2015

Tradeoffs between Anonymity and Quality of Services in Data Networking and Signaling Games

Abhishek Mishra
Lehigh University

Tradeoffs between Anonymity and Quality of Services in Data Networking and Signaling Games

By

Abhishek Mishra

A thesis

Presented to the Graduate and Research Committee

of Lehigh University

in Candidacy for the Degree of

Doctor of Philosophy

in

Electrical Engineering

January 2015

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

Date

Prof. Parv Venkitasubramaniam(Thesis Adviser)

Prof. Rick Blum

Prof. Joseph Yukich

Prof. Vladimir Dobric

Acknowledgement

First and foremost, I would like to thank my advisor Prof. Parv Venkitasubramaniam. He taught me the constant effort for striving for the perfection and the foremost requirement of discipline in research and in life.

I also thank Parv to provide me financial help during my Ph.D. research, therefore, without any thought of financial trouble, I was able to conduct my thesis.

I would like to thank five of my friends, named: Rahul Agarwal, Rohit Nagpal, Abhinav Pandey, Anand Srinivas Guruswami, and Raghu Srinivas Vishnubhotla with whom discussions on various topics leads to some very good and interesting contributions in my research.

I would like to thank my office mates, Jiyun Yao, Omid Javid, and Parth Pradhan for presenting some interesting papers in our group meetings that motivated me to look further into that direction.

I would like to thank Professor Joseph Yukich for teaching me two courses Real Ananlysis I and Real Analysis II and for being a member of my thesis committee. I would like to emphasize here that these two courses proved really helpful for me to understand the literature of stochastic optimization and game theory which turn out to be crucial in proving some optimality results in this work.

I would like to thank Professor Vladimir Dobric for teaching me courses named Advanced Probability, Wavelet Theory, and Financial Calculus and for being in my thesis committee. Although, I like all the three courses but my favourite course among them was Financial Calculus for two reasons: it introduced me to completely new and fascinating area of modelling stock prices, and it taught me stochastic integration.

I would like to thank Professor Rick Blum for teaching me Signal Detection and Estimation and for being a member in my thesis committee. I am really thankful for this course to Prof. Blum and especially for the final project in this course which resulted in two conference papers and one journal paper.

Outline

List of Figures

Abstract

Timing analysis has long been used to compromise users' anonymity in networks. Even when data is encrypted, an adversary can track flows from sources to the corresponding destinations by merely using the correlation between the inter-packet timing on incoming and outgoing streams at intermediate routers. Anonymous network systems, where users communicate without revealing their identities, rely on the idea of Chaum mixing to hide 'networking information'. Chaum mixes are routers or proxy servers that randomly reorder the outgoing packets to prevent an eavesdropper from tracking the flow of packets. The effectiveness of such *mixing* strategies is, however, diminished under constraints on network Quality of Services (QoS)s such as memory, bandwidth, and fairness.

In this work, two models for studying anonymity, *packet based anonymity* and *flow based anonymity*, are proposed to address these issues quantitatively and a trade-off between network constraints and achieved anonymity is studied. Packet based anonymity model is proposed to study the short burst traffic arrival models of users such as in web browsing. For packet based anonymity, an information theoretic investigation of mixes under memory constraint and fairness constraint is established. Specifically, for memory constrained mixes, the first single letter characterization of the maximum achievable anonymity for a mix serving two users with equal arrival rates is provided. Further, for two users with unequal arrival rates the anonymity is expressed as a solution to a series of finite recursive equations. In addition, for more than two users and arbitrary arrival rates, a lower bound on the convergence rate of anonymity is derived as buffer size increases and it is shown that under certain arrival configurations the lower bound is tight.

The adverse effects of requirement of *fairness* in data networking on anonymous networking is also studied using the packet based anonymity model and a novel temporal fairness index is proposed to compare the tradeoff between fairness and achieved anonymity of three diverse and popular fairness paradigms: First Come First Serve, Fair Queuing and Proportional Method. It is shown that FCFS and Fair Queuing algorithms have little inherent anonymity. A significant improvement in anonymity is therefore achieved by relaxing the fairness paradigms. The analysis of the relaxed FCFS criterion, in particular, is accomplished by modeling the problem as a Markov Decision Process (MDP). The proportional method of scheduling, while avoided in networks today, is shown to significantly outperform the other fair scheduling algorithms in anonymity, and is proven to be asymptotically optimal as the buffer size of the scheduler is increased.

Flow based anonymity model is proposed to study long streams traffic models of users such as in-media streaming. A detection theoretic measure of anonymity is proposed to study the optimization

of mixing strategies under network constraints for this flow based anonymity model. Specifically, using the **detection time** of the adversary as a metric, the effectiveness of mixing strategies is maximized under constraints on memory and throughput. A general game theoretic model is proposed to study the mixing strategies when an adversary is capable of capturing a fraction of incoming packets. For the proposed multistage game, existence of a Nash equilibrium is proven, and the optimal strategies for the mix and adversary were derived at the equilibrium condition.

It is noted in this work that major literature on anonymity in Internet is focused on achieving anonymity using third parties like mixes or onion routers, while the contributions of users' individual actions such as accessing multiple websites to hide the targeted websites, using multiple proxy servers to hide the traffic routes are overlooked. In this thesis, *signaling game model* is proposed to study specifically these kind of problems. Fundamentally, signaling games consist of two players: senders and receivers and each sender belongs to one of multiple types. The users who seek to achieve anonymity are modeled as the sender of a signaling game and their types are identified by their personal information that they want to hide. The eavesdroppers are modeled as the receiver of the signaling game. Senders transmit their messages to receivers. The transmission of these messages can be seen as inevitable actions that a user have to take in his/her daily life, like the newspapers he/she subscribes on the Internet, online shopping that he/she does, but these messages are susceptible to reveal the user identity such as his/her political affiliation or his/her affluence level. The receiver (eavesdropper) uses these messages to interpret the senders' type and take optimal actions according to his belief of senders' type. Senders choose their messages to increase their reward given that they know the optimal policies of the receivers for choosing the action based on the transmitted message. However, sending the messages that increases senders' reward may reveal their type to receivers thus violating their privacy and can be used by eavesdropper in future to harm the senders. In this work, the payoff of a signalling game is adjusted to incorporate the information revealed to an eavesdropper such that this information leakage is minimized from the users' perspective. The existence of Bayesian-Nash equilibrium is proven in this work for the signaling games even after the incorporation of users' anonymity. It is also proven that the equilibrium point is unique if the desired anonymity is below a certain threshold.

1 Introduction

1.1 Motivation

The word **anonymity** has its root in the Greek word "anonymia" meaning the nameless. Anonymity refers to the state of ones personal identity or personal identification information being unknown. Personal Identification Information refers to any information or set of information that can be used to identify an individual. For example, occupation and residence alone could be sufficient enough to identify an individual without explicitly disclosing his/her name.

Anonymity is a very old concept. Different people may have different motivations for being anonymous. For example many authors and poets have published numerous novels and poems anonymously often for political and legal reasons. Anonymity is also provided to people who were subjects of science experiments while reporting the results of the experiment.

In the dawn of 21^{th} century, the evolution of Internet provided numerous ways to peep into people's personal lives. Surveys show that an average American users spend 13 hours per week using the Internet and everyday people exchange numerous messages through the Internet. Securing this enormous amount of information from eavesdropping and providing anonymity has become an increasingly difficult task and it requires us to carefully look and understand what anonymity on the Internet really means, how it can be guaranteed and what the costs of achieving it are.

According to [1], in any network "anonymity is the state of being not identifiable within a set of subjects, the *anonymity set*. For any observed action, the anonymity set is the set of all possible subjects who may have caused that action. Therefore, a sender may be anonymous only within a set of potential senders, his/her sender anonymity set, which itself may be a subset of all subjects worldwide who may send messages from time to time. The same is true for the recipient, who may be anonymous within a set of potential recipients, which form his/her recipient anonymity set. Both anonymity sets may be disjoint, identical, or they may overlap."

Anonymity on the Internet requires this anonymity set to be as large as possible for each of its user, consequently, hiding the identities of communicating parties and more generally, the paths of data flow in the network topology. Enabling the retrieval of such information is a violation of users' right to privacy, and further, equips malicious adversaries to launch targeted attacks to disrupt network operations.

In this era of big data, there have been numerous incidents where users' privacy and anonymity have been compromised. Some of these events happened owing to the failure of social networking giants such as Facebook, Twitter, and Google Plus to secure the privacy of their users. For instance,

in November 2007, Facebook launched Facebook Beacon which gathers Facebook users' personal information from their activities on some partner websites of Facebook and put this information on the users' news feed on Facebook without their permission. Sean Lane, a Facebook user, had purchased an intended surprise diamond ring from Overstock.com for his wife. Without his knowledge, this purchase was broadcast to hundreds of people in his network on Facebook, including his wife, resulting in a court case that was successfully fought by plaintiff Sean Lane against Facebook.

The search engine giant Google recently announced that Google opens email messages and scans it for keywords – even when the message is from a non-Gmail user and has not agreed to Google's legal terms. It then uses those keywords to target advertisements at the users and their contacts.

Edward Snowden, former employee of the Central Intelligence Agency (CIA) and former contractor for the National Security Agency (NSA), stirred the world by disclosing the NSA PRISM program that allows the US government to collect Internet users' data from companies such as Microsoft, Google, Apple, Yahoo, and others. Since most of the world's Internet traffic passes through United States, the PRISM program allows US government to look into personal life of people of other countries, thus causing substantial geopolitical discord.

A huge number of companies, commonly known as data brokers, have spread like mushrooms across the World Wide Web, and sell people's personal information without their knowledge for profit. These companies mostly use third-party cookies to gather information about users' browsing histories which are downloaded in users' computers when they click some pop-up messages while browsing through the Internet and collect a lot of sensitive information about people. Based on these collected information, the data broker company easily predict peoples' religion, political affiliation, monthly income, sexual orientation and even more sensitive and personal information.

As the awareness for privacy and secrecy is increasing among Internet users, they are using different protection mechanisms to hide their identity and to secure their personal information. For example, to protect themselves against third-party cookies, users disable the option of storing cookies or delete them in regular intervals on the web-browsing applications on their computers. To prevent the Internet Service Providers (ISP)s to look into their transmitted messages, the use of secure Internet protocols like https is rapidly increasing.

Sophisticated users employ anonymous remailers such as Cypherpunk anonymous remailers, Mixmaster anonymous remailers, and nym servers to hide the identities of the recipients of their messages. Generic Interrnet applications such as JuicyCampus, AutoAdmit, 2channel, and other Futaba-based image boards (such as 4chan) are becoming popular because of their support for users' anonymity.

Anonymous web surfing–browsing the World Wide Web while hiding the user's IP address and any other personally identifiable information from the websites that one is visiting–is rapidly being used by people from all over the world. There are mainly two ways of accomplishing anonymous web browsing. The first is using proxy servers which acts as a wall between the user and the website that he/she is visiting. The second is through network applications such as Tor(The Onion Router), which sends information through a net of routers to hide the destination of information.

The main challenge with proxy servers is that they can be compromised and can be proved a security hazard rather than providing security. For example, if a trojan is installed in a proxy server, then it can communicate sensitive information such as credit card numbers or passwords passing through the proxy servers. Moreover, government and other regulatory authorities can order managers of proxy servers to reveal the identity of their users as was the case with Penet remailer and Church of Scientology [2].

Tor takes a different approach for providing anonymity by employing encryption and random routing of the data packets. Each Internet user who wants to be anonymous using Tor network typically installs Tor software for browsing the Internet. This software first chooses a random path from Tor network's trusted routers and encrypts the transmitting data in layered fashion [3] where each router in the selected Tor network strips the message from its encryption and send the message to the next router. Due to this layered encryptions of packets, the routers in Tor network are known as *onion routers*. Furthermore, each onion router knows only the immediate sender from which it received the message and knows the immediate destination to which it need to send the shuffled packet, therefore, end-to-end anonymity of source destination pairs can still be maintained even if some routers are compromised.

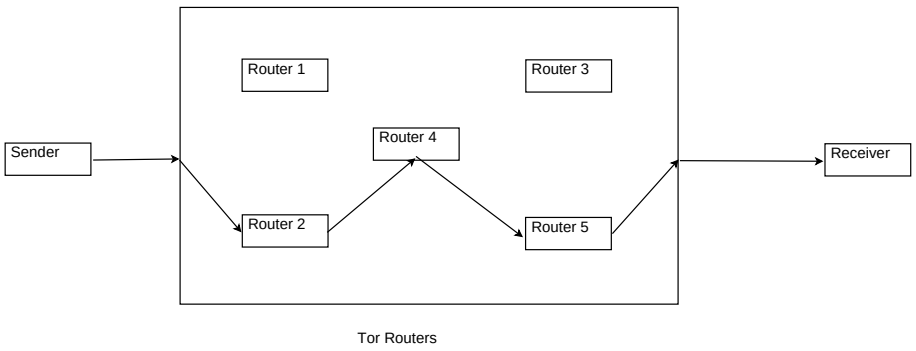


Figure 1: Sender chooses a path consists of router 2, router 4 and router 5 and sends its data through this route to the receiver.

By choosing this random routing of packets, Tor network tries to provide anonymity to its users.

An eavesdropper who controls links of the Internet but not any link in Tor network, can be fooled into thinking that the exit node of the Tor network (Router 5 in Figure 1) is actually the source of packets. However, a pervasive eavesdropper who monitors all the links of the Internet used by Tor network, can see the traffic originated at the sender in Figure 1, then passed through Router 2, Router 4, and Router 5, before it reaches the destination, therefore, no anonymity is provided against this pervasive eavesdropper to the clients of Tor network even by using the random routing. Government agencies, ISPs or search giants like Google control a bulk of internet links and can play the role of a pervasive eavesdropper by collaborating with each other. Even if the routers of the trusted Tor network are physically very far apart and far from control of any single agency thus reduce the possibility of a pervasive adversary, the Tor network is not *provably secure* because **timing correlation** of packets at the entry and exit nodes of Tor network can reveal who is talking to whom as is explained in Figure 2. In fact, a careful read of the disclaimers in the Tor manual reveals an open admittance of the vulnerability to timing analysis. Indeed, as described in [4], the NSA did use the timing correlation between incoming incoming and outgoing flow in entry and exit node of a Tor network to determine sources of data packets.

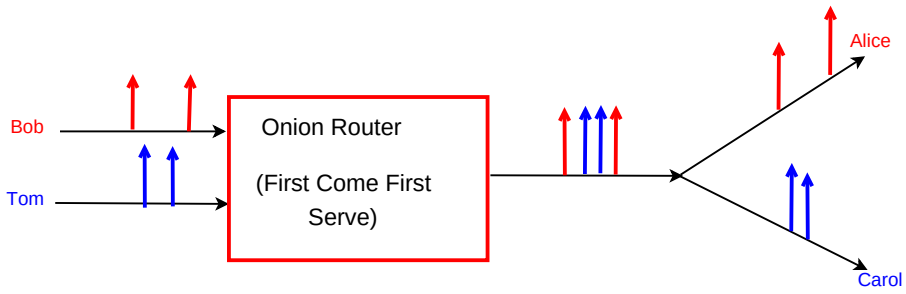


Figure 2: Packets from two sources, Bob and Tom, arrive to a router. Router schedules the packets in First Come First Serve order. An eavesdropper who cannot decrypt the packets, but can see the arrival and departure in each link of the network, is still able to know the destination of these packets because departure order is same as the arrival order because of First Come First Serve Scheduling Policies.

To prevent the information retrieval from timing analysis of communicated message, mix networks were proposed to modify the transmission and relaying *schedules* in a network. Mix network is a web of mixes where each mix is a router/server that receives packets from different sources and employ packet padding and layered encryption (same as Tor networks) to ensure packets in the outgoing streams are "indistinguishable", thus making it infeasible for an eavesdropper to retrieve any information about the communicating parties from the contents and structure of the packets.

Importantly, mixes reduce the correlation between the timing of incoming and outgoing packets by randomly reordering the arrived packets prior to transmission that makes mixes different from Onion routers in Tor network.

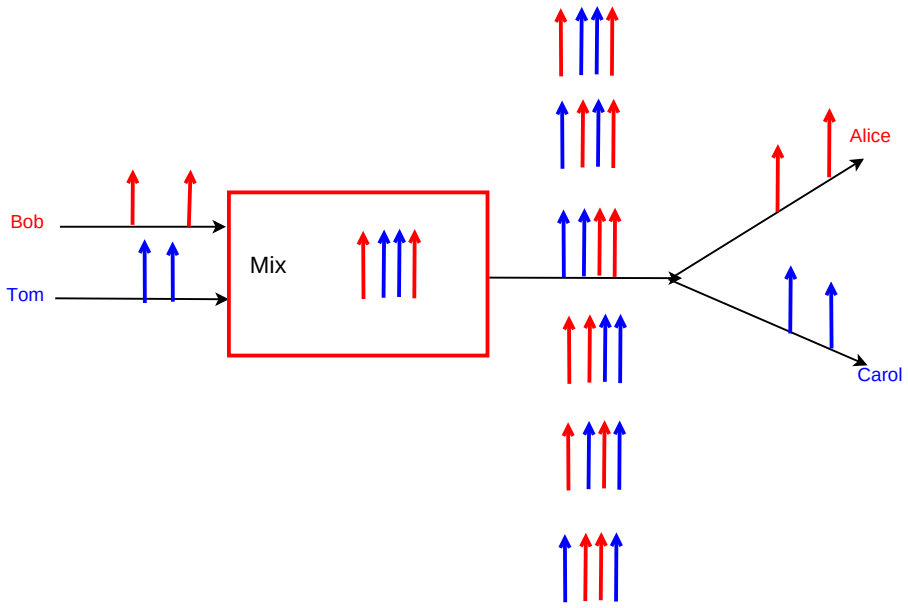


Figure 3: Mix waits until it receives two packets from both the sources: Tom and Bob. Mix chooses one from all the 6 possible combinations of packets and transmits the packets to their respective receivers, Alice and Carol, in the chosen order.

Figure 3 shows that how a mix uses random ordering of packets to destroy the timing correlation of its incoming and outgoing streams of packets. A mix can choose various different ways of ordering packets as compare to the example given in Figure 10, but all the random orderings of packets require that mix has packets from different senders to shuffle or reorder.

At this juncture of my thesis, I would like to draw the attention of the reader to two points that are the basis of this work. The first point is although anonymity is important to network users, they mostly give it lower priority than most of the other network Quality of Service metrics (QoS) such as bandwidth, throughput, delay, and fairness. This fact can be observed from the popularity of Tor network which even when unable to provide complete anonymity to its users but by maintaining low latency in their services draws more attention than the mix networks, although, the mix networks' ability to overcome the timing analysis that leaves Tor network vulnerable. The main reason for the mix networks falling short on traditional QoS criteria lies in their requirement of waiting for packets from different users. It is trivial to see that this requirement can cause unnecessary long delay to its users with high arrival rates when some of its users have disproportionately low arrival rates, thus could violate the delay constraint of the network. Similarly, memory limitation of mixes

can force them to drop packets of its users in case of burst of traffic from some users, consequently, reduces the network throughput. The fairness requirement on the Internet (equal distribution of network resources to users paying equally) can be affected severely from the random ordering of packets by mixes as is shown in Figure 4. To provide higher degree of anonymity that is resilient to timing analysis in the Internet, it is imperative to develop scheduling policies for mix networks that are robust under QoS constraints of data network. It is this analytical study of the anonymity maximizing scheduling policies of mix networks under different Quality of Service (QoS) constraints of networks that this work throws light upon.

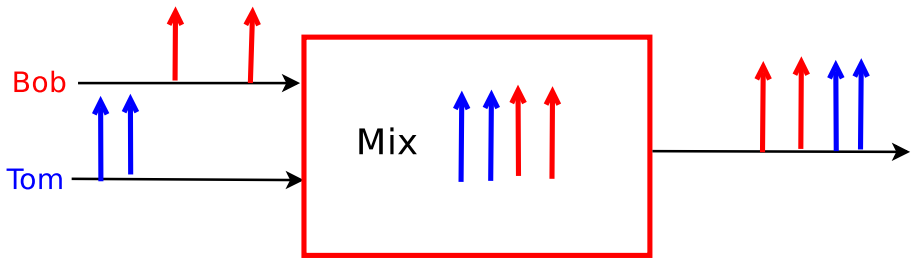


Figure 4: Mix receives first packets from Bob and then receives packets from Tom, but while choosing the random order for serving the packets, it chooses the packets of Tom first, thus creating a unfair situation for Bob.

The second important point that is illustrated in our work and is overlooked in the literature of anonymity on the Internet is in the modeling and study of anonymity maximizing strategies when users, themselves, implement various techniques like accessing websites of varying nature, choosing multiple proxy serves located in different countries etc. to give confusing signals to an eavesdropper who is trying to peep into their private lives. We model these problems with the help of special kind of games, known as signaling games, well studied in literature of game theory but never used to study problem of anonymity.

Broadly speaking, this thesis lays a scientific foundation for anonymity from timing analysis and through the process provides key elements in the design of user and network strategies to provably guarantee any desired degree of anonymity to network users.

1.2 Summary of Contributions

We investigate formally the anonymity achieved using mixes under different traditional QoS constraints namely memory, fairness and throughput. All of these QoS constraints have one thing in common *i.e.* they affect the mixes' ability to randomly shuffle or reorder packets, consequently, reducing the anonymity they can achieve.

The main challenge in quantifying this reduction in anonymity is to provide a mathematical framework under which anonymity of mixes can be studied. We use two different mathematical frameworks for this purpose. One framework that we refer as **packet based anonymity** treats each packet as an individual entity and uses an information theoretic approach to quantify anonymity. We refer to the second framework as **flow based anonymity** where packets are treated as part of a common stream or flow and use a statistical inference driven approach to model the anonymity. The reason behind considering these two models lie in different arrival models of packets. Where packet based anonymity is suitable for short packet burst traffic such as web browsing, the flow based anonymity is apt where long streams of packets are involved in communication such as media streaming.

It is important to note here that the packet and flow based models are useful to study anonymity in data networking when third party hardware such as mixes or onion routers are available for hiding their clients' identity, they are inflexible to study and model the incurred anonymity when users, themselves, transmit confusing signals to obfuscate an eavesdropper about their identity. We propose a **signaling game model** to study specifically these kind of problems.

The other challenges to study anonymity lie in rendering a model for network traffic that is both close to real world and at the same time analytically tractable, in modeling eavesdropper, mixes and their QoS constraints, and in defining metrics to quantify anonymity for packet based model, flow based model, and signaling game model such that these metrics ably represent the uncertainty of the identities of communicating parties without making restricting assumptions on an eavesdropper's observation or computational abilities. For each of the aforementioned frameworks, a metric that best reflects the anonymity achieved therein is proposed, as is explained below.

1.2.1 Packet Based Anonymity

For packet based anonymity, we use the entropy rate of departure process of the mix as a measure of anonymity as proposed in [5–9]. To understand this, consider the example given in figure 5, where the mix receives packet from two sources, Bob and Tom, and transmits them in a random order

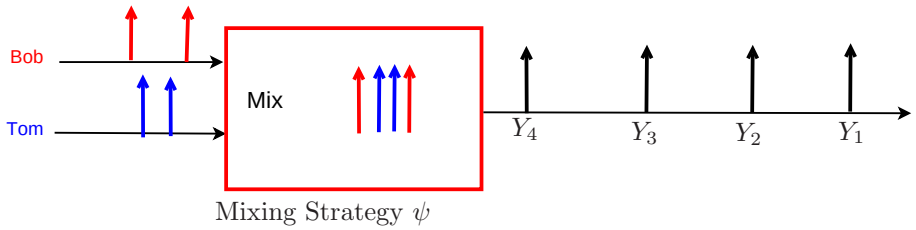


Figure 5: Packet based anonymity model

using the mixing strategy ψ. Because of this random ordering of packets, an Eavesdropper, who monitors all the incoming and outgoing links of the mix, may not know the sources of packets in the outgoing link of the mix but has aposteriori probability distribution over the sources of packets (Bob or Tom) based on his observation from timing of packets in the links and knowledge of mixing strategy ψ. Let Y_i be the random variable that represents the source of the i^{th} packet transmitted by the mix using the eavesdropper's aposteriori probability distribution. For any mixing strategy ψ, the per-packet source anonymity is defined as:

$$\mathcal{A}^{\psi} = \lim_{n\to\infty} \frac{H(Y_1, Y_2, Y_3, ..., Y_n)}{n}, \tag{1}$$

where $H(Y_1, Y_2, Y_3, ..., Y_n)$ represent the Shannon entropy of the joint distribution of $(Y_1, ..., Y_n)$ which is, in fact, the aposterior distribution of packet sources of the n packets based on the eavesdropper's knowledge of the arrival times in links and the mixing strategy ψ.

To model the network traffic for studying the packet based anonymity, we use the Poisson arrival model. Poisson processes have been used to model packet arrivals into network routers [10, 11] primarily since they are statistically a rich class of processes [12], and the analytical tractability allows explicit characterization of required performance metrics and system properties. From the perspective of the Internet, slight variants of Poisson processes such as Markov modeled Poisson [13, 14] or non-stationary Poisson processes [15] have been shown to have broad modeling applicability. Although simple Poisson processes are used as models in this work, the closed form characterizations in this work rely purely on the renewal nature of the arrival process and independence across packet identities. Therefore arrival processes with heavy tail distributions, as is common in Internet traffic, fit into our analysis provided the independence in packet source identities hold. Furthermore, the Markovian framework for analysis proposed in this work could naturally address the more practi-

cal models in [13–15] as well. Whether these general models would result in similar closed form characterization remains an open question, and is beyond the scope of this paper.

We model the eavesdropper as a pervasive eavesdropper who can monitor all the incoming and outgoing links in the network and also knows the mixing strategy. We note that this is a very strict model for eavesdropping, anonymity provided under our model will serve as a lower bound when the eavesdropper could monitor only a limited number of links of the network. For modeling the mixes under QoS constraints, we provide a general approach and allow mixes to do all kind of shuffling of packets within the QoS constraints of the network.

Equipped with this mathematical framework and measure of anonymity, we quantify the trade-off between anonymity and two QoS constraints namely: buffer and fairness. Specifically, when the mixes are memory limited, for the packet based anonymity, one of our important contribution lies in finding the maximum achievable anonymity as a function of the buffer size of a mix and in proving that the achievable anonymity converges to the maximum possible anonymity, as the buffer size approaches to infinity and in characterizing this convergence rate. For some special cases, we also answer the variation of achievable anonymity with number of users and arrival rates. The analysis, in particular, of finding the optimal mixing strategy of a buffer constraint mix relies on reducing the problem into a Markov Decision Process, subsequently, solving the resulting Bellman equations.

Another key contribution of our work is to find the relationship between an important QoS requirement, fairness, and anonymity in data networking that was not explored before, despite the fact that fairness criteria play a significant role in the design of network protocols to limit the threat of congestion collapse–when little or no useful communication is happening due to congestion. The main obstacle in quantifying the anonymity of mixes under fairness constraint lies in the inherent subjectivity of fairness and the consequent vagaries in its definition. In this work, we overcome the problem using the quantitative framework of anonymity and by defining a common fairness index to measure achieved fairness by the popular and well studied fairness paradigms.

Specifically, we quantify and compare the achieved anonymity of three well known fair scheduling policies: First Come First Serve (FCFS), Fair Queuing (FQ), and Proportional Method (PM). FCFS is a popular and intuitively fair scheduling policy that transmits packets in the order of their arrival. Fair queuing, which is the implementable counterpart of Processor Sharing [16, 17] scheme, is the most commonly employed fair scheduling policy owing to its congestion control performance. The proportional method, which schedules packet transmissions so that service rate is proportional to a users backlog, is generally unpopular in network protocols owing to occasional uncontrollable delay, but is considered a fair scheme in broader resource allocations problems [18].

In this thesis, we compare these fair scheduling policies by characterizing their anonymity and using a common scale to measure their temporal fairness. The main result that comes from this study of anonymity of fair scheduling policies is that the Proportional Method, although unpopular in scheduling, secures the best tradeoff between temporal fairness and anonymity. Moreover, the achieved anonymity by the PM is demonstrably close to the maximum achievable anonymity (without any fairness requirement) and is in fact, provably optimal asymptotically as the buffer size is increased. Through our analytical approach, we also prove that the FCFS and Fair Queuing policies have little or zero inherent anonymity. We consequently relax the fairness restrictions of these scheduling policies and find that a significant improvement in anonymity can be achieved by a little relaxation in fairness. The analysis of the relaxed FCFS scheme, in particular, is accomplished by posing the problem as a stochastic control system and solving the resulting dynamic program.

1.2.2 Flow based anonymity

In contrast to the packet based anonymity described thus far, the flow based anonymity requires that an entire stream of packets that have a common identity, be protected from adversarial inference. For flow based anonymity, we model the adversary as an optimal detector, and use the maximum duration of a packet stream *protect-able* (able to hide source-destination pairs of streams) by a mix to quantify the achievable anonymity of the mixing strategies as shown in Figure 6. The main motivation for choosing this metric to quantify the anonymity lies in the result of [19] which shows that any packet preserving mixing strategy would, given a long enough stream of packets, eventually reveal the sources of outgoing packets. It is, therefore, important to characterize the *admissible length* of packet streams, where mixing strategies are effective. While the length of packet stream protectable by mixes does not directly measure the degree of anonymity achieved, this characterization allows us to determine the range of applications and operating conditions under which the desired degree of anonymity (as measured by entropy) is achievable in high data rate applications.

Consequent to the result in [19], the anonymity achieved by a mix for long streams is always limited unless *dummy transmissions* – spurious packets that are added to create additional confusion– by the mix are allowed. For flow based anonymity, our main contribution lies in finding the variation of admissible length as the function of buffer capacity and allowable rate of dummy traffic of mixes. While sufficient insertion of dummy packets can sustain perfect anonymity for an indefinite packet stream, the rate of dummy packets required for such unobservability could reduce data throughput below desired QoS levels, therefore, it is imperative to study the maximization of the admissible length when a desired throughput QoS limits the allowed rate of dummy transmission. Further, this

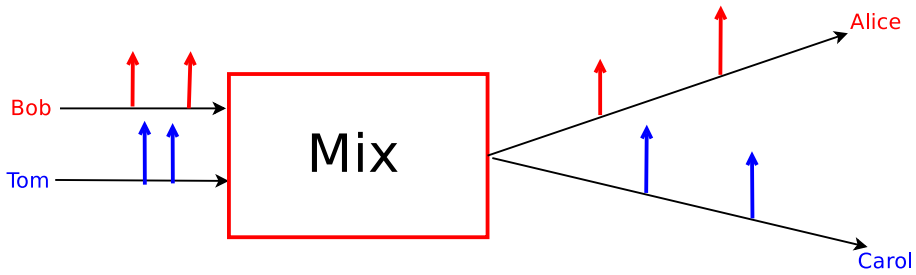


Figure 6: Mix receives packet from two sources Bob and Tom and transmits them to their respective destinations in a random order while maintaining the QoS constraints. Eavesdropper, monitoring each link, wants to know who is talking to whom as soon as possible thus acts as an optimal detector. Mix's goal is to use the scheduling policies that can prevent eavesdropper from knowing the source destination pairs as long as possible.

work also classifies the optimal strategy for transmission of dummy traffic against an active adversary who captures packets from incoming streams of mixes to create its signature that can be used to identify the corresponding outgoing streams using a game theoretic approach. The analysis, in particular, of optimal dummy rate relies on theory of stopping time and of optimal mixing strategies against the active adversary relies on stochastic shortest path algorithms.

1.2.3 Signaling Game Model

Signaling game model incorporates the effect of users' actions while studying the problem of anonymity. Signaling games are an important class of games in the literature of game theory, finding wide spread applications in modelling financial behaviour of a market, economic behaviour in a job market, and evolutionary behaviour in emergence of a language. Fundamentally, signaling games consist of two players: senders and receivers. We model the users who wants to hide their identity as the senders of signaling games and the eavesdropper as the receiver of the signaling games. Each sender belongs to one of multiple types which represent his personal identification information that he/she wants to hide from the eavesdropper. On the Internet, the website a user visits can be identified as his/her type that he/she wants to hide from the eavesdropper. Senders transmit their messages to receivers which, in data network, can be seen as the observations by the eavesdropper of the network traffics of each user. The receiver (eavesdropper) uses these messages to interpret the senders' type and takes optimal actions according to his belief of senders' type such as which advertisements to target to a particular user. Senders choose their messages to increase their reward such that a Internet user can choose the optimal path (delay, throughput, or congestion optimal) for the destination of

his/her messages. However, sending the messages that increases senders' reward can reveal their type to the receiver thus violating their privacy and can be used by eavesdropper in future to harm the senders as is shown in the example given in the Figure 7.

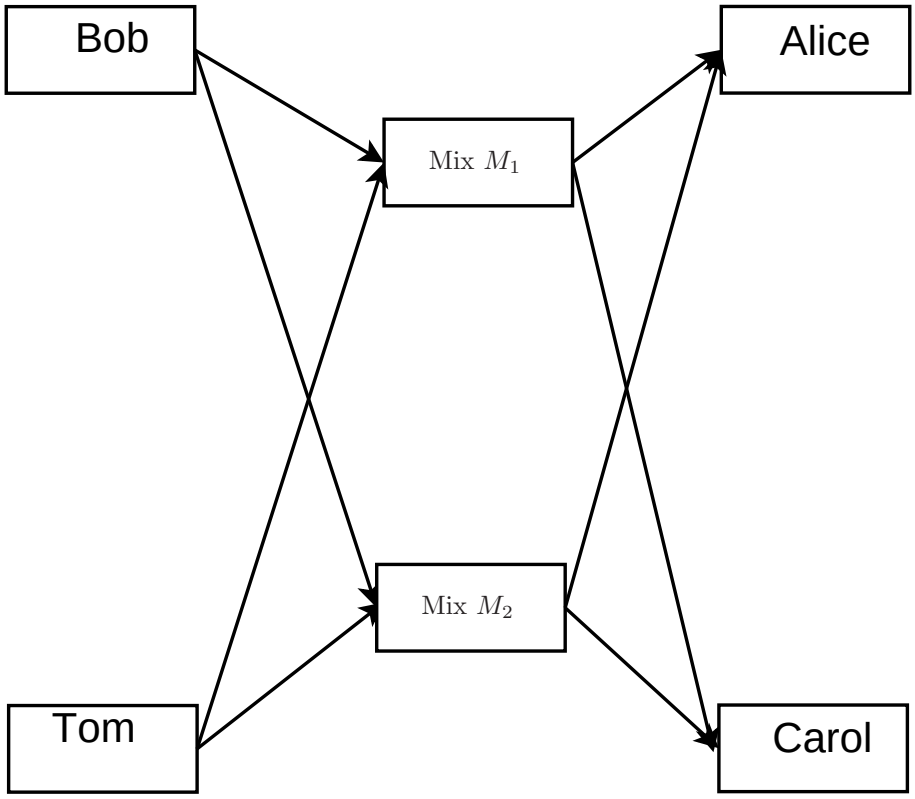


Figure 7: Bob and Tom are sending messages to Alice and Carol. The optimal paths (delay, throughput, or congestion optimal) for Bob and Tom to their destinations are through the mixes M_1 and M_2 respectively, however, if they choose their optimal paths they reveal the destinations of their packets to an eavesdropper who is monitoring the links. Although, by choosing the paths through same mixes (either M_1 or M_2) they can achieve anonymity but one of them have to compromise through suboptimal network conditions like high delay or low throughput.

As it should be clear from the example in Figure 7, the signaling games provide an approach to model a scenario where choosing the best actions jeopardizes our anonymity. In the same manner, it is not difficult to see, in our everyday lives, the actions we take according to our best interest without thinking of anonymity, reveal some information about ourselves thus compromising our privacy. For instance, purchasing receipts reveal our brand preferences, the cars we drive reveal the degree of our affluence and the textbooks we carry reveal our profession. With our online behaviour under constant surveillance, it is imperative that we understand and minimize the leakage of sensitive information through our observed actions.

In this work, we adjust the payoff of a signaling game with the help of Shannon entropic measure of anonymity to incorporate the information revealed to the receivers such that this information

leakage is minimized from the sender's perspective. Further, we prove the existence of Bayesian-Nash equilibrium for the signaling games even after the incorporation of "type anonymity". It is also proven that the equilibrium point is unique if the desired anonymity is below a certain threshold. With the help of an example, we also show that this proposed signaling game model is suitable to formulate the problem of routing in the datagram networking where Quality of service (delay or throughput) along with the source-destination anonymity are competing requirements.

To the best of our knowledge, this thesis provides the first comprehensive analytical framework to study anonymity-QoS tradeoffs in networks without making any assumptions on adversarial ability. Furthermore the signaling game model we study is not only the first mathematical model to incorporate user strategies to increase anonymity, but it's application goes well beyond standard networking applications to include broader commercial and social contexts.

The construction of the paper is as follows: We delineate a brief history of timing analysis and its prevention in the context of network anonymity along with some information theoretic and game theoretic approaches in achieving secrecy and privacy in Chapter 2. In Chapter 3, we study the achievable anonymity of memory constrained mixes and also provide the system model and quantitative definition of anonymity that we used to study packet based anonymity. In Chapter 4, we describe the different fair scheduling methods in data networks, define the common temporal fairness index, and used it to compare the anonymity-fairness tradeoff of the policies for packet based anonymity model. In Chapter 5, using a detection theoretic approach for quantifying anonymity, we analysed the tradeoff between anonymity and memory limitation of mixes and anonymity and allowable rate of dummy transmition. We also analyse the impact of adversaries' power of capturing packets from incoming streams on anonymity and the efficacy of mixes' counter-attack using dummy traffic against these active adversaries using a game-theoretic approach in Chapter 5. Signaling games, their role in modelling problem related to anonymity, and the existence and characteristics of equilibrium points of signaling games for such problems are presented in Chapter 6. Finally, some concluding remarks and pointers to future directions of this work are provided in 7.

2 Related Work

The history of information retrieval through timing analysis can be traced back to middle of twentieth century when in World War II, the US Army Traffic Intelligence group (OP-G-20) on Corregidor island [20] were able to use transmission timing to identify enemy chain of command and to a good extent, predict troop movements. Timing analysis has been a major concern in computer network security owing to the ease of extraction of timing information and the potential for significant disruption. For instance, in [21], Paul Kocher proposed a methodology to weaken keys of RSA, DSS and other asymmetric cryptosystems by measuring the execution time for the overall cryptographic operation. Similarly, in [22], the authors showed that the passwords communicated through the popular two host communication protocol, SSH, are vulnerable to timing analysis.

Timing analysis can also be used to correlate flows in a datagram network, thus compromising users' anonymity which is explained distinctly in [23]. The first major contribution to protect users' anonymity against timing analysis was Chaum Mixes [3] which was mainly intended for anonymously sending and receiving emails. The main idea in [3] was to wait until emails from a certain number of users arrive to the mix, and then transmit them in a batch, however, the waiting for emails caused them unnecessary long delay. Subsequently, there were several other mixing strategies defined to overcome this issues as described in the following section.

2.1 Mixing Strategies

A comprehensive survey of mixing strategies can be found in [24]. Here, we only give a brief introduction to some of the widely known mixing strategies. These mixing strategies were developed, typically, in an ad-hoc way to reduce the delay and increase the anonymity of users.

Threshold mixes: The mixing strategy of Threshold mixes is to wait until n packets arrives to them and then transmit them in a single batch in a random order where n is a natural number representing the threshold over the minimum number of packets required for mixing. It is important to note here that Chaum mixes are actually threshold mixes for which the maximum delay of packets can be unbounded if the arrival rates of some of its users is extremely low.

Timed Mixes: Timed mixes wait until t seconds from the previous round of transmission of packets and transmit all the packets arrived in this t time interval in a random order. Timed mixes certainly bound the maximum delay suffered by users but at the cost of anonymity because there may be some time intervals in which except one particular user, no other users' packets are present in the mix, consequently, anonymity of the user can be compromised.

Threshold pool mixes: Threshold pool mixes always have a certain number of packets in their buffer, lets say f. When they receive n packets, they mix these packets with the f packets already present in their buffer and choose n packets from total $n + f$ packets, transmit them, and keep the remaining f packets in their buffer. Threshold pool mixes can suffer the same problem of unbounded delay as threshold mixes but can provide higher anonymity compare to threshold mixes because of presence of some extra packets to mix.

Timed pool mixes: Similar to threshold pool mixes, timed pool mixes always have f packets in their buffer, but they transmit packets only at every t seconds. If fewer than $f + 1$ packets are present in the mix in a time interval, then no packet would be transmitted. In comparison to timed mixes, timed pool mixes can provide higher anonymity because of the presence of extra packets to mix, however, at the cost of unbounded maximum delay when the traffic from users are low.

Generalized mixes: Generalized mixes use a probability function to represent their mixing strategies that maps the number of packets present in the mix in a round of transmission to the fraction of number of packets transmitted in that round. Generalized mixes are, essentially, a generalization of above defined mixes, consequently, prone to suffer infinite delay or low anonymity.

Stop-and-Go mixes or Continuous mixes: In Stop-and-Go mixes, each packet is randomly delayed where delay is chosen using an exponential distribution embedded within the header in each packet. Stop-and-Go mixes can suffer the problem of both long delay because of unboundedness of exponential distribution, although, with a low probability, or of low anonymity when packets of a single user are transmitted from a link, however, they provide robustness against bending or $(n-1)-$ attacks where an adversary impersonates as the users of mixes to destroy their anonymity [25].

Although these mixing strategies were mostly developed in an ad-hoc way, there have been few approaches towards a systematic study of these mixing strategies which also tried to quantify the anonymity achieved by these strategies. A brief survey of metrics used to quantify the anonymity in these approaches is given in the following section.

2.2 Metrics of Anonymity for mixess

The metrics proposed to quantify anonymity achieved by mixes belong to one of two categories: **Packet based Anonymity** and **Flow based Anonymity** which is similar to the classification proposed in Chapter 1 for studying anonymity of mixes. I would like to remind the reader, where packet based anonymity treats each packet as a separate individual entity and measures the uncertainty in source-destination pair of each packet, the flow based anonymity considers each packet as a

part of a stream and measure the uncertainty in source-destination pairs of each stream. The different types of metrics of anonymity proposed for packet based anonymity and flow based anonymity are briefly described below:

2.2.1 Metrics for packet based anonymity:

- **Counting the mixed messages (CMM):** In [26], the authors mentioned CMM as a measure of anonymity. Assume that at a certain time, a Chaum mix shuffles m messages and transmits them, then the per packet anonymity of each message according to the metric CMM would be m. This measure of anonymity suffers from two drawbacks: 1)All mixed messages can belong to the same source and therefore even after mixing the messages there would be no anonymity for the sources of each message. 2) The CMM metric is vulnerable against injection attack where an eavesdropper can insert its $m-1$ packets in the mix and can distinguish the source and destination of the only other shuffled packet by the mix even though according to the CMM metric the measure of anonymity is high.

