March 2014.

[76] ——, "Delay anonymity tradeoff in mix networks: Optimal routing," *IEEE/ACM Transactions on Networking (TON)*, vol. 25, no. 2, pp. 1162–1175, 2017.

[77] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies.* Springer, 2003, pp. 41–53.

[78] A. Serjantov and R. E. Newman, “On the anonymity of timed pool mixes,” in *Security and Privacy in the Age of Uncertainty*. Springer, 2003, pp. 427–434.

[79] P. Venkitasubramaniam and A. Mishra, “Anonymity of memory limited chaum mixes under timing analysis: An information theoretic perspective,” 2015.

[80] J. Ghaderi and R. Srikant, “Towards a theory of anonymous networking,” in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[81] D. J. Kelly, *A taxonomy for and analysis of anonymous communications networks*. ProQuest, 2009.

[82] M. Backes, A. Kate, P. Manoharan, S. Meiser, and E. Mohammadi, “Anoa: A framework for analyzing anonymous communication protocols,” in *Computer Security Foundations Symposium (CSF), 2013 IEEE 26th*. IEEE, 2013, pp. 163–178.

[83] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.

[84] L. Muscariello, M. Mellia, M. Meo, M. Ajmone Marsan, and R. Lo Cigno, “Markov models of internet traffic and a new hierarchical mmpp model,” *Computer Communications*, vol. 28, no. 16, pp. 1835–1851, 2005.

[85] C. Dwork, “Differential privacy: A survey of results,” in *International Conference on Theory and Applications of Models of Computation*. Springer, 2008, pp. 1–19.

[86] S. M. Kay, *Fundamentals of statistical signal processing: Practical algorithm development*. Pearson Education, 2013, vol. 3.

[87] C. D. Meyer, Jr, “The condition of a finite markov chain and perturbation bounds for the limiting probabilities,” *SIAM Journal on Algebraic Discrete Methods*, vol. 1, no. 3, pp. 273–283, 1980.

[88] A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–492, 2016.

[89] T. J. Holmes, “The effects of third-degree price discrimination in oligopoly,” *The American Economic Review*, vol. 79, no. 1, pp. 244–250, 1989.

[90] M. Armstrong and J. Vickers, “Competitive price discrimination,” *rand Journal of economics*, pp. 579–605, 2001.

[91] Q. Liu and K. Serfes, “Quality of information and oligopolistic price discrimination,” *Journal of Economics & Management Strategy*, vol. 13, no. 4, pp. 671–702, 2004.

[92] R. C. Blattberg and J. Deighton, “Interactive marketing: Exploiting the age of addressability,” *Sloan management review*, vol. 33, no. 1, p. 5, 1991.

[93] D. A. Pitta, “Jump on the bandwagon–itâĂŹs the last one: new developments in online promotion,” *Journal of Consumer Marketing*, vol. 27, no. 2, 2010.

[94] C. Narasimhan, “A price discrimination theory of coupons,” *Marketing Science*, vol. 3, no. 2, pp. 128–147, 1984.

[95] H. Bester and E. Petrakis, “Coupons and oligopolistic price discrimination,” *International Journal of Industrial Organization*, vol. 14, no. 2, pp. 227–242, 1996.

[96] K. Hill, “How target figured out a teen girl was pregnant before her father did,” *Forbes, February*, vol. 16, 2012.

[97] C. Diaz, S. Seys, J. Claessens, and B. Preneel, “Towards measuring anonymity,” in *International Workshop on Privacy Enhancing Technologies.* Springer, 2002, pp. 54–68.

[98] R. Renner, “Security of quantum key distribution,” *International Journal of Quantum Information*, vol. 6, no. 01, pp. 1–127, 2008.

[99] J. Filar and K. Vrieze, *Competitive Markov decision processes.* Springer Science & Business Media, 2012.

[100] T. Başar and G. J. Olsder, *Dynamic noncooperative game theory.* SIAM, 1998.

[101] B. Sturmfels, *Solving systems of polynomial equations.* American Mathematical Soc., 2002, no. 97.

Biography

Omid Javidbakht received the bachelor's degree in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2012. Upon completion of his bachelor studies, Omid joined Lehigh University to pursue his PhD in electrical engineering, under the supervision of Prof. Parv Venkitasubramaniam. His research interests broadly span the areas of stochastic control, information theory, machine learning, and statistical signal processing.

Curriculum Vitae

Omid Javidbakht

Contact Information

- **Email:** omid.javidbakht@gmail.com
- **Cellphone:** (610)217-5493

Education

- **Ph.D.**, Electrical and Computer Engineering, *Lehigh University*, Bethlehem, PA, 2012-2018
  Advisor: Professor Parv Venkitasubramaniam
  Research Interest: Tradeoff between privacy and Quality of Service (QoS) in networks, privacy in data collection, Security of cyber physical systems

- **M.Sc.**, Electrical and Computer Engineering, *Lehigh University*, Bethlehem, PA, 2012-2015
  Advisor: Professor Parv Venkitasubramaniam

- **B.Sc.**, Electrical Engineering, *Sharif University of Technology*, Tehran, Iran, 2007-2012

Employment

- Summer Associate, Quantitative Research, *J.P. Morgan Chase & Co.*, New York, NY, June 2017 - September 2017

- Graduate Research Assistant, *Lehigh University*, Bethlehem, PA, September 2012 - July 2018

