Towards a Theory of Anonymous Networking

J. Ghaderi and R. Srikant

Department of ECE, and Coordinated Science Lab.
University of Illinois at Urbana-Champaign
{jghaderi, rsrikant}@illinois.edu

Abstract—**The problem of anonymous networking when an eavesdropper observes packet timings in a communication network is considered. The goal is to hide the identities of source-destination nodes, and paths of information flow in the network. One way to achieve such an anonymity is to use *Mixes*. Mixes are nodes that receive packets from multiple sources and change the timing of packets, by mixing packets at the output links, to prevent the eavesdropper from finding sources of outgoing packets. In this paper, we consider two simple but fundamental scenarios: double input-single output Mix and double input-double output Mix. For the first case, we use the information-theoretic definition of the anonymity, based on average entropy per packet, and find an optimal mixing strategy under a strict latency constraint. For the second case, perfect anonymity is considered, and maximal throughput strategies with perfect anonymity are found under a strict latency constraint and an average queue length constraint.**

I. INTRODUCTION

Secure communication has become increasingly important. Privacy and anonymity considerations apply to all components of a communication network, such as contents of data packets, identities of source-destination nodes, and paths of information flow in the network. While a data packet's content can be protected by encrypting the payload of the packet, an eavesdropper can still detect the addresses of the source and the destination by *traffic analysis*. For example, observing the header of the packet can still reveal the identities of its corresponding source-destination pair. *Onion Routing* [1] and *Tor* network [2] are well-known solutions that provide protection against both eavesdropping and traffic analysis. The basic idea is to form an overlay network of Tor nodes, and relay packets through several Tor nodes instead of taking the direct path between the source and the destination. To create a private network, links between Tor nodes are encrypted such that each Tor node only knows the node from which it receives a packet and the node to which it forwards the packet. Therefore, any node in the Tor network sees only two hops (the previous and next nodes) but is not aware of the whole path between the source and the destination, Therefore, a compromised node cannot easily identify source-destination pairs. But Tor cannot solve all anonymity problems. If an eavesdropper can observe the traffic in and out of some nodes, it can still correlate the incoming and outgoing packets of relay nodes to identify the source and the destination or, at least, discover parts of the route between the source and the destination. This kind of statistical analysis is known as timing analysis since the eavesdropper only needs packet timings. For example, in Figure 1, if the processing delay is small, there is a high correlation between output and input processes, and the eavesdropper can easily identify the source of each outgoing packet.

To provide protection against the timing analysis attack, nodes in an anonymous network need to perform an additional task, known as mixing, before transmitting packets on output links. A node with mixing ability is called a *Mix*. In this solution, a Mix receives packets from multiple links, re-encrypts them, and changes the timings of packets, by mixing (reordering) packets at the output links, in such a way that the eavesdropper cannot relate an outgoing packet to its corresponding sender.

The original concept of Mix was introduced by Chaum [3]. The Mix anonymity was improved by random delaying [4] (Stop-and-go MIXes), and dummy packet transmission [5] (ISDN-MIXes), and used for the various Internet applications such as email [6] and WWW [7](Crowds). Other proposed anonymity schemes are JAP [8], MorphMix [9], Mixmaster [10], Mixminion [11], Buses [12], etc.

However, theoretical analysis of the performance of Chaum mixing is very limited. The information-theoretic measure of anonymity, based on Shannon's equivocation [13], was used in [14], [15] to evaluate the performance of a few mixing strategies, under some attack scenarios, however, their approach does not take into account the delay or traffic statistics; whereas, modifying packet timings to obfuscate the eavesdropper indeed increases the transmission latency. In [16], [17], the authors consider the performance of so-called generalized Mixes, e.g., a timed pool Mix, under some active attack scenarios. In a timed pool Mix, the Mix collects input messages that are placed in a pool during a round/cycle of the Mix, and then flushes the messages out with some probability. The flushing probability is characterized by a function $P(n)$ representing the probability of the messages being sent in the current round, given that the Mix contains n messages in the pool. Again, this is a very specific type of Mix and it is not clear if this is optimal. So, the question of interest is the following: what is the maximum achievable anonymity under a constraint on delay?

Characterizing the anonymity as a function of traffic load and the delay constraint has been considered in [18]. The authors in [18] have considered a Mix with two input links and one output link, where arrivals on the input links are two

Fig. 1. The double input-single output Mix. The capacity of each input link is 1 packet/time slot and the capacity of the output link is 2 packets/time slot.

Fig. 2. The double input-double output Mix. The capacity of each link is 1 packet/time slot.

poisson processes with equal rates, and they characterize upper and lower bounds on the maximum achievable anonymity under a strict delay constraint. The basic idea is that the Mix waits for a certain amount of time, collects packets from two sources, and sends a batch containing the received packets to the output. The implicit assumption in [18] is that there is no constraint on the capacity of the output link, i.e., the batch can be transmitted instantaneously at the output, no matter how many packets are contained in the batch.

The path between any source-destination pair in an anonymous network contains several nodes; each of which has, possibly, several input links and several output links. At each node, to perform routing, traffic generated by two or more sources can be merged into one outgoing stream, or the merged stream can be decomposed at several output links for different destinations. To expose the main features of mixing strategies, we focus on two fundamental cases: a double input-single output Mix, Figure 1, and a double input-double output Mix, Figure 2. Compared to [18], our model considers cases with finite link capacities and we derive optimal solutions for certain cases. The remainder of the paper is organized as follows. In section II, the double input-single output Mix is considered, and the optimal mixing strategy is found to maximize the anonymity under a strict latency constraint. Section III is devoted to the double input-double output Mix, where the optimal mixing strategy is found under a strict latency constraint and an average queue length constraint. Finally, we end the paper with some concluding remarks.

II. Double Input-Single Output Mix

Consider Figure 1 where there are two incoming flows, red and blue, and one outgoing link. The capacity of each input link is 1 packet/time-slot, and the capacity of the output link is 2 packets/time-slot. This model ensures that packets do not have to be dropped due to lack of capacity, even when the input links bring in data at maximum rate. Red and blue packets arrive according to i.i.d. Bernoulli processes with rates λ_R and λ_B respectively. There is an eavesdropper observing the incoming and outgoing packets. Assume the eavesdropper knows the source of each incoming packet, i.e., its color. This might be made feasible by traffic analysis if the Mix is the first hop of the route or, otherwise, by timing analysis of the

previous hop. Given the source of each incoming packet, the eavesdropper aims to identify the source of each outgoing packet, i.e., assign colors, red and blue, to the outgoing stream of packets.

First, consider the case where we do not allow for any delay, i.e., the Mix must send packets out in the same slot in which they arrived. Note that this is possible, without any packet drop, since at most two packets arrive in each slot, and the capacity of the output link is 2 packets/slot. Then, the only way to confuse the eavesdropper is to send out a random permutation of received packets in each slot.

By allowing a strict delay $T \geq 1$ for each packet, the Mix can do better; it can select and permute packets from the current slot and also from the previous slots, up to T slots before.