- **Cardinality of Anonymity Set (CAS):** For each message, the anonymity set comprises all the sender-receiver pairs that have non-zero probability of being the source and the destination of the message. [26] considered the cardinality of this anonymity set as the measure of packet based anonymity. The anonymity measure, CAS, does not take into account that all the sender-receiver pairs in the anonymity set are not equally likely to be the source-destination pairs of a message, therefore, CAS is not able to give a good measure of anonymity. To understand this, consider a threshold pool mix (also called Cortell mix) as shown in Figure 8.

  It is easy to see that there is always a non-zero probability for any senders whose packet has arrived to the mix to be the sender of a present outgoing packet of the Cortell mix, hence CAS metric of anonymity for the Cortell mix goes towards infinity as number of different senders who are using the Cortell mix increases. While CAS goes toward infinity, it does not capture the fact that senders who has transmitted packet in the past are very less likely to be the source of the present outgoing packet.

- **Entropy of the Anonymity Set (EAS):** To overcome the problem of CAS, [27] proposed EAS as a metric to measure the anonymity. Instead of choosing cardinality of the anonymity set as the metric, EAS computes the probability distribution over the anonymity set that specifies the probability of a particular sender-receiver pair of the anonymity set to be the source-destination pair of the message under consideration. EAS designates the Shannon entropy

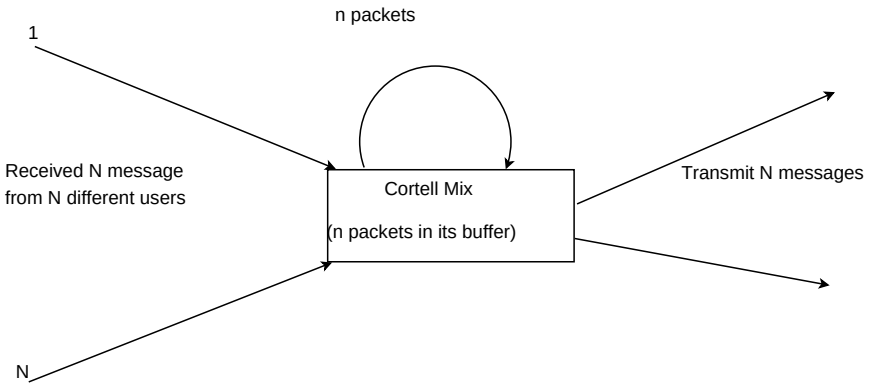


Figure 8: Cortell Mix uses a feedback based policy for mixing the packets of different users. A Cortell mix always has n packets in its buffer. After receiving N packets, it choose n packets from $n+N$ packets to store in its buffer, and transmit the remaining N packets.

of this probability distribution as the measure of anonymity. Note that EAS overcomes the problem of CAS for quantifying the anonymity of Cortell mix by giving low weight to sender-receiver pairs which are less likely to be the source-destination pair of a given message.

However, the EAS metric does not fully incorporate the knowledge of an attacker or eavesdropper. Consider the example given in Figure 9 . Note that each packet in every outgoing link of the mix is equally likely to belong to any of the source S_1, S_2, and S_3. Therefore, EAS metric of anonymity would assign $\log(3)$ anonymity to each packet in the outgoing link of the mix, consequently, per packet anonymity is $\frac{3\log(3)}{3} = \log(3)$. The problem with EAS is that it does not incorporate the fact that knowledge of the source of the packet in the outgoing link D_1 affects the eavesdropper uncertainty over the sources of packets in the outgoing link D_2 and D_3. Specifically, by choosing a marginal probability distribution over the source of packets in each outgoing link, EAS overestimates the anonymity.

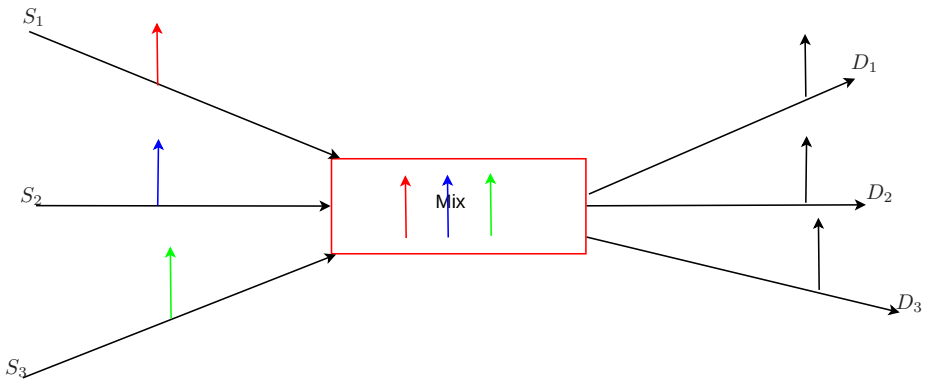


Figure 9: Mix receives packets from three sources S_1, S_2 and S_3, randomly reorders them, and transmits them to their respective destinations.

- **Entropy rate of departure process:** To overcome the problem of EAS and incorporate all the knowledge available to an eavesdropper, [5–9] uses the entropy rate of departure process of the Chaum mix as the measure of anonymity. It is to be noted here that this is the metric that we use in this work to quantify packet based anonymity of mixes as explained in Chapter 1.

  This metric differs from EAS, as the anonymity here is measured using the joint entropy rather than the marginal entropy of each packet source. To understand the difference between the metrics, consider the example in Figure 9 . As is explained earlier, the measured anonymity by EAS is log(3). However, since the 3 packets must necessarily be from 3 different sources, the number of possible orderings of the packets is $3! = 6$. Consequently the mean uncertainty per packet is $\frac{\log(6)}{3} < \log(3)$. Thus, the joint entropy captures the fact that knowledge of one source would automatically limit the possible sources of the other two packets while the marginal entropy fails to capture the dependence. Since conditioning reduces entropy, the anonymity as defined by EAS overestimates the actual entropy.

2.2.2 Metrics for flow based anonymity:

The flow based anonymity is used for mix networks where sources transmit long streams of packets to their respective destinations. A common attack against these mixes is to find the correlation of all the outgoing flow of the mix with the incoming flow of the mix for which the attacker is interested in knowing the destination. The outgoing flow which have highest correlation with the incoming flow is likely to be the destination of the incoming flow. The following metrics were introduced to measure the effectiveness of flow correlation attacks against the mixes.

- **Detection Probability:** [19] proposed the detection probability as the measure of flow based anonymity which is essentially the probability of correctly predicting the source-destination pairs for each flow as a function of the number of packets observed of each flow. The authors showed that the detection probability for all widely used Internet protocols goes towards one if the number of observed packets are sufficiently large.

- **Cross-over error probability:** [28] proposed cross-over error probability to measure the effectiveness of mixing strategies against flow correlation attack for threshold based adversarial strategies where the adversary determines a communication between two links if the correlation coefficient of the traffic between these two links is greater than a threshold and the threshold is computed by equalizing the probability of false positive (declaring a communication when

actually there is no communication) to probability of false negative (declaring no communication when there is actually a communication). Cross-over error probability is, factually, the probability of false positive of the mixing strategy which is, in turn, also equal to probability of false negative because of the strategy of the adversary.

It is important to note here that all of the above metrics show that mixes' ability of anonymizing communicating parties decreases by limiting delay of packets. Several methods especially inclusion of dummy traffic and dropping of packets are introduced to increase the achievable anonymity of mixes with minimizing the delay, albeit, at the cost of other QoS constraints such as bandwidth and throughput, and, importantly, some optimal mixing strategies were proposed especially for constrained latency mix networks as explained in the next section.

2.3 Tradeoff between anonymity and QoS constraints in networks

Increasing the anonymity of mixes using dummy traffic is first proposed in [29, 30], albeit, at the price of network bandwidth. It is shown in [29] that by generating dummy messages (although users may also generate dummies) mixes can increase their anonymity level and at the same time, can prevent end-to-end intersection attacks. It is to be noted here that dummy packets are typically transmitted only to another mix instead of a real recipient.

[31] proposed the Pipenet system which heavily uses dummy traffic and maintains a constant traffic in the links between mixes by padding them with dummy messages whenever the real traffic is not enough to fill them. However, this system provides unobservability along with anonymity where an adversary cannot even detect, whether, there is a communication happening or not, it is impractical because of exceptionally over use of network bandwidth.

To prevent the dummy packets from consuming excessive network bandwidth, several policies were proposed to optimize their use. For Stop-and-Go mixes, it is proposed by Reliable, one of the mixes that composes the Mixmaster network, to generate a certain number of dummies every period of time, selecting their delay (amount of time they are kept in the mix from their generation until the moment in which they are sent) from a random distribution.

[32] proposed two different strategies to incorporate dummy transmission in pool mixes. One technique is to insert the dummies in the pool from which the mix chooses packets for transmission where these dummies are treated as real messages by the mix. The second way is to insert the dummy packets at the output of the mix, where, the mix adds the dummies to the batch of real messages taken from the pool. It is shown in [32] that inserting the dummies in the pool provides

lesser anonymity and lesser delay compare to when dummies are inserted in the output of the mixes.

[28] proposed an adaptive padding strategy to add dummy traffic in flows of mixes that is firstly dividing all the incoming flows into bins corresponding to their arrival rates, subsequently, maintaining a different traffic rate for each bins using dummy packets, thus, reducing the demand of dummy traffic when flow rates of users are disproportionate, but at the same time compromising anonymity by reducing the cardinality of the anonymity set of its users.

[33] presents an adaptive technique for artificially delaying packets from multiple connections at intermediate mixes in order to reduce the amount of dummy traffic. A similar technique without any cover traffic was also proposed in [19].

One common thing with the above approaches to achieve higher anonymity with lower delay is the use dummy packets, which in turn affects the network bandwidth. [34] was the first work to take a direct approach towards analytically finding the optimal mixing strategies for delay constraint mixes and subsequently provide an upper and lower bound on the anonymity of mixes, under a Poisson assumption of arrival process, when the mixes are delay constraint which means they cannot delay packets more than a certain limit but free to transmit packets any time within the delay limit, thus provide bounds on anonymity for a generalized version of timed mixes. The authors extended their work in [35] and characterized the optimal derivative of anonymity under light traffic conditions for mixes with delay restrictions.

While the works in [34, 35] centred towards characterizing the optimal mixing strategies under continuous time model of network traffics, [7] found the optimal scheduling strategy in a discrete arrival time model when the mixes are constrained to delay packets for maximum one time unit using a reformulation of the problem as a Markov Decision Process that is also used in our work while characterizing the optimal strategy of memory constrained mixes.

While the low latency in mix networks is usually the important concern of their users, their achieved anonymity can be severely limited by the memory constraint of mixes as shown in [36]. Further, [36] proposed an asymptotically optimal mixing strategy under buffer constraints and quantified the anonymity of a single destination mix network, however, the optimal mixing strategy and convergence rate of anonymity was not explored.

The main reason for success of [7,34–36] in quantifying the optimal mixing strategies stays in their analytically tractable information theoretic metric of anonymity that are also capable to encompass all the knowledge of eavesdropper along with resource and network constraints. However, the use of information theory in secrecy and privacy related issues is not limited to mix networks, it goes well beyond them as explained in the following section.

2.4 Secrecy and information theory

While cryptography is based on the assumption of limited computing power of an adversary and vulnerable against large scale deployment of quantum computers, the information theoretic secrecy of a system ensures the security of the system even against the infinite computing capability of adversaries.

The era of information theoretic secrecy starts from the work of Shannon in [37] where he proved that providing information theoretic secrecy (no information revealed to eavesdropper about communicated message) in a noiseless wireless environment is possible, only, through a completely secure noiseless channel between sender and receiver with the same rate of secret keys as the rate of message symbols. In this work, the author used Shannon entropy of the actual message transmitted to receiver given that the message received by eavesdropper to quantify the information revealed to eavesdropper which is also used in our work as the measure of anonymity for packet based anonymity model.

The first major breakthrough for providing secrecy for noisy channel in comparison to noiseless channel of Shannon's work is done by Wyner in [38] by introducing wiretap channel and by proving that secure communication is possible when the channel between sender and receiver is better than the channel between sender and eavesdropper. [38] used the same, Shannon equivocation, as the metric to measure information revealed to eavesdropper and importantly, with the help of the metric characterized the tradeoff between maximum information rate possible between sender and receiver at the level of secrecy achieved from the eavesdroppers perspective.

Csiszar and Korner extended the work of [38] in [39] and proved that the secret communication is still possible if the channel between sender and adversary is better than the channel between sender and receiver. Specifically, with the help of Shannon equivocation metric of information revealed to eavesdropper, they characterized the triplet (R_1, R_e, R_0) where R_1 is the maximum information rate from sender to receiver and R_0 is the maximum rate of common information from sender to receiver and eavesdropper for a given rate R_e of the information revealed to eavesdropper about the message intended for receiver.

While [38,39] analysed the tradeoff between maximum information rate possible between sender and receiver for a given rate of information revealed to eavesdropper for discrete memoryless wiretap channel, Leung-Yan-Cheong and Hellman extended the work for Gaussian wiretap channel in [40] and proved that when the channel between sender and receiver is not better than the channel between sender and eavesdropper, then to achieve any non-zero information rate between sender and receiver,

there would be a non-zero rate of information leakage to eavesdropper, in other words, completely secure communication is not possible.

Although, as is proved in [40] that to achieve any information theoretic secrecy, we need to be at the mercy of nature *i.e.* the channel between sender and receiver should be better than the channel between sender and eavesdropper, there have been some recent approaches using time diversity of fading channels [41], using beam forming with the help of multiple antennas (MIMO) [42, 43], and using cooperative jamming in multiple access wiretap channels [44] to better the tradeoff between information rate between sender and receiver at the cost of information revealed to eavesdropper.

It is important to note here that in comparison to the above works where the tradeoff between information leaked to eavesdropper and maximum information rate between sender and receiver is analyzed, our work also characterizes the tradeoff between information leaked to eavesdropper but at the cost of network QoS constraints.

Timing channel where secret messages are encoded in the timing of the message rather than in the content of the message is another field of research for covert transmission where information theory is extensively used to characterized secrecy capacity. The first information theoretic study of timing channel is done in [45] where Anantharam and Verdu proved the secrecy capacity of timing channel for a single serve queue with independent service time. Further advancement in this directions are done by [46] and [47] where [46] developed decoding and encoding schemes for timing channels for exponential and non-exponential servicing time of the queue and [47] developed a theoretical and experimental analysis of timing channels with bounded servicing times of queues.

A noteworthy approach of studying the secrecy capacity of timing channels is provided in [48] where a game is formulated between jammer and encoder such that the goal of the jammer is to alter the packet timing with in the constraint of delay and buffer to minimize the information flow while simultaneously the goal of the encoder is to develop the encoding scheme to maximize the information flow.

It is important to note here that [48] was not the first work to introduced game theory for studying the secrecy related problems, there has been a huge work done on this area on which we shed some light in the next section.

2.5 Game theoretic approaches for network security and privacy

A detailed survey on the use of game theory in network security and privacy related issues can be found in [49] which covers many diverse fields ranging from physical layer security to intrusion

detection (network layer security) to cryptography (application layer security). In this section, we briefly explain some of the important works done in this area.

The game theory is used to model conflicting role between jammers and network manager towards the network performance where the goal of the network manager is to increase the performance while jammers intend to decrease the network performance. This interplay between jammers and networks managers is studied for Gaussian channel in [50], for multiple-input-multiple-output (MIMO) Rayleigh-fading channel in [51], and for multiple access channel (MAC) in [52] using zero-sum game.

Specifically, [50] considered the problem where transmitter sends a sequence of independent Gaussian random variables over a memoryless Gaussian channel with average power constraint on transmitted signal and jammer used the measurement received by tapping the channel to introduce additional bounded noise in the transmitted signal. The payoff of the game is measured as the average square distortion error between the received signal and the actual transmitted signal. The author proved that the best policy of the jammer in equilibrium is either to choose a linear function of the measurement it receives through the tapping or to choose, in addition, an independent Gaussian noise sequence, depending on the region where the tapping parameters lie. The optimal policy of the transmitter is to amplify the input sequence to the given power level by a linear transformation, and that of the receiver is to use a Bayes estimator.

In comparison to [50], [51] considered the mutual information between input to the channel and output of the encoder of the receiver as the measure of effectiveness of the communication between sender and receiver where the channel is modeled as Rayleigh-fading additive White Gaussian noise channel. In this mutual information game, the goal of transmitter-receiver pair is to develop encoding-decoding strategies to maximize the mutual information while the the jammer minimizes the same quantity using the insertion of noise. [51] proved an interesting result that shows that a jammer with access to the channel input can inflict only as much damage to communication as one without access to the channel input. For this zero-sum game, the author showed that the saddle-point strategy of the encoder is to transmit a circularly symmetric complex Gaussian (CSCG) signal and that of the jammer is to inject a CSCG signal independent of the transmitters signal.

Similar to [51], [52] also considered a zero-sum mutual information game, but, for two users, one receiver and one jammer model for both fading and non-fading additive white Gaussian noise channel. For non-fading environment author showed that Gaussian signalling for users and linear jamming for the jammer are the saddle points of the game when either the jammer knows the transmitted signals or the jammer taps the channel to get a noisy version of transmitted signal. For fading channels, with no channel state information at the receiver and at the jammer, the authors proved a generalization

of [51] for multiuser case and showed that a jammer with no access to channel input information can inflict as much damage as the jammer with channel input information, subsequently, also proved the optimality of Gaussian signaling and linear jamming for users and the jammer respectively.

In contrast to above approaches based on zero-sum game, [53] used the Bayesian game approach to model the incomplete information game between malicious nodes (jammer who want to destroy the communications between nodes) and selfish nodes (users of the network who wants to maximize their network's performance) where the identity of each node is not a common knowledge. It is assumed in this work that malicious nodes are at a conflict with only selfish nodes, attempting to minimize their utility; however, do not have any incentive to jam other malicious nodes. The authors showed the existence of different conditions under which nodes conceal their identity or reveal the identity to improve their individual performance as a selfish nodes or to reduce the system performance as a malicious nodes. The authors, further, extended the one-stage game to a dynamic multi-stage game with incomplete information and used Bayes rule to update the beliefs on different types in this dynamic setting.

[54] proposed a notable approach based on stochastic game to model the jamming problem in cognitive radios where a jammer emulates as a primary user of the cognitive radios to discourage a secondary user from using an unoccupied channel. In the proposed model in [54], the authors assumed that the primary user dictates the system state and its transition probabilities whereas the secondary users access the spectrum opportunistically by sensing unoccupied channels for data communication while the jammer launches a primary user emulation attack to block a secondary user from using the channel, regardless of the channel state. The main result of [54] is in proving that the secondary users can increase their long-term payoffs by using their sensing capabilities to choose to communicate under states where the available channels are less prone to jamming.

It is to be noted here that while jammers actively try to disrupt a network communication, eavesdroppers passively hear network communications to gain secret information. [9] proposed a game-theoretic formulation of anonymous networking for finite wireless networks against eavesdropping. The network managers use dummy packets within the limit of QoS constraints to hide the network session by generating constant flows in some nodes of the network while the eavesdropper chooses a subset of wireless nodes from all available nodes to monitor, thus a zero-sum game between network managers and the eavesdropper is formulated with the payoff as the Shannon entropy of the network session conditioned on players strategies. It was proven that there exist a saddle point equilibrium such that the equilibrium strategy of the network designer is to ensure that any subset of node monitored by adversary reveal same amount information about network session.

While the above works utilizing game theory assume that jamming or eavesdropping is inevitable, game theory is also used to model intrusion detection to determine the presence of jammer from the anomaly in network traffic, consequently, to secure and prevent unauthorised use of network. [55] used the transition probabilities of a stochastic game to model an expected attacker behaviour and used the transition in the states of the stochastic game to determine the attack. [56] used the zero-sum stochastic game to model the interaction between jammer and intrusion detector and optimize their strategies using Q-learning and Markov Decision Process.

Along with eavesdropping, jamming, and intrusion detection, game theory is also used to measure the effectiveness of cryptographic techniques. Specifically, information hiding games have been studied in literature [57–59] to quantify the hiding capacity of watermarking and steganography. The hiding capacity is represented as solution of a zero-sum mutual information game between attacker and information hider where the distortion in the carrier signal by the hider and distortion in watermarked data by the attacker are considered to be bounded.

In addition to its extensive use in modelling the interaction between network managers and adversaries, game theory is also heavily used in modeling of general privacy utility tradeoffs as explained in the next section.

2.6 General privacy utility tradeoffs

Security and privacy can be seen as common good where everybody reaps the benefit of a secure network while everyone also suffers the consequence of breaching in a network link. This interdependence of security was first studied in [60] by addressing the question of whether agents have adequate incentives to invest in protection against a risk whose magnitude depends on the actions of other agents. The authors proved that the Nash equilibriums of this interdependent security problem can be broadly classified into two classes for identical agents depending on their cost and risk parameters of security: 1. every agent invests in protection 2. no agent invest in the protection. Moreover, the authors also showed that the incentive to invest in protection approaches zero as the number of unprotected agents increases.

For the case of multi-agent security problems, 'trust' plays an important role where agents can share some private information to enhance trust among their peers while at the same time make themselves vulnerable against malicious agents. This interaction between trust and privacy is studied in [61] where the authors proposed a multistage zero-sum game such that the players of the game are divided into two classes: attacker and defender, with two possible actions: send attributes

(personal information) to a information verifier or wait until the next stage. By sending the personal information, defenders increases the level of trust among its peers but the attackers can surpass it in the next stage, thus can force defender to disclose even more attributes in the subsequent stage. The winner of the game is the class of players who first achieve trust more than a desired level. The authors prove that in Nash equilibrium, both attacker and defender would wait till the last stage of the game to transmit their attributed to the information verifier. Accordingly, author introduced incentives for players to disclose information and show that in this incentive driven trust-privacy game, the information verifier does not have to wait till the last stage of the game to verify players.

[62] proposed an approach based on both complete and incomplete information games to model the interaction between different mobile nodes at the mixing zone of the mobile network in obtaining location privacy at the cost of exchanging pseudonyms. Specifically, the proposed models based on complete and incomplete information game incorporate in it the beliefs of users about the tracking power of the adversary, the amount of anonymity that users obtain in the mix zones, the cost of pseudonyms, and the time of changing pseudonyms. The author assumed that each mobile node has two strategies: they can cooperate and change their pseudonyms or they can defect. For an $n-$player complete information static game, the authors showed that the all defection strategies profile are always an equilibrium point and an equilibrium with cooperation does not always exist, as payoffs in a $n-$player game can be very asymmetric. For incomplete information game, they designated the level of privacy requirement of a user as his/her type and proved that probabilities of cooperation is small if the number of users with lower types are in abundance.

[63] used the repeated-simultaneous game to model the cooperation from users in enhancing the anonymity provided in a mix network depending on some extra incentives (like money, bandwidth etc.) given to them and also introduced a cost of using the mix network to prevent free riders. The main result of the paper lies in proving that incentives are necessary to prevent the system from collapsing.

It is important to note here that, similar to [63], our work can also be seen as tradoff between privacy and utility where we consider the network QoS requirements as the utility and for a given QoS requirement, we optimize mixing strategies to enhance anonymity of mix networks as explained in detail in subsequent chapters.

3 Packet based Anonymity of Mixes under the constraint of Memory

In this chapter, we address the effect of memory limitation on anonymity of mixes using an information theoretic framework to study optimal mixing strategies. The key to answering these questions lies in defining a quantitative measure of anonymity. In this chapter, we use the Shannon entropy of the a-posterior distribution of packet sources on the destination link to measure the achieved anonymity. Consider the simple two hop setup in Figure 10 as an example. Sources transmit packets to the destination through the intermediate mix. The mix, in addition to the layered encryption, uses a specific shuffling strategy to reorder the packets prior to transmission to the destination. Assuming an eavesdropper can perfectly detect the timing of packets on each link, her knowledge of the mixing strategy would result in a-posterior distribution of the sources of packets on the departure process $Y(t)$. We use the Shannon entropy of this distribution to measure the source anonymity provided by the mix. Using this metric, we characterize the maximum achievable anonymity for a single mix serving two equal rate independent Poisson sources; for a mix with buffer size k, the maximum achievable anonymity is shown to be $\log\left(2\cos\frac{\pi}{k+3}\right)$. The approach we use in this paper to derive the single letter characterization of the maximum anonymity as a function of the buffer size relies on a reduction of the problem to a Markov Decision Process and solving the resulting Bellman equation. Although the maximum anonymity for a general multiuser system is as yet unknown, we prove that as $k \to \infty$, the maximum anonymity converges to the entropy of source arrival rates at a convergence rate no lesser than $\frac{1}{k^2}$. If the normalized arrival rates of the general multiuser system can be expressed as a rational fraction $\frac{m}{2^n}$ for some fixed m and n, we show that this convergence rate is indeed achievable. In this chapter, we also study the anonymity achievable in a single destination network of mixes; specifically, we show that the anonymity achieved by a network of mixes is lower bounded by a weighted sum of the anonymity achieved by individual mixes, and the lower bound is asymptotically tight (as buffer size increases).

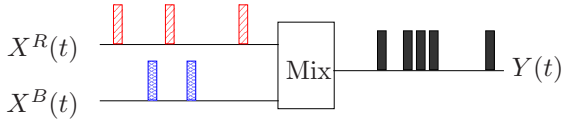


Figure 10: Chaum mix: The eavesdropper observes the arrival processes $X_R(t)$ and $X_B(t)$ from the two sources and the departure process from the mix $Y(t)$.

3.1 Problem Setup

We consider the problem of hiding sources of packets transmitted to a particular destination node in a network. Such a system can be modelled as a *single-destination network*; a 3−tuple $\mathcal{M} = (\mathcal{G}, \mathcal{B}, \Lambda)$, where $\mathcal{G}$ is the graph that describes the network topology, $\mathcal{B}$ is the set of buffer sizes and Λ is the set of arrival rates. These parameters are described in better detail as follows.

$\mathcal{G} = (\mathbf{V}, \mathbf{E})$ is an *in-tree* directed graph, where the set of nodes $\mathbf{V}$ can be divided into a set of leaf nodes $\mathbf{S} = \{S_1, \cdots, S_u\}$ denoting the sources, a set of intermediate nodes $\mathbf{M} = \{M_1, \cdots, M_m\}$ denoting the mixes, and the root node R that represents the final destination. We assume all sources transmit to single-destination and study the maximum achievable source anonymity of packets arriving at the common destination link. Without loss of generality, we let $M_m \in \mathbf{M}$ be the only node in the graph connected to R[1].

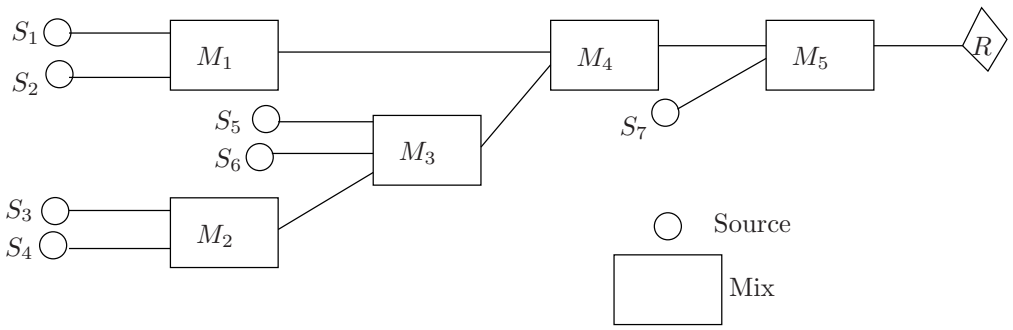


Figure 11: A Mix Network:$E_s = \{(S_1, M_1), (S_2, M_1), (S_3, M_2), (S_4, M_2), (S_5, M_3), (S_6, M_3), (S_7, M_5)\}$, $E_m = \{(M_1, M_4), (M_2, M_3), M_3, M_4), (M_4, M_5)\}$.

We partition the set of edges as $\mathbf{E} = E_s \bigcup E_m \bigcup E_r$ where

$$\begin{aligned} E_s &= \{(A, B) \in E : A \in \mathbf{S}\} \text{ (Source Edges)}, \\ E_m &= \{(A, B) \in E : A, B \in \mathbf{M}\} \text{ (Intermediate Edges)}, \\ E_r &= \{(M_m, R)\} \text{ (Destination Edge)}. \end{aligned}$$

$\mathcal{B} = (k_1, \cdots, k_{|\mathbf{M}|})$ is the set of buffer sizes of the mixes where $k_j \in \mathcal{Z}^+$ denotes the maximum number of packets that can be stored in mix M_j at any given time. $\Lambda = (\lambda_1, \cdots, \lambda_{|\mathbf{S}|})$ is the set of arrival rates of sources. In part of the discussion we shall also refer to arrival probabilities $\{q_i, S_i \in \mathbf{S}\}$ where $q_i \stackrel{\triangle}{=} \frac{\lambda_i}{\sum_j \lambda_j}$ refers to the prior probability that an arriving packet belongs to a particular source.

[1]Since we assume that sources resort to single path transmission, if there are multiple mixes connected to the same destination, then these "final" mixes would effectively divide the system into distinct independently functioning single destination mix networks of the model considered in this work.

An example of a single-destination system is shown in Figure 11. Although single destination systems are the focus of this work, we believe our framework can be extended to study multiple destination networks as well. It is easy to see that the additional uncertainty in destinations can only result in higher anonymity in multi-destination systems.

During the operation of the network, on each edge $(A, B) \in \mathbf{E}$, a stream of packets is transmitted by node A to B, which is denoted by a point process $\mathcal{X}_{(A,B)}(t)$ (set of arrival times). We assume the sources transmit packets according to independent Poisson processes with rates as specified in Λ. Due to the independent Poisson assumption, the arrival processes can be viewed as a single marked Poisson process of rate $\lambda \stackrel{\triangle}{=} \sum_i \lambda_i$, where each point is independently marked as belonging to source S_i with probability q_i. Note that while the source arrival processes $\{\mathcal{X}_e(t), e \in E_s\}$ are Poisson, the intermediate and destination processes are not constrained to be so.

Mix: For a mix $M_i \in \mathbf{M}$, let $E_{M_i} = \{(A, M_i) : (A, M_i) \in E\}$ denote the set of incoming links to M_i. Mix $M_i \in \mathbf{M}$ observes only the set of incoming streams $\{\mathcal{X}_e(t) : e \in E_{M_i}\}$. All packets on any particular stream $\mathcal{X}_{A,M_i}(t)$ have identical headers due to layered encryption, and the contents do not reveal any information about the path of the packet prior to arriving at node A.

Each mix has exactly one outgoing stream (as is evident from the tree structure of the network). The mix M_i may collect up to k_i packets beyond which, any further arrival mandates an immediate departure; in other words no packets can be dropped. Since mixes cannot drop any packets or create new packets, the average packet transmission rates on the outgoing link of any mix is a deterministic function of the topology and Λ. We use a slight abuse of notation and allow λ_e to denote the rate of packets on edge $e \in \mathbf{E}$, *i.e.* the rate of the point process $\mathcal{X}_e(t)$. A mix is allowed to transmit multiple packets in a single batch, in which case the order of packets within a batch is random[2]. The mixing strategies are designed with knowledge of the topology and arrival rates of the sources. During the operation of the network, the mixes do not possess shared randomness and do not communicate with each other. The strategy ψ_i for mix M_i generates a departure process that is a causal function of the arrival processes while satisfying the packet conservation and buffer constraints. Let $\Psi(\mathcal{M})$ denote the set of all valid mixing strategies for the network $\mathcal{M}$. Sinces we assume no shared randomness and no communication between mixes, a strategy $\psi \in \Psi(\mathcal{M})$ for a network $\mathcal{M}$ is a set of strategies $\psi_1, \cdots, \psi_m$ for the respective mixes.

[2]From a practical standpoint, a batched transmission implies that the mix picks a random ordering of the packets in the batch, and transmits them accordingly in quick succession

Eavesdropper (Eve): The omniscient eavesdropper observes the arrival time of every packet on every link. As in the case of the mixes, the individual packets on each stream are indistinguishable to the eavesdropper. He is aware of the topology of the network and the mixing strategies of all nodes, but does not have access to the realization of the private randomness used by each mix to implement its mixing strategy (private randomness would correspond to ordering of packets in a batch, the choice of packets from the buffer etc). Using his complete knowledge, his goal is to determine the original sources of the packets on the link of interest (in this case, the destination stream $\mathcal{X}_{(M_m,R)}(t)$.

3.1.1 Source Anonymity

In a single destination mix network, one can view the network of mixes as a "boxed" system where all the sources feed packets into the box, and the box outputs a stream of packets to the final destination. The eavesdropper wishes to determine the sources of packets at the output link (from the box to the destination node) using his observation of the internal and external point processes, and knowledge of the functioning of the components in the box. For any strategy of the mixes (that adhere to the buffer and packet conservation restrictions), the output process would be a sequence of departing packets on this final destination link. Since no mix can predict the future arrivals, and the mixes do not communicate with each other, the a-posterior probability of sources of every departing packet on the link would only be a function of the arrivals until that time. Let the packets on the destination link be numbered according to their time of departure.

For purposes of defining anonymity, it is important to start at an initial state known to all participants of the system. We assume Eve starts observing the system at time $t = 0$, at which point all mixes are empty. The point processes observed by Eve are therefore one-sided. To determine the sources of packets on the destination link, Eve can utilize the knowledge of all point processes in the entire time duration $[0, \infty)$.

Definition 1 *For a given observation of all point processes $\{\mathcal{X}_e(t), e \in E\}$, the knowledge of the set of mixing strategies denoted by ψ results in a-posterior distribution of sources of packets on the destination link (M_m, R). Let Y_i be the random variable (using the eavesdropper's a-posteriori probability distribution) that represents the source of the i^{th} packet transmitted on the destination link after $t = 0$. For the set of mixing strategies ψ, the per-packet source anonymity is defined as:*

$$\mathcal{A}^{\psi}(\mathcal{M}) = \liminf_{n\to\infty} \frac{1}{n}\mathbb{E}(H_{\psi}(Y_1, Y_2, Y_3, \cdots, Y_n)), \tag{2}$$

where H_ψ is the Shannon entropy of the joint a-posterior distribution (from Eve's perspective) of $(Y_1, \cdots, Y_n)$ generated by the mixing strategy ψ for the specific realization of the arrival and departure processes, and the expectation is over the realization of the arrival and departure processes.

Specifically, when $(x_1, t_1, x_2, t_2, \ldots)$ is a realization of arrival process such that x_i is the source and t_i is the arrival time of i^{th} arrival to the mix and the set of mixing strategies ψ, the realization $(x_1, t_1, x_2, t_2 \ldots)$, and Eve's observations on each link of the network $\mathcal{M}$ impose a probability distribution $\mathbb{P}$ on the random variable $(Y_1, \cdots, Y_n)$, then

$$H_\psi(Y_1, Y_2, \cdots, Y_n) = \sum_{y_n=1}^{u} \sum_{y_{n-1}=1}^{u} \cdots \sum_{y_1=1}^{u} \mathbb{P}(y_1, \cdots, y_n) \log \frac{1}{\mathbb{P}(y_1, \cdots, y_n)}$$

and the expectation in (2) is over all possible realizations of $(x_1, t_1, x_2, t_2 \cdots)$.

Using the properties of Shannon entropy, we know that for a $u-$source mix, $0 \leq \mathcal{A}^\psi(\mathcal{M}) \leq \log u$. $\mathcal{A} = 0$ implies the eavesdropper perfectly identifies the source of every outgoing packet, and $\mathcal{A} = \log u$ implies that from the eavesdropper's perspective, every outgoing packet is equally likely to have arrived from any of the sources. The general implication of this metric can be understood using Fano's inequality [64], which states that the adversary's probability of error in determining the source of an outgoing packet is lower bounded by the normalized conditional entropy.

In the subsequent sections, we use this definition to study optimal mixing strategies and prove the following key results:

1. Let $\mathcal{M}_1 = (G_1, k, (\lambda, \lambda))$ denote a single mix serving two equal rate poisson sources (see Figure 10). Then
$$\sup_{\psi \in \Psi(\mathcal{M}_1)} \mathcal{A}^\psi = \log \left[2 \cos \left(\frac{\pi}{k+3} \right) \right].$$

2. For a general mix network defined by $\mathcal{M} = (\mathcal{G}, \mathcal{B}, \Lambda)$, let $\mathcal{M}_i = (G_i, \Lambda_i, k_i)$ denote a sub network containing exactly one mix M_i with the number of sources equal to the number of incoming links of mix M_i in $\mathcal{M}$ and where each source in $\mathcal{M}_i$ transmits according to an independent Poisson process with a rate equal to the net arrival rate on the corresponding incoming link in $\mathcal{M}$. Let ψ_i denote the strategy used by mix M_i in the sub network $\mathcal{M}_i$. Then, under certain conditions on the mixing strategies:
$$\mathcal{A}^\psi(\mathcal{M}) = \sum_{i=1}^{m} \frac{\lambda^i}{\lambda} \mathcal{A}^{\psi_i}(\mathcal{M}_i)$$
where $\psi = (\psi_1, \cdots, \psi_m)$, λ^i is the total arrival rate in the sub-network $\mathcal{M}_i$ and λ is the total

arrival rate to the network $\mathcal{M}$.

3. For any mix network $\mathcal{M}$ with u sources transmitting at rates $\lambda_1, \cdots, \lambda_u$ respectively ($\lambda = \sum \lambda_i$), the maximum achievable anonymity is upper bounded as:

$$\sup_{\psi \in \Psi(\mathcal{M})} \mathcal{A}^{\psi}(\mathcal{M}) \leq -\sum_{i=1}^{u} \frac{\lambda_i}{\lambda} \log\left(\frac{\lambda_i}{\lambda}\right) - \Omega\left(\frac{1}{k_{total}^2}\right)$$

where k_{total} is the total buffer size available in the network.

4. If in a mix network $\mathcal{M}$, the arrival rates are such that there exists a positive integers $n, n_1, \cdots, n_u$ and $\frac{\lambda_i}{\lambda} = \frac{n_i}{2^n}$ $\forall 1 \leq i \leq u$, then the maximum achievable anonymity is lower bounded as:

$$\sup_{\psi \in \Psi(\mathcal{M})} \mathcal{A}^{\psi}(\mathcal{M}) \geq -\sum_{i=1}^{u} \frac{\lambda_i}{\lambda} \log\left(\frac{\lambda_i}{\lambda}\right) - O\left(\frac{1}{k_{\min}^2}\right)$$

where $k_{\min}$ is the minimum buffer size across the mixes of the system.

3.2 Anonymity of a Single Mix serving Two Sources

In this section, we analyze the anonymity of a single Chaum mix serving two users; this system is represented by the 3−tuple $\mathcal{M}_1 = (\mathcal{G}_1, k, (\lambda_1, \lambda_2))$ where $\mathcal{G}_1$ is as shown in Figure 12. For this simple system, we will derive the optimal mixing strategy, and characterize the achievable anonymity as a function of the buffer size k. Prior to describing the results, we will present two key reductions to the class of possible mixing strategies that simplifies the analysis without losing generality.

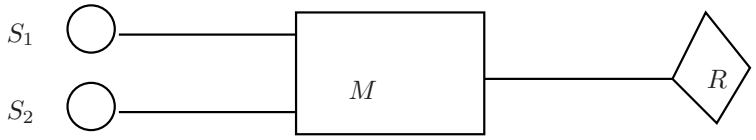


Figure 12: Two User Single Mix Network.

First, we claim that it suffices to consider only those mixing strategies where a packet is transmitted only upon a new arrival to a full buffer, *i.e.* only when the mix has no other choice but to transmit. To understand that this reduction does not lose generality, consider any strategy ψ that does not belong to this class. Such a strategy would make a decision to transmit a packet when the buffer is not full, or at a time when no new packet has arrived. Consider a modified version of this strategy, say ψ', described as follows. If at time t, there was no arrival point on any incoming stream, and strategy ψ chooses to transmit a packet stored in its buffer, then strategy ψ' also chooses (at time t) the identical packet to transmit from its buffer, but does not transmit

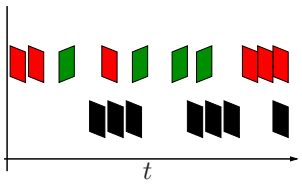


Figure 13: Original Strategy ψ: Arbitrary Departure Process

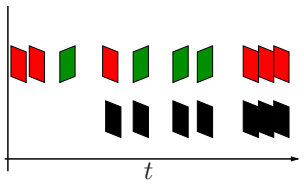


Figure 14: Modified Strategy ψ': Departure Process is a deterministic function of Arrival Process

Figure 15: Arrival and Departure Process for a mix with buffer size 3 serving two users: Red and Blue packets denote arivals and black packets denote departures.

the packet immediately. Instead, the strategy waits until the buffer is full and when a new packet arrives (thus making it necessary to transmit), say at time $t' > t$, transmits the packet chosen at time t. If multiple packets were chosen between t and t', the packets are transmitted one at a time upon a new arrival and in the order they were chosen. Note that according to this modification, the state (time ordered contents) of the buffer for strategy ψ at any time t will be contained in the state of the buffer for strategy ψ' at time t, and consequently at all t, the information available to the mix using ψ to make decisions is available to that using ψ' as well. Therefore, assuming identical realization of arrival processes and private randomness for both mixes, the realization of the **sequence** of sources of the departing packets will be identical for both strategies. Note however that when applying strategy ψ', starting from the first instant that the buffer is full, a packet departs from the mix at time t if and only if a new packet arrives at time t. Consequently, the departure process is a fixed deterministic function of the arrival process independent of the sequence of sources of arriving packets, and independent of the private randomness used by the mix (see Figure 15). If, when the mix uses strategy ψ', a genie were to provide Eve the point process representing the departures were the original strategy ψ used, then the achieved entropy from Eve's perspective for any realization of the arrival and departure processes would be identical in both scenarios (original strategy and genie aided ψ' strategy). Since the actual departure process for strategy ψ' is a fixed deterministic function of the arrival process, the relationship between the entropy achieved by the strategy ψ' when the genie is absent and the entropy achieved when the genie is present is identical to that between conditional entropy and entropy. Since conditioning reduces entropy, the anonymity achieved by strategy ψ' is always greater than or equal to that achieved by ψ thus justifying our first reduction.