Awards and Recognition

- **PC Rossin Doctoral Fellow**, Lehigh University, April 2015
- **Esty Fellowship**, Lehigh University, August 2013
- **Dean's Doctoral Assistantship**, Lehigh University, August 2012
- **Ranked 139th** among more than 250,000 participants in the Nationwide University Entrance Exam for BS degree, Tehran, Iran, September 2007

Publications

Journal Publications

1. **O. Javidbakht**, P. Venkitasubramaniam,"Relay Selection and Operation Control for Optimal Delay Anonymity Tradeoff in Anonymous Networks," IEEE Transactions on Control of Network Systems. vol. 5, no. 1, pp. 607-617, March 2018
2. **O. Javidbakht**, P. Venkitasubramaniam,"Delay Anonymity Tradeoff in Mix Networks: Optimal Routing," IEEE/ACM Transactions on Networking (TON). 2017 Apr 1;25(2):1162-75.
3. **O. Javidbakht**, P. Venkitasubramaniam, A.J. Lamadrid, "Coupon Targeting Competition in Privacy Sensitive Markets," working paper (2018).
4. S.A. Hosseini, **O. Javidbakht**, P. Pad, F. Marvasti, "A Review on Synchronous CDMA Systems: Optimum Overloaded codes, Channel Capacity, and Power Control," EURASIP Journal on Wireless Communications and Networking 2011, no. 1 (2011): 1-22.

Refereed Conference Publications

1. **O. Javidbakht**, P. Venkitasubramaniam, "Inference Resistant Policy for Markov Decision Processes," Submitted to GlobalSip 2018.
2. **O. Javidbakht**, P. Venkitasubramaniam, "Differential Privacy in Networked Data Collection," in Proc. of the 50th Conf. on Information Science and Systems(CISS2016), Princeton, NJ, March2016.

3. **O. Javidbakht**, P. Venkitasubramaniam, “Relay Selection for Optimal Delay Anonymity Tradeoff in AnonymousNetworks,” in Proc. of the 34th Anniversary of the Premier International Conference for Military Communications (MILCOM2015), Tampa, FL, October 2015.

4. **O. Javidbakht**, P. Venkitasubramaniam, “Relay Selection in Wireless Networks for Optimal Delay Anonymity Tradeoff,” in Proc. of 16th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC2015), Stockholm, Sweden, June2015.

5. **O. Javidbakht**, P. Venkitasubramaniam, “Rate Allocation for Multihop Routing in Anonymous Networking,” in Proc. of the 48th Conf. on Information Science and Systems(CISS2014),
Princeton, NJ, March2014.

6. M. Abolhassani, **O. Javidbakht**, S. Asaad , H. Behroozi,“ Hybrid Digital-Analog Codes for Sending Correlated Gaussian Sources over an AWGN Channel”, in Proc. 6th International
Symposium on Telecommunications (IST2012), Tehran, Iran, Nov. 2012.

7. **O. Javidbakht**, N. Naderi Alizadeh, S. M. Razavizadeh, “Dynamic Relay Selection and Resource Allocation in Cooperative Networks based on OFDM”, in Proc. European Wireless2011,Vienna, Austria, April 27-29, 2011.

Ph.D. Thesis

1. **O. Javidbakht**, “*Privacy in Dynamical Systems and Networks: Anonymous Routing, and Retail Competition,*” Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA, 2018.

PRESENTATIONS & ABSTRACTS

- INVITED TALK

    1. “Differential Privacy in Networked Data Collection,” in Proc. of the 50th Conf. on Information Science and Systems (CISS2016), Princeton, NJ, March2016.

- SEMINARS & CONFERENCE PRESENTATION

1. “Coupon Targeting Competition in Privacy Sensitive Market,” 2017 Informs Annual Meeting, Houston, TX, October 2017.
2. “Relay Selection for Optimal Delay Anonymity Tradeoff in Anonymous Networks,” International Conference for Military Communications (MILCOM2015), Tampa, FL, October 2015.
3. “Relay Selection in Wireless Networks for Optimal Delay Anonymity Tradeoff,” North America School of Information Theory, San Diego, CA, August 2015.
4. “ Optimizing the Delay Anonymity Tradeoff in Data Networks,” IEEE North Jersey Advanced Communications Symposium, Hoboken, NJ, September 2014.
5. “Rate Allocation for Multihop Routing in Anonymous Networking,” Conference on Information Science and Systems (CISS2014), Princeton, NJ, March 2014.

Professional Service

- Reviewer, *IEEE Signal Processing Letters*, 2017-Present
- Reviewer, *IEEE/ACM Transactions on Networking*, 2017-Present
- Reviewer, *IEEE Transactions on Information Forensics and Security*, 2017-Present
- Reviewer, *IEEE Transactions on Signal Processing*, 2017-Present
- Reviewer, *IEEE Transactions on Communications*, 2016-Present
- Reviewer, *Conference on Decision and Control (CDC)*, 2016-Present
- Reviewer, *International Conference for Military Communications (MILCOM)*, 2015-Present
- Reviewer, *IEEE International Conference on Communications (ICC)*, 2012

Teaching Experience

- Teaching Assistant, Introduction to Reinforcement Learning, Department of Electrical and Computer Engineering, Lehigh University, 2018

- Teaching Assistant, Signals and Systems Lab, Department of Electrical and Computer Engineering, Lehigh University, 2015

- Teaching Assistant, Computer Architecture and Microprocessor, Department of Electrical Engineering, Sharif University of Technology, 2011

- Teaching Assistant, Digital Circuits Design Lab, Department of Electrical Engineering, Sharif University of Technology, 2010

- Teaching Assistant, Analog Circuits Design Lab, Department of Electrical Engineering, Sharif University of Technology, 2010