Next, we introduce a few notations and then define the mixing strategy under a strict delay constraint T per packet. The definitions are quite general and could be used to describe the mixing strategy and its anonymity for any multiple input-single output Mix, under a delay constraint T.

Let the random variable I_k denote arrivals in k-th slot. Therefore, for the double input-single output Mix, I_k can be $\emptyset$, R, B, or RB, where they respectively denote the cases of no arrivals, red arrival but no blue arrival, blue arrival but no red arrival, and both red and blue arrivals. Similarly define a random variable O_k for the output at slot k. For the double input-single output Mix, $O_k \in \{\emptyset, R, B, RR, BB, RB, BR\}$ (note that ordering of RB or BR at the output matters). There is an eavesdropper (Eve) who knows whether there is a packet at the output or not, i.e., at each time k, Eve knows a random variable $G_k := |O_k|$. For any stochastic process $\{X_k\}_{k \geq 1}$, define $X^{(N)} := X_1 \cdots X_N$.

Since we work with a discrete-time system, we have to specify the order in which different events occur: at each time slot k, first packet arrivals occur at the beginning of the time slot, and then departures occur. At the end of time slot k, let $Q_k(j)$ be a queue containing packets that have been in the system for j time slots, $0 \leq j \leq T - 1$ ($j = 0$ corresponds to packets arrived in the current slot but have not transmitted). In the case of double input-single output Mix, obviously, $Q_k(j) \in \{\emptyset, R, B, RB\}$, for $0 \leq j \leq T - 1$. Let $Q_k := [Q_k(0), Q_k(1), \cdots Q_k(T - 1)]$ be the collection

of such queues which represent existing packets in the Mix at the end of slot k. A mixing strategy consists of a *selection* strategy followed by a *permutation* strategy. At each time k, the Mix randomly selects packets from Q_{k-1}, and also from the newly arrived packets I_k, and then send a random permutation of the selected packets to the output. Let $D_k(j+1)$ denote the packets selected from $Q_{k-1}(j)$ by the Mix at slot k, for $0 \leq j \leq T - 1$[1]. Then, the queue dynamics can be described as

$$Q_k(j+1) = Q_{k-1}(j)\backslash D_k(j+1), \tag{1}$$

and

$$Q_k(0) = I_k\backslash D_k(0) \tag{2}$$

where $D_k(0)$ denoted the packets selected from new arrivals I_k and "$\backslash$" is the set difference operator. Note that $Q_k(T) = \emptyset$ because for any mixing strategy, under delay constraint T, packets that have been in the system for T time slots have to be transmitted, i.e., $D_k(T) = Q_{k-1}(T - 1)$. Let $D_k := [D_k(0), \cdots D_k(T)]$. Hence, $D_k = \Upsilon(Q_{k-1}, I_k)$, for some random selection strategy Υ, and $O_k = \Pi(D_k)$ for some permutation strategy Π, thus $O_k = \psi(Q_{k-1}, I_k)$ where $\psi = \Pi \circ \Upsilon$ is the mixing strategy. Let Ψ_T denote the set of all possible mixing strategies that satisfy the strict delay constraint T.

Next, we define anonymity of a mixing strategy $\psi \in \Psi_T$, based on the average conditional entropy of the output sequence given the input sequence and the sequence G, as follows.

Definition 1. *The anonymity A^ψ of a mixing strategy ψ is defined as*

$$A^\psi = \lim_{N \to \infty} \frac{1}{N(\lambda_R + \lambda_B)} H(O^{(N)}|I^{(N)}, G^{(N)}). \tag{3}$$

Note that in the above definition, the numerator is the entropy of the output sequence of length N given that Eve: (i) observes the input sequence of length N, and (ii) detects packet transmissions at the output. The denominator is the average number of red and blue arrivals in N slots. So, as $N \to \infty$, anonymity is the amount of uncertainty in each outgoing packet, bits/packet, observed by Eve.

Remark 1. *By using the Fano's inequality, the anonymity provides a lower bound for the probability of error in detection incurred by the eavesdropper [19].*

Without loss of generality, we can assume that the optimal mixing strategy does not change the ordering of packets from the same flow. This can be justified as follows. For any input sequence of length N, consider the set of possible output sequences of length N, under the mixing strategy ψ. If, for example, the red packets do not appear at the output in the same order as their arrival order, we can simply reorder them according to their arrival order, without changing the conditional probability of the appearance of the output sequence given the input sequence. Note that this does not

[1]At the moment that we move from slot $k - 1$ to slot k, the delay of each remaining packet increases by 1, hence we have used the notation $D_k(j+1)$ for packets selected from queue $Q_{k-1}(j)$ at time k.

reduce the anonymity and also will not violate the delay constraint (Eve is only interested in detecting the colors of the packets at the output, not their arrival times.). This also means that the mixing strategy is compatible with network protocols such as TCP, as it does change the sequence numbers of packets from the same flow.

A. Structure of Optimal Mix Strategy

We wish to find the optimal strategy $\psi^* \in \Psi_T$ that maximizes the anonymity. For mixing under a strict delay T, the output packets at time k are selected from the packets received in the current slot or the past T time slots that have not been transmitted before; however, in general, the rule, which determines which packet has to be transmitted, itself could possibly depend on the entire history up to time k. In other words, if we let $\mathcal{F}_k := \{I^{(k-1)}, O^{(k-1)}\}$ denote the history up to the beginning of time slot k, $O_k = \psi_{k,\mathcal{F}_k}(Q_k, I_k)$. Here, we assume that the Mix strategy and the Eve detection strategy are both causal and online meaning that transmission and detection decisions for O_k, has to be made at time k, and only depend on the history up to time k. Then, we show that the optimal mixing strategy, in fact, only needs a finite memory T and does not need the entire history, i.e., $O_k = \psi_{Q_{k-1}}(Q_{k-1}, I_k)$.

By the chain rule [20], the conditional entropy in (3) can be written as

$$H(O^{(N)}|I^{(N)}, G^{(N)})$$

$$= \sum_{k=1}^{N} H(O_k|I^{(N)}, G^{(N)}, O^{(k-1)}) \tag{4}$$

$$= \sum_{k=1}^{N} H(O_k|I^{(k)}, G^{(k)}, O^{(k-1)}) \tag{5}$$

$$= \sum_{k=1}^{N} H(O_k|I^{(k)}, G_k, O^{(k-1)}) \tag{6}$$

$$= \sum_{k=1}^{N} H(O_k|I^{(k)}, G_k, O^{(k-1)}, Q_{k-1}) \tag{7}$$

$$\leq \sum_{k=1}^{N} H(O_k|G_k, Q_{k-1}, I_k), \tag{8}$$

where (5) is because the Mix strategy and the Eve detection strategy are both causal and online, (6) follows from the fact that given $O^{(k-1)}$, $G^{(k-1)}$ does not contain any information, (7) holds because given $I^{(k-1)}$ and $O^{(k-1)}$, Q_{k-1} is known, and finally (8) follows from the fact that conditioning reduces the entropy.