The second reduction is motivated by the reduced strategy space which ensures that the departure process provides no information about the sources of departing packets. Specifically, since each

departure occurs only upon a new arrival, it is sufficient for the strategy to decide which packet to transmit only at the time of a new arrival. Any strategy that makes decisions without being triggered by a new arrival can be modified thusly without reducing anonymity. Note that since no delay constraints are imposed on the packets, an important consequence of this reduction is that the actual times of arrival of packets are unimportant as long as the order of sources of arriving packets are fixed. Consequently, the system can now be reduced to a discrete event model wherein each event corresponds to a new arrival which instantaneously triggers a departure. By defining such a discrete event model, the following result on the optimal anonymity for a two source mix is obtained. On a broader note, since actual timing of arrivals is information that is perfectly available to the eavesdropper, using the timing in the mix's decision making process cannot increase the anonymity.

Theorem 1 *The maximum achievable anonymity $\mathcal{A}(k)$ of a Chaum mix with buffer capacity k serving two users*

1. *when arrival rate of both users are equal is*

$$\mathcal{A}(k) = 1 + \log_2 \left(\cos \left(\frac{\pi}{k+3} \right) \right) \tag{3}$$

2. *when the arrival rate of users are respectively $q\lambda$ and $(1-q)\lambda$ for $q \in [0,1]$ is*

$$\mathcal{A}(k) = t \log_2 \psi_1$$

where ψ_ns are obtained by solving following equations

$$\begin{aligned} \psi_0 &= 1 \\ \psi_n^{t^n} + \psi_{n-2}^{t^n} &= \psi_1^t \psi_{n-1}^{t^n} \ \ \forall 2 \leq n \leq k+1 \\ \psi_1^t \psi_{k+1}^{t^{k+2}} &= \psi_k^{t^{k+2}} \end{aligned} \tag{4}$$

where $t = \frac{1-q}{q}$.

Proof: Since any strategy has to make decisions only upon a new arrival, the actual times of arrival are irrelevant, and we reformulate the anonymity using a discrete event system model, wherein the time $n \in \mathbb{N}$ corresponds to the the n^{th} arrival point in the joint arrival process. To ease explanation of the ideas we will henceforth refer to the packets from the two users as being *red* and *blue* respectively. Let $X_1, \cdots, X_n$ be the sequence of random variables representing the sources of arriving packets. Let $X_i = 1$ denote a red arrival and $X_i = 0$ denote a blue arrival. Due to the Poisson assumption,

X_is are i.i.d Bernoulli random variables with parameter q. Likewise $Y_1, \cdots, Y_n$ is the sequence of random variables from Eve's perspective denoting the sources of outgoing packets on the destination link (M, R). Eve perfectly observes $X_1, \cdots, X_n$ and using the knowledge of the mixing strategy wishes to determine the sequence $Y_1, \cdots, Y_n$.

At time n, the contents of the mix's buffer **including the new arrival** are used to denote the state of the discrete event system. Although the contents of the mix's buffer at any time are represented by a time ordered sequence of sources of packets in the buffer, we claim that since

1. the mix makes no distinction between packets that arrive from a particular source

2. no delay constraints are imposed

3. the sources of arriving packets are distributed i.i.d across time

the order of arrival of packets (including the new arrival) within the mix's buffer can be ignored in the decision making process of the mix. If a strategy ψ utilized the order of arrivals in deciding which packet to transmit, then amongst all possible orderings of packets within the buffer, there must exist one that results in the maximum entropy of departing packets. A modified strategy that always makes a decision assuming the order of packets in the buffer is this entropy maximizing order regardless of the actual arrival order would then achieve a higher anonymity than the strategy ψ. Consequently, it is sufficient to denote the contents of the mix's buffer by the number of packets from each source. For a two source mix, the state of the mix's buffer is a vector valued random variable that takes values in $\{0, 1, \cdots, k+1\}^2$ such that if the state $S = (r, b)$, then $r + b \leq k + 1$ where r and b denote the number of red and blue packets in the mix. Without loss of generality, we assume that the buffer at time $n = 0$ contains zero packets.

The reduction in strategy space ensures that the buffer is full at all times $n > k$, and since no decisions are made by the strategy before time $n = k$, we let S_i to denote the state of the buffer at time $k + i$. Note that since the buffer is full at all times $n > k$, if at any time $n > k$, $S_n = (r, b)$, then $r + b = k + 1$. We therefore represent the buffer state at time $n > k$ as a scalar random variable taking values in $\{0, \cdots, k+1\}$. In other words, if at time $n > k$, $S_n = r$ then the buffer contains r red packets, $k + 1 - r$ blue packets.

In this discrete event model, we can rewrite the anonymity for a strategy ψ as defined as

$$\begin{aligned} A^{\psi}(k) &= \lim_{n\to\infty} \frac{\mathbb{E}[H_\psi(Y_1,\cdots,Y_n|X_1,\cdots,X_{n+k+1})}{n} && (5)\\ &\overset{(a)}{=} \lim_{n\to\infty} \frac{\mathbb{E}[H_\psi(Y_1|X_1,\cdots,X_{n+k+1})]+\cdots+\mathbb{E}[H_\psi(Y_n|Y_1^{n-1},X_1,\cdots,X_{n+k+1})]}{n} && (6)\\ &\overset{(b)}{=} \lim_{n\to\infty} \frac{\mathbb{E}[H_\psi(Y_1|S_1)]+\cdots+\mathbb{E}[H_\psi(Y_n|S_n,Y_1^{n-1})]}{n} && (7)\\ &\overset{(c)}{\leq} \lim_{n\to\infty} \frac{\mathbb{E}[H_\psi(Y_1|S_1)]+\cdots+\mathbb{E}[H_\psi(Y_n|S_n)]}{n} && (8) \end{aligned}$$

(a) follows from the chain rule of entropy.

(b) follows from the observation that $(X_1,\cdots,X_{n+k+1})$ has a one-one correspondence with $(Y_1,\cdots,Y_{n-1})$ and S_n, and that the source of a particular departing packet is independent of future arrivals.

(c) follows from the fact that conditioning reduces entropy.

In the above reduction, note that if a strategy ψ ensures that $Y_n - S_n - (Y_1,\cdots,Y_{n-1})$ is a Markov chain for every n, then equality is achieved in (c). Indeed any strategy that does not satisfy this Markov property can be modified to one that does by using the marginal distribution $\Pr\{Y_n|S_n\}$ in making the choice of packet to transmit thus increasing the achieved entropy. Consequently, we only consider those strategies wherein conditioned on the state, the choice of packet to transmit is independent of past departures. In effect the entropy achieved by such strategies is equal to the sum of expected conditional entropies of outgoing packets at each time.

In this model, we denote the action of the mix at time n as a function $p : \{0,1,\cdots,k+1\}\times\mathcal{Z}^+ \mapsto [0,1]$ where $p(S_n,n)$ denotes the probability of transmitting a red packet at time n if the state is S_n (with probability $1-p(S_n,n)$, the mix would transmit a blue packet). We can then write $H(Y_n|S_n = r) = h_2(p(r,n))$ where $h_2(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function. Furthermore, since only the present state is used in the decision, and the source of every arriving packet is independent of the state and the history of the system, the discrete time state process follows a Markovian evolution.

$$S_{n+1} = \begin{cases} S_n+1 & \text{w.p. } (1-p(S_n,n))q \\ S_n-1 & \text{w.p. } p(S_n,n)(1-q) \\ S_n & \text{w.p. } p(S_n,n)q+(1-p(S_n,n))(1-q) \end{cases}. \quad (9)$$

The anonymity achieved by the strategy defined by probability function p is computed using (44)

as:

$$\mathcal{A}^p(\mathcal{M}_1) = \liminf_{n\to\infty} \frac{1}{n}\mathbb{E}\left(\sum_{i=1}^{n} h_2(p(S_n, n))\right)$$

where S_n evolves as in (9). Since the state evolution follows a Markov process such as that depicted in Fig 16, and the anonymity is an average sum of rewards in each state over an infinite horizon, the maximum achievable anonymity is in fact a solution to a Markov Decision Process (MDP) with an infinite horizon and average rewards. The following known result from [65] about MDP proves that the optimal strategy is stationary ($p(n, r) = p_r$) and reduces the optimization to solving the corresponding Bellman equation.

Lemma 1 *If s represents the present state of a Markov process, s_1 represent the next future state of the Markov process, U represent the decision space, $\xi(s, u)$ represent the cost incurred by the decision $u \in U$ at state s, and there exists a constant f and a bounded function ϕ, unique up to an additive constant, satisfying the following optimality equation (where S_0 is the random variable denoting the initial state of the system)*

$$f + \phi_s = \max_{u\in U}\{\xi(s, U) + \mathbb{E}[\phi_{s_1}|S_0 = s, U_0 = u]\}$$

Then f is the maximal average-cost and optimal stationary policy is the one that chooses the optimal action u that solves the Bellman equation for that state. □

Since ϕ is unique upto an additive constant, we would assume that $\phi_0 = 0$. The optimality equation in Lemma 1 when applied to the MDP for the two user mixing strategy gives rise to the following recursive equations

$$\begin{aligned}
f + \phi_0 &= q\phi_1 + (1-q)\phi_0 && (10)\\
f + \phi_r &= \max_{p_r}\{h_2(p_r) + p_r(q\phi_r + (1-q)\phi_{r-1}) + \cdots \\
&\quad (1-p_r)(q\phi_{r+1} + (1-q)\phi_r)\}1 \le r \le k && (11)\\
f + \phi_{k+1} &= q\phi_{k+1} + (1-q)\phi_k && (12)
\end{aligned}$$

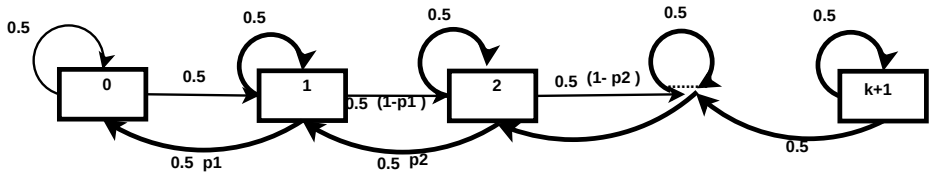


Figure 16: Markov Chain for the strategy Ψ^* for equal arrival rate

The maximization in (11) can be solved using a simple Entropy power maximization [64] yielding:

$$\begin{aligned} p_r^* &= \arg\max_{p_r}\{h_2(p_r) + p_r(q\phi_r + (1-q)\phi_{r-1}) + (1-p_r)(q\phi_{r+1} + (1-q)\phi_r)\} \\ &= \frac{2^{q\phi_r+(1-q)\phi_{r-1}}}{2^{q\phi_r+(1-q)\phi_{r-1}} + 2^{q\phi_{r+1}+(1-q)\phi_r}} 1 \leq r \leq k \qquad (13) \\ f + \phi_r &= \log\left(2^{q\phi_r+(1-q)\phi_{r-1}} + 2^{q\phi_{r+1}+(1-q)\phi_r}\right) 1 \leq r \leq k \qquad (14) \end{aligned}$$

Replacing $\frac{2^{\phi_r}}{2^{\phi_{r-1}}} = \left(\frac{\psi_r}{\psi_{r-1}}\right)^{\frac{1}{q}} t^r$ the result for the general two user system in the theorem is obtained.

When arrival rates are equal, $q = \frac{1}{2} \implies t = 1$ and (4) reduces to the following set of equations:

$$\begin{aligned} \psi_0 &= 1 \\ \psi_r + \psi_{r-2} &= \psi_1\psi_{r-1} \forall r = 2, \cdots, k+1 \\ \psi_1\psi_{k+1} &= \psi_k \end{aligned}$$

Let $\psi_1 = 2\cos\theta$. The above recursion can be solved resulting in $\psi_r = \frac{\sin((r+1)\theta)}{\sin(\theta)}$ where $\theta = \frac{\pi}{k+3}$, and the optimal average reward for the MDP is given by:

$$f = \log\left[2\cos\left(\frac{\pi}{k+3}\right)\right].$$

Using equation (13) the optimal mixing strategy that achieves the above anonymity is given by:

$$p_r^* = \frac{\psi_{r-1}}{\psi_{r-1} + \psi_{r+1}} = \frac{\sin(r\theta)}{\sin(r\theta) + \sin((r+2)\theta)} \qquad (15)$$

where p_r^* is the probability of transmitting a red packet when the mix contains r red packets in its buffer (including the new arrival). □

Theorem 1 represents the first closed form characterization of the maximum anonymity of a buffer limited Chaum mix, and provides the optimal strategy to achieve the maximum anonymity. When $q \neq 0.5$, the resulting series of nonlinear equations are hard to solve, and consequently a single letter characterization is as yet unknown. However, numerical analysis and algebraic reduction can

be used in some special cases. For instance, when $k = 1$, and $q = \frac{1}{n}$ where $n \in \mathbb{N}$, then anonymity $\mathcal{A}(1) = -q \log_2(1-t)$ where t is the unique solution of polynomial $x^{n-1} + x - 1 = 0$ which lies in $(0, 1)$.

From the above theorem, we can write that for a two user system with equal arrival rates,

$$\mathcal{A}(b) = 1 + \log_2(\cos\frac{\pi}{k+3}) \geq 1 + \log_2\left(1 - \frac{\pi^2}{2(k+3)^2}\right) \geq 1 - \frac{\pi^2}{2\ln(2)(k+3)^2}. \tag{16}$$

Therefore, the optimal mixing strategy asymptotically (as $k \to \infty$) achieves the maximum possible anonymity in a two user system, the prior source entropy of 1, and the convergence rate is $O(\frac{1}{k^2})$

It is important to note that although formalizing the definition of anonymity required the buffer at time 0 to contain 0 packets from either source, the proof reduces the system to a Markov decision process and the optimal strategy results in a stationary distribution of the system state regardless of the initial conditions. The anonymity of the optimal strategy therefore does not depend on the initial composition of the mix's buffer as long as Eve is perfectly aware of the initial state.

The analytical method can be extended to systems with more than two users and the resulting multidimensional Markov chain results in a series of multidimensional recurrence relations which limits the analytical tractability of the problem. Although the closed form characterization for the optimum anonymity is as yet unknown for a general multi user configuration, in Section 3.4, we study the asymptotic behavior of anonymity with respect to buffer size, and demonstrate that for several multi user systems, the optimal convergence rate of the anonymity is $\Theta(1/k^2)$.

In the next section, we study the anonymity of a mix network and characterize a lower bound as a weighted sum of anonymities of individual mixes.

3.3 Achievable Anonymity in a Network of Mixes

The layered encryption described in [3], ensures that each mix in the system is only aware of the immediate preceding and immediate succeeding node of any packet that arrives to it. Further, we assume that mixes do not share common randomness nor do they communicate with each other during network transmission (aside from forwarding packets). Consequently, each intermediate mix performs its reordering without explicitly knowing the path/original source of any arriving packet prior to the node it was transmitted by. It is possible that mixing strategies are designed such that information is communicated implicitly, for instance through the timing of transmissions. Note however that such implicitly communicated information, in the absence of shared randomness, would automatically be deciphered by an eavesdropper as well. We therefore follow the reduction in class

of strategies for individual mixes wherein the output process of any mix in a single destination network will be a deterministic function of the net incoming process to that mix. Consequently, given the topology, and the realization of the source arrival processes, the destination process and all intermediate processes are deterministic in our analysis. We do note that while such an approach is optimal in a single mix system, it may not be so in a network. In this work, we would like to express the *achievable* anonymity of a network of mixes as a function of the anonymity achievable by individual mixes.

By virtue of the single destination topology, the reordering of packets occurs in a fixed and known sequence. Starting backward from the final mix M_m, each mix shuffles packets independent of the actions of the prior mixes in the paths of the arriving packets and the actual time points of arrival (due to the reduction). From the perspectve of an eavesdropper interested in determining the sources of packets on the destination link, the sequence of actions of the mixes results in a probability distribution over bijective graphs from the source arrival points to the destination points through the intermediate processes. The independence in the actions of the mixes in this viewpoint would corespond to an independence between the intermediate bijective graphs corresponding to individual mixes. Formalizing this idea provides the following result which expresses the achievable anonymity as a linear function of the anonymities of individual mixes.

Theorem 2 *In a general mix network $\mathcal{M} = (G, \mathcal{B}, \Lambda)$, let $\mathcal{M}_i = (\mathcal{G}_i, k_i, \Lambda_i)$ denote a single mix sub-network containing only mix M_i with buffer size k_i and the number of sources equal to the number of incoming links to mix M_i in $\mathcal{M}$, where each source in $\mathcal{M}_i$ transmits according to an independent Poisson process with a rate equal to the arrival rate λ_e on the corresponding incoming link $e \in E_{M_i}$ in $\mathcal{M}$. If ψ_i denotes the strategy used by mix M_i in the sub network $\mathcal{M}_i$. Then, there exists $\psi \in \Psi(\mathcal{M})$ such that:*

$$A^{\psi}(\mathcal{M}) \geq \sum_{i=1}^{m} \frac{\lambda^i}{\lambda} A^{\psi_i}(\mathcal{M}_i) \tag{17}$$

where $\lambda^i = \sum_{e \in E_{M_i}} \lambda_e$ is the total arrival rate to mix M_i and $\lambda = \sum_{i=1}^{m} \lambda^i$ is the total arrival rate to the network $\mathcal{M}$.

Proof: In the network $\mathcal{M}$, we assume each mix M_i uses the modified version of the strategy ψ_i such that the departures are only triggered by arrivals to a full buffer. Therefore, given the joint arrival process, the point processes denoting the intermediate and the destination processes are determinstically known. Consequently we can study the discrete event model described in the proof of Theorem 1.

As with the single mix system, every time point n corresponds to a new arrival from some source node in the network. Consider the joint arrival process from all sources in the system, let $\mathbf{X} = X_1, \cdots, X_n$ be the random variables denoting the sequence of sources of the first n packets arriving to the network. Since Eve can perfectly observe $\mathbf{X}$, and has knowledge of the network topology, the timing on the intermediate processes are also perfectly known to her; note that each intermediate process will have packets arriving at different sets of discrete time points depending on the original sources of arriving packets. Each mix has a set of incoming links, and the reduced strategy space of all mixes will ensure that at each discrete time point at most one packet can arrive on any one incoming link of a mix. We define the following random vectors from Eve's perspective:

1. Consider the joint incoming process to a mix M_j; let N_j denote the total number of arrivals to mix M_j until time n, and $\mathbf{Z}_j = Z_{j,1}, \cdots, Z_{j,N_j(n)}$ denote the sequence of *incoming edges* of packets arriving to the mix where $N_j(n)$ is the total number of arrivals to mix M_j at time n. We know that $E_{M_j} = \{e_{j,1}, \cdots, e_{j,|E_{M_j}|}\}$ is the set of incoming edges to the mix, therefore $Z_{j,i} = l$ indicates that the i^{th} packet that arrived to mix M_j arrived on incoming edge $e_{j,l}$. Eve has perfect knowledge of the variables N_j and $\mathbf{Z}_j$ for every mix $M_j \in \mathcal{M}$.

2. Let N_e be the random variable that denotes the number of packets transmitted on edge $e \in \mathbf{E}$. Let $\mathbf{Y}^e = Y_1^e, \cdots, Y_{N_e(n)}^e$ be the random variables representing the original source identities of the packets observed on edge e in the network from Eve's perspective.

While the variables $\mathbf{X}, \mathbf{Z}_j$ are perfectly visible to Eve, there is uncertainty in the $Y_i^e, e \notin E_s$ generated by actions of the mixes. Let d denote the destination edge (M_m, R) (and N_d denote the number of packets transmitted on the destination edge until time n). Then, the anonymity achieved by the network using strategy ψ can be written in the discrete event model as:

$$A^{\psi}(\mathcal{M}) = \liminf_{n \to \infty} \frac{H^{\psi}(\mathbf{Y}^d | \mathbf{X}, \mathbf{Z}_1, \cdots \mathbf{Z}_m)}{n}. \tag{18}$$

Note that given $\mathbf{X}$ and the topology of the network, the reduced strategy space will ensure that $\mathbf{Z}_1, \cdots, \mathbf{Z}_m$ are deterministic functions of $\mathbf{X}$, and removing the conditioning on variables $\mathbf{Z}_1, \cdots, \mathbf{Z}_m$ will not make a difference in the above equation. In the rest of the proof, we shall express the conditional entropy $H^{\psi}(\mathbf{Y}^d | \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m)$ as a sum of the conditional entropies corresponding to the actions of each mix by working our way backwards starting from the action of the final mix.

Final Mix Let $e_{m,1}, \cdots, e_{m,|E_{M_m}|} \in E_{M_m}$ denote the incoming edges to the final mix. In a single destination mix network, it is easy to see that the sets of original sources leading into any two edges

$e_{m,i}$ and $e_{m,j}$ are mutually exclusive for $i \neq j$. Let $\mathcal{S}_{m,i} \subset \mathcal{S}$ denote the set of sources transmitting packets through edge $e_{m,i}$ to mix M_m. We define random variables $W_1, \cdots, W_{N_d}$ such that

$$W_i = e_{m,j} \text{ if } Y_i^d \in \mathcal{S}_{m,j}.$$

In other words, W_i identifies the incoming edge $e_{m,j} \in E_{M_m}$ of a particular departing packet from mix M_m. Let $\mathbf{W} = W_1, \cdots, W_{N_d}$. Since W_i is a deterministic function of Y_i^d, for any set of strategies ψ in the network,

$$H(\mathbf{W}|\mathbf{Y}) = 0$$

We can then rewrite (18) as:

$$H^{\psi}(\mathbf{Y}^d|\mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) = H^{\psi}(\mathbf{W}|\mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) + H^{\psi}(\mathbf{Y}^d|\mathbf{W}, \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m). \tag{19}$$

The entropy $H^{\psi}(\mathbf{W}|\mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m)$ is the entropy of the incoming edges (to M_m) for the departing packets on the destination link (M_m, R), given the complete observation of Eve. Since the final mix can only observe its own incoming links, conditioned on $\mathbf{Z}_m$, the variables $\mathbf{X}, \mathbf{Z}_j, j \neq m$ do not impact the action of mix M_m. Further, since the uncertainty in $\mathbf{W}$ is only dependent on the action of the final mix M_m, $\mathbf{W} - \mathbf{Z}_m - (\mathbf{X}, \{\mathbf{Z}_j, j \neq m\})$ is a Markov chain and

$$H^{\psi}(\mathbf{W}|\mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) = H^{\psi}(\mathbf{W}|\mathbf{Z}_m).$$

We assume that n is large enough that the buffers of all mixes are full. At this point it is easy to see that a new arrival from one of the sources in the set $\mathcal{S}_{m,i}$ would trigger a sequence of departures, one from each mix on the path from the source to the destination. In particular, it would result in an immediate arrival on the incoming edge $e_{m,i}$ to the final mix M_m. Since sources transmit according to independent Poisson processes, the probability that an incoming packet to mix M_m arrives on edge $e_{m,i}$ is then given by:

$$\frac{\sum_{S_j \in \mathcal{S}_{m,i}} \lambda_j}{\lambda}$$

independent of past and future arrivals, where λ is the total arrival rate to the system. Consider a sub-network $\mathcal{M}_m = (\mathcal{G}_m, \Lambda_m, B_m)$ containing only the final mix M_m, such that each incoming edge to M_m in the original network corresponds to a source edge in $\mathcal{M}_m$. The source arrival rate on incoming edge $e_{m,i}$ in $\mathcal{M}_m$ is equal to the net arrival rate from sources in the set $\mathcal{S}_{m,i}$ in the original network $\mathcal{M}$, given by $\sum_{S_j \in \mathcal{S}_{m,i}} \lambda_j$. If a particular strategy ψ_m achieves anonymity $A^{\psi_m}(\mathcal{M}_m)$ in

this sub-network, then if the mix M_m applies the same strategy to arriving packets in the original network $\mathcal{M}$ then

$$\liminf_{n\to\infty} \frac{H^{\psi}(\mathbf{W}|\mathbf{Z}_m)}{n} = A^{\psi_m}(\mathcal{M}_m) \tag{20}$$

since all packets have to eventually arrive to the final mix (ie. $\frac{\sum_i N_{e_{m,i}}}{n} \to 1$).

Residual Entropy Consider the conditional entropy term in (19)

$$H(\mathbf{Y}^d|\mathbf{W}, \mathbf{X}, Z_1, \cdots, Z_n)$$

The above term is the entropy of original sources of the departing packets given the incoming edges they arrived to the final mix M_m. Given $\mathbf{W}$ we can split the departing packets into mutually exclusive sets $\mathcal{I}_i \in \{1, \cdots, n\}$, $i = 1, \cdots, |E_{M_m}|$ such that

$$j \in \mathcal{I}_i \text{ iff } W_j = i$$

In other words, all packets with indices in the set $\mathcal{I}_i$ arrived on the incoming edge $e_{m,i}$ to the final mix. Since the final mix cannot distinguish packets on a particular incoming edge, we assume the mix transmits packets that arrived on a given incoming edge on a first-come-first-serve basis. Therefore, the order of original sources of packets on an incoming edge is preserved even after the actions of the final mix. The conditional entropy $H(\mathbf{Y}^d|\mathbf{W}, \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m)$ is then equivalent to the sum of entropies of the packets on each incoming edge.

$$\begin{aligned} H(\mathbf{Y}^d|\mathbf{W}, \mathbf{X}, Z_1, \cdots, Z_m) &= \sum_{i=1}^{|E_{M_m}|} H(\{Y_j^d, j \in \mathcal{I}_i\}|\mathbf{W}, \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) \\ &= \sum_{i=1}^{|E_{M_m}|} H(Y_1^{e_{m,i}}, \cdots, Y_{N_{e_{m,i}}}^{e_{m,i}}|\mathbf{W}, \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) \end{aligned} \tag{21}$$

where $N_{e_{m,i}}$ is the number of packets that arrived on incoming link $e_{m,i}$ to the final mix. Note that since the randomness in $W_1, \cdots, W_n$ is generated solely by the action of the final mix, which functions without knowledge of the original sources of packets on any incoming link, namely $Y_1^{e_{m,i}}, \cdots, Y_{N_{e_{m,i}}}^{e_{m,i}}$, removing the conditioning on $\mathbf{W}$ does not change the entropy in (21).

Consider the sub-network, denoted by $\mathcal{M}_{m,i}$ that connects the sources in $\mathcal{S}_{m,i}$ to the incoming edge $e_{m,i}$. Since all source processes are independent of each other, the uncertainty in $\mathbf{Y}^{e_{m,i}}$ is independent of all intermediate processes that arrive to or depart from mixes not present in the

sub-network $\mathcal{M}_{m,i}$. In other words, we can write

$$H(\mathbf{Y}^{e_{m,i}}|\mathbf{W}, \mathbf{X}, \mathbf{Z}_1, \cdots, \mathbf{Z}_m) = H(\mathbf{Y}^{e_{m,i}}|\{\mathbf{Z}_j, M_j \in \mathcal{M}_{m,i}\})$$

The above entropy is identical to that achieved by the sub-network $\mathcal{M}_{m,i}$ from the perspective of an eavesdropper who only observes the processes in the sub-network $\mathcal{M}_{m,i}$. Therefore, when normalized by the total number of packets that arrived to the sub-network can therefore on incoming edge $e_{m,i}$, we can write:

$$\lim_{n\to\infty} \frac{H(\mathbf{Y}^{e_{m,i}}|\{\mathbf{Z}_j, M_j \in \mathcal{M}_{m,i}\})}{N_{e_{m,i}}} = A^{\psi}(\mathcal{M}_{m,i})$$

By iteratively applying this reduction on each sub-network and working backwards to the sources, the expression in the theorem is obtained. The weighting term for the anonymity of each mix is obtained by using the fact that $\frac{\mathbb{E}(N_{e_{m,i}})}{n}$ converges to $\frac{\lambda_{e_{m,i}}}{\lambda}$ as $n \to \infty$. □.

The above theorem expresses the anonymity achievable in a single destination network of mixes as a linear sum of anonymity achievable by the individual mixes. As long as all mixes utilize strategies that belong to the reduced strategy space described in Section 3.2, the theorem holds. Within this class of mixing strategies, if each mix uses the optimal strategy (obtained by solving the Bellman equation described in Theorem 1), then the anonymity characterized by the Theorem is optimal within the reduced class of strategies. We reiterate that while the reduced strategy space is optimal for a single mix, it has not been proved to be optimal when the mix belongs to a network of mixes. As a result, if mixes utilize strategies outside the reduced class, the anonymity characterized by the above Theorem would serve as an achievable lower bound.

An Extension to Multipath Systems Although in-tree networks of the form described in Section 3.1 (and shown in Figure 11) is the primary focus of this paper, we present an extension of the above result to a multipath system where sources can split their traffic through multiple paths to the destination (see Figure 17). This extension will prove particularly useful when demonstrating the optimal convergence rate of anonymity in a general multiuser system.

A single destination network with multipath is represented by a $3-$tuple $\mathcal{M} = (\mathcal{G}, \mathcal{B}, \lambda)$ where $\mathcal{G}$ is a multipath tree shown in Figure 17, wherein sources can transmit to multiple mixes while mixes have single outgoing links. $\mathcal{B}$ is the set of buffer sizes of mixes and $\lambda = (\lambda_{i,j}, i = 1, \cdots, s, j = 1, \cdots, m\})$ is a matrix of arrival rates where $\lambda_{i,j}$ denotes the arrival rate of packets from source S_i directly to mix M_j. Let $\Lambda_i = \{\lambda_{i,1}, \cdots, \lambda_{i,m}\}$ denote the vector of arrival rates from source S_i. Let $p_{i,j} = \frac{\lambda_{i,j}}{\lambda_i}$ denote the fraction of packets transmitted by source S_i to mix M_j. We assume that given Λ_i, each

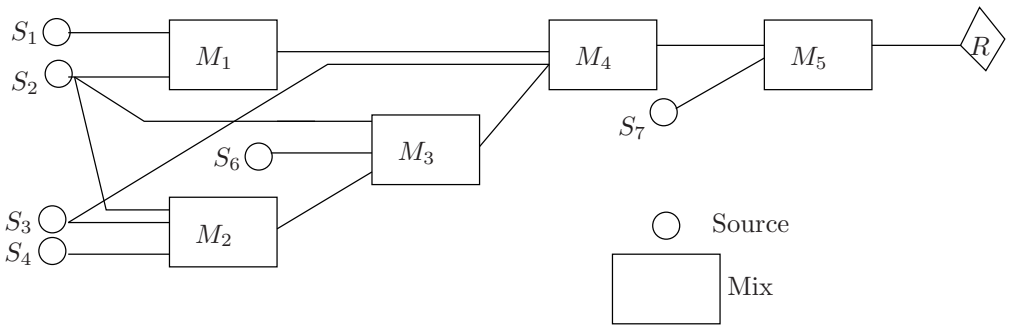


Figure 17: A Single Destination Mix Network with Multipath:$E_s = \{(S_1, M_1), (S_1, M_2), (S_1, M_3), (S_2, M_1), (S_3, M_2), (S_4, M_2), (S_4, M_4), (S_5, M_3), (S_6, M_3), (S_7, M_5)\}$, $E_m = \{(M_1, M_4), (M_2, M_3), M_3, M_4), (M_4, M_5)\}$.

individual process $\mathcal{X}_{S_i,M_j}$ is an independent Poisson process with rate $\lambda_{i,j}$.

Theorem 3 *In a single destination mix network with multipath $\mathcal{M} = (G, \mathcal{B}, \lambda)$ let $\mathcal{M}_j = (G_j, \Lambda_j, B_j)$ denote a sub-network containing only mix M_j with buffer size k_j and the number of sources equal to the number of incoming links of mix M_j in $\mathcal{M}$, where each source in $\mathcal{M}_j$ transmits according to an independent Poisson process with a rate equal to the net arrival rate on the corresponding incoming link in $\mathcal{M}$. Let ψ_j denote the strategy used by mix M_j in the sub network $\mathcal{M}_j$. Then, there exists a set of strategies $\psi \in \Psi(\mathcal{M})$ such that:*

$$A^{\psi}(\mathcal{M}) \geq \sum_{j=1}^{m} \frac{\lambda^j}{\lambda} A^{\psi_j}(\mathcal{M}_j) + \sum_{i=1}^{u} \frac{\lambda_i}{\lambda} \left(\sum_{j=1}^{m} p_{i,j} \log p_{i,j} \right) \tag{22}$$

where λ^j is the total arrival rate in the sub-network $\mathcal{M}_j$, λ_i is the net arrival rate from source S_i and λ is the total arrival rate to the network $\mathcal{M}$.

Proof: Note that the key difference between the single path and multi path systems is the negative entropy term corresponding to the splitting of traffic by the sources. The key idea driving the multipath result is in viewing the anonymity in two stages: in the first stage the sources split their traffic into multiple streams depending on the specified topology, in the second stage the network of mixes shuffle the packets assuming each split stream arrives from a different source (see Figure 18). Specifically, the mixes assume that every incoming link corresponds to a different source, and performs the shuffling actions. The achieved anonymity with respect to this set of artificial sources in the inner system of Figure 18 is given by (17) in Theorem 2. By bounding the difference between the entropy of the actual sources and artificial sources, the result is proved.

Specifically, consider a modified network $\mathcal{M}'$ where each incoming link from a source in network $\mathcal{M}$ corresponds to a different source, albeit artificial. For a given realization of arrivals denote

by $\mathbf{X} = X_1, \cdots, X_n$, let $Y'_1, \cdots, Y'_n$ be the random variables that denote the artificial sources of departing packets in $\mathcal{M}'$. Using Theorem 2, we know that there exists a set of strategies ψ such that

$$\liminf_{n\to\infty} \frac{H^{\psi}(Y'_1, \cdots, Y'_n|\mathbf{X})}{n} = \sum_{j=1}^{m} \frac{\lambda^j}{\lambda} A^{\psi_j}(\mathcal{M}_j). \tag{23}$$

Let $Y_1, \cdots, Y_n$ be the random variables that denote the actual sources of departing packts from the mix M_m in $\mathcal{M}$. Assuming the mixes in $\mathcal{M}'$ behave identically to that in $\mathcal{M}$, for an identical realization of arrival processes, we can write:

$$\begin{aligned} H^{\psi}(Y_1, \cdots, Y_n|\mathbf{X}) &= H^{\psi}(Y'_1, \cdots, Y'_n|\mathbf{X}) + H^{\psi}(Y_1, \cdots, Y_n|Y'_1, \cdots, Y'_n, \mathbf{X}) && (24) \\ &\quad - H^{\psi}(Y'_1, \cdots, Y'_n|Y_1, \cdots, Y_n, \mathbf{X}) && (25) \end{aligned}$$

Since each artificial source corresponds to a unique original source, for a fixed known realization,

$$H^{\psi}(Y_1, \cdots, Y_n|Y'_1, \cdots, Y'_n) = 0. \tag{26}$$

In any large window of observation, where $n >> \sum_i k_i$, let N_i denote the number of packets that arrived from source S_i and $N_{i,j}$ be the number of departing packets that were transmitted by source S_i directly to mix M_j on edge (S_i, M_j) (alternatively the number of packets the corresponding artificial source transmitted to mix M_j), then if $N_i >> \sum_i k_i$,

$$|\mathbb{E}(N_{i,j}|N_i) - np_{i,j}| \leq \sum_i k_i \tag{27}$$

regardless of the mixing strategies utilized. If the condition in (27) were not satisfied then the probability of buffer overflow will be non zero which is unacceptable. Although $N_{i,j}$ is not explicitly known to the eavesdropper, when $n >> \sum_i k_i$, the number of packets stored in the buffer is negligible compared to the number of transmitted packets. In other words, as $n \to \infty$,

$$\frac{N_{i,j}}{n} \to p_{i,j} \text{ a.s.}$$

Consequently, we can assume that the eavesdropper is perfectly aware of how many packets among the departing packets belong to each artificial source; it is the permutation of packets from multiple sources that provides the uncertainty in $H^{\psi}(Y'_1, \cdots, Y'_n|Y_1, \cdots, Y_n, \mathbf{X})$.

Consider the conditional entropy $H(Y'_1, \cdots, Y'_n|Y_1, \cdots, Y_n, \mathbf{X})$. This is the uncertainty in arti-

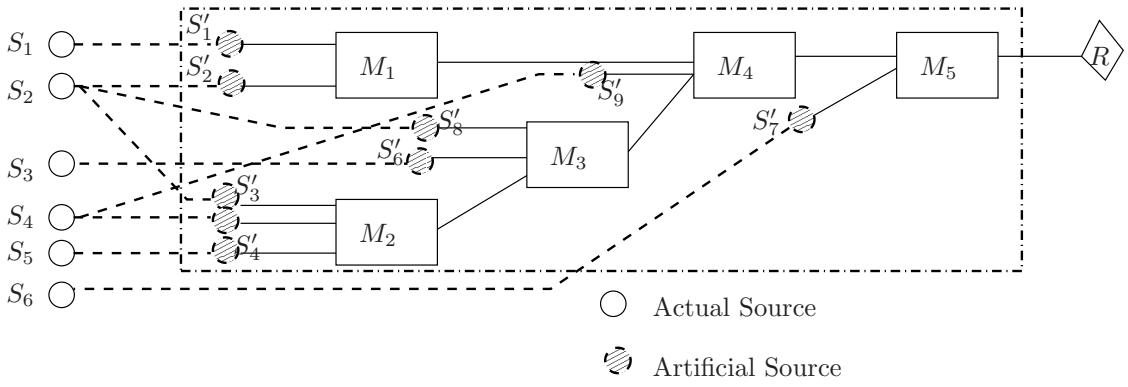


Figure 18: Two Stage Analysis of Single Destination Network with Multipath

ficial sources of departing packets, given that the original sources of departing packets are known. Since each artificial source corresponds to a unique original source, the knowledge of $Y_1, \cdots, Y_n$ can be used to divide the departing packets into mutually exclusive sets $\mathcal{I}_1, \cdots, \mathcal{I}_s$, where

$$j \in \mathcal{I}_i \text{ iff } Y_j = i$$

Since conditioning reduces entropy, and given $\mathbf{X}$, Eve's normalized uncertainty (divided by n) about the variables $N_i, \{N_{i,j}\}$ is vanishing as $n \to \infty$

$$H(Y'_1, \cdots, Y'_n | Y_1, \cdots, Y_n, \mathbf{X}) \leq \sum_{i=1}^{s} H^{\psi}(\{Y'_j, j \in \mathcal{I}_i\} | N_i, \{N_{i,j}\}) \tag{28}$$

Given $N_i, \{N_{i,j}\}$, the entropy $H^{\psi}(\{Y'_j, j \in \mathcal{I}_i\} | N_i, \{N_{i,j}\})$ is upper bounded by the logarithm of possible permutation of packets, ie

$$H^{\psi}(\{Y'_j, j \in \mathcal{I}_i\} | N_i, \{N_{i,j}, \mathbf{X}\}) \leq \log \left(\frac{N_i!}{N_{i,1}! N_{i,2}! \cdots N_{i,m}!} \right)$$

Since for large N_i, we can write $\mathbb{E}(N_{i,j}|N_i) = N_i p_{i,j} + O(1)$, from Stirling's bound [66] and the log-concavity of the multinomial coefficient, we can write:

$$\mathbb{E}(H^{\psi}(\{Y'_j, j \in \mathcal{I}_i\} | N_i, \{N_{i,j}\}) | N_i) \leq -N_i \sum_{j=1}^{m} p_{i,j} \log p_{i,j} + O(1). \tag{29}$$

Combining (23)-(29)and using the fact that $\frac{\mathbb{E}(N_i)}{n} = \frac{\lambda_i}{\lambda}$ the result in (22) follows. □.

3.4 Asymptotic Anonymity: Rate of Convergence

In any network, the achievable entropy rate of sources of departing packets cannot exceed the prior entropy rate of the arrival processes owing to the finite buffer size restriction. For instance, if in a single mix system $\mathcal{M}_1$ with buffer size k, the arrival rates are given by $\lambda_1, \cdots, \lambda_u$, then for any mixing strategy ψ

$$A^{\psi}(\mathcal{M}_1) \leq -\sum_{j=1}^{u} \frac{\lambda_i}{\lambda} \log\left(\frac{\lambda_i}{\lambda}\right) \tag{30}$$

where $\lambda = \sum_i \lambda_i$. A simple argument for this inequality is as follows. As the number of arrivals $n \to \infty$, since the buffer size is fixed, the uncertainty in the composition of the departing packets from Eve's perspective which does not scale with n goes to zero. Given the composition, the uncertainty in the sources of departing packets arises only from the permutation of packets which is upper bounded by the logarithm of the multinomial coefficient which in turn converges to the entropy in (30) as $n \to \infty$. A rigorous proof formalizing this argument is provided as part of the convergence rate analysis.

For the single mix system, let $\psi(k), k = 1, 2, \cdots$, denote a sequence of strategies that varies with the buffer size k of the mix. The sequence of strategies is asymptotically optimal for the single mix system if:

$$\lim_{k\to\infty} A^{\psi(k)}(\mathcal{M}_1) = -\sum_{j=1}^{u} \frac{\lambda_i}{\lambda} \log\left(\frac{\lambda_i}{\lambda}\right)$$

That such a sequence of strategies exists for any single mix system is not difficult to prove. Indeed the proportional method of scheduling studied in [67], demonstrates that this limit is achievable asymptotically in the buffer size, with a rate of convergence $O(1/\sqrt{k})$. For a two user equal rate system, we know from Theorem 1 that this limit is achievable in a two user equal rate system with a better convergence rate $O(\frac{1}{k^2})$. The focus of this and the subsequent section is to study the optimal convergence rate in general multiuser systems. Prior to that, we note an important corollary of Theorems 2 and 3, wherein if each mix in a network utilizes an asymptotically optimal sequence of strategies, then the anonymity of the network as the total buffer size (keeping the relative proportions constant) increases converges to the prior entropy of the arrival processes to the network. Therefore, as long as we demonstrate the convergence properties of a single mix system, the extension to a network of mixes will automatically follow.

3.5 Lower Bound on Rate of Convergence

As observed in (16), the optimal convergence rate of anonymity with buffer size in a two user equal rate system is $O(\frac{1}{k^2})$. In the following theorem, we prove that in any multiuser system with unequal arrival rates, the convergence rate of the anonymity of a Chaum mix is no better than $(\frac{1}{k^2})$.

Theorem 4 *For a single mix system $\mathcal{M}_1$ serving u users with arrival rates $\lambda_1, \cdots, \lambda_s$, the anonymity achievable by any strategy ψ is upper bounded as*

$$A^{\psi}(\mathcal{M}_1) \leq h_u(q_1, \ldots, q_u) - \Omega\left(\frac{1}{k^2}\right)$$

where $q_i = \frac{\lambda_i}{\sum_i \lambda_i}$ $\forall$ $i = 1, \ldots, u$ and h_u is the $u-$ary entropy function

$$h_s(q_1, \cdots, q_u) = -\sum_{i=1}^{u} q_i \log_2 q_i$$

Proof: We will first prove the result for a general two user system with arrival rates in the ratio $q : 1-q$. We then provide an argument to show that the convergence rate for the multiuser system can be no better than that for a two user system.