Hence, for any mixing strategy $\psi \in \Psi_T$,

$$A^\psi \leq \lim_{N \to \infty} \frac{1}{N(\lambda_R + \lambda)} \sum_{k=1}^{N} H(O_k|G_k, Q_{k-1}, I_k). \tag{9}$$

Next, consider maximizing the Right-Hand-Side (RHS) of (9). We can define Q_k to be state of a Markov chain Q at the end of time k (at the beginning of time $k + 1$). Note that, for the double input-single output Mix, under strict delay T, $Q_k \in \{\emptyset, R, B, RB\}^T$. Hence, maximizing RHS of (9) can be interpreted as an average reward maximization problem

over an appropriately defined *Markov Decision Process* (MDP) Q_k with finite number of states. More accurately, maximizing RHS of (9) can be written as

$$\max_{\psi \in \Psi_T} \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} \mathbb{E}_{q_{k-1}}[c(q_{k-1}, \psi_k)], \quad (10)$$

where the reward function is given by

$$
\begin{aligned}
c(q_{k-1}, \psi_k) &= H(O_k | q_{k-1}, I_k, G_k) \\
&= \mathbb{E}_{i_k}[H(O_k | q_{k-1}, i_k, G_k)], \quad (11)
\end{aligned}
$$

where q_k and i_k are realizations of random variables Q_k and I_k respectively[2]. Hence, we have a finite state MDP with bounded rewards. Consider the class of stationary (and Markov) policies $S_T \subset \Psi_T$, where, at each time k, decision is made only based on Q_{k-1}, i.e., $O_k = \psi_{Q_{k-1}}(Q_{k-1}, I_k)$. A sufficient condition for existence of an optimal stationary policy for (10) is given by the following lemma [21], [25].

Lemma 1. *Suppose there exists a constant w and a bounded function ϕ, unique up to an additive constant, satisfying the following optimality equation*

$$w + \phi(q) = \max_u \{c(q, u) + E[\phi(Q_1) | Q_0 = q, \psi_1 = u]\}, \quad (12)$$

then w is the maximal average-reward and the optimal stationary policy ψ^* is the one that chooses the optimizing $u(.)$.

Next, we show that (12) always has a solution. Let $\tau := \min\{k \geq 1 : Q_k = \emptyset\}$ where by $Q_k = \emptyset \equiv \{\emptyset\}^T$ we mean a state where there are no packets in the Mix waiting for transmission. Next, consider the class of stationary policies $S_T \subset \Psi_T$, i.e., $O_k = \psi_{Q_{k-1}}(Q_{k-1}, I_k)$. Then we have, for any $\psi \in S_T$, and for any initial state q,

$$\mathbb{E}^{\psi}[\tau | Q_0 = q] \leq \frac{T}{(1 - \lambda_R)^T (1 - \lambda_B)^T} < \infty. \quad (13)$$

This is because starting from any initial state, after a null input sequence of length T, i.e., no arrivals for T time slots, the Markov chain has to return to $\emptyset$ state. Such a sequence occurs with probability $(1 - \lambda_R)^T (1 - \lambda_B)^T$ and the expected time is bounded as in (13) for any stationary Markov policy as long as λ_R and λ_B are strictly less than one. The following lemma is a corollary of Theorem (6.5) of [25] (page 164).

Lemma 2. *Assume $\mathbb{E}^{\psi}[\tau | Q_0 = q] \leq B < \infty$ for all $\psi \in S_T$ and all q, then there exists a w and $\phi(.)$ satisfying DP equation (12).*

Hence, it follows from Lemmas 2 and 1 that the maximizer of RHS of (9) is a stationary policy. Moreover, observe that for any stationary policy, the inequality in (8) and accordingly in (9) can be replaced by equality, and therefore, the stationary policy ψ^* given by (12) always exists and actually maximizes the anonymity and the maximum achievable anonymity, by definition, is given by

$$A^{\psi^*} = \frac{w}{\lambda_R + \lambda_B}.$$

[2]Throughout the paper, we use a capital letter for a random variable and the corresponding lower-case letter to denote a realization of that random variable.

Note that the above argument is still valid for any multiple input-single output Mix and any link capacities as long as the output link capacity is greater than or equal to the sum of input-links' capacities to ensure that there is no need to drop packets.

In general, the DP equation (12) can be written in form of the following LP

$$\max \ w \quad (14)$$
$$w + \phi(q) \leq c(q, u) + E[\phi(Q_1) | Q_0 = q, u_1 = u] \ ;$$
$$\forall q \in \{\emptyset, R, B, RB\}^T$$

which can be solved numerically. However, the number of states grows exponentially in T which makes the characterization of strategies and computation of the optimal strategy complicated especially for large T. For small T, we might be able to find the optimal solution explicitly. To illustrate the structure of the optimal solution, we present the explicit solutions for $T = 0$ and $T = 1$ in the following two subsections.

B. The Optimal Mix Strategy for $T = 0$

The case of $T = 0$ is trivial since, in this case, for stationary policies, the output sequence is i.i.d. as well, and therefore

$$
\begin{aligned}
\text{RHS of (9)} &= \frac{1}{N} \sum_{k=1}^{N} H(O_k | I_k, G_k) \\
&= H(O_1 | I_1, G_1) \\
&= \lambda_R \lambda_B H(O_1 | I_1 = RB, G_1 = 2).
\end{aligned}
$$

Therefore, to maximize the anonymity, the Mix must send a random permutation of the received packets, in the case of both read and blue arrival, with equal probability to get $H(O_1 | I_1 = RB, G_1 = 2) = 1$. Correspondingly, the maximum anonymity is given by

$$A^{\psi^*} = \frac{\lambda_R \lambda_B}{\lambda_R + \lambda_B}.$$

In the rest of this section, we consider the more interesting case of $T = 1$, where each packet has to be sent out in the current slot or in the next slot.

C. The Optimal Mix Strategy for $T = 1$

As we proved in section II-A, we only need to consider the class of stationary policies that maximize the RHS of (9). Therefore, for $T = 1$, the optimal mixing strategy is the solution to the following average entropy maximization problem

$$\max \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} E_{q_{k-1}}[H(O_k | I_k, q_{k-1}, G_k)],$$

where now $q_{k-1} \in \{\emptyset, R, B, RB\}$. Recall that the random variable Q_{k-1} ($= Q_{k-1}(0)$ here) denotes what has been left in the queue, at the end of time slot $k - 1$, for transmission in the time slot k, where we have defined the initial condition as $Q_0 = \emptyset$, and q_{k-1} is the realization of Q_{k-1}. Roughly speaking, the action ψ_k is to randomly select some packets

from I_k and q_{k-1}, and send the permutation of the selected packets to the output. Let w denote the maximum value of the above average entropy maximization problem, then, by definition, $A^{\psi^*} = \frac{w}{\lambda_R + \lambda_B}$, and the optimal mixing strategy ψ^* is the one that chooses the corresponding optimal policy for the average entropy maximization problem. In order to solve the problem, next we identify the possible actions for different states which will allow us to define the reward function in more detail and provide an explicit solution.

1) Set of possible actions and corresponding rewards for different states: There is a set of possible actions for each state depending on different arrival types. In the following, we identify the set of actions and their corresponding rewards for each case.

(a) Assume $Q_{k-1} = \emptyset$, then
   (i) If $I_k = \emptyset$: In this case, obviously, there will be no transmission at the output link, $G_k = 0$, and the queue will remain empty as well, i.e., $O_k = \emptyset$ and $Q_k = \emptyset$. The corresponding entropy is $H(O_k|I_k = \emptyset, Q_{k-1} = \emptyset, G_k) = 0$.
   (ii) If $I_k = R$: Two options are possible; the Mix can queue the arrived packet ($G_k = 0$) with probability α_k, or send the packet in the current slot ($G_k = 1$) with probability $1 - \alpha_k$. No matter what the Mix does, the entropy in this slot $H(O_k|I_k = R, Q_{k-1} = \emptyset, G_k) = 0$. Correspondingly, the queue is updated as $Q_k = R$, with probability of α_k, or $Q_k = \emptyset$, with probability of $1 - \alpha_k$.
   (iii) If $I_k = B$: This case is similar to the previous case except that we use β_k instead of α_k. Therefore, $Q_k = B$, with probability β_k, or $Q_k = \emptyset$, with probability $1 - \beta_k$, and $H(O_k|I_k = B, Q_{k-1} = \emptyset, G_k) = 0$.
   (iv) If $I_k = RB$: The Mix has four options; it can queue both packets (with probability $1 - s_k$), send both out (with probability $s_k(1 - y_k)$), keep only R and send B out (with probability $s_k y_k(1 - p_k)$), or keep only B and send R out (with probability $s_k y_k p_k$). Note that the parameters s_k, y_k, and p_k have been used to characterize the probabilities of different options. Intuitively, s_k is the probability that a transmission at the output link happens at all, y_k is the probability of sending only one packet out given a transmission must happen, and p_k is the probability of sending R out given that only one packet is transmitted at the output. Accordingly,

$$H(O_k|I_k = RB, Q_{k-1} = \emptyset, G_k) = s_k(y_k \mathcal{H}(p_k) + 1 - y_k),$$

where $\mathcal{H}$ is the binary entropy function given by

$$\mathcal{H}(p) = -p \log(p) - (1-p)\log(1-p)$$

for $0 < p < 1$.

(b) Assume $Q_{k-1} = R$, then
   (i) If $I_k = \emptyset$: The Mix has to send the content of the queue to the output, therefore $O_k = R$, and obviously, $H(O_k|I_k = \emptyset, Q_{k-1} = R, G_k) = 0$ and $Q_k = \emptyset$.
   (ii) If $I_k = R$: The Mix can queue the recent R, with probability γ_k, and send Q_{k-1} to the output, or can send both Q_{k-1} and the recent arrival to the output, with probability $1 - \gamma_k$. Therefore, $Q_k = R$ ($O_k = R$) with probability γ_k, or $Q_k = \emptyset$ ($O_k = RR$) with probability $1 - \gamma_k$. The corresponding entropy will be zero, i.e., $H(O_k|I_k = R, Q_{k-1} = R, G_k) = 0$.
   (iii) If $I_k = B$: Again the Mix has two options; it can send a random permutation of R and B to the output, i.e., $Q_k = \emptyset$, with probability a_k, or it can queue the B and send only the R out, i.e., $Q_k = B$, with probability $1 - a_k$. The entropy is $H(O_k|I_k = B, Q_{k-1} = R, G_k) = a_k$.
   (iv) If $I_k = RB$: The Mix has three options; it can queue both arrivals, i.e., $Q_k = RB$, with probability $1 - t_k$, keep only the red arrival in the queue, i.e., $Q_k = R$, with probability $t_k(1 - d_k)$, or keep only the blue arrival in the queue, i.e., $Q_k = B$, with probability $t_k d_k$. Correspondingly, in this case,

$$P(O_k = o_k | I_k = RB, Q_{k-1} = R, G_k = 2)$$
$$= \begin{cases} d_k & ; o_k = RR \\ (1 - d_k)/2 & ; o_k = RB \\ (1 - d_k)/2 & ; o_k = BR. \end{cases} \quad (15)$$

and

$$H(O_k | I_k = RB, Q_{k-1} = R, G_k) = t_k(\mathcal{H}(d_k) + 1 - d_k).$$

(c) Assume $Q_{k-1} = B$, then this case is similar to the previous case and the details are omitted for brevity.
   (i) If $I_k = \emptyset$: Obviously, $H(O_k|I_k = \emptyset, Q_{k-1} = B, G_k) = 0$, and $Q_k = \emptyset$.
   (ii) If $I_k = B$: $H(O_k|I_k = B, Q_{k-1} = B, G_k) = 0$. Options are $Q_k = B$, with probability δ_k, or $Q_k = \emptyset$, with probability $1 - \delta_k$.
   (iii) If $I_k = R$: $H(O_k|I_k = R, Q_{k-1} = B, G_k) = b_k$. Options are $Q_k = R$, with probability $1 - b_k$, or $Q_k = \emptyset$, with probability b_k.
   (iv) If $I_k = RB$: The Mix can keep both arrivals in the queue, i.e., $Q_k = RB$, with probability $1 - z_k$, keep only the red arrival in the queue, i.e., $Q_k = R$, with probability $z_k r_k$, or keep only the blue arrival in the queue, i.e., $Q_k = B$, with probability $z_k(1 - r_k)$. The entropy is

$$H(O_k | I_k = RB, Q_{k-1} = B, G_k) = z_k(\mathcal{H}(r_k) + 1 - r_k).$$

(d) Assume $Q_{k-1} = RB$, then the Mix has to send the contents of the queue to the output, i.e., $O_k = RB$ or BR with equal probabilities, and queue all the recent arrivals, i.e., $Q_k = I_k$. The entropy is simply $H(O_k|I_k, Q_{k-1} = RB, G_k) = 1$.

Next, we calculate the reward for each state. Recall that the reward function is

$$C(x_k, \psi_k) = H(O_k|I_k, q_{k-1}, G_k) = E_{i_k}[H(O_k|i_k, q_{k-1}, G_k)],$$

where i_k denotes a realization of I_k. Therefore, averaging over 4 possible arrivals in each state, the reward function and queue updates, for each state are the following.

(a) $Q_{k-1} = \emptyset$:

The reward function is given by

$$C(\emptyset, \psi_k) = \lambda_R \lambda_B s_k \left(y_k \mathcal{H}(p_k) + 1 - y_k \right),$$

and the queue is updated as

$$P(Q_k = q | Q_{k-1} = \emptyset, \psi_k) = \begin{cases} \lambda_R(1 - \lambda_B)\alpha_k + \lambda_R \lambda_B s_k y_k (1 - p_k) & ; q = R \\ \lambda_B(1 - \lambda_R)\beta_k + \lambda_R \lambda_B s_k y_k p_k & ; q = B \\ \lambda_R \lambda_B (1 - s_k) & ; q = RB \\ - - - & ; q = \emptyset \end{cases}$$

where we used the notation " $- - -$ " for the probability of having an empty queue, since we will not need the explicit expression for this probability, although, it can be, obviously, derived from the other three probabilities. Note that ψ_k is specified by 5 parameters $0 \le \alpha_k, \beta_k, y_k, s_k, p_k \le 1$.