Without loss in generality let $q \leq 1-q$. The argument in the proof of Theorem 1 reformulates the optimization problem as a Markov Decision Process with a continuous action space, and using the lemma from [65], the optimal mixing strategy in a two user system was shown to be stationary. Consequently, for the optimal strategy, the state of the system also follows a stationary distribution. Since the sources of outgoing packets are deterministic functions of the state and input, once the system has attained stationarity, the distribution of sources of outgoing packets will also be stationary. In this stationary regime, let random variable S denote the state at a time point of interest. Let random variables $Y_1, \cdots, Y_n$ denote the sources of n consecutive outgoing packets immediately following this time point, and $X_1, \cdots, X_n$ denote the sources of incoming packets that triggered these departures. The anonymity achieved by the optimal strategy ψ^* can be written in the form:

$$\mathcal{A}(\mathcal{M}_1) = \frac{\mathbb{E}(H_{\psi^*}(Y_1, \cdots, Y_n | S, X_1, \cdots, X_n)))}{n}$$

for any strictly positive n. For the purpose of this proof, we use a light abuse of notation wherein we let Y_i denote binary random variables wherein $Y_i = 0$ denotes a packet from source S_1 and $Y_i = 1$ denote a packet from source S_2. We let $n = 4Ck^2$, where C is a large constant. Since the mix can

hold at most k packets in its buffer, the stationary distribution of the random variable:

$$W = \sum_{i=1}^{4Ck^2} Y_i$$

should necessarily have mean $\mathbb{E}(W) = 4Ck^2q$. We further note that given the observed sources of incoming packets $X_1, \cdots, X_{Ck^2}$,

$$|W - \sum_{i=1}^{4Ck^2} X_i| \leq k$$

Therefore, $H(W|X_1, \cdots, X_{4Ck^2}) \leq \log(2k)$. Then

$$\begin{aligned}
\mathcal{A}^{\psi}(\mathcal{M}_1) &= \frac{\mathbb{E}(H_{\psi^*}(Y_1, \cdots, Y_{4Ck^2}|S, X_1, \cdots, X_{4Ck^2})))}{4Ck^2} \\
&= \frac{\mathbb{E}(H_{\psi^*}(Y_1, \cdots, Y_{4Ck^2}, W|S, X_1, \cdots, X_{4Ck^2})))}{4Ck^2} \\
&= \frac{\mathbb{E}(H_{\psi^*}(W|S, X_1, \cdots, X_{4Ck^2})))}{4Ck^2} + \frac{\mathbb{E}(H_{\psi^*}(Y_1, \cdots, Y_{4Ck^2}|W, S, X_1, \cdots, X_{4Ck^2})))}{4Ck^2} \\
&\leq \frac{\log(2k)}{4Ck^2} + \frac{\mathbb{E}(H_{\psi^*}(Y_1, \cdots, Y_{4Ck^2}|W)}{4Ck^2} \qquad (31)
\end{aligned}$$

The term $(H(Y_1, \cdots, Y_{4Ck^2}|W))$ is the entropy of the random binary sequence conditioned on its sum which is upper bounded as:

$$H(Y_1, \cdots, Y_{4Ck^2}|W) \leq \log \binom{4Ck^2}{W}$$

Therefore:

$$\begin{aligned}
A^{\psi}(\mathcal{M}_1) &\leq \frac{\log(2k)}{4Ck^2} + \frac{\mathbb{E}(\log \binom{4Ck^2}{W}}{4Ck^2} \\
&\leq \frac{\log(2k)}{4Ck^2} + \sup_{p(W):\mathbb{E}(W)=4Ck^2q} \frac{\mathbb{E}(\log \binom{4Ck^2}{W}}{4Ck^2}
\end{aligned}$$

which due to log-concavity of $\binom{n}{k}$ for a fixed n

$$A^{\psi}(\mathcal{M}_1) \leq \frac{\log(2k)}{4Ck^2} + \frac{\log \binom{4Ck^2}{\lceil 4Ck^2q \rceil}}{4Ck^2} \qquad (32)$$

From Sterling's inequality we know that for large n and m such that $n >> m$

$$\log \binom{n}{m} \leq nh_2(m/n) - \frac{1}{2}\log(n) + O(1) \qquad (33)$$

For C large enough, combining (31)-(33), the upper bound is proved for the general two user system.

We now present the argument for the general multiuser system with arrival rates in the proportion $q_1 : q_2 : \cdots : q_u$. Without loss of generality we assume $q_1 \leq \sum_{i \neq 1} q_i$. Let Z_i denote the indicator random variable (from Eve's perspective) that determines weather i^{th} departure belongs to source S_1 or not. Specifically,

$$Z_i = \begin{cases} 1 & Y_i = 1 \\ 0 & Y_i \neq 1 \end{cases} \tag{34}$$

Since Z_i is a deterministic function of Y_i,

$$H(Y_1, \cdots, Y_n|\mathbf{X}) \quad = \quad H(Z_1, \cdots, Z_n|\mathbf{X}) + H(Y_1, \cdots, Y_n|Z_1, \cdots, Z_n, \mathbf{X}) \tag{35}$$

Given the variables $Z_1, \cdots, Z_n$, the variables $Y_1, \cdots, Y_n$ can be split into two mutually exclusive sets defined by index sets $\mathcal{I}_1$ and $\mathcal{I}_2$, where

$$\forall j \in \{1, \cdots, n\}, \quad j \in \mathcal{I}_1 \text{ iff } Y_j = Z_j = 1 \text{ else } j \in \mathcal{I}_2.$$

Therefore, we can write

$$H(Y_1, \cdots, Y_n|Z_1, \cdots, Z_n, \mathbf{X}) = H(\{Y_i, i \in \mathcal{I}_2\}|Z_1, \cdots, Z_n, \mathbf{X})$$

which using arguments similar to the proof of Theorem 2 is upper bounded by the entropy achievable in a $u-1$ user system with arrival rates $\lambda_2, \cdots, \lambda_u$, and is consequently upper bounded using the prior entropy of arrival probabilities as:

$$\frac{H(\{Y_i, i \in \mathcal{I}_2\}|Z_1, \cdots, Z_n, \mathbf{X})}{|\mathcal{I}_2|} \leq h_2\left(\frac{q_2}{1-q_1}, \ldots, \frac{q_s}{1-q_1}\right) \tag{36}$$

Using the two user analysis in (31)-(33), we know that

$$\lim_{n \to \infty} \frac{H(Z_1, \cdots, Z_n|\mathbf{X})}{n} \leq h_2(q_1) - \Omega(1/k^2) \tag{37}$$

Combining (35)-(37), and using the independent Poisson assumption to show that

$$\lim_{n \to \infty} \frac{|\mathcal{I}_2|}{n} = 1 - q_1$$

the theorem is proved. □

3.6 Upper Bound on the Convergence Rate

Thus far, we have shown that for a two source equal rate mix, the maximum achievable anonymity as a function of the buffer size is given by:

$$\mathcal{A}(k) = 1 + \log\left(\cos\left(\frac{\pi}{k+3}\right)\right) = 1 - O(\frac{1}{k^2})$$

In combination with Theorem 3, we can prove that this convergence rate is achievable for a range of multiuser systems. In particular, consider a binary tree single destination network as shown in Figure 19 where all mixes have equal buffer size k. In this network, each one of the $u = 2^n$ sources transmits at an equal arrival rate, and each mix utilizes the optimal mixing strategy that achieves the maximum anonymity characterized in Theorem 1. Since all arrival rates are equal, the incoming links to any mix must have equal arrival rates. Using Theorems 1 and 2, we know that the anonymity of the system is given by:

$$A^{\psi}(\mathcal{M}) = n\log\left(2\cos\left(\frac{\pi}{k+3}\right)\right) = \log(u) - O(\frac{1}{k^2}) \tag{38}$$

Consider a single mix system $\mathcal{M}_1$ with arrival rates $\lambda_1, \cdots, \lambda_u$ such that $\exists n, n_1, \cdots, n_u \in \mathcal{Z}^+$ and:

$$\frac{\lambda_i}{\sum \lambda_i} = \frac{n_i}{2^n} \forall i \tag{39}$$

If the mix divided its buffer into $2^n - 1$ equal parts, and simulated a binary tree network of mixes (as in Figure 19) with 2^n artificial sources, then using Theorem 3 and (38) above, the anonymity achieved is lower bounded as:

$$A(\mathcal{M}_1) \geq -\sum_{i=1}^{u} \frac{n_i}{2^n}\log\frac{n_i}{2^n} - O(\frac{2^{n-1}}{k^2})$$

Since n is a constant independent of the buffer size, the system exhibits optimal convergence rate as $k \to \infty$.

We do note that although the closure of the set of rates that satisfy the condition in (39), it is a countable set. This is a consequence of the closed form expression for maximum anonymity being available only for the two user equal arrival rate system. We believe that the convergence rate should hold true for any proportion of arrival rates, but the proof remains elusive.

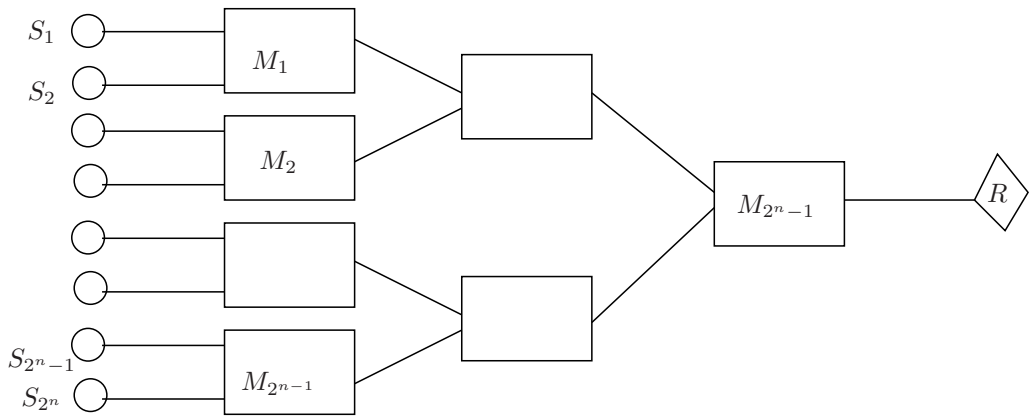


Figure 19: Binary Tree Mix Network: All sources transmit at equal rates

3.7 Summary

One of the key contributions in this work is the theoretical model for anonymous communication in networks under memory restrictions. To the best of our knowledge, this is the first comprehensive analysis of buffer constrained anonymous systems. Based on the metric, we designed scheduling and relaying strategies to maximize anonymity in arbitrary single destination networks of mixes. The general quantitative framework we have used can be adapted to study anonymity under other resource restrictions such as bandwidth, processing power etc and QoS constraints such as delay and fairness. Although source anonymity is the focus of this article, the theory and results can be extended to source-destination anonymity, by considering multi-destination systems. Note that the adversary is considered to be omniscient here; from a practical standpoint, this is quite conservative. Nevertheless, the anonymity achievable in real situations would only be better than the guaranteed results in this model.

4 Packet based Anonymity of Mixes under the constraint of Fairness

In this chapter, using the framework developed in the previous chapter for buffer constraint mixes, we study the anonymity of mixes under three fairness paradigms : First Come First Serve (FCFS), Fair Queuing (FQ) and Proportional Method (PM). FCFS and FQ have widespread use in packet switched data networks, the former because it satisfies an intuitive notion of fairness, and the latter owing to its application in congestion control. PM, on the contrary, is an unpopular method for scheduling because it may cause users with less demands to suffer disproportionately high delay, but in comparison to FCFS and FQ, PM has an inherent randomness in the scheduling policies which makes it amenable to anonymous communication. In the next section, we explain these fair scheduling policies in details and define a measure to quantify their fairness.

4.1 Fair Scheduling Algorithms and Temporal Fairness Measure

It is important to note here that, although, there have been many different measures of fairness proposed, most in the context of resource allocation for varying user demands [68–70], the notion of fairness considered in this work arises not due to allocation of resources such as bandwidth or memory, but due to the out-of-order transmissions and the resulting violation of *temporal fairness*. Since the randomized shuffling of packets prior to transmission is critical to any anonymous scheduling, our focus in this chapter is to understand and quantify how different fair scheduling policies fare when trading temporal fairness for anonymity. In particular, we shall focus on the anonymity achieved through a single mix, and the resulting relationship with temporal fairness. For this specific purpose, we compare the maximum anonymity achievable by the class of schedules adhering to a relaxed FCFS, Fair Queuing and the Proportional Method paradigms respectively. Although these fair scheduling methodologies achieve inherently different notions of fairness, we will compare them by defining a common measure of fairness, referred to as the Temporal Fairness Index (TFI), a quantity that measures the degree of *out-of-order* transmissions.

4.1.1 FCFS

FCFS satisfies the intuitive notion of temporal fairness *i.e.* a packet that arrived earlier deserves to be transmitted earlier. FCFS is a deterministic scheduling policy and consequently, provides no anonymity. We, therefore, consider a relaxation of FCFS that allows limited swapping of packets

from different users and show in section 4.2 that a slight relaxation can result in a significant increase in anonymity.

4.1.2 Fair Queuing

The Fair Queuing paradigm satisfies an important notion of fairness called max-min fairness. Max-min fairness requires maximizing the share of the user receiving the lowest fraction of a resource, thereafter, maximizing the share of the user receiving the second lowest fraction of the resource, and so forth.

The FQ algorithm is the emulation of a hypothetically fair scheme called Processor Sharing (PS) [16]. Under the processor sharing scheme, a server simultaneously processes the request of u users at a rate of $1/u$. In many shared routers, at most one packet can be transmitted at any given time, rendering the PS scheme impractical. In this respect, the FQ algorithm proposed in [17] is viewed as the implementable counterpart of PS, wherein a packet which has the least finishing time (time at which the packet is completely processed) in the corresponding PS scheme is chosen for serving. When packets from all users require equal service time, which is the case in mix networks, the algorithm reduces to serving each packet in a round robin fashion.

As will be shown in Section 4.3, the inherent anonymity of FQ lies far below from the maximum possible anonymity even for a mix with infinite buffer capacity. We, therefore, propose a relaxation of FQ that expands the window of fairness measurement of the round robin scheme, and show that any desirable anonymity can be achieved by a sufficient relaxation of the fairness window.

4.1.3 The Proportional Method

The Proportional Method paradigm distributes resources among users proportional to their demands *i.e.* if i^{th} user demands x_i units of a resource, then a single unit of the resource is served to user i with probability $\frac{x_i}{\sum_i x_i}$. The PM uniquely satisfies the equity and consistency criteria of fairness described in [18].

It is easy to see that under the PM, users with lesser demands face disproportionately high delays because packets of users with high demands are preferred more often. Although this shortcoming has rendered the policy unpopular in data networks, Our analysis in Sections 4.4 and 5.7 shows that the PM asymptotically achieves maximum possible anonymity without any relaxation and offers the best tradeoff between anonymity and temporal fairness amongst the three paradigms.

4.1.4 Temporal Fairness Measure

The algorithms considered achieve philosophically different notions of fairness. However, from the point of view of anonymity, the tradeoff is one of sacrificing temporal fairness (through out-of-order transmissions) for anonymity from timing analysis. To that extent, we measure temporal fairness using the average degree of out-of-order transmissions. In particular, each departing packet carries a *fairness state* which equals the number of packets from other sources that departed prior to the packet despite arriving after it. The fairness measure of the protocol is given by the temporal average of fairness states across all departing packets. Since this metric quantifies the degree of out-of-order transmissions, a higher value implies a greater violation of temporal fairness and consequently, lower fairness.

Temporal Fairness-index (TFI) of the scheduling policy Ω: Let the i^{th} departing packet belong to source S_i. Let random variable $\zeta(i)$ denote the number of packets that arrived after this packet from a source different from S_i, but departed prior to it as per the scheduling policy ψ. Then, the Temporal Fairness-index of the scheduling policy is defined as

$$\mathrm{TFI}(\psi) = \liminf_{N\to\infty} \frac{\sum_{i=1}^{N} \mathbb{E}_{\psi}[\zeta(i)]}{N} \tag{40}$$

where $\mathbb{E}_{\psi}[\cdot]$ represent the expectation operator in the probability space determined by the arrival process and scheduling policy ψ.

In subsequent sections, we shall quantify the achievable anonymity of the three scheduling policies and compare the resulting tradeoffs with their respective temporal fairness indices.

4.2 Anonymity of relaxed FCFS

Classical FCFS, by virtue of its determinism, renders the mix incapable of providing any anonymity. We propose the following *relaxation* of the temporal fairness of FCFS; for any given packet that arrived from a particular source, at most $\eta - 1$ packets that arrived from other sources can be transmitted prior to the given packet despite arriving after it. We refer to this relaxation as $\eta-$**fair FCFS**, and all scheduling policies that satisfy this relaxed criteria are said to belong to the $\eta-$fair FCFS class of scheduling policies. The classical FCFS scheduling policy does not allow any packet to be transmitted out of order and is the unique $1-$fair policy. The definition of the TFI in the previous section can be viewed as the average version of the $\eta-$fairness notion defined here. Indeed,

any policy belonging to the $\eta-$fair FCFS class will have a TFI less than or equal to $\eta - 1$.

We are interested in the $\eta-$fair FCFS policy that achieves maximum anonymity. In that regard, let $\mathcal{A}^{\text{FCFS}}(\eta, k)$ be the supremum of anonymity achieved by the scheduling policies belonging to the $\eta-$fair FCFS class for a mix with buffer capacity k receiving packets from two users at equal rates. In the forthcoming discussion, for ease of exposition, we will refer to packets from the sources as being red and blue respectively.

To understand how this relaxation provides anonymity, consider a simple scenario, where the mix's buffer can hold at most 1 packet and the mix is allowed to transmit packets under the 2-fair FCFS criterion, *i.e.* for a given arrival from a user, at most one packet from an alternate user can be transmitted ahead of the given packet despite arriving after it. This is the minimum possible relaxation of the FCFS fairness constraint. In this scenario, if a blue packet arrives to an empty buffer, the mix can choose to transmit it or wait until a second packet arrives. If the second packet also happens to be a blue packet, the mix has no choice but to transmit the first packet (so that the new arrival can be stored in the buffer). In this case there is no uncertainty in the source of the departing packet. If, however, the second packet happens to be a red packet, the mix has a choice to either transmit the red packet ahead of the blue (thus exercising the fairness relaxation), or transmit the blue and store the new red arrival in its buffer. If the mix makes this choice probabilistically, then uncertainty is created about the source of the departing packet from Eve's perspective. Under the $2-$fair requirement, the fairness relaxation can be exercised at most once for a given packet: For instance, in this example, if the red packet was transmitted ahead of the blue, then the mix can no longer transmit other packets ahead of the blue packet. The mix has to necessarily transmit the blue packet before restarting the decision making process. Characterizing the optimal probabilities of transmission is the key to evaluating the maximum anonymity of an $\eta-$fair FCFS policy.

In the context of privacy in stochastic systems, this optimization presents an important challenge since eavesdroppers have access to the complete time window extending into the future to determine the source information of a particular packet. Mathematically, the conditioning variables in the definition of anonymity in (2) extend across the infinite time horizon, and is *non-causal*. The key to resolving this challenge lies in a reduction of the policy domain into a class of strategies where packets are transmitted by the mix only upon a new arrival to a full buffer. That this reduction does not lose generality relies on the fact that no idling or delay constraints are imposed on the mix. Consequently, any decision made by the mix at a time when the buffer is not full can be delayed to the arrival time of a new packet to a full buffer without reducing anonymity. This reduction ensures that the current and future departure times conditioned on the entire arrival process are

uncorrelated, and the non-causality of the anonymity definition is removed. Additionally, when the memory of a mix is limited, it is sufficient for Eve to know the sequence of arriving packets in place of the complete timing information of the arrival point process; packets necessarily wait in the buffer until the next packet arrives regardless of what time it arrives, so given the source of next arrival, the actual timing is irrelevant, and the system reduces to a discrete event model. Under this discrete event model, the optimization for a general $\eta-$fair system can be derived using a dynamic programming model which is described in the following theorem.

Theorem 5 *Let* $s = \begin{bmatrix} b_1 & b_2 & \cdots & b_{k+1} \\ f_1 & f_2 & \cdots & f_{k+1} \end{bmatrix} \in \mathcal{S}$ *where* $\mathcal{S} = \{R, B\}^{k+1} \times \{0, \cdots, \eta - 1\}^{k+1}$. *Let*

$$\begin{aligned}
s_R^R(s) &= \begin{bmatrix} R & b_1 & b_2 & \cdots & b_{i_R-1} & b_{i_R+1} & \cdots & b_{k+1} \\ 0 & f_1 & f_2 & \cdots & f_{i_R-1} & f_{i_R+1} & \cdots & f_{k+1} \end{bmatrix} \\
s_B^R(s) &= \begin{bmatrix} B & b_1 & b_2 & \cdots & b_{i_R-1} & b_{i_R+1} & \cdots & b_{k+1} \\ 0 & f_1 & f_2 & \cdots & f_{i_R-1} & f_{i_R+1} & \cdots & f_{k+1} \end{bmatrix} \\
s_R^B(s) &= \begin{bmatrix} R & b_1 & b_2 & \cdots & b_{i_B-1} & b_{i_B+1} & \cdots & b_{k+1} \\ 0 & f_1 & f_2 & \cdots & f_{i_B-1} & f_{i_B+1} & \cdots & f_{k+1} \end{bmatrix} \\
s_B^B(s) &= \begin{bmatrix} B & b_0 & b_1 & \cdots & b_{i_B-1} & b_{i_B+1} & \cdots & b_{k+1} \\ 0 & f_1 & f_2 & \cdots & f_{i_B-1} & f_{i_B+1} & \cdots & f_{k+1} \end{bmatrix}
\end{aligned}$$

when $i_R(s) = \max_i\{s(1,i) = R\} \in \{1, 2, \ldots, k+1\}$ *and/or* $i_B(s) = \max_i\{s(1,i) = B\} \in \{1, 2, \ldots, k+1\}$.

Then, the maximum anonymity achievable by a strict $\eta-$fair policy using a mix of buffer size k is given by

$$\mathcal{A}^{FCFS}(\eta, k) = \log c$$

where c is the solution to the set of recurrence relations:

$$\psi(s) = 1 \text{ if } s = \begin{bmatrix} B & B & \cdots & B \\ 0 & 0 & \cdots & 0 \end{bmatrix} \tag{41}$$

$$\forall s,\ \psi^2(s)c = \begin{cases} \psi(s_R^R(s))\psi(s_B^R(s)) & s(1,j) = R \forall j \text{ or } f_{i_R} = \eta - 1 \\ \psi(s_R^B(s))\psi(s_B^B(s)) & s(1,j) = B \forall j \text{ or } f_{i_B} = \eta - 1 \\ \psi(s_R^R(s))\psi(s_B^R(s)) + \psi(s_R^B(s))\psi(s_B^B(s)) & o.w. \end{cases} \tag{42}$$

The above theorem expresses the maximum anonymity achievable by a strict $\eta-$fair FCFS policy

as a solution to a series of recurrence relations. These recurrence relations are in fact a reduction of a dynamic program based on an infinite horizon average reward Markov Decision Process. Although, it is not possible to characterize the maximum achievable anonymity as a function of η and k in closed form, it is numerically straightforward to compute. In fact, each of the equations in (42) is a solution to the maximization in the original dynamic program and can be viewed as a step in value iteration [65] with variables on the LHS of the equation being the new iterate computed using previous iterates on the RHS.

Proof of Theorem 5: As argued earlier, since no idling constraints are imposed on the mix and it is sufficient for the mix to make decisions to transmit a packet only when a new packet arrives to a full buffer. We then rewrite the system using a discrete event model, wherein the time $n \in \mathbb{N}$ corresponds to the the n^{th} arrival point in the joint arrival process. Let $X_1^n = \{X_1, \cdots, X_n\}$ be the sequence of random variables representing the sources of arriving packets. Let $X_i = 1$ denote a red arrival and $X_i = 0$ denote a blue arrival. Likewise $Y_1^n = \{Y_1, \cdots, Y_n\}$ is the sequence of random variables from Eve's perspective denoting the sources of outgoing packets. Eve perfectly observes $X_1, \cdots, X_n$ and using the knowledge of the mixing strategy wishes to determine the sequence $Y_1, \cdots, Y_n$.

Analyzing the discrete event model requires defining the state space of the mix upon every new arrival. At time n, the complete contents of the mix's buffer **including the new arrival** contribute to the state of the discrete event system. Specifically, we define the state of the system to be the time ordered sequence of sources of packets in the buffer and the respective *fairness states* of the packets. The fairness state of a particular packet in the buffer refers to the number of packets from other sources that have departed the mix despite having arrived after that packet. In other words, the fairness state of a packet refers to the number of times the fairness relaxation has been exercised on that packet, which is upper bounded by $\eta - 1$. Every new packet that arrives starts with a fairness state of 0, and as packets that arrive after it depart ahead, the fairness state of the packet increases until it reaches $\eta - 1$ at which point, no packet from any other source can be transmitted until the packet with fairness state $\eta - 1$ departs. Mathematically, we define the state of the system at time t using a matrix $S_t \in \{R, B\}^{k+1} \times \{0, \cdots, \eta - 1\}^{k+1} \triangleq \mathcal{S}$.

Take for instance, a mix with buffer size $k = 3$. If the first four packets belong to sources red, blue, red and blue respectively, then the state of the system upon the arrival of the fourth packet is given by $S_4 = \begin{bmatrix} B & R & B & R \\ 0 & 0 & 0 & 0 \end{bmatrix}$. Note that $S_4(1,4)$ denotes the head of the queue and $S_4(1,1)$ denotes the newest arrival. Since no packets have been transmitted, the fairness states of all packets are 0. If at this time, if the mix transmits a blue packet, then the fairness state of the red packet

at the head of the queue is increased while those of the others remain 0. Consequently, the mix can move into one of two possible states $S_5 = \begin{bmatrix} B & B & R & R \\ 0 & 0 & 0 & 1 \end{bmatrix}$ if the next arrival is a blue packet, or $S_5 = \begin{bmatrix} R & B & R & R \\ 0 & 0 & 0 & 1 \end{bmatrix}$ if the next arrival is a red packet. Designing the probabilities of choosing red or blue packets in each state is the key to optimizing the strategies.

Note that, not all vectors in the domain $\mathcal{S} = \{R, B\}^{k+1} \times \{0, \cdots, \eta - 1\}^{k+1}$ denote valid states. The $\eta-$fairness restriction and the fact that amongst all packets from the same source, the order of departure is necessarily FCFS limits the number of states realized in the domain. As will be seen later, defining a valid state and computing the number of valid states for a given (η, k) pair is not critical to maximizing the anonymity of an η-fair FCFS policy.

The reduction in strategy space ensures that the buffer is full at all times $n > k$, and since no decisions are made by the strategy before time $n = k$, we let S_i to denote the state of the buffer upon arrival of the $(k+i)^{th}$ packet. In this discrete event model, we can rewrite the anonymity for a strategy ψ as defined as

$$
\begin{aligned}
& A^{\psi}(\eta, k) \\
= \quad & \lim_{n\to\infty} \frac{\mathbb{E}[H_{\psi}(Y_1^n | X_1^{n+k+1})}{n} && (43) \\
\overset{(a)}{=} \quad & \lim_{n\to\infty} \frac{\mathbb{E}[H_{\psi}(Y_1 | X_1^{n+k+1})] + \cdots + \mathbb{E}[H_{\psi}(Y_n | Y_1^{n-1}, X_1^{n+k+1})]}{n} \\
\overset{(b)}{\leq} \quad & \lim_{n\to\infty} \frac{\mathbb{E}[H_{\psi}(Y_1 | S_1)] + \cdots + \mathbb{E}[H_{\psi}(Y_n | S_n, Y_1^{n-1})]}{n} \\
\overset{(c)}{\leq} \quad & \lim_{n\to\infty} \frac{\mathbb{E}[H_{\psi}(Y_1 | S_1)] + \cdots + \mathbb{E}[H_{\psi}(Y_n | S_n)]}{n} && (44)
\end{aligned}
$$

(a) follows from the chain rule of entropy.

(b)(c) follow from the fact that conditioning reduces entropy and S_n is completely determined by Y_1^{n-1} and X_1^{n+k+1}.

In the above reduction, note that if a strategy ψ ensures that $Y_n - S_n - (Y_1, \cdots, Y_{n-1}, X_1, \cdots, X_{n+k+1})$ is a Markov chain for every n, then equality is achieved in (b) and (c). Indeed any strategy that does not satisfy this Markov property can be modified to one that does by using the marginal distribution $\Pr\{Y_n | S_n\}$ in making the choice of packet to transmit thus increasing the achieved entropy. Consequently, we only consider those strategies wherein conditioned on the state, the choice of packet

to transmit is independent of past departures. In effect the entropy achieved by such strategies is equal to the sum of expected conditional entropies of outgoing packets at each time as given in (44).

The following observations are true for the discrete event model:

A1. At any state, the subsequent state is perfectly determined by the current state, the current action and the subsequent new arrival.

A2. Conditioned on present state, the action (transmission probability) is independent of the past.

A3. The net reward is expressed as a sum of instantaneous rewards at each state, and the instantaneous reward depends only on the present state and the action.

Since Markov strategies are optimal, and the reward can be expressed as a sum of rewards in every time step, the solution for the optimal $\eta-$fair strategy can be obtained using a Markov Decision Process Optimization over a continuous action space. The Bellman equation resulting from the MDP can be characterized by modeling the state transitions appropriately, and the equation can further be reduced to the recurrence relations in (42) by applying an Entropy Power maximization as shown below.

Let the state S_n of the mix at time step n, be denoted by $S_n = (s(i,j), i \in \{1,2\}$ and $j \in \{1,2,\ldots,k+1\})$ where $\forall j, s(1,j) \in \{B,R\}$ and $\forall j, s(2,j) \in \{0,\cdots,\eta-1\}$. The vector $\{s(1,j)\}$ denotes the time ordered sequence of packets in the buffer ($s(1,k)$ is the source of the earliest arrival and $s(1,1)$ is the source of the latest) , and the vector $\{s(2,j)\}$ denotes their respective fairness states. We categorize the set of states into the following three groups according to the anonymity they are likely to provide:

- Group $\mathcal{C}_1$: $s \in \mathcal{C}_1$ if $\{s(1,j) = B\ \forall j\}$ or $\{s(1,k+1) = B$ and $s(2,k+1) = \eta - 1\}$. In these states, the mix has to transmit a blue packet and given the states no anonymity is achieved.

- Group $\mathcal{C}_2$: $s \in \mathcal{C}_2$ if $\{s(1,j) = R\ \forall j\}$ or $\{s(1,k+1) = R$ and $s(2,k+1) = \eta - 1\}$. In these states, the mix has to transmit a red packet and given the states no anonymity is achieved.

- Group $\mathcal{C}_3$: $s \in \mathcal{C}_3$ if $s \notin \mathcal{C}_1 \bigcup \mathcal{C}_2$. These are the only states where the mix has the freedom to choose between red or blue packets for transmissions. Let the mix choose a red packet to transmit with probability p_s for transmission of red packets when $s \in \mathcal{C}_3$.

From A_1 - A_3, and the expression of instantaneous rewards in (44), we know that the system can be described as an infinite horizon average reward Markov Decision Process. The transition probabilities can be obtained using the transmission probability p_s and the arival probability of a

new packet. Consider the instantaneous reward term in (44) given by $H(Y_i|S_i)$. For states belonging to $\mathcal{C}_1 \bigcup \mathcal{C}_2$, this instantaneous reward is 0. For all other states, this is the entropy of the departing packet which, if state $S_i = s$ is given by:

$$H(Y_i|S_i) = h(p_s). \tag{45}$$

We use the above arguments in the 1.

Since $\phi(s)$ is unique up to an additive constant in the above lemma, we assume that $\phi(s_1) = 0$ when $s_1 = \begin{bmatrix} B & B & \cdots & B \\ 0 & 0 & \cdots & 0 \end{bmatrix}$

Further, the optimality condition in Lemma 1 for our model gives

$$\begin{aligned} \phi(s) + v &= 0.5\phi(s_R^B) + 0.5\phi(s_B^B) \quad s \in \mathcal{C}_1 \\ \phi(s) + v &= 0.5\phi(s_R^R) + 0.5\phi(s_B^R) \quad s \in \mathcal{C}_2 \\ \phi(s) + v &= \max_{p_s} \left\{ h(p_s) + p_s \left(\tfrac{1}{2}\phi(s_R^R) + \tfrac{1}{2}\phi(s_B^R) \right) \right. \\ &\quad \left. + (1 - p_s) \left(\tfrac{1}{2}\phi(s_R^B) + \tfrac{1}{2}\phi(s_B^B) \right) \right\} \quad s \in \mathcal{C}_3 \end{aligned} \tag{46}$$

where $s_R^R, s_B^R, s_R^B,$ and s_B^B are defined in Theorem 5.

The supremum in (46) can be solved using the classical Entropy Power maximization yielding:

$$p_s = \begin{cases} 0 & s \in \mathcal{C}_1 \\ 1 & s \in \mathcal{C}_2 \\ \frac{\psi(s_R^R(s))\psi(s_B^R(s))}{\psi(s_R^R(s))\psi(s_B^R(s)) + \psi(s_R^B(s))\psi(s_B^B(s))} & s \in \mathcal{C}_3 \end{cases}$$

and consequently the recurrence relation

$$\psi^2(s)c = \psi(s_R^B(s))\psi(s_B^B(s)) + \psi(s_B^R(s))\psi(s_R^R(s))) \quad s \in \mathcal{C}_3$$

where $\psi(s) = 2^{0.5\phi(s)}$ and $v = \log c$. □

The use of the Entropy Power maximization to solve the Bellman equation of the dynamic program also provides the anonymity maximizing policy in the class of $\eta-$fair FCFS which is expressed using the probability of transmitting a red packet as a function of state. Specifically, from (46), we get that the probability of transmission of a red packet as a function of the state is given by:

$$p(s) \quad = \quad \begin{cases} 1 \text{ when } s(1,j) = R \forall j \text{ or } f_{i_R} = \eta - 1 \\ 0 \text{ when } s(1,j) = B \forall j \text{ or } f_{i_B} = \eta - 1 \\ \frac{\psi(s_R^R(s))\psi(s_B^R(s))}{\psi(s_R^R(s))\psi(s_B^R(s))+\psi(s_R^B(s))\psi(s_B^B(s))} \text{ o.w.} \end{cases} \tag{47}$$

where $\psi(\cdot)$ is the solution to the recurrence relations in (42).

A special case of this theorem, when $k = 1$, the recurrence relations simplify to:

$$\begin{aligned} \psi(\eta - 1) &= 1 \\ \psi^2(i) &= 1 + \tfrac{\psi(i+1)}{\psi(0)} \quad 0 \leq i \leq \eta - 2 \end{aligned} \tag{48}$$

which is an equation for the Mandelbrot set [71], albeit with different initial conditions. For $\eta = 2$ and $k = 1$, the cubic equation resulting from (48) yields

$$\mathcal{A}_2^{\text{FCFS}}(1) = \log \psi(0) \sim 0.4066.$$

which is the anonymity achievable with minimum possible relaxation of the FCFS fairness criterion and smallest buffer size.

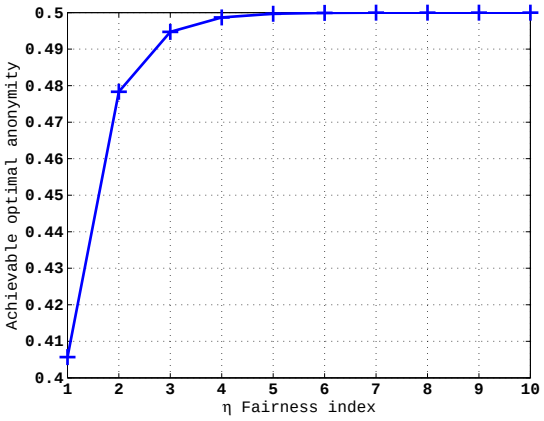
It is important to note that for a fixed buffer size k, the achievable anonymity as fairness relaxation parameter η is increased would converge to the maximum anonymity achievable by a mix with buffer size k and no fairness constraints, which was characterized in Chapter 3 as:

$$\mathcal{A}(k) = \log \left[2 \cos \left(\frac{\pi}{k+3} \right) \right] \tag{49}$$

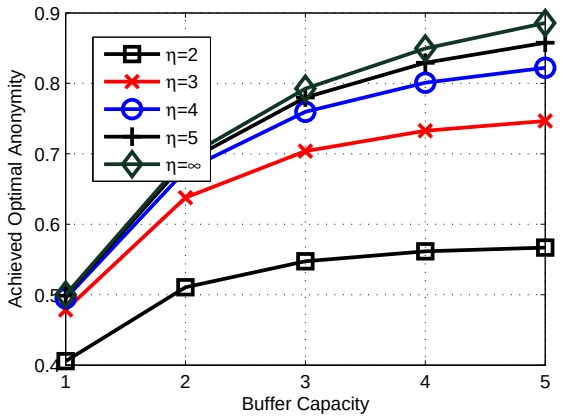
Figure 30a demonstrates this for $k = 1$, where the anonymity as η is increased converges to $\mathcal{A}(1) = 0.5$. We do note that the dimensionality of the state space increases exponentially with buffer size, and polynomially in the fairness parameter η thus making it computationally harder to implement for large buffer sizes.

Figures 30a and 30b plot the anonymity-fairness-buffer relationship for the optimal $\eta-$fair FCFS policies, obtained by solving the recurrence relations numerically. As evidenced from the plots, for slight relaxations on the FCFS fairness criterion, the anonymity increases significantly and for $\eta = 5$, the optimal policy performs close to the unconstrained anonymity ($\eta = \infty$) computed using (49).

Note that the anonymity is plotted as a function of the parameter η which, as argued earlier, is strictly greater than the achieved Temporal Fairness Index defined in (40). The TFI for the $\eta-$fair FCFS is easily computed using the derived optimal policy. Specifically, the optimal policy for the



(a) Anonymity vs η: Buffer Size $k = 1$



(b) Anonymity vs k: $\eta > 1$

Figure 20: Anonymity - Temporal Fairness Tradeoff: $\eta-$Fair FCFS

MDP model of the $\eta-$fair system provides the stationary transition probabilities between the states, which can be used to compute the stationary distribution of states. The TFI for the $\eta-$fair FCFS is then computed as the expected fairness state of the departing packet, where the expectation is over the states and actions. In Section 5.7, we compute the TFI for the $\eta-$fair FCFS numerically and plot the tradeoff between the anonymity and TFI of the $\eta-$fair FCFS in comparison with the respective tradeoffs of the Fair Queuing and the Proportional Method scheduling algorithms.

Based on the arguments described in this section for deriving the optimal $\eta-$fair FCFS policy, it seems conceivable that such a stochastic control approach can be adopted to determine the maximum achievable anonymity as a function of TFI (instead of η); in other words a fundamental tradeoff between temporal fairness and anonymity. Unfortunately, such a model would require a countably infinite state space, since TFI is a temporal average and the fairness state of any individual packet can be indefinitely large with non zero probability, thus making it impractical to compute. The characterization of the fundamental tradeoff between anonymity and temporal fairness remains an open question.

4.3 Anonymity of fair queuing

In a general networking context, the fair queuing algorithm serves packets in decreasing order of their required service times. In anonymous systems based on mix networks, the layered encryption and packet padding ensures that all packets in the outgoing stream of the Mix have identical length, in which case, the FQ algorithm is equivalent to scheduling packets in round robin fashion. The classical round robin implementation needs to be modified in the context of mix networks for two

reasons: First, the mix can store a limited number of packets in its buffer. Second, classical round robin requires packets to be served in a deterministic order, which does not provide any uncertainty from Eve's perspective. In the following, we describe a randomized round robin scheme (referred to as $\psi_{RR}(k)$) for the buffer constrained mix that achieves the desired max-min fairness.

Randomized Round Robin Scheme ($\psi_{RR}(k)$):

The mix's action, under the strategy $\psi_{RR}(k)$, upon the arrival of n^{th} packet is described as follows:

- At any given time, the mix waits until one of two events occur

  E1. At least one packet from each user is present in the buffer: At this time, the mix chooses the respective packet that arrived earliest from each source, reorders them uniformly randomly (equal likelihood across all $u!$ permutations), and transmits them in that order.

  E2. The buffer is full and not all users have packets present in the buffer: At this time, the mix chooses the respective packet that arrived earliest from each user (whose packets are present in the buffer), reorders them uniformly randomly, and transmits them in that order.

According to the strategy, for a two source mix, at any time the buffer of the mix would only hold packets from one user, and uncertainty in the departure is generated only when a packet arrives from the other user and is then shuffled along with a packet present in the buffer and transmitted. This observation is used to evaluate the anonymity of the strategy.

More specifically, evaluation of the anonymity of the relaxed round robin scheme can be accomplished by modeling the system as yet another Markov decision process, and expressing the anonymity as the expected reward per state, which is shown in the following theorem.

Theorem 6 *For a mix with a maximum buffer capacity of k packets, receiving packets from 2 users at rates λ_1 and λ_2 respectively, the anonymity achieved using strategy $\psi_{RR}(k)$ is given by:*

$$\mathcal{A}(k) = \begin{cases} \frac{\sigma(\sigma^{2k}-1)}{(\sigma+1)(\sigma^{2k+1}-1)} & \sigma \neq 1 \\ \frac{k}{2k+1} & \sigma = 1 \end{cases}$$

where $\sigma = \frac{\lambda_1}{\lambda_2}$.

Proof: At any instant t, we model the mix's buffer to be in state $S_t = x_r$ if it contains x_r red packets or in state $S_t = -x_b$ if it contains x_b blue packets. According to the strategy, the state

transitions only when a new packet arrives, at which point, if neither of the two events E_1 or E_2 occurs, the mix merely adds the arrived packet to its buffer. If one of the events occur, the mix transmits one or more packets, thus influencing the state transition. Note that the action and the subsequent state transition only depends on the current state and the subsequent new arrival, thus the state of the mix's buffer evolves as a Markov chain (see Figure 21). Furthermore, the choice of packets to transmit is also dependent only on the state, and is thus a classical MDP policy. At any state, a non zero reward (conditional entropy) is generated only if event E_1 occurs. The expected entropy achieved at each state would give the anonymity of the strategy $\psi_{RR}(k)$.

Prior to characterizing this intuition for quantifying anonymity, we prove a redefinition of the anonymity metric for a class of stationary mixing strategies that is key in proving the theorem.

In the following exposition, it is assumed that the strategy transmits a 'batch' of packets upon every new arrival (the number of packets in a batch could, however, be zero). Since the mix has a finite buffer, every batch would contain a finite number of packets. Let w be the total number of batch sizes that a mix can transmit, and let $l_1, l_2, \cdots, l_w$ denote their respective lengths.

Lemma 2 *Consider a strategy ψ_1 that satisfies the following conditions:*

1. *The strategy is stationary i.e.the probability distribution of system's states defined under strategy ψ_1 converges to a fixed probability distribution.*

2. *The randomness in reordering packets in a batch depends only on the number of packets in that batch independent of past or future actions of the mix. Let $a_1, a_2, \cdots, a_w$ denote the entropy of batches with lengths $l_1, \cdots, l_w$ respectively.*

If L_n is the random variable that represents the length of the batch transmitted upon the n^{th} arrival and $\lim_{n\to\infty} P(L_n = i) \to p_i$, $\forall i = 1, \cdots, k$. where p_is are constant, then anonymity of the strategy ψ_1 is

$$\mathcal{A}_{\psi_1} = \sum_{i=1}^{w} p_i a_i$$

Proof: Let $N_i(n)$ be the random variable that represents the number of batches of length l_i in n transmissions. Also consider a random variable $N_{residue}(n)$ that represents number of packets of the last batch of this n transmissions. The reason behind considering the last batch separately is because the anonymity definition given in (2) is valid for all n, and it is possible that last batch is not completely allotted in the first n transmissions. It is easy to follow from the definition that residual packets in the transmission $N_{residue}(n) < \max_i\{l_i\}$, and the entropy of this partial last batch, $a_{residue} \leq \max_i\{a_i\}$. Therefore, both $N_{residue}$ and $a_{residue}$ are finite.

Using the arguments in the proof of Theorem 5 on the Markov strategy ψ_1,we can express the anonymity as the sum of instantaneous rewards such that $\mathbb{E}[H(Y_1, \cdots, Y_n|\Phi)] = \sum_{i=1}^{k} \mathbb{E}[N_i(n)]a_i + a_{residue}$. But, owing to the stationarity of the strategy ψ_1, $\mathbb{E}[N_i(n)] \to \bar{M}p_i$ as $n \to \infty$, where $\bar{M}$ is the average number of arrivals that are required for the n transmissions. Furthermore, $\frac{\bar{M}}{n} \to 1$ as $n \to \infty$ because $n \leq \bar{M} \leq n + k$. The lower bound follows from the fact that at least n arrivals are required for first n transmissions, and the upper bound is a consequence of the finite buffer size of the Chaum mix which necessitates that at least n departures should occur prior to the arrival of the $(n + k + 1)^{th}$ packet. Further, as stated above, $a_{residue}$ is finite which implies $\frac{a_{residue}}{n} \to 0$. Combining the above arguments, we can see that $\frac{\mathbb{E}[H(Y_1,\cdots,Y_n|\Phi)]}{n} = \sum_{i=1}^{w} p_i a_i$ which completes the proof. □

From Lemma 2, we can see that for strategies satisfying the conditions of the lemma, the only unknowns in calculating the anonymity of strategies are the limiting probabilities p_i and batch entropies a_i. That the randomized round robin falls into this class is easy to ascertain. Specifically, according to the randomized round robin strategy $\psi_{RR}(k)$, the state of the mix is given by $S_n = +x_r$ if the buffer has x_r red packets, or $S_n = -x_b$ if the buffer contains x_b blue packets. The mix transmits packets in batches of lengths 1 or 2. When only 1 packet is transmitted, the eavesdropper is aware of the source of the packet, and the batch has zero entropy *i.e.*$a_1 = 0$. A batch of two packets always contains one packet from each user ordered according to a fair coin flip which implies that $a_2 = 1$. Since transmissions are history independent, the state of the mix's buffer follows a Markov chain (see Figure 21). Futhermore, the the Markov Chain is finite, irreducible and aperiodic, and the limiting distribution of this Markov chain is unique and identical to its stationary distribution. Therefore, the strategy satisfies the conditions of Lemma 2.

The stationary distribution of the Markov chain is given by

$$\mu_0 = \begin{cases} \frac{(p-q)p^k q^k}{p^{2k+1}-q^{2k+1}} & p \neq q \\ \frac{1}{2k+1} & p = q \end{cases} \tag{50}$$

$$\mu_i = \mu_0 \left(\frac{p}{q}\right)^i \quad i = -k, \cdots, k \tag{51}$$

where $p = \frac{\lambda_1}{\lambda_1+\lambda_2}$ and $q = 1 - p$.

Let π_i be the limiting probability of transmitting packets in a batch of length i by the mix under strategy $\psi_{RR}(k)$. π_is can be easily calculated from the stationary distribution of the Markov chain

as shown in the following equations:

$$\begin{aligned} \pi_1 &= \mu_k p + \mu_{-k} q \\ \pi_2 &= \textstyle\sum_{i=-k}^{-1} \mu_i p + \sum_{i=1}^{k} \mu_i q \\ \pi_0 &= 1 - \pi_1 - \pi_2 \end{aligned} \tag{52}$$

Since $a_1 = 0$ and $a_2 = 1$, using Lemma 2, we get

$$\mathcal{A}(k) = \pi_2. \tag{53}$$

(50)-(53) proves the result of the theorem. □

As is evident from the theorem, the anonymity is maximum when arrival rates of users are equal. We can also see that as the buffer size increases anonymity saturates to $\min\{p, q\}$. In other words, the maximum achievable anonymity of the randomized round robin can never exceed 0.5 which is far below the maximum anonymity of 1. We, therefore, propose a relaxation to the max min fairness criterion in the subsequent discussion and demonstrate that any desired anonymity can be achieved by sufficiently relaxing fairness.

4.3.1 Relaxed Round Robin Scheduling Policy

The conventional definition of max-min fairness requires that the minimum fairness be computed on every pair of packets, one from each user, which limits the mix's ability to maximize anonymity. We consider a relaxed round robin strategy $\psi_{RRR}(n, k)$ that does not satisfy the criterion in the conventional pairwise sense; instead, the window of computation of minimum fairness is expanded to

---

$$\mu(0,0) = p\mu(n-1,n) + q\mu(n,n-1) \tag{54}$$

When $k+1-2n < x_r < k$ and $x_r \equiv k+1 \mod 2$ or $k+1-2n < x_b < k$ and $x_b \equiv k+1 \mod 2$, then

$$\mu(x_r,0) = p\mu(x_r-1,0) + q\mu\left(\frac{k+1+x_r}{2}, \frac{k-1-x_r}{2}\right) + p\mu\left(\frac{k-1+x_r}{2}, \frac{k+1-x_r}{2}\right) \tag{55}$$

$$\mu(0,x_b) = q\mu(0,x_b-1) + p\mu\left(\frac{k-1-x_b}{2}, \frac{k+1+x_b}{2}\right) + q\mu\left(\frac{k+1-x_b}{2}, \frac{k-1+x_b}{2}\right) \tag{56}$$

$$\mu(k+1-2n,0) = p\mu(k-2n,0) + q\mu(k+1-n,n-1) \text{ and } \mu(0,k+1-2n) = q\mu(0,k-2n) + p\mu(n-1,k+1-n) \tag{57}$$

When ($0 < x_r < k+1-2n$ or $x_r > k+1-2n$ and $x_r \equiv k \mod 2$) or ($0 < x_b < k+1-2n$ or $x_b > k+1-2n$ and $x_b \equiv k \mod 2$), then

$$\mu(x_r,0) = p\mu(x_r-1,0) \text{ and } \mu(0,x_b) = q\mu(0,x_b-1) \text{ and } \mu(k,0) = \frac{p}{q}\mu(k-1,0) \text{ and } \mu(0,k) = \frac{q}{p}\mu(0,k-1) \tag{58}$$

When $x_r, x_b > 0$, and $x_r + x_b \leq k$, and x_r and x_b are not simultaneously greater than or equal to n, then

$$\mu(x_r,x_b) = p\mu(x_r-1,x_b) + q\mu(x_r,x_b-1) \tag{59}$$

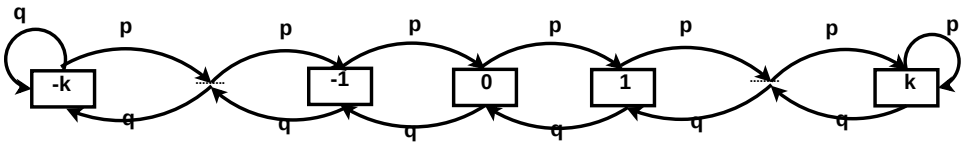


Figure 21: Mix states represented as a Markov process where $p = \frac{\lambda_1}{\lambda_1+\lambda_2}$ and $q = \frac{\lambda_1}{\lambda_1+\lambda_2}$

$2n$ packets, wherein at most n packets from each user can be arbitrarily shuffled prior to transmission. This class of strategies can be viewed as max-min fair with a $2n$-length window. Specifically, the strategy $\psi_{RRR}(n,k)$ for the $2-$user system, parametrized by integer n where $n \in [1, \lfloor \frac{k+1}{2} \rfloor]$ is described as follows:

- The mix stores all arrived packets in its buffer until one of the following two events occur:

  $E1n$. The buffer contains at least n packets from each user: At this point, the mix picks n packets that arrived earliest from each user, reorders them uniformly randomly (equal likelihood over the $\binom{2n}{n}$ permutation) and transmits them in a batch.

  $E2n$ The buffer is full prior to the mix receiving at least n packets from each user, and a new packet arrives. At this point, the mix chooses the first $x = \min\{x_r, x_b\}$ packets that arrived from each user, where x_r and x_b denote the number of packets in the buffer from the red and blue sources respectively. The mix reorders the $2x$ packets uniformly randomly and transmits the $2x$ packets in a batch.

Extending the argument from the simple randomized round robin described earlier, the state of this system can also be modeled using a Markov chain, albeit with multidimensional states. We use the stationary distribution of the Markov chain resulting from the policy to obtain the following theorem on anonymity of strategy $\psi_{RRR}(n,k)$

Theorem 7 *For $n \in [1, \lfloor \frac{k+1}{2} \rfloor]$, the anonymity of strategy $\psi_{RRR}(n,k)$ is*

$$\mathcal{A}(k) = \sum_{i=1}^{n} \pi_i \log_2 \binom{2i}{i}$$

where

$$\begin{aligned} \pi_i &= p(\mu(k-i,i) + \mu(i-1,k-i+1)) + \\ &\quad q(\mu(k-i+1,i-1) + \mu(i,k-i)) \;\; 0 < i < n \\ \pi_n &= q\left(\sum_{i=n}^{k} \mu(i,n-1)\right) + p\left(\sum_{i=n}^{k} \mu(n-1,i)\right) \end{aligned}$$

$p = \frac{\lambda_1}{\lambda_1+\lambda_2}$, $q = \frac{\lambda_2}{\lambda_1+\lambda_2}$ and $\mu(x_r, x_b)$s are the stationary distribution of the Markov chain associated with strategy $\psi_{RRR}(n,k)$ given by the solution to the stationarity equations given in (54)-(59) combined with $\sum_{(x_r,x_b)} \mu(x_r, x_b) = 1$.

Proof: The Markov chain formulation for $\psi_{RRR}(n,k)$ would be two-dimensional since the mix's buffer can hold packets from both users at any given time. Let $\{S_n\} = (x_r, x_b)$ be the state of the mix when n^{th} packet arrives, where x_r and x_b are the number of red and blue packets in the buffer respectively. According to the strategy, the state transitions only when a new packet arrives, at which point either one the events $E1n, E2n$ occurs or the mix does not transmit any packet. Conditioned on the present state, the action of the mix, the instantaneous anonymity reward, and the subsequent state transition are independent of the past, thus forming a classical MDP. Moreover, the resulting Markov chain is finite (because of the finite buffer size), aperiodic (because of presence of self loop in the Markov chain), and irreducible. Hence its limiting distribution exists and limiting probabilities can be calculated from the stationarity criterion of the Markov chain. Consequently, the stationarity requirement of the Lemma 2 is satisfied. Further, as it is clear from the description of the strategy, anonymity of a batch only depends on its length, hence condition 2 of the Lemma 2 is also satisfied.

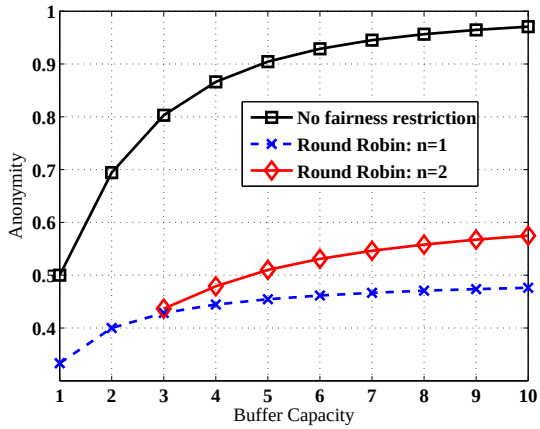
Under the strategy $\psi_{RRR}(n,k)$, whenever the mix transmits $2i$ packets in a batch, the Shannon entropy associated with this batch is $\log \binom{2i}{i}$ $\forall i = 1, \cdots, n$. Hence, using Lemma 2, the anonymity of strategy $\psi_{RRR}(n,k)$ is

$$\mathcal{A}(k) = \sum_{i=1}^{n} \pi_i \log_2 \binom{2i}{i}$$

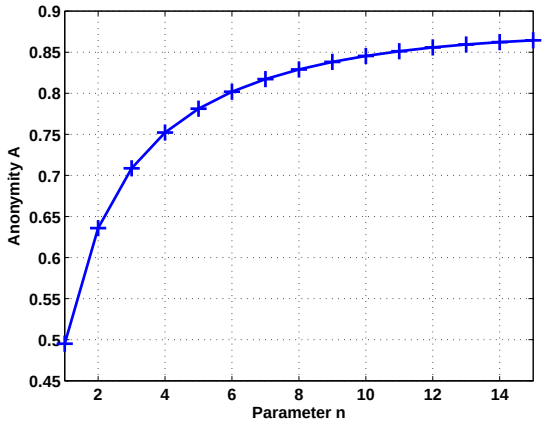
which completes the proof. □

Since the Markov chain for the mix's buffer state for strategy $\psi_{RRR}(n,k)$ is two dimensional and analytically intractable, we numerically compute the anonymity for strategy $\psi_{RRR}(n,k)$ and plot it in Figure 22b for equal arrival rates. It is easy to verify that for equal arrival rates, anonymity of strategy $\psi_{RRR}(n,k)$ asymptotically reaches 1 as $n \to \lfloor \frac{k+1}{2} \rfloor$ and $k \to \infty$.

Note that the fairness metric considered here, window size n, is inherent to the fair queuing paradigm and the tradeoff curves in Figure 22 do no quite reflect the relationship between anonymity and the corresponding TFI. It is intuitive that the degree of out-of-order transmissions increases with the fair queuing window n, and consequently the relationship between the TFI and n will be monotonic. However, computing the TFI for the relaxed round robin algorithm requires a dynamic program similar to that described for the $\eta-$fair FCFS. Specifically, the state of the mix should be



(a) Comparison of relaxed round robin scheme with optimal strategy for equal arrival rate



(b) Anonymity of relaxed RR for $k = 35$ and equal arrival rate of users

Figure 22: Anonymity of relaxed round robin and comparison with the optimal scheme for no fairness restriction

redefined to reflect the time ordered sequence of packets in the buffer along with their temporal fairness states. The relaxed round robin algorithm will ensure that the fairness state for any departing packet does not exceed $\eta = k + n$, thus making it a finite state MDP. According to the randomized round robin policy, the system with the expanded definition of state will continue to be a Markov Decision Process, and the computation of the TFI for the algorithm amounts to solving a system of linear equations (stationary distribution of states) albeit over a high dimensional space. In Section 5.7, the TFI for different round robin policies are computed numerically and used to plot the tradeoff between anonymity and TFI for the relaxed fair queuing algorithm.

We note that the idea of a batched transmission used in this section, rather than referring to a mode of transmission, specifies the group of packets whose order of transmission has been decided

regardless of subsequent arrivals. The eavesdropper with his knowledge of the policy, is also aware of the size of the batch, but not the order of packets. Consequently, the actual implementation of the batched transmission does not influence the results with regards to anonymity. The mix can send these packets in quick succession, or wait for a full buffer to transmit the current packet at the head of the batch.

Thus far, the analytical results presented for the $\eta-$fair FCFS and the FQ paradigms were focused on the 2−user system. The 2−user system was considered solely as a matter of convenience to ease presentation of the results and enhance the understanding of the reader. The key reductions that allowed the analysis of the algorithms, such as the discrete event model, the Markov Decision Process formulation, and the derived recurrence relations can be imminently generalized to systems with more than 2 users. In the evaluation of the anonymity of the Proportional Method (PM) of scheduling described in the subsequent section, the generalization to systems with more than 2 users is shown to be straightforward and is described in clear detail.

4.4 Anonymity of the Proportional Method

The Proportional Method (PM) for a buffer constrained mix serves users' packets in proportion to their demands. Translating this idea in the scheduling context, the probability of transmitting a packet from a particular source is proportional to the number of packets from that source in the shared buffer. To ensure that Eve does not get any information from the departure times of packets, we resort to the reduction mentioned in the FCFS discussion wherein a packet is transmitted if and only if a new packet arrives to a full buffer; *i.e.* the $(n+k)^{th}$ arrival to the mix triggers the n^{th} departure. Following this reduction, the description of the Proportional Method of scheduling is as follows:

At the time of arrival of new packet to a full buffer, let there be a_i untransmitted packets from the user i where the new arrival is included in the collection of untransmitted packets. At that time:

- The mix randomly chooses one user such that the probability that user i is chosen is equal to $\frac{a_i}{k+1}$.
- The packet in the buffer that arrived earliest from the selected user is then transmitted.

Using a state space description identical to that uilized in the analysis of the relaxed round robin algorithm, the following theorem characterizes the anonymity of the proportional method of scheduling in a 2−user system:

Theorem 8 *Under the PM, for a two source mix with arrival rate λ_1 and λ_2 respectively, the anonymity is given by*

$$\mathcal{A}(k) = \sum_{r=0}^{k} \mu_r \left(ph\left(\frac{r}{k+1}\right) + qh\left(\frac{r+1}{k+1}\right)\right)$$

where $\mu_r = \binom{k}{r} p^r q^{k-r}$, $p = \frac{\lambda_1}{\lambda_1+\lambda_2}$, *and* $q = \frac{\lambda_2}{\lambda_1+\lambda_2}$.

Proof: Following the arguments in the analysis of the randomized round robin, we define the state of the mix at any time n to be a vector $S_n = (r, k-r)$ when there are r red packets and $k-r$ blue packets in the buffer. According to the strategy, the choice of packet to transmit and the subsequent state transition are independent of the past conditioned on the present state. Therefore, the states of the mix follow a Markov process as illustrated in Figure 23. Let $(\mu_0, \cdots, \mu_k)$ denote the stationary distribution of this Markov process. Then using the properties of stationarity distribution of the Markov process, we obtain:

$$(k-r+1)p\mu_{r-1} = qr\mu_r \implies \mu_r \binom{k}{r} \left(\frac{p}{q}\right)^r \mu_0 \quad 1 \le r \le k$$

Furthermore,

$$\sum_{r=0}^{k} \mu_r = 1 \implies \mu_0 = q^k \text{ and } \mu_r = \binom{k}{r} p^r q^{k-r} \tag{60}$$

Rewriting the anonymity for the Markov process as a sum of the instantaneous conditional entropies, we get

$$\begin{aligned} & \lim_{n\to\infty} \frac{\mathbb{E}[H(Y_1,\cdots,Y_n|\Phi)]}{n} \\ \overset{(a)}{=} & \mathbb{E}\left[\lim_{n\to\infty} \frac{H(Y_1,\cdots,Y_n|\Phi)}{n}\right] \\ \overset{(b)}{=} & \mathbb{E}\left[\lim_{n\to\infty} H(Y_n|Y_1,\cdots,Y_{n-1},\Phi)\right] \\ \overset{(c)}{=} & \mathbb{E}\left[\lim_{n\to\infty} H(Y_n|S_n,X_n)\right] \\ = & \sum_{r=0}^{k} \mu_r \left(qh\left(\frac{r}{k+1}\right) + ph\left(\frac{r+1}{k+1}\right)\right) \end{aligned} \tag{61}$$

(a) follows from dominated convergence theorem and $\frac{H(Y_1\cdots Y_n)}{n} \le 1 \ \forall \ n \ge 1$.

(b) follows because states of the mix under the PM forms a Markov process.

(c) follows from the fact that knowledge of source of first $n-1$ departures and Eves observation completely determines the mix's state and given the state of the mix S_n and the n^{th} arrival, Y_n is independent from all previous departures and future arrivals. □

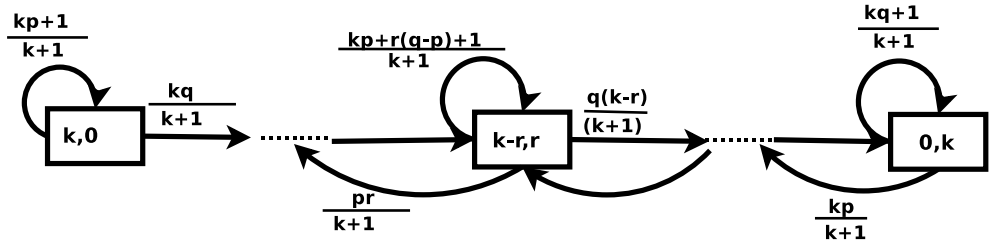


Figure 23: Mix states under PM

In the above theorem, μ_r, the limiting probability of the buffer being in state $(r, k-r)$ was shown to be the binomial distribution with parameter k and p. The anonymity is the expressed using the expected conditional entropy of departing packets from each state. Based on the binomial state distribution for a two user case, intuition suggests that for more than two users, the limiting probability would satisfy the multinomial distribution. This intuition is confirmed in the following theorem which allows us to characterize the anonymity for a general multiuser system.

Theorem 9 *For a mix with buffer size k receiving packets from u users with arival rates* $\{\lambda_1, \cdots, \lambda_u\}$*, the anonymity of the proportional method is given by:*

$$\mathcal{A}(k) = \sum_{\substack{x_1,\cdots,x_u \\ x_1,\cdots,x_u \geq 0}}^{x_1+\cdots+x_u=k} \mu(x_1, \cdots, x_u) \sum_{i=1}^{u} p_i h\left(\frac{x_1}{k+1}, \cdots, \frac{x_i+1}{k+1}, \cdots \frac{x_u}{k+1}\right)$$

where $\mu(x_1, \cdots, x_u) = \frac{k!}{x_1! \cdots x_u!} p_1^{x_1} \cdots p_u^{x_u}$ *and* $p_i = \frac{\lambda_i}{\sum_{j=1}^{u} \lambda_j} \forall \ i = 1, \ldots, u.$

Proof: For a $u-$user system, the state of the mix at any instant is represented as a vector $(x_1, \cdots, x_u)$ where x_i is the number of packets of i^{th} user present in the buffer respectively. The arguments that determined the Markovian property of the state space and the action continue to hold for the $u-$user case as well. Furthermore, using the fact that in state $(x_1, \cdots, x_u)$ the probability of transmitting a packet from user i is given by $\frac{x_i}{k+1}$, we get he following equations for the state transitions in stationarity:

Case1: $0 < x_i < k$

$$\mu(x_1, \cdots, x_u) = \sum_{i=1}^{u} p_i \frac{x_i+1}{k+1} \mu(x_1, \cdots, x_u) + \cdots \sum_{1 \leq i,j \leq u}^{i \neq j} p_i \frac{x_j}{k+1} \mu(x_1, \cdots, x_i - 1, \cdots, x_j + 1, x_u)$$

Case 2: WLOG $x_1, \cdots, x_m = 0$ and $1 \leq m \leq n-1$

$$\mu(x_1, \cdots, x_u) = \sum_{i=1}^{u} p_i \frac{x_i + 1}{k+1} \mu(x_1, \cdots, x_u) + \cdots \sum_{1 \leq i,j \leq u}^{i \neq j \text{ and } i \neq 1, \cdots, m} p_i \frac{x_j}{k+1} \mu(x_1, \cdots, x_i - 1, \cdots, x_j + 1, x_u)$$

For the state transition equations delineated above, it is easy to ascertain that

$$\mu(x_1, \cdots, x_u) = \frac{k!}{x_1! \cdots x_u!} p_1^{x_1} \cdots p_u^{x_u}$$

is a solution to the system of equations. Since the Markov process is finite, irreducible and aperiodic for any buffer size k, the multinomial distribution is the unique stationary distribution. The rest of the proof follows the same argument as for the 2−user case. □

Figure 24 plots the variation of anonymity with respect to buffer size for different number of users. As it can be observed in Figures 24a and 24b, the anonymity saturates with buffer size. This limiting anonymity of the strategy as buffer size increases is, in fact, the maximum achievable anonymity $h(p)$ which is proven in the following theorem.

Theorem 10 *Under the PM, for a mix with two users, if the probability of a red packet arrival is p and a blue packet is q, then asymptotic behaviour of anonymity with buffer size k is*

$$\mathcal{A}(k) = h(p) - \mathcal{O}\left(\frac{1}{k^{1/2}}\right)$$

Proof: Let $\delta = k^{-\frac{1}{2}+\epsilon}$ where $0 < \epsilon << \frac{1}{2}$. From Theorem 8,

$$\begin{aligned} \mathcal{A}(k) &= \sum_{r=0}^{k} \mu_r \left(qh\left(\frac{r}{k+1}\right) + ph\left(\frac{r+1}{k+1}\right)\right) \\ &= \sum_{|r-kp| \leq kp\delta} \mu_r \left(qh\left(\frac{r}{k+1}\right) + ph\left(\frac{r+1}{k+1}\right)\right) + \sum_{|r-kp| > kp\delta} \mu_r \left(qh\left(\frac{r}{k+1}\right) + ph\left(\frac{r+1}{k+1}\right)\right) \end{aligned}$$

Without loss of generality, we let $p < \frac{1}{2}$. Let k be large enough so that $\frac{kp(1+\delta)+1}{k+1} \leq \frac{1}{2}$. When $|r - kp| \leq kp\delta$, then

$$h\left(\frac{kp(1-\delta)}{k+1}\right) \leq h\left(\frac{r}{k+1}\right) \leq h\left(\frac{kp(1+\delta)}{k+1}\right) \tag{62}$$

since $h(x)$ is an increasing function of x if $0 \leq x \leq \frac{1}{2}$. Note that

$$\frac{h\left(\frac{kp}{k+1}+\frac{kp\delta}{k+1}\right)-h\left(\frac{kp}{k+1}\right)}{\frac{kp\delta}{k+1}} \leq \left.\frac{dh(x)}{dx}\right|_{x=\frac{kp}{k+1}} \tag{63}$$

since $h(x)$ is a continuous and concave function of x. Therefore,

$$h\left(\frac{kp(1+\delta)}{k+1}\right) \leq h\left(\frac{kp}{k+1}\right)+\frac{kp\delta}{k+1}\log_2\frac{1-p+\frac{1}{k}}{p} \tag{64}$$

It is easy to see that $\frac{kp}{k+1}\log_2\frac{1-p+\frac{1}{k}}{p}$ is bounded by some finite positive constant for all $0<p<1$ for all k , therefore,

$$h\left(\frac{kp(1+\delta)}{k+1}\right) \leq h\left(\frac{kp}{k+1}\right)+\mathcal{O}(\delta)$$

Using the same method as above, we can show that

$$h\left(\frac{kp}{k+1}\right) = h(p)+\mathcal{O}\left(\frac{1}{k}\right)$$

Therefore,

$$h\left(\frac{kp(1+\delta)}{k+1}\right) \leq h(p)+\mathcal{O}\left(\frac{1}{k^{\frac{1}{2}-\epsilon}}\right) \tag{65}$$

Similarly, we can show that

$$h\left(\frac{kp(1-\delta)}{k+1}\right) \geq h(p)-\mathcal{O}\left(\frac{1}{k^{\frac{1}{2}-\epsilon}}\right) \tag{66}$$

Therefore, using the (62,65, 66) we can see that

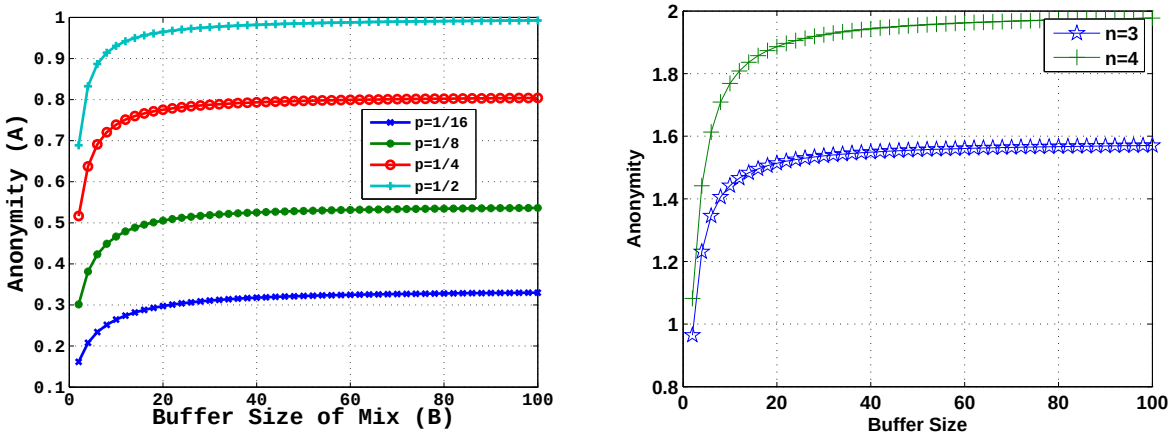
$$h\left(\frac{r}{k+1}\right) = h(p)-\mathcal{O}\left(\frac{1}{k^{\frac{1}{2}-\epsilon}}\right) \forall \ \ |r-kp| \leq kp\delta \tag{67}$$

Similarly, we can show that

$$h\left(\frac{r+1}{k+1}\right) = h(p)-\mathcal{O}\left(\frac{1}{k^{\frac{1}{2}-\epsilon}}\right) \forall |r-kp| \leq kp\delta \tag{68}$$

Using the Chernoff bound, we know that

$$\sum_{|r-kp|\leq kp\delta} \mu_r \geq 1-2\exp\left(-\frac{k^{2\epsilon}p}{3}\right)$$



(a) Two user case

(b) Multi-user case

Figure 24: Anonymity of the PM as a function of buffer size of the Chaum Mix

Therefore

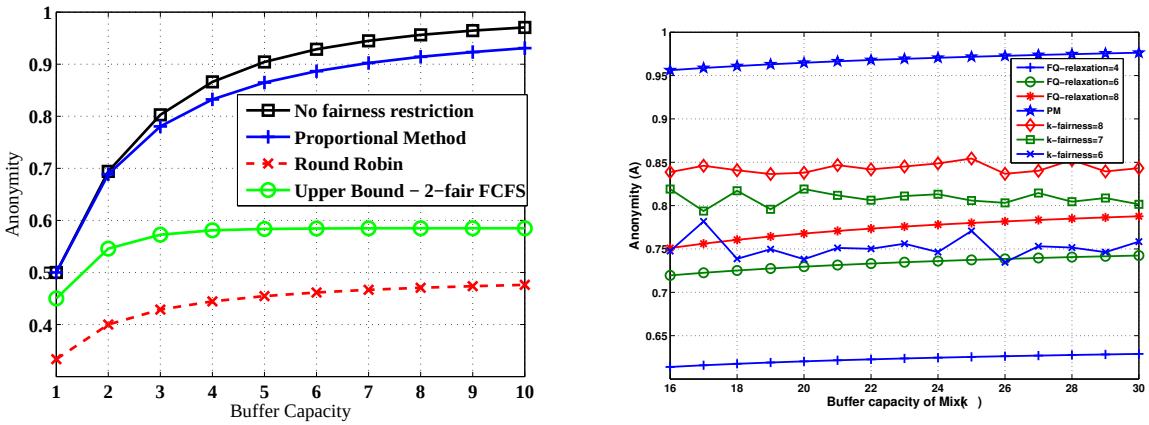
$$\mathcal{A}(k) \quad = \quad h(p) - \mathcal{O}\left(\frac{1}{k^{\frac{1}{2}-\epsilon}}\right)$$

Since the above equation is true for all $0 < \epsilon < \frac{1}{2}$, we get $\mathcal{A}(k) = h(p) - \mathcal{O}\left(\frac{1}{k^{\frac{1}{2}}}\right)$. □

The result in Theorem 10 shows that the PM achieves the maximum possible anonymity as the buffer size increases thus demonstrating the asymptotic optimality of the scheduling policy with regard to anonymity. It remains to be seen, how the proportional method trades off temporal fairness for anonymity. Unlike the FQ and $\eta-$fair FCFS, the TFI for the Proportional Method can not be computed using the expanded state space model described in Theorem 5. Since a packet can be stored in the buffer indefinitely by the Proportional Method, the fairness state of the stored packet can also grow indefinitely thus requiring countably infinite states which makes the analysis impractical. In the subsequent section, we use Monte Carlo simulations to compute the TFI for the Proportional Method as a function of the buffer size, and plot the tradeoff between temporal fairness and anonymity.

4.5 Comparative analysis of Scheduling policies

A comparative picture of the three fair scheduling paradigms, namely the PM, $\eta-$fair FCFS, and Fair Queuing is drawn in Figure 35. From this figure, it appears that for a fixed buffer size the PM provides a higher anonymity compared to the FQ and FCFS algorithms. This is true in part due to the natural randomization in the Proportional Method of scheduling. It is however to be



(a) Comparison of the Proportional Method, 2− fair FCFS and round robin with the optimal scheme for no fairness restriction(b) Comparison of the PM, FQ, and η-fairness for high buffer capacity of the mix

Figure 25: Comparison of anonymities of different scheduling scheme

noted that with sufficient relaxation of their inherent fairness paradigms, FQ and FCFS can provide an anonymity comparable to that of the PM. We would also state here that rather than viewing this plot as a comparison of different schemes to achieve anonymity, it should be looked at from the perspective of relaxing different notions of fairness to increase anonymity. Although the Proportional Method and optimal strategies achieve higher anonymity for similar buffer size, the actual choice of a scheduling algorithm would also depend on the notion of fairness desired in the application.

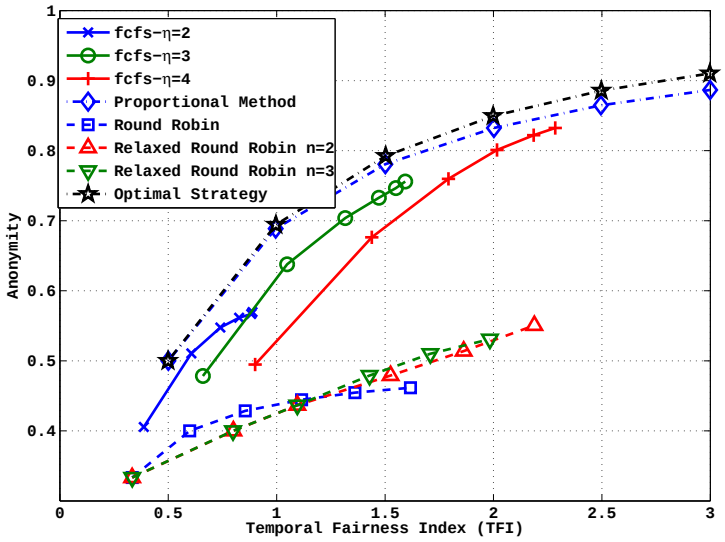


Figure 26: TFI index as a function of maximum achievable anonymity for different scheduling policies

In Figure 26, we compare the tradeoffs between anonymity and the TFI for the three classes of

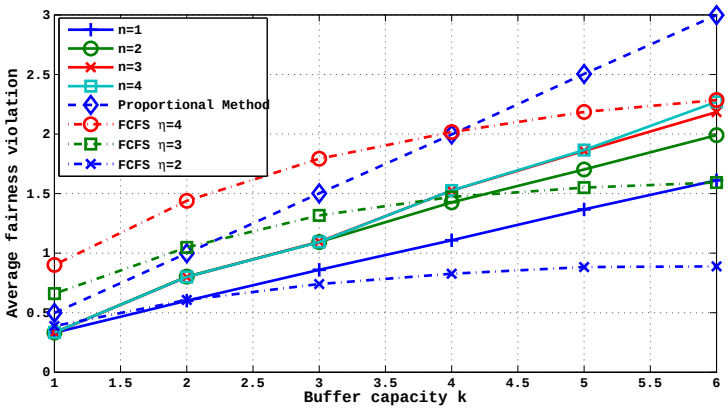


Figure 27: TFI index as a function of k for different scheduling policies

scheduling algorithms. These plots were obtained by using the analysis in the previous sections to evaluate the anonymity, and using Monte Carlo simulations to compute the respective TFI for the different algorithms. As it appears in Figure 26, the Proportional Method and the optimal strategy achieve the minimum TFI for a given level of anonymity while the round robin scheme achieves the maximum. For higher value of anonymity, the $\eta-$fair FCFS approaches the performance of the PM as the inherent fairness parameter η is increased. It is important to note here that although optimal scheduling strategy for a finite buffer capacity developed in Section 3 provides the best tradeoffs between temporal fairness and anonymity, we still need to investigate the performance of the optimal strategy from the perspective of throughput, delay, and congestion control before making a case for the strategy in data networking.

Figure 27 which plots the TFI for the algorithms as a function of the buffer size, suggests that the TFI of the PM increases linearly with buffer capacity. As described in the previous section, when the PM is employed, there is no upper bound on the fairness state of any individual packet, and the probability that fairness state exceeds any positive integer is non zero. The TFI for a relaxed round robin scheme with relaxation criteria n also increases with buffer size. This is not surprising since the maximum fairness state of a packet when employing the round robin algorithm with fairness window n is $k+n$. It is interesting to note that the TFI of an $\eta-$fair FCFS, which by definition is less than $\eta-1$, saturates to a value less than $\eta-1$. Determining the asymptotic TFI for a given $\eta-$fair FCFS is an interesting problem to consider for future extensions of this work.

4.6 Summary

In this work, we studied a previously unexplored dimension in fair scheduling algorithms, the source anonymity. An important conclusion for our analyses is that the Proportional Method, although thus far unpopular in the context of data networks, can, in fact, be a valuable fair scheduling scheme in anonymous networking systems. More generally, this work takes an important step in identifying the relationship of anonymity to fairness in the landscape of different metrics of evaluating scheduling strategies. We have used Poisson processes to model packet arrivals. However, since the analyses reduce the system to discrete event models, the actual times of arrivals do not impact the achievable anonymity as long as the source of each arrival is independent and identically distributed. Although the focus of this paper is the anonymity of a single mix, an extension of the results to network of mixes can be obtained by applying the networking arguments in [72]. In particular, the results in [72] characterize the anonymity achieved by a network of mixes as a weighted sum of the anonymity achievable by each individual mix.

5 Flow based Anonymity of Mixes under the constraints of Memory and Throughput

In comparison to previous chapters where we study the effect of resource constraints on packet based anonymity of mixes, in this chapter we study the optimization of mixing strategies under buffer and throughput constraints for flow based anonymity using a detection theoretic approach. We will also propose a general game theoretic model to study the mixing strategies when an adversary is capable of capturing a fraction of incoming packets. For this proposed multi-stage game, we will prove the existence of a Nash equilibrium, and will derive the optimal strategies for the mix and adversary at the equilibrium condition. The key to study the flow based anonymity in our work is the use of the **detection time** of the adversary (time required to know the source-destination pair of flows) as a metric that is explained in detail in the system model in the following section.

5.1 System Model

Consider a mix receiving packets from multiple users where every user has a unique incoming and outgoing stream as shown in Figure 28.

The key elements of the system model are described as follows:

Arrival Process: We consider a continuous time system model, where the mix receives packets from u users; arrival processes of these users are modelled as independent Poisson processes with arrival rates $\lambda_i \ \forall \ i \in \{1, \ldots, u\}$. In the game theoretic model described in Section 5.6, we propose a discrete time approximation of the Poisson process to study the multistage game. This approximation will be described in better detail in Section 5.6.

Chaum Mix: As is explained earlier, the mix is a relay node or a proxy server that uses layered encryption and packet padding, so that packets in outgoing streams of the mix cannot be linked to packets of incoming streams using its contents. The key design task for the mix is to randomly reorder the packets so that outgoing streams cannot be linked to their corresponding incoming streams using their timing. We assume that the mix can store a maximum of k packets in its buffer to facilitate the reordering of packets, and this random ordering of packets is known only to the mix. The mix is not allowed to drop any packets; if the buffer of the mix is full and a new packet arrives then the mix necessarily has to transmit at least one packet. In order to increase the degree of achievable anonymity, we allow the mix to transmit dummy packets; the maximum rate of dummy packets is, however, bounded so that the desired throughput QoS is achieved. Specifically, the mix

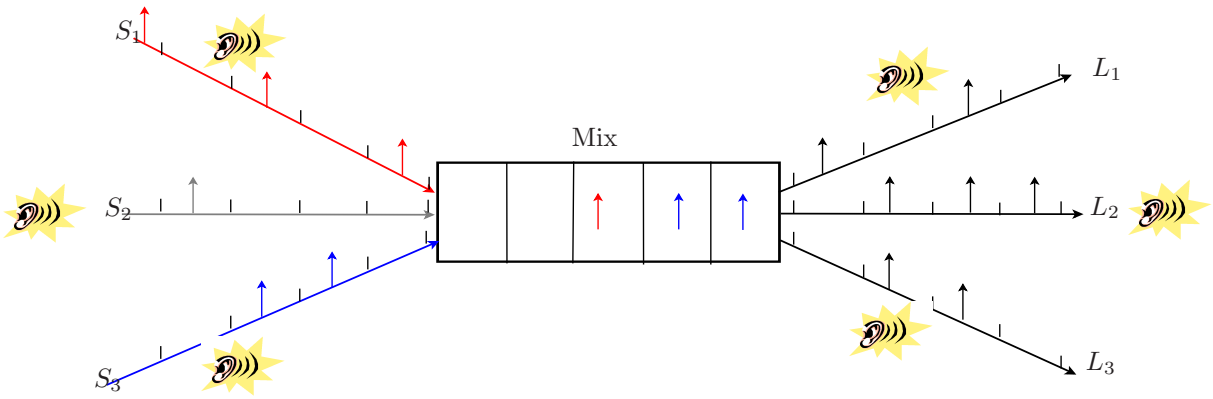


Figure 28: Mix receives packets from three users, encrypts and randomly reorders them, and transmits them in their corresponding outgoing link. Eve observes the arrival and departure processes.

can transmit $d(t)$ dummy packets in t seconds such that $\frac{d(t)}{t} \leq r \quad \forall t \in \mathbb{R}^+$ for a given constant r (determined based on QoS requirements).