(b) $Q_{k-1} = R$:

The reward function is given by

$$C(R, \psi_k) = \lambda_B(1 - \lambda_R)a_k + \lambda_R \lambda_B t_k \left(\mathcal{H}(d_k) + 1 - d_k \right),$$

and the queue is updated as

$$P(Q_k = q | Q_{k-1} = R, \psi_k) = \begin{cases} \lambda_R(1 - \lambda_B)\gamma_k + \lambda_R \lambda_B t_k(1 - d_k) & ; q = R \\ \lambda_B(1 - \lambda_R)(1 - a_k) + \lambda_R \lambda_B t_k d_k & ; q = B \\ \lambda_R \lambda_B (1 - t_k) & ; q = RB \\ - - - & ; q = \emptyset \end{cases}$$

Note that, in this state, ψ_k is specified by 4 parameters $0 \le a_k, t_k, \gamma_k, d_k \le 1$.

(c) $Q_{k-1} = B$:

The reward function is given by

$$C(B, \psi_k) = \lambda_R(1 - \lambda_B)b_k + \lambda_R \lambda_B z_k \left(\mathcal{H}(r_k) + 1 - r_k \right),$$

and the queue is updated as

$$P(Q_k = q | Q_{k-1} = B, \psi_k) = \begin{cases} \lambda_R(1 - \lambda_B)(1 - b_k) + \lambda_R \lambda_B r_k z_k & ; q = R \\ \lambda_B(1 - \lambda_R)\delta_k + \lambda_R \lambda_B z_k(1 - r_k) & ; q = B \\ \lambda_R \lambda_B (1 - z_k) & ; q = RB \\ - - - & ; q = \emptyset \end{cases}$$

Note that here ψ_k is specified by 4 parameters $0 \le b_k, z_k, \delta_k, r_k \le 1$.

(d) $Q_{k-1} = RB$:

The reward function is given by

$$C(RB, \psi_k) = 1,$$

and the queue is updated as

$$P(Q_k = q | Q_{k-1} = RB, \psi_k) = \begin{cases} \lambda_R(1 - \lambda_B) & ; q = R \\ \lambda_B(1 - \lambda_R) & ; q = B \\ \lambda_R \lambda_B & ; q = RB \\ - - - & ; q = \emptyset \end{cases}$$

Note that, here, there is no degrees of freedom for ψ_k (The Mix has to send out Q_{k-1}).

2) The Optimal Stationary Mix strategy: Having formally defined the reward function and the dynamics of the system in subsection II-C1, we use Lemma 1 to solve the average reward maximization problem. It turns out that the optimal strategy is specified by only three parameters p, r, and d, and all the other parameters must be one. The following proposition states one of our main results.

Proposition 1. *For the double input-single output Mix, and $T = 1$, the optimal Mix strategy is the following. At each time k, given Q_{k-1} and I_k, if*

1) $Q_{k-1} = \emptyset$
  - *$I_k = \emptyset, R, B$: $Q_k = I_k$, $O_k = \emptyset$.*
  - *$I_k = RB$: send R out with probability p^* or B with probability $1 - p^*$, $Q_k = I_k \backslash O_k$.*

2) $Q_{k-1} = R$
  - *$I_k = \emptyset, R$: $Q_k = I_k$, $O_k = Q_{k-1}$.*
  - *$I_k = B$: transmit a random permutation of R and B, $Q_k = \emptyset$.*
  - *$I_k = RB$: transmit RR with probability d^* ($Q_k = B$), or transmit a random permutation of R and B with probability $1 - d^*$ ($Q_k = R$).*

3) $Q_{k-1} = B$
  - *$I_k = \emptyset, B$: $Q_k = I_k$, $O_k = Q_{k-1}$.*
  - *$I_k = R$: transmit a random permutation of R and B, $Q_k = \emptyset$.*
  - *$I_k = RB$: transmit BB with probability r^* ($Q_k = R$), or transmit a random permutation of R and B with probability $1 - r^*$ ($Q_k = B$).*

where probabilities p^*, d^*, and r^* depend on arrival rates λ_R and λ_B.

In the special case $\lambda_R = \lambda_B$, $p^* = \frac{1}{2}$, $d^* = \frac{1}{3}$, and $r^* = \frac{1}{3}$.

Proof of Proposition 1: Recall the optimality equation (12):

$$w + \phi(q) = \max_u \left\{ C(q, u) + E[\phi(Q_1) | Q_0 = q, \psi_1 = u] \right\}.$$

Since ϕ is unique up to an additive constant, without loss of generality, assume $\phi(\emptyset) = 0$. Then, for $q = \emptyset$, the optimality equation can be written as

$$\begin{aligned} w = \max_{s,p,y,\alpha,\beta} &\{ \lambda_R \lambda_B s \left(y\mathcal{H}(p) + 1 - y \right) \\ &+ [\lambda_R(1 - \lambda_B)\alpha + \lambda_R \lambda_B sy(1 - p)]\phi(R) \\ &+ [\lambda_B(1 - \lambda_R)\beta + \lambda_R \lambda_B syp]\phi(B) \\ &+ [\lambda_R \lambda_B (1 - s)]\phi(RB) \}. \end{aligned}$$

Obviously, $\alpha = 1$ and $\beta = 1$ maximize the right hand side if $\phi(R)$ and $\phi(B)$ are nonnegative. We will later see that $\phi(R)$ and $\phi(B)$ are indeed nonnegative. Therefore, the right hand side of the optimality equation can be written as

$$\begin{aligned} \lambda_R \lambda_B s &\left[y \left(\mathcal{H}(p) - 1 + (1 - p)\phi(R) + p\phi(B) \right) + 1 - \phi(RB) \right] \\ &+ \lambda_R(1 - \lambda_B)\phi(R) + \lambda_B(1 - \lambda_R)\phi(B) + \lambda_R \lambda_B \phi(RB). \end{aligned}$$

First, consider the term $\mathcal{H}(p) - 1 + (1 - p)\phi(R) + p\phi(B)$. This term is maximized by choosing

$$p^* = \frac{1}{1 + 2^{\phi(R) - \phi(B)}}. \tag{16}$$

We will later show that

$$\mathcal{H}(p^*) - 1 + (1-p^*)\phi(R) + p^*\phi(B) \geq 0, \quad (17)$$

and therefore $y^* = 1$. Furthermore, for $y^* = 1$, we will see that the term inside the brackets is always nonnegative, i.e.,

$$\mathcal{H}(p^*) + (1-p^*)\phi(R) + p^*\phi(B) - \phi(RB) \geq 0, \quad (18)$$

and therefore $s^* = 1$. Finally, w is given by

$$\begin{aligned} w &= \lambda_R\lambda_B\mathcal{H}(p^*) + \lambda_R(1-\lambda_Bp^*)\phi(R) \\ &+ \lambda_B(1-\lambda_R(1-p^*))\phi(B). \end{aligned} \quad (19)$$

Next, consider the optimality equation for $q = R$. It can be written as

$$\begin{aligned} w + \phi(R) &= \max_{\gamma,d,t,a} \{\lambda_B(1-\lambda_R)a + \lambda_R\lambda_Bt\,(\mathcal{H}(d)+1-d) \\ &+[\lambda_R(1-\lambda_B)\gamma + \lambda_R\lambda_B(1-d)]\phi(R) \\ &+[\lambda_B(1-\lambda_R)(1-a) + \lambda_R\lambda_Btd]\phi(B) \\ &+\lambda_R\lambda_R(1-t)\phi(RB)\}. \end{aligned}$$

Similar to the argument for $q = \emptyset$, $\gamma^* = 1$, if $\phi(R) > 0$, and $a^* = 1$ if $\phi(B) < 1$. Furthermore, taking the derivative respect to d, setting it to zero, and solving it for d^* yields

$$d^* = \frac{1}{1+2^{1+\phi(R)-\phi(B)}}. \quad (20)$$

Finally, $t^* = 1$ if

$$\mathcal{H}(d^*)+1-d^*+(1-d^*)\phi(R)+d^*\phi(B)-\phi(RB) \geq 0, \quad (21)$$

and the optimality condition is simplified to

$$\begin{aligned} w + \phi(R) &= \lambda_B(1-\lambda_R) + \lambda_R\lambda_B\,(\mathcal{H}(d^*)+1-d^*) \\ &+[\lambda_R(1-\lambda_B)+\lambda_R\lambda_B(1-d^*)]\phi(R) \\ &+\lambda_R\lambda_Bd^*\phi(B). \end{aligned} \quad (22)$$

Next, consider the optimality equation for $q = B$

$$\begin{aligned} w + \phi(B) &= \max_{\delta,r,z,b} \{\lambda_R(1-\lambda_B)b + \lambda_R\lambda_Bz\,(\mathcal{H}(r)+1-r) \\ &+[\lambda_B(1-\lambda_R)\delta + \lambda_R\lambda_Bz(1-r)]\phi(B) \\ &+[\lambda_R(1-\lambda_B)(1-b) + \lambda_R\lambda_Bzr]\phi(R) \\ &+\lambda_R\lambda_R(1-z)\phi(RB)\}. \end{aligned}$$

In parallel with the argument for $q = R$, $\delta^* = 1$ if $\phi(B) \geq 0$, and $b^* = 1$ if $\phi(R) \leq 1$. Moreover, $z^* = 1$ if

$$\mathcal{H}(r^*)+1-r^*+(1-r^*)\phi(B)+r^*\phi(R)-\phi(RB) \geq 0, \quad (23)$$

where

$$r^* = \frac{1}{1+2^{1+\phi(B)-\phi(R)}}. \quad (24)$$

The optimality condition is simplified to

$$\begin{aligned} w + \phi(B) &= \lambda_R(1-\lambda_B) + \lambda_R\lambda_B\,(\mathcal{H}(r^*)+1-r^*) \\ &+[\lambda_B(1-\lambda_R)+\lambda_R\lambda_B(1-r^*)]\phi(B) \\ &+\lambda_R\lambda_Br^*\phi(R). \end{aligned} \quad (25)$$

Finally, the optimality equation for $q = RB$ is given by

$$\begin{aligned} w + \phi(RB) &= 1 + \lambda_R(1-\lambda_B)\phi(R) \\ &+\lambda_B(1-\lambda_R)\phi(B) + \lambda_R\lambda_B\phi(RB). \end{aligned} \quad (26)$$

(a) Anonymity

(b) $\phi(R)$

Fig. 3. Anonymity and $\phi(R)$ for the case of $\lambda_R = \lambda_B = \lambda$.

Therefore, we need to solve equations (19), (22), and (25) to find w, $\phi(R)$, and $\phi(B)$. Then, (26) can be used to find $\phi(RB)$. Eventually, what remains to be shown is that $0 \leq \phi(R), \phi(B) \leq 1$, and, in addition, $\phi(R)$, $\phi(B)$, and $\phi(RB)$ satisfy inequalities (17), (18), (21), and (23).

First, consider the special case of $\lambda_R = \lambda_B = \lambda$. By symmetry, $\phi(R) = \phi(B)$ which yields $p^* = 1/2$ and $d^* = r^* = 1/3$. Then, by solving equations (19) and (22), we have,

$$\phi(R) = \phi(B) = \frac{\lambda^2(\log 3 - 2) + \lambda}{-\lambda^2 + \lambda + 1},$$

and

$$w = \frac{\lambda^2}{-\lambda^2 + \lambda + 1}\left[-\lambda^2(\log 3 - 1) + 2(\log 3 - 2)\lambda + 3\right].$$

Then, the anonymity is $A^{\psi^*} = w/2\lambda$, and it is easy to check that the solutions satisfy all the inequalities. Figures 3(a) and 3(b) show the anonymity A^{ϕ^*} and $\phi(R)$ as functions of λ.

Next, consider the general case with, probably, unequal arrival rates. We prove that the solutions indeed exist and they satisfy the required conditions. Using (19) to replace w in (22)

and (25) yields

$$\phi(R) = \lambda_B[1 - \phi(B)(1 - \lambda_R)] + \lambda_R\lambda_B g(\xi), \quad (27)$$

$$\phi(B) = \lambda_R[1 - \phi(R)(1 - \lambda_B)] + \lambda_R\lambda_B f(\xi), \quad (28)$$

where,

$$g(\xi) = (d^* - p^*)(-\xi) + \mathcal{H}(d^*) - \mathcal{H}(p^*) - d^*,$$
$$f(\xi) = (r^* + p^*)\xi + \mathcal{H}(r^*) - \mathcal{H}(p^*) - r^* - \xi,$$

and,

$$\xi = \phi(R) - \phi(B).$$

Therefore, the optimal probabilities can be expressed as functions of ξ by

$$p^* = \frac{1}{1 + 2^\xi},$$
$$d^* = \frac{1}{1 + 2^{1+\xi}},$$
$$r^* = \frac{1}{1 + 2^{1-\xi}}.$$

Lemma 3. *The function $g(\xi)$ is an increasing function of ξ and $f(\xi)$ is a decreasing function of ξ (see Appendix for the proof).*

For any pair $(\phi(R), \phi(B))$ chosen from $[0,1] \times [0,1]$, we have $-1 \le \xi \le 1$, and therefore, by Lemma 3, functions f and g can be bounded from below and above by

$$g(-1) \le g(\xi) \le g(1),$$

and

$$f(1) \le f(\xi) \le f(-1).$$

But it is easy to check that

$$g(1) = f(-1) = \log(5/3) - 1, \; g(-1) = f(1) = 1 - \log 3,$$

and therefore,

$$-1 < f(\xi), g(\xi) < 0.$$

Consequently, the right-hand sides of (27) and (28) form a continuous mapping from $[0,1] \times [0,1]$ to $[0,1] \times [0,1]$, and therefore, by the Brouwer fixed point theorem ([22], p. 72), the system of nonlinear equations, (27), (28), has a solution $(\phi(R), \phi(B)) \in [0,1] \times [0,1]$.