Eavesdropper (Eve): Eve observes the incoming and outgoing streams of the packets and attempts to deduce the source of packets on each outgoing stream. Eve knows the mix's buffer capacity, and she also has the ability to capture a limited number of, c, packets on the incoming links. Capturing a limited number of packets can be accomplished by jamming links for short intervals, or by compromising the intermediate nodes between the source and the mix. It is important to note that Eve is aware of the mix's random strategy but does not have access to the realization of the randomness.

5.1.1 Admissible Length: A Detection Theoretic Metric

If an eavesdropper does not observe any arrival or departure process, and has no prior knowledge about the sources of outgoing links, the probability of associating an outgoing link with any particular source would be the prior probability (in this case $\frac{1}{u}$ for each user). A mixing strategy provides **perfect anonymity**, if it ensures that the probability of Eve predicting the outgoing links of users correctly remains $\frac{1}{u}$, independent of the number of packets observed. No mixing strategy can, however, provide perfect anonymity using a limited buffer capacity as is proved in the following lemma.

Lemma 3 *For a mix with buffer capacity k, there exists no mixing strategy that can provide perfect anonymity indefinitely unless the mix is allowed to add or drop packets.*

Proof: Let Eve observe the above system for t seconds. The probability that there exists a sequence of $2k+1$ consecutive arrivals in which packets of only one user arrives goes to 1 as $t \to \infty$. From beginning until the end of these $2k+1$ arrivals, the mix, independent of the strategy it follows, has to transmit at least $k+1$ packets of the user to its outgoing link[3]. At this point Eve, having observed more consecutive outgoing packets on a particular stream than the number of packets stored, can perfectly identify that the outgoing link corresponds to that specific user, hence the perfect anonymity of the system is lost. □

In effect, the objective of any memory limited mix is to maintain perfect anonymity for as long as possible, whereas the objective of Eve is to detect the source of outgoing packets as quickly as possible, thus representing the scenario for a zero-sum game. It is the length of time that the system can be in perfect anonymity, that we designate as the payoff of the aforementioned zero-sum game. Perfect anonymity ensures that for every observed packet, the posterior probability of associating an outgoing stream with any source is equally likely, which would be the case if Eve had zero observations and no knowledge of the mixing strategy. We aim to characterize this stream length as a function of the system parameters, namely buffer size, rate of dummy transmissions and capture capacity. This metric will not only serve as a measure of the effectiveness of the mixing strategy, but would be of practical utility in determining the allowable duration of packet streams from sources.

Let ψ denote a mixing strategy, and $\mathbb{T}_\psi$ denote the average duration of time that Eve requires to violate the perfect anonymity state of the departing packets, where the average is taken over all realizations of arrival processes. Let Ψ_k denote the collection of all valid mixing strategies that require a buffer size no greater than k. We define the **Admissible Length** $\mathcal{A}_k$ of the Chaum Mix as

$$\mathcal{A}_k = \sup_{\psi \in \Psi_k} \mathbb{T}_\psi$$

Although admissible length is a measure of time, in the next lemma, we prove that the average number of arrivals that are required to obtain the information about source-destination pairs is sufficient for calculating the admissible length.

Lemma 4 *Let $\mathbb{E}[\mathbb{N}_\psi]$ be the average number of arrivals that are required to violate the perfect unobservability of the system for strategy ψ, then*

$$\mathbb{E}[\mathbb{T}_\psi] = \frac{\mathbb{E}[\mathbb{N}_\psi]}{\sum_{i=1}^{u} \lambda} \tag{69}$$

[3] Even if the buffer of the mix is filled with only one users' packets, a sequence of $2k+1$ consecutive arrivals of a user will ensure that no other user has more departures.

and

$$\mathcal{A}_k = \max_{\psi \in \Psi_k} \frac{\mathbb{E}[\mathbb{N}_\psi]}{\sum_{i=1}^{u} \lambda_i} \tag{70}$$

Proof: Lets assume that for a given sample path of arrivals, strategy ψ requires N_ψ arrivals and T_ψ time units to know the source-destination pairs. Let T_i be the inter-arrival time between $(i-1)^{th}$ and i^{th} arrival. Then,

$$T_\psi = \sum_{i=1}^{N_\psi} T_i$$

We know that T_i are i.i.d. random variables with mean $\frac{1}{\sum_{i=1}^{u} \lambda}$. We also know from [73] that $\mathbb{E}[N_\psi] < \infty$. Therefore, using Wald's equation [74]

$$\begin{aligned} \mathbb{E}[T_\psi] &= \mathbb{E}[N_\psi]\mathbb{E}[T_1] \\ &= \frac{\mathbb{E}[N_\psi]}{\sum_{i=1}^{u} \lambda} \end{aligned} \tag{71}$$

□

In subsequent sections we characterize this metric analytically as a function of the buffer size, allowable rate of dummy transmissions (r), and the number of packets of Eve can capture (c), and through the process, determine the optimal mixing strategies. Based on the key parameters, we study the system under four different regimes:

1. *Basic model* $\mathcal{G}_B$: $r = 0, c = 0$: In the basic model where the adversary is passive and the mix is not allowed to add dummy transmission, we determine the optimal mixing strategy and provide an analytical characterization of the admissible length as a function of the buffer size. In particular, the admissible length will be shown to scale quadratically in buffer size.

2. *Empowered mix model* $\mathcal{G}_M$: $r > 0, c = 0$: When the mix is allowed to transmit dummy packets, the admissible length for a passive adversary is shown to be inverse linearly related to the allowed rate of dummy transmissions. A special case of our analysis provides the rate of dummy transmissions required to maintain perfect anonymity indefinitely.

3. *Empowered Eve model* $\mathcal{G}_E$: $r = 0, c > 0$: When the adversary is allowed to capture a finite number of packets, the optimal mixing strategy (without dummy transmissions) is shown to be identical to the basic model, and the optimal adversary strategy is shown to be a simple threshold strategy.

4. *General model* $\mathcal{G}_G$: $r > 0, c > 0$: For the general model, when dummy transmissions and capture are allowed, the resulting game is shown to have a pure strategy saddle point equilibrium owing to the existence of a dominant strategy for the mix and a generalized threshold strategy for the adversary.

In subsequent sections, we will characterize the optimal strategies of the players and admissible length for the different models. In particular, we will demonstrate, as intuition would suggest, that the empowered mix model ($\mathcal{G}_M$) achieves the maximum admissible length while the empowered Eve model ($\mathcal{G}_E$) achieves the minimum. The performances of the basic and general model lie between these extremes. We note that while a majority of the analytical results in this paper have been derived for the two user model, the broad inferences about strategies of the mix and Eve would hold in general. We further note that in the subsequent discussion we refer to the two sources in the model as being a *Red* and *Blue* source.

5.2 Basic Model ($\mathcal{G}_B$)

In the basic model, the capture capacity $c = 0$, and the allowable dummy rate $r = 0$; in other words the mix is not allowed to transmit any dummy packets to append to its traffic pattern, and Eve cannot capture any packets from the incoming streams of the mix.

In the basic model, the mix merely stores packets in its buffer, and transmits them in a random order to hide their identities while Eve, not having access to realization of this random ordering, passively observes the arrival and departure process. In this scenario, the only method available to Eve to determine the source of an outgoing stream is to analyse the correlations between the timing on incoming and outgoing streams. Consequently, as long as each outgoing stream is equally correlated to all incoming streams, the system will remain in perfect anonymity (each stream equally likely to belong to each source). More specifically, if the mix ensures that at all times the number of departed packets on any outgoing link is less than the minimum number of arrivals across all incoming links, then it is possible for all outgoing streams to have identical timing, thus maintaining perfect anonymity. This idea is used to prove that the optimal strategy for the mix is to transmit one packet of each user only when packets from all users are present in the buffer, and consequently characterize the admissible length of the system.

Theorem 11 *For a mix with buffer capacity, k, receiving packets from 2 users where arrival rate*

of users are λ_1 and λ_2 respectively, the maximum admissible length is

$$\mathcal{A}_m = \begin{cases} \left(\frac{k+1}{\lambda_1-\lambda_2}\right)\left(\frac{\left(\frac{\lambda_1}{\lambda_2}\right)^{k+1}-1}{\left(\frac{\lambda_1}{\lambda_2}\right)^{k+1}+1}\right) & \lambda_1 \neq \lambda_2 \\ \frac{(k+1)^2}{2\lambda^*} & \lambda_1 = \lambda_2 = \lambda^* \end{cases} \tag{72}$$

Proof:

Let $X_1(t)$, $X_2(t)$, $Y_1(t)$ and $Y_2(t)$ denote four continuous-time counting processes. $X_1(t)$ and $X_2(t)$ represent the number of red and blue packets arrived up to time t respectively. $Y_1(t)$ and $Y_2(t)$ represent the number of packets that have departed on links L_1 and L_2 respectively up to time t . If the number of departed packets of each outgoing link is less than the number of arrived packets on every incoming link, then the mix can ensure that the departure timing on every outgoing process is identical and an eavesdropper has no way of connecting an outgoing and an incoming link. In other words, any strategy that satisfies the conditions;

$$X_1(t) \geq \max\{Y_1(t), Y_2(t)\} \forall t \leq t_0 \tag{73}$$

$$X_2(t) \geq \max\{Y_1(t), Y_2(t)\} \forall t \leq t_0 \tag{74}$$

maintains perfect anonymity until time t_0. However, owing to the memory limitation an strategy is bound to fail at time t if

$$|X_1(t) - X_2(t)| = k+1$$

since, at time t, the number of departures on one outgoing link would be larger than the number of arrivals on one incoming link thus eliminating the source uncertainty and losing anonymity. Consequently, a strategy that ensures that conditions (73) and (74) will be violated for first time for some time t_0 if and only if

$$|X_1(t_0) - X_2(t_0)| = k+1 \text{ and } |X_1(t) - X_2(t)| < k+1 \ \ \forall\, t < t_0 \tag{75}$$

will be an optimal strategy.

Consider a strategy $\overline{\psi}$ that transmits one packet of each user in their outgoing link if packets of both the users are present in the buffer. It is easy to see that strategy $\overline{\psi}$ satisfies the criterion given in (75) and is hence an optimal strategy. We now compute the admissible length for $\overline{\psi}$.

Let $Z(t) = X_1(t) - X_2(t)$. Since $X_1(t)$ and $X_2(t)$ are Poisson process, $Z(t)$ evolves as a simple random walk. Note that jumps of this random walk occurs at irregular time intervals that are

exponentially distributed with mean value of $\frac{1}{\lambda_1+\lambda_2}$. Let i^{th} jump occur at time T_i, the probability distribution of the jump in positive or negative direction is as follows:

$$\begin{aligned}\mathbb{P}(Z(t_i) = Z(t_i^-) + 1) &= \frac{\lambda_1}{\lambda_1+\lambda_2} = p \\ \mathbb{P}(Z(t_i) = Z(t_i^-) - 1) &= \frac{\lambda_2}{\lambda_1+\lambda_2} = q\end{aligned}$$

From (75), we can see that the time at which this random walk hits $k+1$ or $-k-1$, an eavesdropper can determine the source-destination pairs perfectly.

Let N_s be the average number of jumps required from time $t = 0$ by the random walk $Z(t)$ to hit the boundaries $\pm(k+1)$ when $Z(0) = s$. Then N_s would satisfy the following recursive equation

$$N_s = pN_{s+1} + qN_{s-1} + 1 \quad -k \le s \le k$$

and the boundary conditions for the above recursive equation are $N_{k+1} = N_{-k-1} = 0$. The general solution to a recursive equation such as the one described above is given by:

$$N_s = \begin{cases} \frac{s}{q-p} + A_1 + B_1\left(\frac{q}{p}\right)^s & p \neq q \\ -s^2 + A_2 + B_2 s & p = q \end{cases} \tag{76}$$

Solving the recursive equation for A_1, B_1, A_2, and B_2 using the given boundary conditions, we get

$$\begin{aligned} A_1 &= \tfrac{k+1}{p-q}\tfrac{p^{2(k+1)}-q^{2(k+1)}}{p^{2(k+1)}+q^{2(k+1)}} & B_1 &= \tfrac{2(k+1)}{q-p}\tfrac{(pq)^{k+1}}{p^{2(k+1)}+q^{2(k+1)}} \\ A_2 &= (k+1)^2 & B_2 &= 0 \end{aligned} \tag{77}$$

Therefore, we get

$$N_s = \begin{cases} \frac{s}{q-p} + \frac{k+1}{p-q}\frac{p^{2(k+1)}+q^{2(k+1)}-2p^{(k+1-s)}q^{(k+1+s)}}{p^{2(k+1)}-q^{2(k+1)}} & p \neq q \\ (k+1)^2 - s^2 & p = q \end{cases} \tag{78}$$

N_0 is the average number of jumps required to hit the boundary $\pm(k+1)$.

Consider a sample path of a random walk where T is the amount of time it is required to hit the boundary $\pm(k+1)$ and T_i is the inter-arrival time between $(i-1)^{th}$ and i^{th} jump. Let this sample path require N jumps to hit the boundary. Clearly, $T = \sum_{i=1}^{N} T_i$. We know in case of Poisson arrivals, inter-arrival time T_is are i.i.d. exponential random variable with mean $\frac{1}{\lambda_1+\lambda_2}$. Using the theory of stopping time [75], we see $\mathbb{E}[T] = \mathbb{E}[N]\mathbb{E}[T_1] = \frac{N_0}{\lambda_1+\lambda_2}$. Substituting the value of N_0 from

equation (78) gives the desired result. □

Theorem 12 *For a mix with buffer capacity, k, receiving packets from $u(>2)$ users where arrival rates of all users are equal to λ, then admissible length $\mathcal{A}_k$ is $\frac{l(k+1,\cdots,k+1)}{u\lambda}$ where $l(k+1,\cdots,k+1)$ satisfies the following recursive equation*

$$l(v_1,\cdots,v_u) = 1 + \frac{1}{u}\sum_{i=1}^{u} l(v_1+1,\cdots,v_i-u+1,\cdots,v_u+1) \tag{79}$$

where v_is are positive integers satisfying the condition $\sum_i v_i = u(k+1)$. Boundary conditions for the recursive equation are $l(v_1,\cdots,v_u) = 0$ if any v_i is non-positive.

Proof:

In the forthcoming analysis, let $X_i(t)$ be a random variable that denotes the total number of arrived packets of the i^{th} user until time t and $Y_i(t)$ be the number of departed packets from i^{th} outgoing stream until time t. Also assume that $X_{\min}(t) = \min\{X_1(t),\cdots,X_u(t)\}$.

Extending (73), (74) to $u > 2$, if $Y_i(t) \leq \min_{1\leq j\leq u}\{X_i(t)\}$, then Eve cannot extract any information about source-destination pair using timing analysis of packets. But, this condition is bound to fail for time t for which

$$\sum_{j=1}^{u}(X_j(t) - uX_{\min}(t)) = k+1 \tag{80}$$

because the mix's buffer can hold maximum k packets and the mix is not allowed to drop packets. Hence, any strategy that ensures that $Y_i(t) > X_{\min}(t)$ only if $\sum_{j=1}^{u}(X_j(t) - uX_{\min}(t)) = k+1$ will be an optimal strategy. Note that the analogous strategy to two users case, ψ_1, where the mix transmits packets if and only if non-zero packets from all u users are present in the buffer would satisfy this optimality criterion.

$X_i(t)$s are i.i.d. Poisson distributed random variables with parameter λt. Let $S(t)$ be a continuous time stochastic process such that

$$S(t) = \sum_{i=1}^{u} X_i(t) - uX_{\min}(t).$$

Let T be the hitting time of the above stochastic process to the boundary $k+1$. Specifically,

$$T = \min\{t \in \mathbb{R} : S(t) \geq k+1\}$$

Then, admissible length for a Chaum Mix serving u users and buffer capacity k is

$$\mathcal{A}_k(u) = \mathbb{E}[T]$$

Let $X(t) = \sum_{i=1}^{u} X_i(t)$. We know $X(t)$ is a Poisson process with rate $u\lambda$. Let $\{t_i\}_{i=1}^{\infty}$ be a sample path of $X(t)$ which means that i^{th} event of the Poisson process occurs at time t_i. $R(i, j, t_m) = X_i(t_m) - X_j(t_m)$. Note that $S(t_m) = \max_{1 \le j \le u} \sum_{i=1}^{u} R(i, j, t_m)$.

Define for each t_m, a $u \times u$ matrix $H(m)$ such that $H_{i,j}(m) = R(i, j, t_m)$. For a $u \times 1$ vector v, we define "$H(m) < v$" to be the set of following u inequalities

$$\sum_{i=1}^{u} H_{i,j}(m) < v_j, 1 \le j \le u$$

Now for a vector v consisting of integer entries such $\sum_j v_j = u(k+1)$, we define $P(v, n) = \mathbb{P}[H(m) < v, \forall m < n]$.

We know $\mathbb{E}[N] = \sum_{n=1}^{\infty} P([k+1, \cdots, k+1]', n)$ because we assume here that all vectors v have only integer entries.

$P(v, n)$ can be written in the form of a recursive equation based on the arrival of the time t_1 follows:

$$P(v_1, \cdots, v_u, n) = \frac{1}{u} \sum_{i=1}^{u} P(v_1 - 1, \cdots, v_i + u - 1, \cdots, v_u - 1, n-1) \tag{81}$$

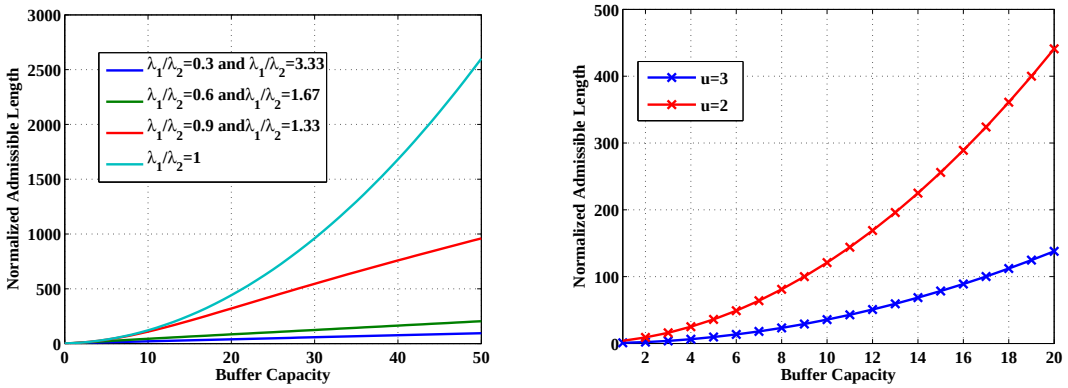
Note that sum of coefficients of variables in the right hand side of equation (81) is $(k+1)u$.

Let $l(v_1, \cdots, v_u) = \sum_{n=1}^{\infty} P(v_1, \cdots, v_u, n)$ and note using the definition of $P(v, n)$ that $P(v_1, \cdots, v_u, 1) = 1$. Adding $P(v_1, \cdots, v_u, n)$ from $n = 2$ to ∞ in (81), we get the desired result. □

The recursive solution for the admissible length is, in general, hard to characterize analytically but can be computed numerically. For $u = 3$, the equation is solvable and the solution is given by $\mathcal{A}_k = \frac{(k+1)^3}{3\lambda(3k+5)}$.

Figure 29a shows the admissible length normalized with respect to total arrival rate of the mix for two users as a function of buffer capacity of the mix for different arrival rates. As expected from eq. (72) and shown in Figure 29a, the normalized admissible length only depends on the relative proportions of the arrival rates (order independent) and achieves its maximum when arrival rates are equal. This is not surprising since unequal arrival rates would result in the mix's buffer to be overfilled with packets of the user having higher arrival rate forcing the mix to transmit an unpaired packet quickly, thus reducing the admissible length.

It is interesting to note from the theorem that the admissible length increases quadratically



(a) Admissible length for two users case as buffer size (b) Admissible length for two users and three users as buffer size

Figure 29: Admissible length when mix is not allowed to transmit dummy packets

with the buffer capacity when users have equal arrival rate. Consequently for network applications which do not require long streams of communication (such as web browsing) but require a smaller latency, the buffer capacity of mixes can be limited sufficiently to prevent traffic analysis while not sacrificing the QoS. As will be seen in Section 5.3, the quadratic relationship is unaltered when the mix is allowed to transmit dummy transmissions, albeit with a larger scaling factor. Note that the adversary, as modelled here, is assumed to have complete information about packet arrivals on all links, and a practical adversary with noisy observations would have a larger admissible length than that characterized above.

Figure 29b compares the admissible length between a 2 user system and a 3 user system as a function of the mix's buffer size. The admissible length for three users is uniformly less than the admissible length for two users. The reason behind this decrement is the increasing difficulty in maintaining source-destination pairs equally probable as their number increases. While anonymity, as measured by entropy [5,25,76], increases with the number of users, the admissible length provides a measure of how long this maximum anonymity is sustainable. The analysis demonstrates that this increased anonymity is indeed temporary from Eve's perspective and applicable only to short bursts of traffic. The burst lengths can be increased by intelligently adding dummy packets, the study of which is the focus of the next section.

5.3 Empowered Mix Model ($\mathcal{G}_M$)

Note that any pattern of traffic flow can be anonymized indefinitely through sufficient insertion of dummy traffic. For example, consider a network where all nodes transmit packets according to

scheduled departure times. If an actual packet is unavailable for transmission at its time of departure, a dummy packet can be transmitted in its place and perfect anonymity is still maintained. But such extensive use of dummy packets will severely reduce network throughput. We consider a scenario where the mix is allowed to transmit dummy packets as long as the maximum rate of dummy packets transmitted is upper bounded by r. Under this model, the achievable admissible length as a function of r can be bounded as in the following theorem:

Theorem 13 *For a Chaum Mix having buffer capacity k and a maximum dummy packet rate r receiving packets from two users with equal arrival rate λ, the admissible length ($\mathcal{A}_{r,k}$) is bounded as*

$$\frac{k^2}{2\lambda - (2k+1)r} \leq \mathcal{A}_{r,k} \leq \frac{(k+1)^2}{2\lambda - (2k+1)r} \tag{82}$$

Proof:

As we have seen in the proof of theorem 11 that optimality conditions for maximizing the admissible length is

$$|X_1(t_0) - X_2(t_0)| = k+1 \text{ and } |X_1(t) - X_2(t)| < k+1 \ \ \forall\, t < t_0$$

However, when the mix has dummy packets and the above situation occurs, it can transmit a dummy packet in the outgoing link of the user with lesser packets and can still maintain the perfect anonymity.

Consider a realization of a random walk for dummy rate r and buffer size k. Let T be the time at which this realization terminates; Eve knows the source-destination pairs at the time T. Due to the dummy rate constraint, the mix can use maximum $\lfloor Tr \rfloor$ dummy packets during this realization which requires that this realization hits the boundaries a total of $\lfloor Tr+1 \rfloor$ times because $\lfloor Tr \rfloor$ dummy packets are generated and utilized during this realization. Let T_0 be the time required in the realization from 0 to hitting the boundaries for the first time, and let T_i be the time duration between i^{th} and $(i+1)^{th}$ hitting. T can be expressed using the T_is as follows.

$$T = T_0 + \sum_{i=1}^{\lfloor Tr \rfloor} T_i \tag{83}$$

$$\mathbb{E}[T] = \mathbb{E}[T_0] + \mathbb{E}\left[\lfloor Tr \rfloor\right] \mathbb{E}[T_1] \tag{84}$$

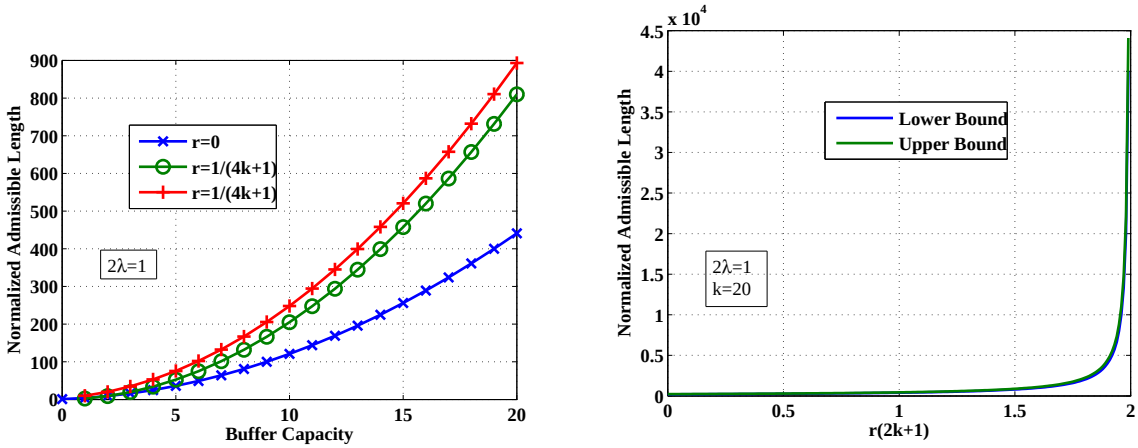
$$\mathbb{E}[T_0] + \left(\mathbb{E}\left[Tr\right] - 1\right) \mathbb{E}[T_1] \leq \mathbb{E}[T] \leq \mathbb{E}[T_0] + \mathbb{E}\left[Tr\right] \mathbb{E}[T_1] \tag{85}$$

$$\frac{\mathbb{E}[T_0] - \mathbb{E}[T_1]}{1 - \mathbb{E}[T_1]r} \leq \mathbb{E}[T] \leq \frac{\mathbb{E}[T_0]}{1 - \mathbb{E}[T_1]r} \tag{86}$$

But we can see from the proof of Theorem 11 that $\mathbb{E}[T_0] = \frac{(k+1)^2}{2\lambda}$ and $\mathbb{E}[T_1] = \frac{2k+1}{2\lambda}$ for equal arrival rate of users. Hence,

$$\frac{k^2}{2\lambda - (2k+1)r} \leq \mathcal{A}_{r,m} \leq \frac{(k+1)^2}{2\lambda - (2k+1)r}$$

It is to be noted that the equality in (84) is an outcome of Wald's equation, hence we need to show that T_is are independent, but it is trivially true when arrival rate of users are equal. □



(a) Admissible length as buffer capacity

(b) Admissible length as dummy rate

Figure 30: Admissible length when mix is allowed to transmit dummy packets

Although the theorem provides bounds in place of exact admissible length, these bounds are fairly close when k is large compared to r (see Figure 30).

Figure 30a shows the normalized admissible length as a function of mix's buffer capacity when the dummy rate $r < \frac{1}{4k+1}$ packets per unit time, and compares it against the condition when mix is not allowed to transmit any dummy packet. Figure 30b shows the variation of admissible length as a function of normalized dummy rate where normalized dummy rate is the product of dummy rate and mix's buffer capacity. As can be ascertained from the theorem and noted from from the Figure 30b, the admissible length approaches infinity (perfect unobservability) for a dummy rate $r = \frac{2\lambda}{2k+1}$, a result previously shown in [77].

It is to be noted that this is the first such analysis of mixing strategies as a function of a fixed rate of dummy transmissions. Further the bounds also confirm that for any fixed fraction of dummy transmission per unit of memory, the admissible length continues to increase quadratically with buffer size.

5.4 Empowered Eve Model ($\mathcal{G}_E$)

In this section, we analyse the admissible length for an active adversary who captures a limited number of packets of the incoming streams while the mix cannot transmit dummy packets. The limitation on capture ability is important in the context of intrusion detection mechanisms. Intrusion detectors monitor the network activity to identify active disruption by adversaries such as modification to traffic patterns. In the context of this work, the more packets captured by Eve, the higher likelihood that the actions are detected by an intrusion detector. In effect, for Eve to ensure that her actions are not detectable by such systems, the number of packets captured should lie below the missed-detection threshold of an intrusion detector. Since the intrusion detection is designed as part of the network operation, it is fair to assume that mixing strategies can be designed with knowledge of the capture capacity of the adversary.

It is important to note that as long as the number of packets captured by Eve is within the specified limit, the mix is assumed to be unaware how many packets, if any, are captured by Eve. As a result, the optimal strategy of the mix will be no different as in the case when Eve does not capture packets. In other words, the mix has to ensure that the departure times are identical across all outgoing streams as long as feasible. For any arrival sequence, regardless of capture or not, the strategy $\overline{\psi}$ described in Theorem 11, that transmits one packet of each user in the corresponding outgoing link as soon as both users' packets are available to the mix achieves the desired optimality from the mix's perspective. Consequently, in this two player game, the optimal strategy for the mix is a dominant strategy. It is easy to see then that under the optimal strategy, $\overline{\psi}$, the mix would always have packets of only one user in its buffer. The space of all possible strategies of Eve is very large and dependent on the state of the mix's buffer and the actions of the mix. In the following theorem, we prove that against the dominant strategy of the mix, the optimal strategy for Eve is a threshold strategy; Eve decides to capture an arriving packet if and only if the number of packets in the mix's buffer is greater than a threshold.

Theorem 14 *The optimal strategy ψ_E of Eve when she is allowed to capture a maximum of c packets from the incoming streams of the mix against the dominant strategy $\overline{\psi}$ of the mix receiving packets from two users with equal arrival rate λ and when the mix's buffer has x red (blue) packets in its buffer is*

- *If the arrived packet is blue (red), then capture it if and only if the $x \geq \tau_c + 1$.*
- *If the arrived packet is red (blue), then Eve let it go to the mix.*

Proof: The key idea behind the threshold strategy is as follows. When there are sufficient number of packets accumulated in the buffer, then capturing a packet of another user would significantly reduce the admissible length per packet captured. When the buffer has few packets, the uncertainty over future arrivals would mean that capturing a packet of another user may not reduce the admissible length, and could possibly, increase the length. This intuition suggests a threshold strategy for Eve, the optimality of which is proven below using a stochastic shortest path algorithm.

In the forthcoming analysis, we model the system to be in state (x, y) if the mix has x red packets and Eve can capture y packets, and our system is in state $(-x, y)$ if the mix has x blue packets and Eve can capture y packets.

If the system is in state (x, y), then Eve's actions and dependent future states can be described as follows:

1. If a red packet arrives, then Eve has two choices:
   - If $y < c$, she can capture the red packet and the next system state would be $(x, y-1)$.
   - She can let the red packet to go to the mix and next system state would be $(x+1, y)$.
2. Similar to previous case, if a blue packet arrives, then Eve has two choices:
   - If $y < c$, she can capture the blue packet and the next system state would be $(x, y-1)$.
   - She can let the blue packet to go to the mix and next system state would be $(x-1, y)$.

It is clear that terminating states of the system are $(k+1, y)$ or $(-k-1, y)$ where $0 \leq y \leq c$.

We use the stochastic shortest path algorithm [78] to choose optimal actions for Eve. Let $D(x, y)$ be the shortest number of average jumps required for Eve to reach any terminating state when the system is in state (x, y). According to the stochastic shortest path algorithm, $D(x, y)$ satisfies the following recursive equation: If $y \geq 1$

$$D(x,y) \quad = \quad 1 + \tfrac{1}{2}\min\{D(x,y-1), D(x+1,y)\} + \tfrac{1}{2}\min\{D(x,y-1), D(x-1,y)\} \tag{87}$$

If $y = 0$, then Eve cannot capture any packet, and the average number of jumps, it would require for Eve to reach the terminating state would be $((k+1)^2 - x^2)$, if the system is in state $(x, 0)$ as shown in Theorem 11.

Note that

$$D(x,y) \leq D(x,y-1) \forall\ 0 \leq y < c \tag{88}$$

because the set of Eve's actions for any possible arrival process under the system state (x, y) contains the set of Eve's actions for that arrival process when mix is in state $(x, y-1)$.

We use mathematical induction to prove the theorem.

The base case: Theorem 14 is true for $c = 1$. Moreover, $D(x, 1)$ decreases as x increases in magnitude.

Proof: To prove the base case we need to show that $\exists\ \tau_1 \in \mathbb{N}$ s.t. $0 \leq \tau_1 < k$ and

$$D(x,1) \geq D(x+1,0) \forall x \geq \tau_1 \quad \text{and} \quad D(x,1) \geq D(x-1,0) \forall x \leq -\tau_1$$
$$D(x,1) \leq D(x+1,0) \forall x < \tau_1 \quad \text{and} \quad D(x,1) \leq D(x-1,0) \forall x > -\tau_1$$

which is equivalent to show that $D(x+1,1) \leq D(x+2,0) \implies D(x,1) \leq D(x+1,0)$ for $x > 0$ and $D(-x-1,1) \leq D(-x-2,0) \implies D(-x,1) \leq D(-x-1,0)$ for $x < 0$.

We know from the boundary conditions that $D(k+1,0) = D(-k-1,0) = 0$. Therefore, $D(k,1) \geq D(k+1,0)$ and $D(-k,1) \geq D(-k-1,0)$ which implies that if there exist a threshold then it should be less than or equal to k.

Let $x > 0$. We know that $D(x,0) = ((k+1)^2 - x^2)$. Therefore $D(x,0) > D(x+1,0)$. Moreover, we know from (88) that $D(x+1,0) > D(x+1,1)$. Therefore $D(x,0) > D(x+1,1)$. Note that $D(x,0) > D(x+1,1)$ implies that it is optimal for Eve not to capture the red packet if the red packets are already present in the mix's buffer. Consequently, we can write (87) as

$$D(x,1) = 1 + \frac{1}{2}D(x+1,1) + \frac{1}{2}\min\{D(x,0), D(x-1,1)\} \tag{89}$$

But we know that $D(x+1,0)$ satisfies the following equation

$$D(x+1,0) \quad = \quad 1 + \frac{1}{2}D(x+2,0) + \frac{1}{2}D(x,0) \tag{90}$$

It is clear from (89) and (90) that

$$D(x+1,1) \leq D(x+2,0) \implies D(x,1) \leq D(x+1,0) \tag{91}$$

Because of symmetry of the system model, an equivalent equation of (91) would exist for $x < 0$.

Now we will show that $D(x,1)$ decreases as x increases in magnitude.

From the preceding argument, we know that $D(x,1)$ satisfies the following equation:

$$D(x,1) = 1 + \frac{1}{2}\left(D(x+1,1) + D(x-1,1)\right) \forall -\tau_1 < x < \tau_1 \tag{92}$$

General solution for the above recursive equation will be $D(x,1) = A_1 + B_1 x - 2x^2$. But, because of symmetry of the system model $D(x,1) = D(-x,1)$, therefore, $B_1 = 0$ and

$$D(x,1) = A_1 - 2x^2$$

Therefore, the $D(x,1)$ decreases as $|x|$ increases for $|x| < \tau_1$. For $x \geq \tau_1$,

we know by definition of τ_1 that $D(x,1) \geq D(x+1,0)\ \forall\ x \geq \tau_1$. But using (88), we know that $D(x+1,0) \geq D(x+1,1)$. Therefore, $D(x,1) \geq D(x+1,1)\ x \geq \tau_1$.

Inductive Step:

Lets assume that $D(x,c-1)$ decreases as $|x|$ increases and there exist a threshold τ_{c-1} such that

$$\begin{aligned} D(x,c-1) &\geq D(x+1,c-2) \forall x \geq \tau_{c-1} \\ D(x,c-1) &\geq D(x-1,c-2) \forall x \leq -\tau_{c-1} \\ D(x,c-1) &\leq D(x+1,c-2) \forall x < \tau_{c-1} \\ D(x,c-1) &\leq D(x-1,c-2) \forall x > -\tau_{c-1} \end{aligned} \tag{93}$$

Note that the optimal strategy of Eve implies that if a blue (red) packet arrives to the mix when the mix has x red (blue) packets in the buffer, then Eve who is allowed to capture y packet, should capture the packet if and only if the mix's buffer has sufficient packet in its buffer otherwise wait for this favourable condition in the future.

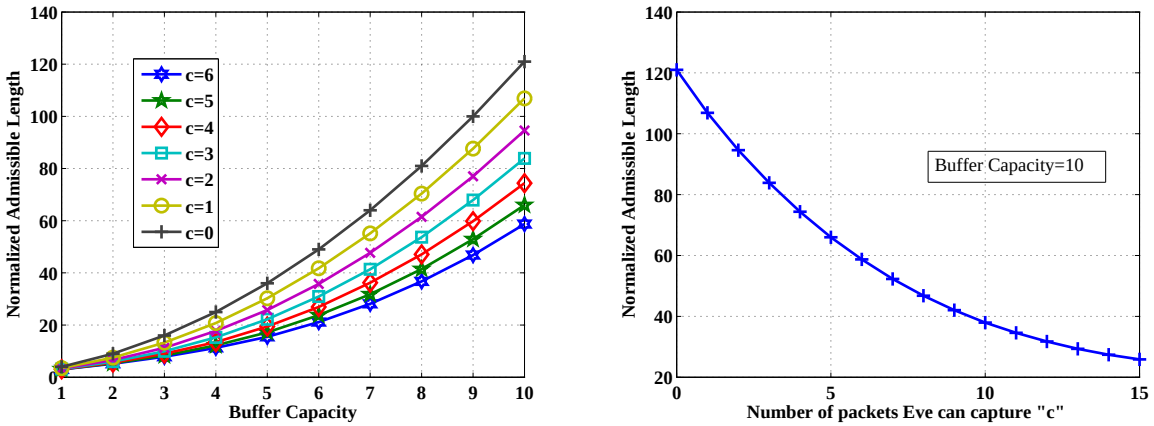
It is obviously true that the optimal strategy of Eve when she can capture y packets form the incoming streams allow her to capture the packet when the mix has x packets in its buffer, then the optimal strategy would always allow her to capture the packet when she can capture more than y packets. Therefore,

$$\begin{aligned} D(x,c) &\geq D(x+1,c-1) \forall x \geq \tau_{c-1} \\ D(x,c) &\geq D(x-1,c-1) \forall x \leq -\tau_{c-1} \end{aligned} \tag{94}$$

Note using the induction hypothesis that

$$D(x,c-1) = 1 + \frac{1}{2} D(x-1,c-1) + \frac{1}{2} D(x,c-1) \forall |x| < \tau_{c-1} \tag{95}$$

The above equation is similar to eq. 90 for $|x| < \tau_{c-1}$ and eq. 94 implies that $D(x,c) \geq$



(a) Normalized admissible length for different values of c

(b) Admissible length as a function of c

Figure 31: Admissible length of the model $\mathcal{G}_E$

$D(x+1, c-1) \forall x > \tau_{c-1}$. Therefore, we can use the same argument as we use to prove the base case to prove the theorem. □

The above theorem provides an existence proof of the optimal strategy of Eve. Although the optimal threshold is not evaluated to a closed form expression, the class of threshold strategies is significantly smaller in dimension than the set of all adversarial strategies, and consequently, an $O(k)$ search is sufficient to determine the optimal threshold.

In Figure 31a, we perform the numerical search for the optimal threshold, and plot the equilibrium payoff of the mix as a function of buffer capacity and compare it with the maximum admissible length of the mix when Eve is not allowed to capture packets. It is clear from the figure that Eve can significantly reduce her detection time in determining the source-destination pairs by effectively capturing packets from the incoming streams. Figure 31b plots the numerically computed admissible length of the model $\mathcal{G}_E$ as a function of maximum number of packets Eve can capture. As is evident from the figure, the admissible length saturates with c. In other words, Eve's capability to shorten the admissible length by capturing changes negligibly beyond a certain value of c, and the admissible length is close to that of an adversary with infinite capture capacity which is explored in the next section.

5.4.1 Asymptotically Optimal Adversary Strategy ($c = \infty$)

In this section, we investigate the scenario in the absence of intrusion detection application. Specifically, we study the admissible length when Eve is allowed to capture any number of packets from the incoming streams of the mix.

As is proved in the previous section, the optimal strategy for the mix is $\overline{\psi}$. It is easy to see that the optimal strategy would still be $\overline{\psi}$ in this limiting case where $c = \infty$ because all the arguments of the proof of Theorem 11 would still follow. In the next theorem, we show that the optimal strategy for Eve is still a threshold strategy where the threshold is 1.

Theorem 15 *The optimal strategy $\psi_E(\infty)$ when $c = \infty$ is*

- *Eve does not capture the first arrived packet.*
- *Eve captures all the subsequent arrivals from different users compare to the first arrival.*

The admissible $\mathcal{A}(k, \infty)$ for the strategy $\psi_E(\infty)$ is

$$\mathcal{A}(k, \infty) = \frac{2k+1}{2\lambda}$$

Proof: The proof of the theorem is a limiting case of the proof of Theorem 14. However, to provide an intuitive argument, assume that the first arrival is red. Note that if Eve decides to capture all subsequent blue (or red) arrivals, then she needs to wait for k (or $(k+2)$) more red (or blue) arrivals to violate the condition in (75). Since each user has equal arrival rate, the former case is more probable.

It is easy to see that the average number of arrivals required for strategy $\psi_E(\infty)$ to violate condition (75) is equivalent to the expected number of coin tosses required to obtain k heads in tosses of a fair coin and including the original stored arrival is equal to $2k+1$ tosses. Subsequently, using Lemma 4, we get the desired result. □

Note that the closed form expression for the optimal strategy $\psi_E(c)$ is as yet uncharacterized. Therefore, we investigate the admissible length of strategy $\psi_E(\infty)$ when Eve is allowed to capture $c < \infty$ packets to provide an upper bound on the admissible length of the equilibrium strategy $\psi_E(c)$ and characterize the admissible length for an adversary who knows all the future arrivals to provide a lower bound on the admissible length of the equilibrium strategy $\psi_E(c)$ in the next section.

5.5 Bounds on the optimal admissible length

5.5.1 Upper Bound

We characterize the admissible length of asymptotically optimal strategy $\psi_E(\infty)$ in the next theorem to provide an upper bound on the admissible length of the strategy $\psi_E(c)$.

Theorem 16 *The admissible length $\mathcal{A}(k,c)$ when Eve is allowed to capture c packets and the mix can store k packets in its buffer is upper bounded as*

$$\mathcal{A}(k,c) \leq \frac{(1+k)^2 - (c+1)^2 + 1 + \sum_{y=1}^{c} \frac{2y(k+1)+y^2}{2^{k+c-y}} \binom{k-1+c-y}{c-y}}{2\lambda} \tag{96}$$

Proof: As is mentioned earlier, the mix's buffer under the dominant strategy $\overline{\psi}$ would have packets of at most one user its buffer. Let $D(x,c)$ be the average number of arrivals required to violate condition (75) under strategy $\psi_E(\infty)$ when the mix has x packets in its buffer and Eve can capture c packets from the incoming streams of the mix. Conditioning on the upcoming arrival, it is easy to check that for all $c \geq 1$

$$D(x,c) = 1 + \frac{1}{2}D(x,c-1) + \frac{1}{2}D(x+1,c) \forall 1 \leq x \leq k \tag{97}$$

For $c = 0$, the following condition is satisfied

$$D(x,0) = 1 + \frac{1}{2}D(x-1,0) + \frac{1}{2}D(x+1,0) \forall 1 \leq x \leq k \tag{98}$$

The boundary conditions for the above recursive equations are $D(k+1,y) = 0 \; \forall \; 0 \leq y \leq c$. From the theory of random walks, we know that $D(x,0) = (k+1)^2 - x^2$.