Next, we show that the solutions indeed satisfy the inequalities. First, we prove that (17) holds. Define

$$\psi_1(\xi) = \mathcal{H}(p^*) + (1 - p^*)\phi(R) + p^*\phi(B)$$
$$= \mathcal{H}(p^*) - p^*\xi + \phi(R).$$

First, consider the case that $-1 \le \xi \le 0$, then

$$\frac{d}{d\xi}(\mathcal{H}(p^*) - p^*\xi) = p^{*\prime}\log\frac{1 - p^*}{p^*} - p^* - p^{*\prime}\xi$$
$$= -p^* \le 0.$$

Hence,

$$\psi_1(\xi) \ge \psi_1(0) = 1 + \phi(R) \ge 1.$$

For the case that $0 \le \xi \le 1$, rewrite $\psi_1(\xi)$ as the following

$$\psi_1(\xi) = \mathcal{H}(p^*) + (1 - p^*)\xi + \phi(B).$$

Then,

$$\frac{d}{d\xi}(\mathcal{H}(p^*) + (1 - p^*)\xi) = 1 - p^* \ge 0,$$

and hence,

$$\psi_1(\xi) \ge \psi_1(0) = 1 + \phi(B) \ge 1.$$

Therefore, for $-1 \le \xi \le 1$, $\psi_1(\xi) \ge 1$, and (17) holds.

Note that from (26), we have

$$\phi(RB) = \frac{1 - \lambda_R\lambda_B\psi_1(\xi)}{1 - \lambda_R\lambda_B}, \quad (29)$$

and since (17) holds, we have

$$\phi(RB) \le 1,$$

and consequently (18) will be satisfied as well.

To show (21), note that $\phi(R) + 1 - \phi(RB) \ge 0$, and therefore, it suffices to prove that

$$\psi_2(\xi) = \mathcal{H}(d^*) - d^* - d^*\phi(R) + d^*\phi(B)$$
$$= \mathcal{H}(d^*) - d^*\xi - d^*$$

is nonnegative. But $\psi_2(\xi)$ is a decreasing function since

$$\frac{d}{d\xi}\psi_2 = d^{*\prime}\log\frac{1 - d}{d} - d^{*\prime}\xi - d^* - d^{*\prime}$$
$$= d^{*\prime}(1 + \xi) - d^{*\prime}\xi - d^* - d^{*\prime}$$
$$= -d^* \le 0$$

So $\psi_2(\xi) \ge \psi_2(1) = \mathcal{H}(1/5) - 2/5 = \log 5 - 2 \ge 0$, and consequently (21) follows. (23) is also proved by a similar argument. Define a function $\psi_3(\xi)$ as

$$\psi_3(\xi) = \mathcal{H}(r^*) - r^* - r^*\phi(B) + r^*\phi(R)$$
$$= \mathcal{H}(r^*) + r^*\xi - r^*.$$

Then, $\psi_3(\xi)$ is an increasing function since

$$\frac{d}{d\xi}\psi_3 = r^* \ge 0.$$

Thus,

$$\psi_3(\xi) \ge \psi_3(-1)$$
$$= \mathcal{H}(1/5) - 2/5$$
$$= \log 5 - 2 \ge 0,$$

and therefore (23) follows. This concludes the proof of Proposition 1. ∎

3) Numerical results: Equations (19), (22), and (25) form a system of nonlinear equations which can be solved numerically, for different values of λ_R and λ_B, by using the following algorithm.

Note that in the step 5 of the algorithm, we solve a linear system of equations (p^*, d^*, and r^* are replaced with their numerical values). Figure 4 shows the maximum anonymity, found by running the algorithm, for different arrival rates. The probabilities p^*, d^*, and r^* of the optimal mixing strategy have been evaluated in Figure 5 for different arrival rates λ_R and λ_B.

Remark 2. *The stationary policy does not exist for $\lambda_R = \lambda_B = 1$ since as $\lambda_R \to 1$ and $\lambda_B \to 1$, $\phi(RB) \to -\infty$*

Algorithm 1

1: $p_0^* \leftarrow 1/2$, $d_0^* \leftarrow 1/3$, $r_0^* \leftarrow 1/3$
2: $i \leftarrow 0$
3: **repeat**
4:     $i \leftarrow (i+1)$
5:     $w, \phi(R), \phi(B) \Leftarrow$ solve (19), (22), and (25)
6:     $p_i^*, d_i^*, r_i^* \Leftarrow$ calculate (16), (20), and (24)
7: **until** $|p_i^* - p_{i-1}^*| \leq \epsilon$ and $|d_i^* - d_{i-1}^*| \leq \epsilon$ and $|r_i^* - r_{i-1}^*| \leq \epsilon$

Fig. 4. Anonymity for different values of λ_R and λ_B.

(see (29)). This makes sense since, in this case, if we start with initial condition $Q_0 = \emptyset$ and use the strategy specified in Proposition 1, we get an anonymity of $A^{\psi^*} = \log(3)/2$; whereas if the initial condition is $Q_0 = RB$, the only possible strategy will be to transmit the contents of the queue, and queue the arrived RB in each time slot. This yields an anonymity of $1/2$ bit/packet. Therefore, the optimal strategy depends on the initial condition for $\lambda_R = \lambda_B = 1$.

III. DOUBLE INPUT-DOUBLE OUTPUT MIX

Figure 2 shows the double input-double output Mix. The capacity of each link is 1 packet/time slot. Compared to the Mix with one output link, i.e., Figure 1, the flows of outgoing packets are separate.

At this point, we would like to clarify the main difference between Sections II and III of the paper. The focus of both sections is on flow-level anonymity. However, in the double input-single output Mix, section II, every packet can be analyzed to see if it belongs to a particular flow. In the double input-double output Mix, even if one packet is identified as belonging to a flow, then it compromises the entire flow at that node. Hence, in this case, the eavesdropper does not need to detect the sender for each outgoing packet; instead, it aims to find the corresponding source of each flow, by observing a sequence of outgoing packets of sufficiently long duration. Let $d_R \in \{1, 2\}$ denote the destination of the red source. Formally, we define the anonymity A^ψ of a Mix strategy ψ

(a) p^*

(b) d^*

(c) r^*

Fig. 5. Probabilities p^*, d^*, and r^* for different arrival rates λ_R and λ_B.

for the double input-double output Mix to be

$$A^\psi = \lim_{N \to \infty} H\big(d_R | I_R^{(N)}, I_B^{(N)}, G_1^{(N)}, G_2^{(N)}\big), \quad (30)$$

where similar to Section II, $I_R^{(N)}$ and $I_B^{(N)}$ are the sequences of red and blue arrivals of length N, and $G_i^{(N)} = (G_i(1), G_i(2), ..., G_i(N))$, $i = 1, 2$, where $G_i(t) \in \{0, 1\}$ indicates whether there is a packet at the output i in time slot t. Without loss of generality, assume that $\lambda_R > \lambda_B$

(the singular case of $\lambda_R = \lambda_B$ will be discussed later). Then, by calculating the long-run average rates of outgoing flows, the eavesdropper can identify the corresponding source-destination pairs. Therefore, it is not possible to get any anonymity without dropping some packets from the red flow. Hence, the maximum achievable throughput for each flow cannot be more than $\min\{\lambda_R, \lambda_B\}(=\lambda_B)$, and, at least, the packets of the flow with higher rate, which is the red flow here, must be dropped at an average rate of $\lambda_R - \lambda_B$.