It is easy to check that $D(x,c) = (k+1)^2 - (x+c)^2 + \sum_{y=1}^{c} \frac{2y(k+1)+y^2}{2^{k+1+c-y-x}} \binom{k+c-y-x}{c-y}$ satisfies (97). To prove the uniqueness of the above solution, consider that there exist another solution $D^{'}(x,c)$. Let $\Delta(x,c) = D(x,c) - D^{'}(x,c)$. Since $D(x,c)$ and $D^{'}(x,c)$ both satisfies the equation (97),

$$\Delta(x,c) = 0.5\Delta(x+1,c) + 0.5\Delta(x,c-1) \tag{99}$$

with boundary conditions $\Delta(x,0) = 0$ and $\Delta(k+1,c) = 0$. It is easy to see using the boundary conditions that $\Delta(x,1) = 0$. Similarly, we can recursively prove that $\Delta(x,c) = 0 \forall x,c$, therefore, $D(x,c) = D^{'}(x,c)$. Note that

$$\begin{aligned} D(0,c) &= D(1,c) + 1 \\ &= (1+k)^2 - (c+1)^2 + 1 + \sum_{y=1}^{c} \frac{2y(k+1)+y^2}{2^{k+c-y}} \binom{k-1+c-y}{c-y} \end{aligned} \tag{100}$$

Using Lemma 4, we get the desired result. □

As is seen the capturing capacity of the Eve can reduce the admissible length significantly. In the next subsection, we investigate the optimal strategy and admissible length for a Clairvoyant Eve who is equipped with additional information of future arrivals to provide a lower bound on the

admissible length of optimal strategy $\psi_E(c)$.

5.5.2 Lower Bound (Clairvoyant Eve)

Theorem 17 *The admissible length $\mathcal{A}(k,c)$ for a Chaum mix with buffer capacity k, serving two users having Poisson arrival process with equal arrival rate λ against an Eve having capture capability c is lower bounded by*

$$\mathcal{A}(k,c) \geq \begin{cases} \frac{(k+1)\left(2-\frac{\binom{2k+2}{k+1}}{2^{2k+1}}\right)+\sum_{i=c+1}^{k}\left(\frac{\binom{k+i}{i}(i-c)(2k+2-i-c)}{2^{k+i}}\right)}{2\lambda} \forall c < k \\ \frac{2(k+1)-(k+1)\frac{\binom{2k+2}{k+1}}{2^{2k+1}}}{2\lambda} \forall c \geq k \end{cases} \tag{101}$$

Proof:

Case 1: $c \geq k$

Since Eve knows all the future arrivals, she knows which source would transmit $k+1$ arrivals earliest. She can capture packets of the other source which transmitted fewer than $k+1$ packets at the time of the system losing anonymity. Therefore, it is easy to see that $\forall c \geq k$ the admissible length would be a constant. Note that the probability of the event that exactly $k+1+i$ total arrivals required such that one user has exactly $k+1$ packets among these $k+1+i$ arrivals is

$$\frac{\binom{k+i}{i}}{2^{k+i}} \forall 0 \leq i \leq k.$$

Therefore, the expected number of arrivals requires to obtain first $k+1$ arrivals of a user is

$$\begin{aligned} N_{CE} &= \sum_{i=0}^{k}(k+1+i)\frac{\binom{k+i}{i}}{2^{k+i}} \\ &= (k+1)\sum_{i=0}^{k}\frac{\binom{k+i+1}{i}}{2^{k+i}} \\ &= (k+1)\sum_{i=0}^{k} \text{ coeff. of } x^{k+1} \text{ in } \frac{(1+x)^{k+i+1}}{2^{k+i}} \\ &= (k+1)\left(2-\frac{\binom{2k+2}{k+1}}{2^{2k+1}}\right) \end{aligned}$$

Using Lemma 69, we get the desired result.

Case 2: $c < k$

Without loss of generality, assume that $k+1$ red packets arrive before $k+1$ blue packets. Let Z be the random variable denoting the number of arrived blue packets when $k+1$ red packets arrive. Clearly, from the assumption, $Z \in \{0,1,\ldots,k\}$ and $\mathbb{P}(Z=i) = \frac{\binom{k+i}{i}}{2^{k+i}}$. If $z \leq c$, the number of arrivals required for Clairvoyant Eve to know the source-destination pairs is $k+1+z$ by capturing the packets of blue user. If $z > c$, it is clear that to achieve condition (75), Clairvoyant eve should

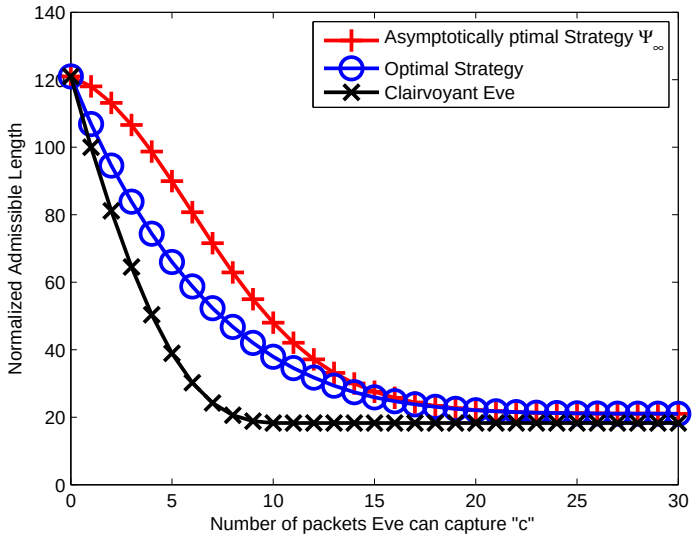


Figure 32: Comparison between admissible length of optimal strategy, Clairvoyant Eve and the asymptotically optimal strategy as the function of number of packets Eve can capture for $k = 10$

be aware when the difference between number of arrived packets from each user becomes $k+1-c$ (by capturing c packets of the user with minimum packets the difference between two users packets would become $k+1$). Note that when one user has $k+1$ packets and other user has z packets where $z \in \{c+1, c+2, \cdots, k\}$, then the additional arrivals required for the difference between the number of packets arrived from the two users to be $k+1-c$ is equivalent to duration of a simple random walk starting from position $k+1-z$ before getting absorbed in the barriers $|k+1-c|$. We know from theory of random walks that the duration is $(z-c)(2k+2-(z+c))$. Therefore, the total time for the Clairvoyant Eve to know the source-destination pairs when $z > c$ is $(k+1+z)+(z-c)(2k+2-(z+c))$. Subsequently,

$$\begin{aligned}
\mathbb{E}[N] &= \mathbb{E}[\mathbb{E}[N|Z]] \\
&= \textstyle\sum_{z=1}^{c} \mathbb{P}(Z=z)\mathbb{E}[N|Z=z] + \sum_{z=c+1}^{k} \mathbb{P}(Z=z)\mathbb{E}[N|Z=z] \\
&= \textstyle\sum_{z=1}^{k} \mathbb{P}(Z=z)(k+1+z) + \sum_{z=c+1}^{k} \mathbb{P}(Z=z)(z-c)(2k+2-z-c)
\end{aligned}$$

Using (101) and Lemma 4, we get the desired result. □

We plot the upper and lower bounds on the normalized admissible length given in Theorem 16 and Theorem 17 as a function of number of packets Eve can capture and compare it against the optimal admissible length. As is obvious, the upper bound provides a very good approximation when c is large compared to k, thus suggests that by applying the simple strategy $\psi_E(\infty)$, instead of $\psi_E(c)$, Eve can achieve almost equal admissible length for large c.

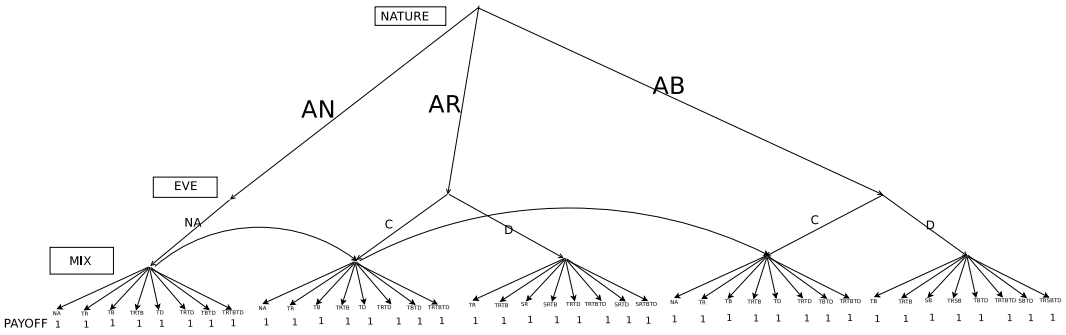


Figure 33: Extensive form of game between Eve and the mix

5.6 General Model ($\mathcal{G}_G$)

The models presented in Sections 5.3 and 5.4 studied the system when only one party, the mix or Eve, have additional capabilities. In this section, we analyse the general model $\mathcal{G}_G$ when both parties are empowered. Specifically, we allow the mix to transmit limited number of dummy packets $d(t)$ in t time units such that $\frac{d(t)}{t} \leq r$ for a given positive constant r, and Eve can capture at most c packets from the incoming streams.

As both parties are empowered, it becomes necessary to describe the system as a game played in stages, where each stage is triggered by an event identifiable to both the mix and Eve. The payoff of the game merely measures the number of stages played until the game stops which then is used to evaluate the admissible length. At any given time point, the mix cannot know if an arrival is captured by Eve or not, therefore an arrival cannot be used to trigger a stage in the game. In fact, the mix, as a player, cannot identify the time of arrival of a captured packet. It is therefore necessary to describe the problem in a discrete time system model where we assume that time is divided into infinitesimal slots of length Δt, so that the stage of a game can be identified with a slot rather than an arrival. Owing to the Poisson assumption, in an infinitesimal slot, the probability of multiple packets arriving is negligible and further, the arrival probability of a packet in each slot is independent.

Discrete Time Approximation of a Poisson Process: A red packet can arrive in a slot with probability $p \approx \lambda_1 \Delta t$, a blue packet can arrive with probability $q \approx \lambda_2 \Delta t$ and the probability that a slot contains no arrivals is $1 - p - q$. Arrivals in each slot are independent of arrivals in any past or future slot. Note that the above slotted arrival process is an accepted approximation of Poisson arrival process as it converges to the continuous time Poisson as $\Delta t \to 0$. In this slotted arrival model, we assume that the mix transmits $d(n)$ dummy packets in n time slots such that $\frac{d(n)}{n} \leq r$.

At every stage of the model $\mathcal{G}_G$, there are three possible arrival sets (a red packet arrives, a

blue packet arrives or no packet arrives) whose probability distribution is fixed. At every stage, Eve needs to decide to capture the arrival or not and the mix needs to decide whether to store an (uncaptured) arrival or/and transmit data or dummy packets. The actions of the mix and Eve are dependent on arrivals and the state of the system. The information available to Eve and the mix are however different in each stage, since the mix is unaware of Eve's actions and consequently is uncertain about the actual arrival set. This necessitates a formal description of the extensive form of the game along with the different information sets.

We reuse the notation $\mathcal{G}_G$ to denote this game between Eve and the mix. To incorporate the random arrivals of packets, we include a third player "nature" which has a fixed strategy known to both players. The game $\mathcal{G}_G$ consists of three elements 1) Actions' space of players, 2) Information sets of Players, and 3) Player's payoff. Let $\{U^E, U^M\}$ and $\{N^E, N^M\}$ denote the action's space and information sets of Eve and the mix respectively.

The extensive form of a single stage of the game is shown in the figure 33. The notations are explained as follows:

1. Nature's Moves (U^N):

   AB: A blue packet arrives **AR:** A red packet arrives **AN:** No packet arrives

2. Eve's Moves (U^E):

   C: Capture the arrived packet **D:** Do not capture the arrived packet

3. Mix's Moves (U^M):

   NA: No action **TR:** Transmit a red packet **SR:** Store the arrived red packet if the buffer space allowed **TB:** Transmit a blue packet **SB:** Store the arrived blue packet if the buffer space allowed **TRSB:** Transmit a red and store the arrived blue packet if the buffer space allowed **TRTB:** Transmit a red and a blue packet. **TD** Transmit a dummy packet. **TRTD** Transmit a red and a dummy packet. **SRTD:** Store the arrived red packet and transmit a dummy packet. **TBTD:** Transmit a blue packet and transmit a dummy packet **SBTD:** Store the arrived blue packet and transmit the dummy packet **SRTBTD:** Store the arrived red packet and transmit the blue packet and dummy packet **TRSBTD:** Transmit the red and dummy packet and store the arrived blue packet

As is clear from the figure, nature plays each move with equal probability from the possible three moves: AR, AB, and AN. Eve perfectly knows nature's moves, therefore, she has three information

sets: $N^E = \{\eta^E_{AB}, \eta^E_{AR}, \eta^E_{AN}\}$ where η^E_x represents that nature played the move x. Eve's alternatives corresponding to these information sets are: $U^E_{\eta^E_{NR}} = \{C, D\}$, $U^E_{\eta^E_{NB}} = \{D, C\}$, and $U^E = \{U^E_{\eta^E_{NB}} \cup U^E_{\eta^E_{AR}}\}$. It is not feasible for the mix to perfectly identify Eve's or nature's move, and its information sets are completely determined by the packets that arrived to it: $N^M = \{\eta^M_{AN}, \eta^M_{AR}, \eta^M_{AB}\}$ where η^M_x represents that x packets arrive to the mix. The mix's alternatives corresponding to its information sets are as follows:

$U^M_{\eta^M_{AN}} = \{NA, TR, TB, TRTB, TD, TRTD, TBTD, TRTBTD\}$

$U^M_{\eta^M_{AR}} = \{TR, TRTB, SR, SRTB, TRTD, TRTBTD, SRTD, SRTBTD\}$

$U^M_{\eta^M_{AB}} = \{TB, TRTB, SB, TRSB, TBTD, TRTBTD, SBTD, TRSBTD\}$

At the end of each stage of the game, the mix receives payoff 1 while Eve receives payoff -1. The game ends when Eve determines the source-destination pairs or equivalently total transmissions of packets of any color by the mix is greater than total arrivals of packets of any color by nature. Therefore, it is trivially true using the definition of the admissible length that the payoff of the game measures the admissible length (in multiples of Δt) exactly.

As is evident from Figure 33, the game between Eve and the mix is not a feedback game [79] because information sets of the mix include nodes corresponding to branches emanating from different information sets of Eve. Although, it is not always true for a non-feedback game to have a pure-strategy Nash equilibrium, we show in the following theorem that there exist a pure dominant strategy for the mix which is identical to that in the model $\mathcal{G}_M$, and the optimal strategy for Eve is a time varying threshold strategy, a generalization of the optimal strategy of Eve in model $\mathcal{G}_E$, which consequently, proves that there exists a pure strategy Nash equilibrium of the game $\mathcal{G}$.

Theorem 18 *For the above mentioned game $\mathcal{G}$, the dominant strategy $\delta^M : N^M \to U^M$ for the mix is*

1. $\delta^M(\eta^M_{AN}) = \{NA\}$

2. $\delta^M(\eta^M_{AR}) = \begin{cases} \{TRTB\} & \textit{if the mix's buffer has blue packets} \\ \{TRTD\} & \textit{If the mix's buffer is full and it} \\ & \textit{can transmit a dummy packet} \\ \{SR\} & \textit{otherwise} \end{cases}$

3. $\delta^M(\eta^M_{AB}) = \begin{cases} \{TRTB\} & \textit{if the mix's buffer has red packets} \\ \{TBTD\} & \textit{If the mix's buffer is full and it} \\ & \textit{can transmit a dummy packet} \\ \{SB\} & \textit{otherwise} \end{cases}$

and the optimal strategy $\delta^E : N^E \to U^E$ *for the Eve which can capture* c *packets against the dominant strategy* δ^M *of the mix at the time epoch* n *is*

1. $\delta^E(\eta^E_{AN}) = \{NA\}$

2. $\delta^E(\eta^E_{AR}) = \begin{cases} \{D\} & \textit{Mix's buffer has red packets} \\ \{D\} & \textit{Mix's buffer has } x \textit{ blue packets} \\ & \textit{and } x \leq \tau_c(n) \\ \{C\} & \textit{Mix's buffer has } x \textit{ blue packets} \\ & \textit{and } x > \tau_c(n) \end{cases}$

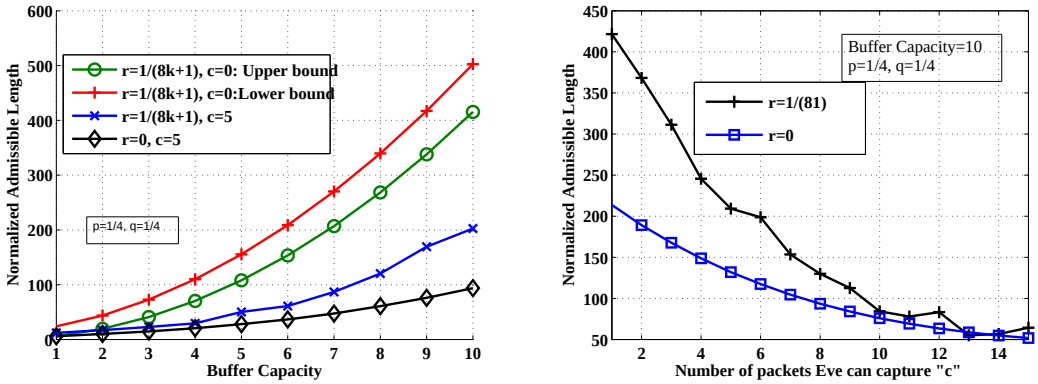
3. $\delta^E(\eta^E_{AB}) = \begin{cases} \{D\} & \textit{Mix's buffer has blue packets} \\ \{D\} & \textit{Mix's buffer has } x \textit{ red packets} \\ & \textit{and } x \leq \tau_c(n) - 1 \\ \{C\} & \textit{Mix's buffer has } x \textit{ red packets} \\ & \textit{and } x > \tau_c(n) - 1 \end{cases}$

where $\tau_c(n) \in \mathbb{N}$ *such that* $\tau_c(n) < k + \lfloor nr \rfloor$

Proof: Refer to appendix. □

The above theorem is the first such characterization of an optimal mixing strategy in the face of an active adversary. Further, the theorem also characterizes the optimal strategy of Eve as a threshold strategy, which allows for numerical methods to compute the optimal thresholds by reducing the dimensionality of the search. Note that the time variance of the threshold is an outcome of the number of dummy packets transmitted by the mix. For a fixed number of dummy transmissions available, the threshold strategy is still time invariant.

The admissible length for this game is not characterized using a closed form expression and we plot the Monte Carlo simulation of the variation of the mix's payoff with its buffer capacity in Figure 34a for $c = 5$ and $r = \frac{1}{8k+1}$ and compare it against the two extreme cases when $c = 5$ and $r = 0$, and $c = 0$ and $r = \frac{1}{8k+1}$. As is expected, the payoff of the modified game when Eve and the mix are both empowered lies between the cases when individual players are separately empowered. In figure 34b,



(a) Comparison of admissible length as a function of buffer capacity for Poisson approximation model of arrival process

(b) Comparison of admissible length for Poisson approximation model as a function of c

Figure 34: Payoff of the game $\mathcal{G}$

we plot the variation of the mix's payoff for game $\mathcal{G}_G$ as a function of the capture capacity when the mix's buffer capacity is 10 and the maximum allowable dummy packet rate is 1/81 packets per slot.

Infinite Capture Capacity It is important to note here that as Figure 34b indicates, the impact of dummy packets on the payoff of the game $\mathcal{G}_G$ can be reduced significantly if Eve is allowed to capture sufficient packets from the incoming streams of the mix. However, decrement in admissible length saturates after a certain c, and the asymptotic admissible length is characterizable analytically. In fact, under asymptotic conditions, the discrete time approximation of the Poisson arrival is not necessary, and the following theorem characterizes the admissible length at the equilibrium of the general model for Poisson arrival process when Eve is allowed to capture any number of packets.

Theorem 19 *The admissible length $\mathcal{A}(r, k, c = \infty)$ when Eve can capture any amount of packets $(c = \infty)$ and the maximum allowable dummy rate of the mix is r serving two users with Poisson arrival process of rate λ , then*

$$\frac{2k-1}{2\lambda - 2r} \leq \mathcal{A}(r, k, c = \infty) \leq \frac{2k+1}{2\lambda - 2r} \tag{102}$$

Proof: When $c = \infty$, the optimal strategy for Eve is to wait for the first arrival, and then capture every subsequent packet that belongs to a source other than that of the packet in the buffer. By applying the stopping time argument used in the proof of Theorem 13, the upper and lower bounds are characterized analytically. The details of the proof can be found in the appendix. □

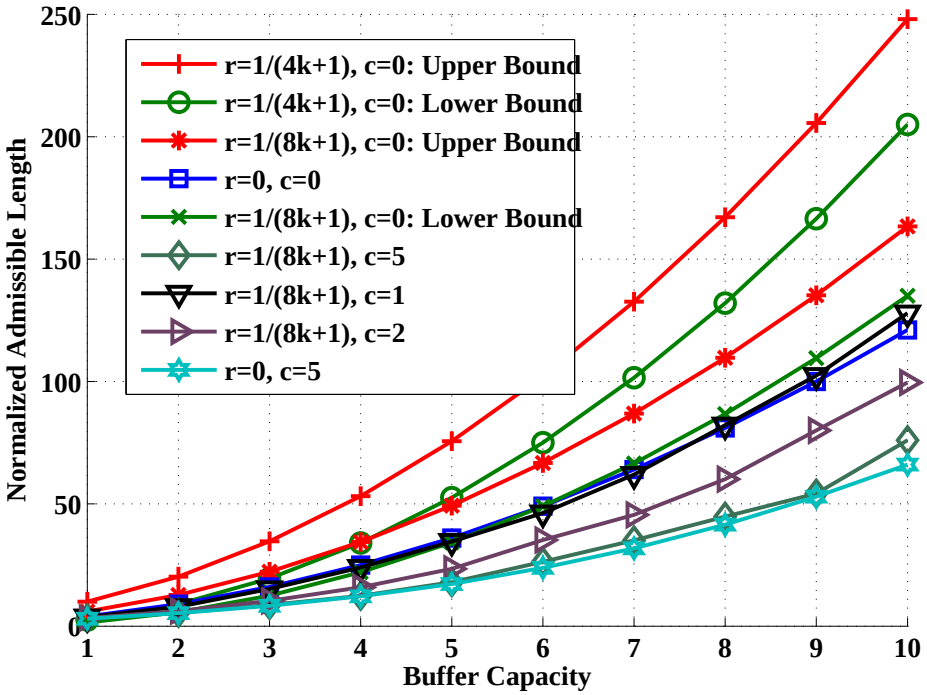


Figure 35: Comparison of admissible lengths as a function of buffer size

5.7 Comparative analysis

Figure 35 plots the variation of admissible length as function of buffer capacity for the different models that we studied. For purposes of comparison, we use the optimal mixing strategy for game $\mathcal{G}$ in Section 5.6 to simulate the normalized admissible length for the system model $\mathcal{G}_G$ when the arrival processes are Poisson. Although the saddle point result was derived using a discrete time approximation, we believe the optimality of the strategies to hold in the general Poisson arrival model.

As is obvious, the admissible length is maximum for the case $(c = 0, r > 0)$ and is minimum for $(c > 0, r = 0)$. The admissible length of the other two cases $(c = 0, r = 0)$ and $(c > 0, r > 0)$ lie between the above two cases. We can also see from the figure that admissible length increases as c decreases for a constant r. Also note that in comparison to the admissible length for the basic model $(c = 0, r = 0)$, the performance of the general model could be greater or lesser depending on the allowed c and r (the admissible length for $(c = 2, r = \frac{1}{8k+1})$ is lesser while the admissible length for $(c = 1, r = \frac{1}{8k+1})$ is greater). In general, for a given allowable dummy rate $r^* > 0$, there exists a minimum capture limit c^* such that the general model has lower admissible length. Determining the relationship between r^* and c^* would provide valuable insights into joint design of intrusion

detection and mixing systems.

5.8 Summary

In this chapter, the admissible length for perfect anonymity was used as a tool to study optimal mixing strategies. The admissible length not only provides the best operating criteria for anonymous systems, but also helps evaluate the effectiveness of mixing strategies in providing maximum anonymity. Furthermore, since the admissible length directly models the adversary action, the framework can be generalized to include active adversaries capable of capturing packets. While equal arrival rates and Poisson models have been used to determine the analytical results in this work, the mixing strategies derived work independent of the nature and rate of arrivals, and only depend on the state of the buffer and dummy packet limitations. Indeed, we believe, for arrivals modelled as general renewal processes, the insights derived in this work would apply directly [80].

6 Tradeoff between anonymity and QoS constraints in signaling games

Signaling games are an important class of games which are used to model financial behavior in markets [81], economic reasoning in a job market [82], and evolutionary behavior in emergence of a language [83]. Signaling games consist of many senders and a common receiver. Each sender belongs to one of multiple types. These types represent sensitive information such as individual economic condition, a company's financial status or political affiliation. In a signaling game, each sender transmits a message to the common receiver, who reads the message and responds with an action. Every transmitted message and it's receiver response results in a pair of rewards for the receiver and the corresponding sender. The rewards are a function of the transmitted message, receiver action and the type of the sender. The sender is perfectly aware of his/her type whereas the receiver generates a belief about the type knowing the senders' strategies. An important aspect of study in signaling games is to find the equilibrium conditions which are characterized by a strategy of the sender and a strategy of the receiver such that they are optimal against each other. In the study of equilibrium conditions in signaling games, there are two types of equilibria that are considered important:

1. **Pooling Equilibrium:** Senders of all types transmit the same message.

2. **Separating Equilibrium:** Each type of sender transmits a distinct message.

Note that under the separating equilibrium, no sender cannot hide its type from the receiver whereas under the pooling equilibrium, senders are completely anonymous. The explicit study of anonymity in signaling games is the focus of this work. In particular we investigate the tension between the tangible rewards of the classical signaling games and the information leaked to the receiver about a senders type. Although not a classical example of signaling games, the following description of a data networking problem captures the underlying theme of our contributions.

Consider a six node network as shown in Figure 36. There are two sources S_1 and S_2 who want to send their packets to their corresponding destination D_1 and D_2 respectively. There are two paths from S_1 to D_1: the path through mix M_1, $S_1 \rightarrow M_1 \rightarrow D_1$ and the path through mix M_2, $S_1 \rightarrow M_2 \rightarrow D_1$. Similarly, there are two paths from S_2 to D_2: the path from mix M_1, $S_2 \rightarrow M_1 \rightarrow D_2$ and the path through mix M_2, $S_2 \rightarrow M_2 \rightarrow D_2$. There is a passive eavesdropper who has access to all the communication links in this network. This eavesdropper wants to know the source-destination pairs while sources want to hide their destination. Assume that all communications are encrypted

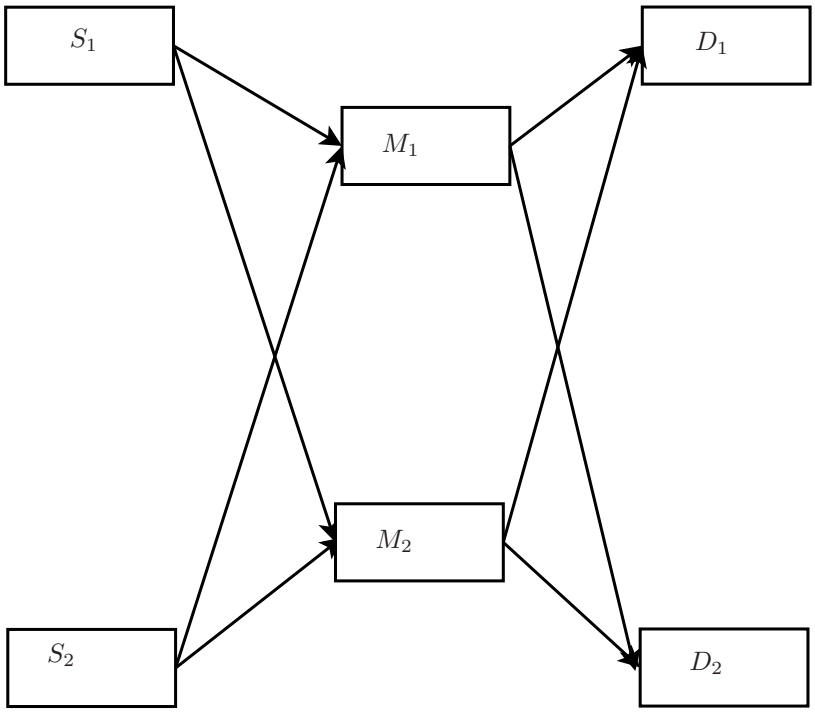


Figure 36: An interpretation of the requirement of anonymity in data network as a signaling game between sources and eavesdroppers

thus the eavesdropper cannot access any information from packets' headers. Consider the following two cases:

1. The optimal path (delay, throughput, or congestion optimal) between $S_1 - D_1$ and $S_2 - D_2$ are the paths through mix M_1 ($S_1 \rightarrow M_1 \rightarrow D_1$ and $S_2 \rightarrow M_1 \rightarrow D_2$) or the paths through mix M_2 ($S_1 \rightarrow M_2 \rightarrow D_1$ and $S_2 \rightarrow M_2 \rightarrow D_2$) which means that all the messages of both the sources go through either mix M_1 or mix M_2.

2. The optimal paths between $S_1 - D_1$ and $S_2 - D_2$ are $S_1 \rightarrow M_1 \rightarrow D_1$ and $S_2 \rightarrow M_2 \rightarrow D_2$ respectively.

In case 1, where all the packets of both the sources go through a common mix (M_1 or M_2), even by choosing their QoS optimal path both the sources can achieve perfect anonymity (if buffer size of the common mix is sufficiently large 3). In contrast, under case 2, when the optimal paths for both users are non overlapping, an eavesdropper can merely monitor the traffic on the links to identify the source destination pairs accurately. This scenario then raises the following questions:

1. How much traffic the sources should divert to their sub-optimal paths to achieve some destination anonymity?

2. How can the tradeoff between anonymity and network QoS be quantified and optimized?

3. If different users have different anonymity requirements, is there an equilibrium solution that no user has incentive to deviate from?

The example described above can be interpreted as a signaling game by considering the path that the sources (senders of the signaling game) choose for transmitting their packets as the message of the signaling game transmitted to the eavesdropper (receiver of the signaling game), by choosing the type of the sources (senders of the signaling game) as its destination (D_1 or D_2), and by choosing a suitable payoff that reflects the requirement of anonymity along with the users QoS.

In this work, we choose the average Shannon entropy over the types of senders of signaling games as the measure of type anonymity which is described in detail in Section 6.1. Such information-theoretic measures, based on Shannon's entropy [37] have been proposed to measure the anonymity provided by mixes and mix-networks [3, 76, 84]. The system model is described in detail in the following section.

6.1 System Model

In this section, we describe the signaling game model and the measure of type anonymity used to derive our results on the equilibrium behaviour. We define the signaling game model $\mathcal{G}_k$ as a $5-$tuple $\mathcal{G}_k = \{\mathcal{T}, \mathcal{M}, \mathcal{A}, \Lambda, \mathcal{R}_D\}$ where each element of this tuple described below:

- **Senders, their types ($\mathcal{T}$), and the message set ($\mathcal{M}$):** A *sender* is the player who transmits messages in a signaling game. Senders can be of different types and $\mathcal{T}$ is the set representing all the possibilities over the type of senders. In this work, we assume $\mathcal{T} = \{\mathcal{T}_1, \mathcal{T}_2\}$. The prior probability of each type is equal and senders are aware of their types which they wish to hide from the receiver. Each sender chooses one message from the message set $\mathcal{M} = \{m_1, m_2, \cdots, m_k\}$ to transmit. We define the strategies of type $\mathcal{T}_1$ and type $\mathcal{T}_2$ senders as probability distributions $\mathbf{p} = \{p_1, \cdots, p_k\}$ and $\mathbf{q} = \{q_1, \cdots, q_k\}$ over the message set $\mathcal{M}$ respectively.

- **Receiver and its action space ($\mathcal{A}$):** A sender transmits its message to the receiver. The receiver after receiving the message m_i where $i \in \{1, 2, \cdots, k\}$ can choose an action from the set $\mathcal{A}_i$. We define $\mathcal{A} \stackrel{\triangle}{=} \cup_{i=1}^{k} \mathcal{A}_i$ as all possible actions to the receiver. In this work, we exclude the effect of actions of the receiver on the game and assume $\mathcal{A}_i$ is a singleton set identical for all i.

- **Direct Payoff:** Since $\mathcal{A}_i$ is a singleton set, the payoff of a sender depends only on the transmitted message. Assume that by transmitting message m_i, the payoff of a type $\mathcal{T}_1$ sender is c_i and a type $\mathcal{T}_2$ sender is d_i where $c_i, d_i \in \mathbb{R}\ \forall i \in 1, ..., k$. This payoff that comes directly from transmitting the signal, we refer as the direct payoff. We define $\mathcal{R}_D \stackrel{\triangle}{=} \{\{c_i\}_{i=1}^k, \{d_i\}_{i=1}^k\}$ as the collection of all possible direct rewards of senders. If the type $\mathcal{T}_1$ and the type $\mathcal{T}_2$ sender use strategy $\mathbf{p}$ and $\mathbf{q}$ respectively then their direct payoffs are defined as

$$\begin{aligned} \text{Type } \mathcal{T}_1 : \mathcal{P}_1^D(\mathbf{p}) &\stackrel{\triangle}{=} \sum_i p_i c_i \\ \text{Type } \mathcal{T}_2 : \mathcal{P}_2^D(\mathbf{q}) &\stackrel{\triangle}{=} \sum_i q_i d_i. \end{aligned}$$

- **Information leakage cost or anonymity reward:** Note that if senders belonging to the two types use different strategies, i.e. $\mathbf{p} \neq \mathbf{q}$, then the received message could provide some information about the type of the sender. We use the average Shannon entropy of this posterior distribution as the measure of anonymity. According to Bayes' rule, if the message m_i is transmitted, then given that the receiver knows the strategy of the sender, the probability that the sender belongs to type $\mathcal{T}_1$ is $p_i/(p_i + q_i)\ \forall i \in \{1, \cdots, k\}$ when $p_i + q_i > 0$. Specifically, the anonymity reward of the senders are defined as:

$$\begin{aligned} \text{Type } \mathcal{T}_1 : \quad \mathcal{P}_1^A(\mathbf{p}, \mathbf{q}) &\stackrel{\triangle}{=} \sum_{i=1}^k p_i h\left(\tfrac{p_i}{p_i+q_i}\right) \\ \text{Type } \mathcal{T}_2 : \quad \mathcal{P}_2^A(\mathbf{p}, \mathbf{q}) &\stackrel{\triangle}{=} \sum_{i=1}^k q_i h\left(\tfrac{p_i}{p_i+q_i}\right) \end{aligned}$$

  where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy for $x \in [0, 1]$ when each types of senders knows the strategy of the other types. In this definition for cost of anonymity, we assume that $0h\left(\frac{0}{0}\right) = 0$.

- **Net payoff ($\mathcal{P}$):** We define the net payoff of $\mathcal{G}_k$ as a linear combination of the direct payoff and anonymity reward. Specifically, the net payoffs of type $\mathcal{T}_1$ and type $\mathcal{T}_2$ senders are defined as

$$\begin{aligned} \mathcal{P}_1(\mathbf{p}, \mathbf{q}) &\stackrel{\triangle}{=} \lambda_1 \mathcal{P}_1^D(\mathbf{p}) + (1-\lambda_1)\mathcal{P}_1^A(\mathbf{p}, \mathbf{q}) \\ \mathcal{P}_2(\mathbf{p}, \mathbf{q}) &\stackrel{\triangle}{=} \lambda_2 \mathcal{P}_2^D(\mathbf{q}) + (1-\lambda_2)\mathcal{P}_2^A(\mathbf{p}, \mathbf{q}) \end{aligned} \tag{103}$$

  respectively.

It is important to note here that the weighting factors λ_is allow us to study the trade-off between the two opposing objectives: anonymity and the direct payoff of the signaling game. Furthermore,

by using different λ_i for different users, we are able to study equilibrium conditions for users with different privacy requirements. To the best of our knowledge, this is the first work to study the joint optimization of strategies for users with differing privacy requirements.

The key component of the analysis of any game theoretic model is the study of equilibrium conditions where no player of the game has an incentive to deviate from. The equilibrium conditions of signaling games are known as Perfect Bayesian-Nash equilibrium conditions which are an extension of Bayes-Nash equilibrium conditions [85]. This Perfect Bayesian-Nash equilibrium conditions require the fulfillment of the following three conditions:

1. Receiver generates a posterior belief on the type of the sender using the received message and knowledge of the strategies of all types of senders.

2. The strategy that receiver chooses must maximize its expected reward based on the derived posterior belief of sender's type.

3. Each sender's strategy is chosen to optimize the net reward for his/her type knowing that the receiver is perfectly aware of the chosen strategies of all types of senders.

In this work, we consider a receiver with a singleton action space, therefore, the Perfect-Bayesian Nash equilibrium would rely on senders of both the types optimizing their strategies knowing the optimal strategies of other types and also knowing that receiver uses the knowledge of the senders' strategies to determine the type from the message.

Definition: A pair of strategies $\mathbf{p}^* = \{p_1^*, ..., p_k^*\}$ and $\mathbf{q}^* = \{q_1^*, ..., q_k^*\}$ is defined to be Perfect Bayesian-Nash equilibrium of $\mathcal{G}_k$ if and only if

$$\begin{aligned} \mathbf{p}^* &= \text{argmax}_{\mathbf{p}}\, \mathcal{P}_1(\mathbf{p}, \mathbf{q}^*) \\ \mathbf{q}^* &= \text{argmax}_{\mathbf{q}}\, \mathcal{P}_2(\mathbf{p}^*, \mathbf{q}) \end{aligned} \tag{104}$$

Note that perfect Bayesian-Nash equilibrium conditions describe the optimal sender's strategy in the worst case scenario from the sender's perspective where an intelligent (perfectly rational) receiver knows the sender's strategy. An important part of the analysis of our signaling game model is to prove the existence of Perfect Bayesian-Nash equilibrium conditions and interpret the outcome of games with the help of these equilibrium conditions.

6.2 Existence of Bayesian-Nash equilibrium

In this section, we show that Perfect Bayesian-Nash equilibrium of a signaling game $\mathcal{G}_2 = \{\mathcal{T}, \{m_1, m_2\}, \{a\}, \{\lambda_1, \lambda_2\}, \{(c_1, c_2), (d_1, d_2)\}$ exists for all $\lambda_1, \lambda_2 \in [0, 1]$. It is important to note that fixed point theorems (such as Kakutani and Brouwer) that are central in proving the existence of equilibrium conditions in game theory [86–88] can not be applied to our analysis because the convexity property of the best response function is not satisfied in our model. In the classical signaling games, the convexity property of the best response function is maintained because the senders' payoff is a deterministic function of receivers and its own actions which is not the case here because the actions of different types of senders affect each other's payoff directly.

In the following theorem, we show the existence of perfect Bayesian-Nash equilibrium in the game $\mathcal{G}_2$ when $\lambda_1 = \lambda_2$. We prove the existence by analyzing different cases separately as shown below:

Theorem 20 *If $\lambda_1 = \lambda_2 = \lambda \in [0, 1]$, a perfect Bayesian-Nash equilibrium point of game $\mathcal{G}_2$ always exists. The pair of sender strategies that achieve the equilibrium are as follows:*

1. $\lambda = 0$*:* $p_1^* = q_1^*$ ***(Pooling)***

2. $0 < \lambda < 1$

   i. $c_1 \leq c_2$, $d_1 \leq d_2 : p_1^* = q_1^* = 0$ ***(Pooling)***

   ii. $c_1 \geq c_2$, $d_1 \geq d_2 : p_1^* = q_1^* = 1$ ***(Pooling)***

   iii. $c_1 > c_2$, $d_1 \leq d_2$ *or* $c_1 \geq c_2$, $d_1 < d_2$*:*

      A. $0 \leq \lambda \leq \lambda^* : p_1^* = 1$, $q_1^* = 1$ *or* $p_1^* = 0$, $q_1^* = 0$ ***(Pooling)***

      B. $\lambda^* \leq \lambda \leq 1$*:* $p_1^* = 1$, $q_1^* = 0$ ***(Separating)***

where $\lambda^* = \max\left\{\frac{1}{1+c_1-c_2}, \frac{1}{1+d_2-d_1}\right\}$.

Proof:

Case1: Note that

$$p_1^* = \underset{p_1}{\operatorname{argmax}}\, p_1 h\left(\frac{p_1}{p_1 + q_1^*}\right) + p_2 h\left(\frac{p_2}{p_2 + q_2^*}\right)$$

Since binary entropy $h(x)$ is maximized at $x = 0.5$, $p_1 = q_1^*$ is a unique maximum of the right hand side in the above equation.

Case 2(i), 2(ii): We know $p_1^* = \text{argmax}_{p_1} \mathcal{P}_1(p_1, q_1)$. Note that

$$\begin{aligned} p^* &= \underset{p}{\text{argmax}}\, \mathcal{P}_1^A(p, q^*) = q^* \ \forall\ q^* \in [0,1] \\ \text{and } p^* &= \begin{cases} \text{argmax}_p\, \mathcal{P}_1^D(p) = 0 & \text{when} \quad c_1 < c_2 \\ \text{argmax}_p\, \mathcal{P}_1^D(p) = 1 & \text{when} \quad c_1 > c_2 \end{cases} \\ \implies p_1^* &= \underset{p_1}{\text{argmax}}\, \lambda \mathcal{P}_1^D(p_1) + (1-\lambda)\mathcal{P}_1^A(p_1, q^*) \\ &< q^* \forall q^* > 0 \text{ when } c_1 < c_2 \\ &> q^* \forall q^* > 0 \text{ when } c_1 > c_2 \end{aligned}$$

Similarly, we can show that $0 \leq q_1^* \leq p^*$ $(p^* \leq q_1^* \leq 1)$ for all $p^* > 0$ when $d_1 \leq d_2$ $(d_1 \geq d_2)$. Therefore, equilibrium point exist only for $p_1^* = q_1^* = 0$ $(p_1^* = q_1^* = 1)$.

Case 2 (iii) A.: Assume that a type $\mathcal{T}_1$ sender's strategy is $p_1^* = 1$, then we investigate the condition on λ such that a type $\mathcal{T}_2$ sender's optimal strategy is $q_1^* = 1$. Specifically, we require

$$\begin{aligned} &\mathcal{P}_2(1,1) > \mathcal{P}_2(1, q_1)\ \forall 0 \leq q_1 < 1 \\ &\implies \lambda < \frac{q_2 + q_1\left(1 - h\left(\frac{q_1}{1+q_1}\right)\right)}{q_2(1+d_2-d_1) + q_1\left(1 - h\left(\frac{q_1}{1+q_1}\right)\right)} \forall 0 \leq q_1 < 1 \end{aligned} \tag{105}$$

Note that

$$\frac{q_2 + q_1\left(1 - h\left(\frac{q_1}{1+q_1}\right)\right)}{q_2(1+d_2-d_1) + q_1\left(1 - h\left(\frac{q_1}{1+q_1}\right)\right)} \geq \frac{1}{1+d_2-d_1} \tag{106}$$

$\forall q_1 \in [0,1)$ and equality occurs in (106) if and only if $q_1 = 0$. Therefore (105) and (106) imply that when

$$\lambda < \frac{1}{1+d_2-d_1} \tag{107}$$

then $\mathcal{P}_2(1,1) > \mathcal{P}_2(1, q_1) \forall q_1 \in [0,1)$. Furthermore, it is trivial to see that

$$p_1^* = \underset{p_1}{\text{argmax}}\, \mathcal{P}_1(p_1, 1) = 1 \tag{108}$$

since $p_1 = 1$ maximizes both the direct and anonymity payoffs in this case. Consequently, $p_1^* = 1, q_1^* = 1$ is an equilibrium point when $\lambda < \frac{1}{1+d_2-d_1}$. Using the similar argument as given in (105)-(108), we can show that the criterion $\mathcal{P}_1(0,0) \geq \mathcal{P}_1(p, 0)\ \forall\ p \in (0,1]$ proves that $p_1^* = 0, q_1^* = 0$ is also an equilibrium point when $\lambda < \frac{1}{1+c_1-c_2}$.

Case 2 (iii) B.: Assume that a type $\mathcal{T}_2$ sender's strategy is $q_1 = 0$, then the condition on λ such

that a type $\mathcal{T}_1$ sender's optimal strategy is $p_1 = 1$, is

$$\begin{aligned} & \mathcal{P}_1(1,0) > \mathcal{P}_1(p_1,0) \ \forall \ p_1 < 1 \\ \implies & \lambda c_1 > \lambda(p_1 c_1 + p_2 c_2) + (1-\lambda) p_2 h\left(\tfrac{p_2}{1+p_2}\right) \\ \implies & \tfrac{\lambda(c_1-c_2)}{1-\lambda} > h\left(\tfrac{p_2}{1+p_2}\right) \forall \ p_2 \in (0,1] \\ \implies & \lambda > \tfrac{1}{1+c_1-c_2} \end{aligned} \tag{109}$$

Using the similar argument as given in (109), we can show that the criterion $\mathcal{P}_2(1,0) > \mathcal{P}_2(1,q) \ \forall \ q \in (0,1]$ results in the condition $\lambda > \frac{1}{1+d_2-d_1}$. Therefore, when $\lambda > \max\left\{\frac{1}{1+c_1-c_2}, \frac{1}{1+d_2-d_1}\right\}$, then $p_1^* = 1$ and $q_1^* = 0$ is an equilibrium point. □

The first case of the above theorem is an extreme case where only anonymity is important for sender, therefore, as long as senders of both types use identical strategies (probability distributions), the posterior probability upon receiving a message is identical to the prior probability. Consequently, the anonymity is maximized and a pooling equilibrium exists. The second case considers the equilibrium point where both anonymity and direct payoff of the signaling game is important to sender. Under the conditions in 2 i. and 2 ii., the direct rewards provide senders of both types incentive to transmit the same message, and therefore a pooling equilibrium exists, albeit trivially.

The most interesting case of the above theorem is 2 iii. case where senders belonging to the two types have opposite incentives for choosing a common message according to their direct payoffs. For this case, we showed that there exists a threshold λ^* such that when $\lambda > \lambda^*$, then each sender chooses to transmit the message that maximizes the direct payoff for his/her type, and when $\lambda < \lambda^*$ then senders of both types choose the same message. It is important to note here that a similar result is proven in [89] in the context of conformity where senders choose to conform if and only if the reward for conforming is greater than a threshold.

The above theorem proves the existence of Bayesian-Nash equilibrium by finding an equilibrium point for all possible values of $\mathcal{R}_D$ and λ but doesn't prove that the equilibrium conditions are unique. In fact, the equilibrium conditions are not always unique. For instance, when $\lambda < \min\left\{\frac{1}{1+c_1-c_2}, \frac{1}{1+d_2-d_1}\right\}$, then both $p_1 = 0, q_1 = 0$ and $p_1 = 1, q_1 = 1$ are equilibrium points.

There are conditions under which the uniqueness of the equilibrium point can be proven. Note that when $c_1 > c_2$ and $d_1 \leq d_2$ and $\lambda > \lambda^*$, senders belonging to the two types choose non-overlapping messages in their equilibrium strategies or in other words, a separating equilibrium exists. In the following theorem, we show that when a separating equilibrium exists, it is a unique equilibrium point.

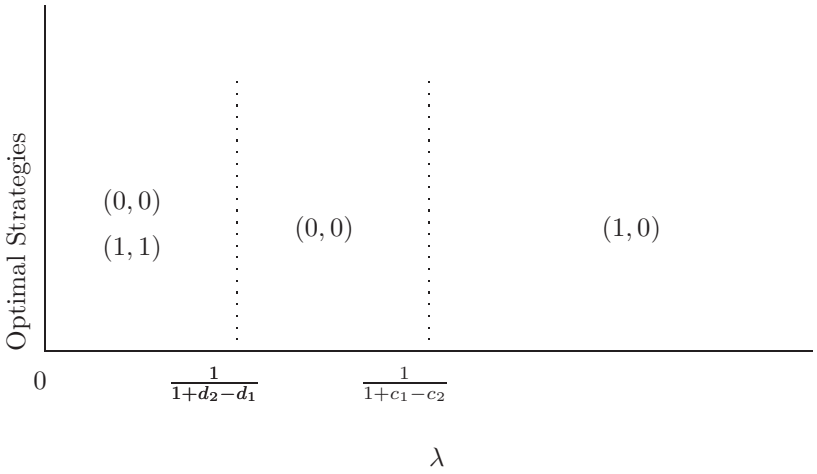


Figure 37: Optimal strategy of types $\mathcal{T}_1$ and $\mathcal{T}_2$ sender for the case 3(*iii*) of Theorem 20 when $c_1 - c_2 < d_2 - d_1$ as a function of λ where $(\cdot, \cdot) = (p_1^*, q_1^*)$

Theorem 21 *If $c_1 > c_2$, $d_1 \leq d_2$, $\lambda > \lambda^*$, then $\mathcal{G}_2$ with $\lambda_1 = \lambda_2$ has a unique Perfect Bayesian-Nash equilibrium point defined by the strategies $\boldsymbol{p}^* = (1, 0)$ and $\boldsymbol{q}^* = (0, 1)$.*

Proof: Using (109), we know that $\lambda > \frac{1}{1+c_1-c_2}$ is required for the existence of a separating equilibrium. To prove that the separating equilibrium is the unique equilibrium, it is sufficient to show that even if a type $\mathcal{T}_2$ sender uses strategy $q_1 > 0$ instead of $q_1^* = 0$, it is optimal for a type $\mathcal{T}_1$ sender to choose strategy $p_1^* = 1$ when $\lambda > \frac{1}{1+c_1-c_2}$. Specifically, we require

$$\begin{aligned} &\mathcal{P}_1(1, q_1) > \mathcal{P}_1(p_1, q_1) \; \forall \; 0 \leq p_1 < 1 \text{ and } q_1 \in [0, 1] \\ &\implies \lambda c_1 + (1-\lambda) h\left(\tfrac{1}{1+q_1}\right) > \lambda(p_1 c_1 + p_2 c_2) + \cdots \\ &(1-\lambda)\left(p_1 h\left(\tfrac{p_1}{p_1+q_1}\right) + p_2 h\left(\tfrac{p_2}{p_2+q_2}\right)\right) \forall \; p_2 \in (0, 1] \end{aligned} \tag{110}$$

Combining (109) and (110), the condition for the uniqueness of the separating equilibrium reduces to

$$p_2 + h\left(\frac{1}{1+q_1}\right) > p_1 h\left(\frac{p_1}{p_1+q_1}\right) + p_2 h\left(\frac{p_2}{p_2+q_2}\right) \tag{111}$$

Note that $h(x)$ is a concave function, and $h(0) = 0$, therefore, $h(tx + (1-t)0) \geq t h(x) \; \forall \; t \in [0, 1]$. Consequently,

$$h\left(\frac{q_1}{p_1+q_1}\frac{p_1+q_1}{1+q_1}\right) > \frac{p_1+q_1}{1+q_1} h\left(\frac{q_1}{p_1+q_1}\right) \; \forall p_1 < 1 \tag{112}$$

(112) along with $h(x) \leq 1$ proves (111).

Using the similar argument as given in (110)-(112), we can show that when $\lambda > \frac{1}{1+d_2-d_1}$, then $\mathcal{P}_2(p_1, 0) > \mathcal{P}_2(p_1, q_1) \; \forall \; 0 < q_1 \leq 1$ and a given $p_1 \in [0, 1]$. □

Note that in the above results, we consider that senders of both types have identical desires for anonymity, i.e. $\lambda_1 = \lambda_2$. In practice, however, different users have different preferences for privacy, and the identical weighting of privacy across users need not hold. The existence of Perfect Bayesian-Nash equilibrium conditions when different types have different requirements for anonymity is proven in the following theorem:

Theorem 22 *The Perfect Bayesian-Nash equilibrium of $\mathcal{G}_2$ exists even if $\lambda_1 \neq \lambda_2$.*

Proof: Without loss of generality, assume that $\lambda_1 \neq 0$ and $\lambda_2 \neq 1$. Lets consider the game $\mathcal{G}_2' = \{\mathcal{T}, \mathcal{M}, \mathcal{A}, \Lambda', \mathcal{R}_D'\}$ such that $\Lambda' = \{\lambda_1, \lambda_1\}$ and $R_D' = \{(c_1, c_2), \left(\frac{1-\lambda_1}{1-\lambda_2}\frac{\lambda_2}{\lambda_1}d_1, \frac{1-\lambda_1}{1-\lambda_2}\frac{\lambda_2}{\lambda_1}d_2\right)\}$. We know from Theorem 20 that there exist p_1^* and q_1^* such that

$$\begin{aligned} p_1^* &= \text{argmax}_p\, \lambda_1 \textstyle\sum_{i=1}^{2} p_i c_i + (1-\lambda_1) p_i h\left(\frac{p_i}{p_i+q_i}\right) \\ q_1^* &= \text{argmax}_q\, \lambda_1 \textstyle\sum_{i=1}^{2} q_i \frac{1-\lambda_1}{1-\lambda_2}\frac{\lambda_2}{\lambda_1} d_i + (1-\lambda_1) q_i h\left(\frac{q_i}{p_i+q_i}\right) \end{aligned} \tag{113}$$

Note that (113) is equivalent to equilibrium conditions given in (104) for $\mathcal{G}_2$ when $\lambda_1 \neq \lambda_2$. Therefore, p_1^* and q_1^* are equilibrium point of $\mathcal{G}_2$. □

The above theorem is important because anonymity is subjective and even amongst users with different privacy requirements there exist equilibrium strategies which neither player has incentive to deviate from. This is of particular importance in the context of the data networking problem presented in Figure 36. If different users have different weights for anonymity, the results show that under a perfect Bayesian-Nash equilibrium, each user still chooses a single path to transmit the packets. This is a parallel result to the work in [90] which shows that under light traffic conditions, the optimal rate allocation that maximizes anonymity under delay constraints results in single paths for the users.

6.3 Equilibrium conditions for general Message sets

In this section, we prove the existence of equilibrium conditions and investigate their properties for some special cases when the users can choose a message from a set of $k > 2$ messages and give a reduction methodology for finding the equilibrium conditions for a general finite set of messages.

Theorem 23 *For $k > 2$, the Perfect Bayesian-Nash equilibrium conditions of $\mathcal{G} = \{\mathcal{T}, \{m_i\}_{i=1}^k, \{a\}, \Lambda, \mathcal{R}_D\}$*

are identical to $\mathcal{G}' = \{\mathcal{T}, \{m_i\}_{\substack{i=1 \\ i\neq n}}^{k}, \{a\}, \Lambda, \mathcal{R}_D\}$ *when*

$$\begin{aligned} c_n &= \min\{c_i\}_{i=1}^{k} \\ d_n &= \min\{d_i\}_{i=1}^{k} \end{aligned} \quad \textit{for some } n \in \{1, 2, ..., k\}$$

Proof: To simplify the mathematical notation, we prove the result for $k = 3$. WLOG assume that $c_3 < \min\{c_1, c_2\}$ and $d_3 < \min\{d_1, d_2\}$. To prove the theorem, it is equivalent to show that when a type $\mathcal{T}_1$ sender uses the strategy $(0, p_2, p_3)$, then the optimal strategy for a type $\mathcal{T}_2$ sender is of the form $(0, q_2, q_3)$. We prove this by contradiction. Assume that the optimal strategy for a type $\mathcal{T}_2$ sender is (q_1, q_2, q_3) where $q_1 > 0$, then its payoff is

$$\mathcal{P}_2(\{p_i\}_{i=2}^{3}, \{q_i\}_{i=1}^{3}) = \lambda \sum_{i=1}^{3} q_i d_i + (1-\lambda) \sum_{i=2}^{3} q_i h\left(\frac{p_i}{p_i + q_i}\right)$$

We know $p_2 + p_3 = 1$ and $q_1 + q_2 + q_3 = 1$, therefore, either $q_2 < p_2$ or $q_3 < p_3$ since $q_1 > 0$. WLOG assume that $q_2 < p_2$, then it is easy to see that the payoff of strategy $(q_1 - \epsilon, q_2 + \epsilon, q_3)$ is greater than the payoff of (q_1, q_2, q_3) because $d_1 < d_2$ and $h\left(\frac{p_2}{p_2+q_2}\right) < h\left(\frac{p_2}{p_2+q_2+\epsilon}\right)$ where $0 < \epsilon < \min\{q_1, p_2 - q_2\}$. □

An important consequence of the above theorem is if there is a message that is uniformly bad for both types of sender, then in equilibrium no type of sender would transmit that message. In the following theorem, we derive sufficient conditions on the direct payoff of $\mathcal{G}_k$ which result in separating and pooling equilibria. However, the above result just give a reduction methodology to find the equilibrium condition, in the following theorem we prove the existence of equilibrium points for a special reward structure of signaling games.

Theorem 24 *For a signaling game* $\mathcal{G}_k$ *with* $k > 2$ *messages, let*

$$c_1 > c_2 \geq \ldots \geq c_k \textit{ and } d_1 \leq d_2 \leq \ldots \leq d_{k-1} < d_k, \tag{114}$$

then

1. *If* $\lambda > \mu^*$, *then* $p_1^* = 1, q_k^* = 1$ *is a perfect Bayesian-Nash equilibrium of* $\mathcal{G}_k$ ***(Separating)***.
2. *If* $\lambda < \mu^*$, *then* $p_1^* = 1, q_1^* = 1$ *and* $p_k^* = 1, q_k^* = 1$ *are perfect Bayesian-Nash equilibria of* $\mathcal{G}_k$ ***(Pooling)***.

where $\mu^* = \max\left\{\frac{1}{1+c_1-c_{k-1}}, \frac{1}{1+d_k-d_1}\right\}$

Proof: To simplify the notations, assume $k = 3$. WLOG, assume that $c_1 > c_2 \geq c_3$ and $d_3 > d_2 \geq d_1$. It is easy to verify that

$$\mathcal{P}_1(\{p_1, p_2, p_3\}, \{0, 0, 1\}) \quad < \quad \mathcal{P}_1(\{p_1 + p_2, 0, p_3\}, \{0, 0, 1\}) \forall p_2 > 0 \tag{115}$$

because $c_2 < c_1$ and transmitting m_2 does not contribute in anonymity given that a type $\mathcal{T}_2$ sender does not transmit m_2. (115) implies that finding the optimal strategy for a type $\mathcal{T}_1$ sender on message set $\{m_1, m_2, m_3\}$ is reduced to finding the optimal strategy on message set $\{m_1, m_3\}$ given that a type $\mathcal{T}_2$ sender is playing the strategy $\{0, 0, 1\}$. Similarly,

$$\mathcal{P}_2(\{1, 0, 0\}, \{q_1, q_2, q_3\}) < \mathcal{P}_2(\{1, 0, 0\}, \{q_1, 0, q_2 + q_3\}) \forall q_2 > 0$$

implies that finding the optimal strategy for a type $\mathcal{T}_2$ sender on message set $\{m_1, m_2, m_3\}$ is reduced to finding the optimal strategy on message set $\{m_1, m_3\}$ given that a type $\mathcal{T}_1$ sender is playing the strategy $\{1, 0, 0\}$. Thereafter, applying the same argument for two messages case as in Theorem 20 given in (105)-(109), we get the result. □

For signaling games that satisfy (114), the above theorem proves that there exists a threshold μ^* such that when $\lambda > \mu^*$, then senders of both the types are interested only in maximizing their direct payoff while ignoring the payoff of the anonymity completely, and this scenario is reversed completely when $\lambda < \mu^*$. Note that the threshold μ^* depends only on the direct payoff of transmitting messages with lowest and highest payoff for both types. Although the above result proves the existence of a separating equilibrium when $\lambda > \mu^*$, it does not prove that the separating equilibrium is unique. We provide in the following theorem a lower bound on λ for the existence of a unique separating equilibrium.

Theorem 25 *If $c_1 > \ldots > c_k$, $d_1 < \ldots < d_k$, $\lambda > \max\{\frac{1}{1+c_1-c_2}, \frac{1}{1+d_k-d_{k-1}}\}$, then game $\mathcal{G}_k$ has a unique Perfect Bayesian-Nash equilibrium point defined by the strategies $p_1^* = 1$ and $q_k^* = 1$.*

Proof: Assume that $\mathbf{e}_1 = \{1, 0, \ldots, 0\}$ and $\mathbf{e}_k = \{0, 0, \ldots, 1\}$. To prove the uniqueness of separating equilibrium, we need to show that $\lambda > \frac{1}{1+c_1-c_2}$ implies that

$$\begin{aligned} &\mathcal{P}_1(\mathbf{e}_1, \mathbf{q}) > \mathcal{P}_1(\mathbf{p}, \mathbf{q}) \ \forall \mathbf{p}, \mathbf{q} \\ &\iff \lambda c_1 + (1-\lambda) h\left(\tfrac{1}{1+q_1}\right) > \textstyle\sum_{i=1}^{k} \lambda p_i c_i + (1-\lambda) p_i h\left(\tfrac{p_i}{p_i+q_i}\right) \\ &\iff \textstyle\sum_{i=2}^{k} p_i \left(\tfrac{\lambda}{1-\lambda}(c_1 - c_i) - h\left(\tfrac{p_i}{p_i+q_i}\right)\right) + h\left(\tfrac{1}{1+q_1}\right) > p_1 h\left(\tfrac{p_1}{p_1+q_1}\right) \end{aligned} \tag{116}$$

Note $\frac{\lambda}{1-\lambda}(c_1 - c_i) \geq \frac{\lambda}{1-\lambda}(c_1 - c_2) > 1 \; \forall \; i \in \{2, \ldots, k\}$, therefore, (112) along with $h(x) \leq 1$ proves (116). Similarly, it can be shown that $\lambda > \frac{1}{1+d_k-d_{k-1}}$ implies that

$$\mathcal{P}_2(\mathbf{p}, \mathbf{e}_k) > \mathcal{P}_2(\mathbf{p}, \mathbf{q}) \forall \; \mathbf{p}, \mathbf{q}. \tag{117}$$

□

6.4 Summary

In this work, we provide basic foundation for encompassing anonymity in signaling games. We proved the existence of equilibrium conditions for a basic scenario where sender could be of two types. Our results prove the intuition that there exists thresholds on the requirement of anonymity, such that above the threshold, all types of senders are incentivized to transmit identical messages.

7 Conclusion and Future Works

To the best of our knowledge, this is the first work that provides a first comprehensive analytical framework to study anonymity-QoS tradeoff in data networks. Moreover, our work also provides a general infrastructure to model utility-privacy tradeoff for broader commercial and social contexts. Using this analytical framework, we present our main findings along with some direction for future works in the following.

7.1 Memory Constrained mixes

One of our key contributions in this work is to find the optimal mixing strategy for a Chaum mix under memory restrictions. To the best of our knowledge, this is the first such characterization. Moreover, for some special cases we show that the convergence rate of the optimal anonymity is $O\left(\frac{1}{k^2}\right)$. The extension of this result to a network of mixes, while investigated in Chapter 3, still ignores the possibility of shared randomness across mixes and is a useful area for further study. In addition, the achievable anonymity of a system under dynamic routing configurations is yet another important topic for further investigation. Another extension that we are currently interested is the topological design given a set of source destination pairs to guarantee anonymity α.

7.2 Mixes performance under fairness restrictions

In this work, we studied a previously unexplored dimension in fair scheduling algorithms, the source anonymity. Specifically, we characterize and compare the anonymity of three popular scheduling policies: First-Come-First-Serve (FCFS), Fair Queuing (FQ), and Proportional Method (PM). Interestingly, the FCFS and FQ while popular metrics to design scheduling algorithms performs poorly from an anonymity perspective unless the fairness criteria are sufficiently relaxed. Indeed, we proved in this work that the anonymity of a modified max-min Fair Queuing algorithm can never exceed .5 and the anonymity achieved by a strict FCFS scheduling policy is zero. We proposed relaxations of the fairness criteria, and demonstrated that any desired anonymity can be achieved by sufficiently expanding the window of fairness computation in Fair Queuing algorithms and by relaxing the fairness criterion in FCFS such that a bounded number of packets of other users that comes after a packet of a user are allowed to be served before the packet. Further, we showed analytically that the proportional method, although thus far unpopular in the context of data networks, can, in fact, be a valuable fair scheduling scheme in anonymous networking systems. With a sufficient buffer size, the scheme can achieve an anonymity arbitrarily close to the maximum desired. Further, this works

takes an important step in identifying the relationship of anonymity to fairness using a temporal measure of fairness that in essence measure the out of order transmission. Extension of this analysis to networks of mixes is an interesting and important step for the future.

7.3 Flow based anonymity of mixes

In this work, the admissible length for perfect anonymity was used as a tool to study optimal mixing strategies. The admissible length not only provides the best operating criteria for anonymous systems, but also helps evaluate the effectiveness of mixing strategies in providing maximum anonymity. Furthermore, since the admissible length directly models the adversary action, the framework can be generalized to include active adversaries capable of capturing packets. While equal arrival rates and Poisson models have been used to determine the analytical results in this work, the mixing strategies derived work independent of the nature and rate of arrivals, and only depend on the state of the buffer and dummy packet limitations. Indeed, we believe, for arrivals modelled as general renewal processes, the insights derived in this work would apply directly [80]. While this paper studies the problem of anonymity using a single shared scheduler, the extension to networks of scheduler is an interesting and necessary subject for future research. A strict capture limit was considered in this work to model an active adversary. An interesting game theoretic extension would be to jointly consider an intrusion detection mechanism, wherein the more packets an adversary captures the higher likelihood of getting caught.

7.4 Role of signaling games for studying anonymity

In this work, we provide a basic foundation for encompassing anonymity in signaling games. We proved the existence of equilibrium conditions for a basic scenario where sender could be of two types and extend the results for some special reward structures of signaling games for more than two types of sender. Our results prove the intuition that there exists thresholds on the requirement of anonymity, such that above the threshold, all types of senders are incentivized to transmit identical messages. The extension of these results to active receiver and stochastic games are promising directions for future investigation.

Bibliography

[1] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudeonymity — a proposal for terminology," in *International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability*, (New York, NY, USA), pp. 1–9, Springer-Verlag New York, Inc., 2001.

[2] R. Newman, "The church of scientology vs. anon.penet.fi," 1996. `http://www.spaink.net/cos/rnewman/anon/penet.html`.

[3] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms," *Communications of the ACM*, vol. 24, pp. 84–88, February 1981.

[4] "Peeling back the layers of tor with egotisticalgiraffe," Oct. 2013. `http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-documentl`.

[5] 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.

[6] P. Venkitasubramaniam and L. Tong, "Anonymous Networking with Minimum Latency in Multihop Networks," in *IEEE Symposium on Security and Privacy*, (Oakland, CA), May 2008.

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

[8] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," *IEEE Trans. Inf. Theor.*, vol. 54, pp. 2770–2784, June 2008.

[9] P. Venkitasubramaniam and L. Tong, "A game-theoretic approach to anonymous networking," *Networking, IEEE/ACM Transactions on*, vol. 20, pp. 892 –905, june 2012.

[10] M. Schwartz, *Telecommunication networks: protocols, modeling and analysis*, vol. 7. Addison-Wesley Reading, MA, 1987.

[11] D. P. Bertsekas and R. Gallager, *Data Networks*. Prentice Hall, 1992.

[12] J. McFadden, "The entropy of a point process," *Journal of the Society for Industrial & Applied Mathematics*, vol. 13, no. 4, pp. 988–994, 1965.

[13] P. Salvador, A. Pacheco, and R. Valadas, "Modeling ip traffic: joint characterization of packet arrivals and packet sizes using bmaps," *Computer Networks*, vol. 44, no. 3, pp. 335–352, 2004.

[14] A. T. Andersen and B. F. Nielsen, "A markovian approach for modeling packet traffic with long-range dependence," *Selected Areas in Communications, IEEE Journal on*, vol. 16, no. 5, pp. 719–732, 1998.

[15] T. Karagiannis, M. Molle, M. Faloutsos, and A. Broido, "A nonstationary poisson view of internet traffic," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 3, pp. 1558–1569, IEEE, 2004.

[16] A. Demers, S. Keshav, and S. Shenker, "Analysis and simulation of a fair queueing algorithm," *SIGCOMM Comput. Commun. Rev.*, vol. 19, pp. 1–12, August 1989.

[17] E. L. Hahne, "Round Robin Scheduling for Max-Min Fairness in Data Networks," *IEEE Journal on selected areas in communication*, vol. 9, pp. 1024–1039, Sept. 1991.

[18] H. Moulin and R. Stong, "Fair queuing and other probabilistic allocation methods," *Mathematics of Operations Research*, vol. 27, no. 1, pp. 1–30, 2002.

[19] X. Fu, B. Graham, R. Bettati, and W. Zhao, "On countermeasures to traffic analysis attacks," in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pp. 188–195, 18-23 June 2003.

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

[21] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '96, (London, UK, UK), pp. 104–113, Springer-Verlag, 1996.

[22] D. X. Song, D. Wagner, and X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH," in *Proc. 10th USENIX Security Symposium*, 2001.

[23] 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* (H. Federrath, ed.), vol. 2009 of *LNCS*, pp. 10–29, Springer-Verlag, 2001.

[24] A. Serjantov, R. Dingledine, and P. Syverson, "From a trickle to a flood: Active attacks on several MIX types," in *Proceedings of the Fifth International Workshop on Information Hiding (IH'02), Lecture Notes in Computer Science*, vol. 2578, (Noordwijkerhout, The Netherlands), pp. 36–52, October 2002.

[25] D. Kesdogan, J. Egner, and R. Buschkes, "Stop-and-go MIXes providing probabilistic security in an open system," in *Second International Workshop on Information Hiding (IH'98), Lecture Notes in Computer Science*, vol. 1525, (Portland, Oregon), pp. 83–98, April 1998.

[26] L. Cottrell, "Mixmaster and Remailer Attacks," ¡http://www.obscura.com/loki/remailer/remailer-essay.html¿.

[27] C. Díaz and A. Serjantov, "Generalizing mixes," in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2003)*, Springer-Verlag, LNCS 2760, April 2003.

[28] M.-H. W. V. Shmatikov, "Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses," in *11th European Symposium on Research in Computer Security, Lecture Notes in Computer Science 1895*, pp. 18–33, 2006.

[29] O. Berthold and H. Langos, "Dummy traffic against long term intersection attacks," in *Proceedings of Privacy Enhancing Technologies workshop (PET 2002)* (R. Dingledine and P. Syverson, eds.), Springer-Verlag, LNCS 2482, April 2002.

[30] C. Diaz and B. Preneel, "Taxonomy of mixes and dummy traffic," in *Proceedings of I-NetSec04: 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems*, August 2004.

[31] W. Dai, "Pipenet 1.1." Post to Cypherpunks mailing list, November 1998.

[32] C. Diaz and B. Preneel, "Reasoning about the anonymity provided by pool mixes that generate dummy traffic," in *Proceedings of 6th Information Hiding Workshop (IH 2004)*, LNCS, May 2004.

[33] M. Rennhard, S. Rafaeli, L. Mathy, B. Plattner, and D. Hutchison, "Analysis of an Anonymity Network for Web Browsing," in *Proceedings of the IEEE 7th Intl. Workshop on Enterprise Security (WET ICE 2002)*, pp. 49–54, June 2002.

[34] P. Venkitasubramaniam and V. Anantharam, "On the Anonymity of Chaum Mixes," in *IEEE International Symposium on Information Theory*, (Toronto, Canada), July 2008.

[35] 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.

[36] P. Venkitasubramaniam, "Anonymity under Buffer Constraints," in *IEEE International Conference on Communications*, (Cape Town, South Africa), May 2010.

[37] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, 1949.

[38] A. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[39] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, May 1978.

[40] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, pp. 451–456, Jul 1978.

[41] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2470 –2492, 2008.

[42] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas #x2014;part ii: The mimome wiretap channel," *Information Theory, IEEE Transactions on*, vol. 56, pp. 5515–5532, Nov 2010.

[43] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel," *Information Theory, IEEE Transactions on*, vol. 55, pp. 4033–4039, Sept 2009.

[44] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *Information Theory, IEEE Transactions on*, vol. 54, pp. 2735–2751, June 2008.

[45] V. Anantharam and S. Verdu, "Bits Through Queues," *IEEE Trans. Inform. Theory*, vol. 42, pp. 4–18, Jan. 1996.

[46] R. Sundaresan and S. Verdu, "Robust decoding for timing channels," *Information Theory, IEEE Transactions on*, vol. 46, pp. 405–419, Mar 2000.

[47] S. Sellke, C.-C. Wang, S. Bagchi, and N. Shroff, "Tcp/ip timing channels: Theory to implementation," in *INFOCOM 2009, IEEE*, pp. 2204–2212, April 2009.

[48] J. Giles and B. Hajek, "An Information-Theoretic and Game-Theoretic Study of Timing Channels," *IEEE Transactions on Information Theory*, vol. 48, pp. 2455–2477, September 2002.

[49] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, pp. 25:1–25:39, July 2013.

[50] T. Basar, "The gaussian test channel with an intelligent jammer," *Information Theory, IEEE Transactions on*, vol. 29, pp. 152–157, Jan 1983.

[51] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on mimo gaussian fading channels," *Information Theory, IEEE Transactions on*, vol. 50, pp. 2119–2123, Sept 2004.

[52] S. Shafiee and S. Ulukus, "Capacity of multiple access channels with correlated jamming," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pp. 218–224 Vol. 1, Oct 2005.

[53] Y. Sagduyu, R. Berry, and A. Ephremides, "Mac games for distributed wireless network security with incomplete information of selfish and malicious user types," in *Game Theory for Networks, 2009. GameNets '09. International Conference on*, pp. 130–139, May 2009.

[54] B. Wang, Y. Wu, K. Liu, and T. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *Selected Areas in Communications, IEEE Journal on*, vol. 29, pp. 877–889, April 2011.

[55] K. Sallhammar, B. E. Helvik, and S. J. Knapskog, "Towards a stochastic model for integrated security and dependability evaluation," in *Proceedings of the First International Conference on Availability, Reliability and Security*, ARES '06, (Washington, DC, USA), pp. 156–165, IEEE Computer Society, 2006.

[56] T. Alpcan and T. Başar, "An Intrusion Detection Game with Limited Observations," in *12th Int. Symp. on Dynamic Games and Applications*, (Sophia Antipolis, France), July 2006.

[57] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *Information Theory, IEEE Transactions on*, vol. 49, no. 3, pp. 563–593, 2003.

[58] J. O'Sullivan, P. Moulin, and J. Ettinger, "Information theoretic analysis of steganography," in *Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on*, pp. 297–, 1998.

[59] M. H. M. Costa, "Writing on dirty paper (corresp.)," *Information Theory, IEEE Transactions on*, vol. 29, no. 3, pp. 439–441, 1983.

[60] G. Heal, M. Broadie, D. Croson, I. Erev, V. Goldberg, J. Hamilton, J. Hershey, D. Kahneman, E. Michelkerjan, F. Oberholzer-gee, Y. Yemini, P. In, H. Kunreuther, and H. Kunreuther, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, pp. 231–249, 2002.

[61] M. Raya, R. Shokri, and J.-P. Hubaux, "On the tradeoff between trust and privacy in wireless ad hoc networks," in *Proceedings of the Third ACM Conference on Wireless Network Security*, WiSec '10, (New York, NY, USA), pp. 75–80, ACM, 2010.

[62] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On non-cooperative location privacy: A game-theoretic analysis," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), pp. 324–337, ACM, 2009.

[63] A. Acquisti, R. Dingledine, and P. Syverson, "On the Economics of Anonymity," in *Proceedings of Financial Cryptography (FC '03)* (R. N. Wright, ed.), Springer-Verlag, LNCS 2742, January 2003.

[64] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[65] D. P. Bertsekas, *Dynamic Programming and Optimal Control*, vol. 1. Athena Scientific, 2nd ed., 2001.

[66] O. Frank and J. Öhrvik, "Entropy of sums of random digits," *Computational statistics & data analysis*, vol. 17, no. 2, pp. 177–184, 1994.

[67] A. Mishra and P. Venkitasubramaniam, "Source anonymity in fair scheduling: A case for the proportional method," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 1118 –1122, june 2012.

[68] T. Lan, D. Kao, M. Chiang, and A. Sabharwal, *An axiomatic theory of fairness in network resource allocation*. IEEE, 2010.

[69] R. Jain, A. Durresi, and G. Babic, "Throughput fairness index: An explanation," tech. rep., Tech. rep., Department of CIS, The Ohio State University, 1999.

[70] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, vol. 49, no. 3, pp. 237–252, 1998.

[71] B. Mandelbrot, *Fractals and chaos: the mandelbrot set and beyond*, vol. 3. Springer, 2004.

[72] P. Venkitasubramaniam and A. Mishra, "Anonymity of Memory Limited Chaum Mixes under Timing Analysis: An Information Theoretic Perspective," *submitted to IEEE Trans. Information Theory*, September 2013.

[73] A. Mishra and P. Venkitasubramaniam, "Thwarting traffic analysis: A signal processing perspective," in *Sensor Array and Multichannel Signal Processing Workshop (SAM), 2012 IEEE 7th*, pp. 169–172, 2012.

[74] A. Wald, "On cumulative sums of random variables," *The Annals of Mathematical Statistics*, vol. 15, no. 3, pp. pp. 283–296, 1944.

[75] W. Feller, *An Introduction to Probability Theory and Its Applications*. Wiley; 3rd edition, 1968.

[76] 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.

[77] T. He and L. Tong, "Detection of information flows," *Information Theory, IEEE Transactions on*, vol. 54, no. 11, pp. 4925–4945, 2008.

[78] D. P. Bertsekas, *Dynamic Programming and Optimal Control I*. Athena Scientific, 2nd ed., 2001.

[79] G. J. O. T. Basar, *Dynamic Noncooperative Game Theory*. San Diego, CA: Academic Press, 1995.

[80] S. Marano, V. Matta, T. He, and L. Tong, "Embedding information flows into renewal traffic," in *Information Theory Workshop (ITW), 2011 IEEE*, pp. 50–54, IEEE, 2011.

[81] S. R. Grenadier and A. Malenko, "Real options signaling games with applications to corporate finance," *Review of Financial Studies*, 2011.

[82] M. Spence, "Job market signaling," *The Quarterly Journal of Economics*, vol. 87, no. 3, pp. 355–374, 1973.

[83] S. M. Huttegger, "Evolution and the explanation of meaning," *Philosophy of Science*, vol. 74, no. 1, pp. 1–27, 2007.

[84] 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.

[85] M. J. Osborne and A. Rubinstein. Cambridge, USA: The MIT Press. electronic edition.

[86] J. F. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950.

[87] J. Nash, "Non-cooperative games," *Annals of Mathematics*, vol. 54, no. 2, pp. 286–295, 1951.

[88] M. J. Sobel, "Noncooperative stochastic games," *The Annals of Mathematical Statistics*, vol. 42, pp. 1930–1935, 12 1971.

[89] B. D. Bernheim, "A Theory of Conformity," *The Journal of Political Economy*, vol. 102, no. 5, pp. 841–877, 1994.

[90] O. Zavidbakht and P. Venkitasubramaniam, "Rate Allocation for Multihop Routing in Anonymous Networking," in *Accepted in Proc. of CISS 2014*, (Princeton, NJ), March 2014.

Biography

Abhishek Mishra was born on 5 May, 1986 to Srikant Mishra and Satyawati Mishra in Lucknow, Uttar Pradesh, India. He attended Saraswati Shishu Mandir, Saraswati Vidya Mandir, and Rani Laxmi Bai schools in Lucknow. He has received his Bachelor of Technology and Master of Technology in Electrical Engineering from Indian Institute of Technology, Kanpur in 2010. Upon completion of his bachelor and master studies, he joined Lehigh University to pursue his PhD in Electrical Engineering. He is also an knowledge seeker and a taekwando enthusiast.

Curriculum Vitae

Education

Ph. D. in Electrical Engineering

Graduation Date: September, 2014

Lehigh University, Bethlehem, PA, USA. GPA: 3.88/4.0

M. Tech in Electrical Engineering

Graduation Date: July, 2010

Indian Institute of Technology Kanpur, Kanpur, India. GPA: 9.2/10.0

B. Tech in Electrical Engineering

Graduation Date: July, 2009

Indian Institute of Technology Kanpur, UP, India. GPA: 7.3/10.0

Research Experience

Graduate Research Assistant, Dept. of Electrical Engineering,

Lehigh University, Bethlehem, PA, USA. 2010 - 2014

Research Experience for Masters Program, Dept. of Electrical Engineering

Indian Institute of Technology Kanpur, UP, India. 2009-2010

Research Experience for Undergraduate Program, Dept. of Electrical Engineering

Indian Institute of Technology Kanpur, UP, India. 2008-2009.

Industry Experience

Summer Intern

Blue Vector India, Bangalore, Karnataka, India

Summer 2008.

Publications in peer-reviewed journals

Journal Publications

J1 P. Venkitasubramaniam and **A. Mishra**, "Anonymity of Mix Networks under Memory Limitations: An Information Theoretic Perspective," submitted to IEEE Transactions on Information Theory, Aug. 2013.

J2 **A. Mishra** and P. Venkitasubramaniam, "Anonymity and Fairness in Packet Scheduling: A Quantitative Tradeoff," submitted to IEEE Transactions on Networking, Nov. 2012 (revised January 2014).

J3 **A. Mishra** and P. Venkitasubramaniam, "Admissible Length Study in Anonymous Networking: A Detection Theoretic Perspective," Selected Areas in Communications, IEEE Journal on , vol.31, no.9, pp.1957-1969, September 2013

Conference Publications

C1 **Abhishek Mishra** and P. Venkitasubramaniam, "Encompassing Anonymity in Signaling Games," in Proc. 2014 Conference on Information Systems and Sciences, Princeton, NJ, Mar. 2014.

C2 **Abhishek Mishra** and P. Venkitasubramaniam, "Anonymity of a Buffer Constrained Chaum Mix: Optimal Strategy and Asymptotics," in Proc. 2013 IEEE International Symposium on Information Theory (ISIT), Istanbul, Turkey, July 2013.

C3 **Abhishek Mishra** and P. Venkitasubramaniam, "Anonymity in Wireless Networks under Capture or Selective Jamming" in Proc. 2013 IEEE International Symposium on Wireless Personal Multimedia Communications, Atlantic City, NJ, June 2013.

C4 **Abhishek Mishra** and P. Venkitasubramaniam, "Thwarting Traffic Analysis: A Signal Processing Perspective," in Proc. 2012 IEEE Sensor and Multichannel Signal Processing Conference, Hoboken, NJ, June 2012.

C5 **Abhishek Mishra** and P. Venkitasubramaniam, "Anonymity in Fair Scheduling: A Case for the Proportional Method," in Proc. IEEE Conference on Communication, Ottawa, Canada, June 2012.

C6 **Abhishek Mishra** and P. Venkitasubramaniam,"Anonymity in Packet Scheduling under Max-Min Fairness Criterion," in Proc. 2012 Conference on Information Systems and Sciences, Princeton, NJ, Mar. 2012.

C7 **Abhishek Mishra** and P. Venkitasubramaniam, "Anonymity of an Almost Fair Chaum Mix," in Proc. 50th Annual Allerton Conference on Communication, Control and Computing, Monticello, IL, Sep. 2011.

C8 **Abhishek Mishra**, Ankesh Garg, and Adrish Banerjee, "Selection Based Detection Method for Spectrum Sensing for Cognitive Radio", in IEEE International Conference on Signal Processing and Communications, Bangalore, India, July 2010

Poster Publications

P1 **Abhishek Mishra** and Parv Venkitasubramaniam, "The Price of your Anonymity," presented in Lehigh University Graduate Research Symposium, April 2013, Bethlehem, PA.

P2 **Abhishek Mishra** and Parv Venkitasubramaniam, "Anonymity of a Buffer Constrained Router: Optimal Strategy and Asymptotic," presented at DIMACS Workshop on Information-Theoretic Network Security, Nov. 2012, Camden, New Jersey.

P3 **Abhishek Mishra** and Parv Venkitasubramaniam, "Thwarting Traffic Analysis: A Signal Processing Perspective," presented at School of Information Theory, June 2012, Ithaca, New York.

P4 **Abhishek Mishra** and Parv Venkitasubramaniam, "Anonymity in Buffer Constrained Mix Networks," poster 2011 ACM SIGCOMM, Toronto, Canada, Aug. 2011.

P5 **Abhishek Mishra** and Parv Venkitasubramaniam, "Anonymity of an almost fair Chaum Mix," presented at School of Information Theory, June 2011, Austin, Texas.

Leadership and other activities

- Member of the Lehigh University chess team that won the first prize in a collegiate chess tournament held by Princeton University in January 2012.
- Member of Lehigh University Taekwondo Club holding a green belt with blue stripe.

- Member of Lehigh University Meditation Club.
- Got a scholarship for learning Buddhist philosophy from Spic Macay under His Holiness the Dalai Lama in summer of 2009.
- A travelling enthusiast and an avid reader.