We now present our model for a Mix with two queues for red and blue arrivals. Let $A_R[0,t]$ and $A_B[0,t]$ be the number of arrivals for the red and blue arrivals in $[0,t]$. Also let $D_1[0,t]$ and $D_2[0,t]$ denote the number of departures from the output links 1 and 2 by the end of time slot t. Then, to assure any nonzero anonymity, i.e, we need

$$D_i[0,t] \le \min\{A_R[0,t], A_B[0,t]\}; \ \forall t \ge 1; \ \text{for } i = 1, 2 \tag{31}$$

This is clear, because, for example, if there exists a time t_1 such that $A_R[0,t_1] \ge D_1[0,t_1] > A_B[0,t_1]$, then obviously the red source is connected to the output 1 and the anonymity is zero.

A. Mix under a strict delay constraint T

Suppose that each arrival has to be transmitted within T time slots. In this case, in addition to red packets, blue packets have to be dropped as well. This is because it might happen that there is a blue arrival but no red packets for a time duration of T, in which case transmitting the blue packet will immediately reveals the corresponding destination of the blue source. Hence, the throughput of each flow will be less λ_B. Recall the queue model of the Mix described earlier and consider the following strategy.

Mix strategy under strict delay T: For each queue, transmit the *head-of-the-line* (HOL) packet along with the HOL packet of the other queue simultaneously at the corresponding output links. If the HOL packet has been in the queue for more than T time slots and there is no arrivals in the other queue, drop the HOL packet.

Proposition 2. *The above strategy is optimal in the sense that it yields perfect anonymity with maximum possible throughput.*

Perfect anonymity, means that $A^\psi = 1$, i.e., by observing the output sequence, the eavesdropper cannot obtain any information and each outgoing flow is equally likely to belong to one of sources.

Proof: Noting that any strategy with non-zero anonymity must satisfy (31), it is easy to observe that packets that are dropped under our strategy will be dropped under any strategy that satisfy (31). Hence, our strategy has the maximum throughput. Clearly our strategy has also perfect anonymity because $G_1(t) = G_2(t)$ at all times t. Also note that in our strategy, packets will be immediately transmitted once a different color packet appears in the other queue. This is the earliest time that a packet can be transmitted under (31). Hence, the average delay of those packets transmitted successfully is also minimized under our strategy. ∎

Next, consider the case that there is no strict delay constraint. In this case, one does not know how to measure the average delay because any Mix with non-zero anonymity has to drop some of the packets and the delay of the dropped packets is infinity. So, instead, we use the average queue size as the QoS metric.

B. Mix with an average queue length constraint

In this case, instead of a per-packet latency constraint, we consider the average queue size as the QoS metric. Similar to the previous case, we consider strategies that achieve both maximum throughput and perfect anonymity. Among all such strategies, we will find an optimal strategy that minimizes the mean queue length.

First note that, to get the smallest queue size, we would like (31) to hold with equality, i.e.,

$$D_1[0,t] = D_2[0,t] = \min\{A_R[0,t], A_B[0,t]\}; \ \forall t \ge 1 \tag{32}$$

Then, it is clear that red and blue packets must be transmitted simultaneously on output links, i.e., red packets are only transmitted when there is a blue packet in the second queue, and similarly, the blue packets are served when there is a red packet in the first queue.

Also note that dividing both sides of (32) by t and taking the limit as $t \to \infty$ shows that the maximum throughput should be $\min\{\lambda_R, \lambda_B\}$. Therefore, the optimal strategy must drop the Red packets at an average rate $\lambda_R - \lambda_B$, in a way that minimizes the mean queue length, while retaining equality (32).

Next, consider the problem of minimizing the mean queue length. This problem can be posed as an infinite-state Markov decision problem with unbounded cost. It follows from checking standard conditions, e.g., [23], [24], that a stationary optimal policy exists for our problem, however, the average-cost optimality equation (12) may not hold. Therefore, we follow a different approach.

Recall that when a red packet and a blue packet are both available, to minimize queue length, it is best to transmit them immediately. Therefore, when one of the queues (blue or red) hits zero, from that point onwards, only one of the queues can be non-empty. Thus in steady-state, we can assume that one queue can be non-empty. As a result, we have the Markov decision process described next. Let (i,j) represent the state of the system where there are i packets in the red queue and j packets in the blue queue. The transition probabilities are given by

$$
\begin{aligned}
P[(0,y)|(0,y)] &= \lambda_R\lambda_B + (1-\lambda_R)(1-\lambda_B) \\
P[(0,y-1)|(0,y)] &= \lambda_R(1-\lambda_B) \\
P[(0,y+1)|(0,y)] &= \lambda_B(1-\lambda_R),
\end{aligned}
$$

and

$$
\begin{aligned}
P[(x,0)|(x,0)] &= \lambda_R\lambda_B + (1-\lambda_R)(1-\lambda_B) \\
&\quad + \lambda_R(1-\lambda_B)\delta_x \\
P[(x-1,0)|(x,0)] &= \lambda_B(1-\lambda_R) \\
P[(x+1,0)|(x,0)] &= \lambda_R(1-\lambda_B)(1-\delta_x),
\end{aligned}
$$

Fig. 6. The optimal threshold to minimize the average queue length.

where δ_x denotes probability of dropping the red packet in state $(x, 0)$, if there is a red arrival but no blue arrival. Note that stability of the system (finiteness of mean queue length) implies that the red packets must be dropped at an average rate of $\lambda_R - \lambda_B$. So our problem is to determine δ_x for each x to minimize the mean queue length. We will show that the optimal policy is a threshold policy, which is defined below.

Definition 2. *A threshold policy, with threshold m, is a policy that has the following properties: $\delta_x = 0$ for all $0 \leq x \leq m-1$, and $\delta_m = 1$, where m is a nonnegative integer number.*

The following proposition presents the main result regarding the optimal strategy.

Proposition 3. *For the double input-double output Mix, the threshold policy is optimal, in the sense that it minimizes the average queue size among all maximum throughput policies with perfect anonymity. Moreover, the threshold is given by*

$$m^* = \begin{cases} \lceil -\frac{1}{\log \rho} \rceil - 1 & ; \frac{1}{2} < \rho < 1 \\ 0 & ; 0 \leq \rho \leq \frac{1}{2}, \end{cases} \quad (33)$$

where $\rho = \frac{\lambda_B(1 - \lambda_R)}{\lambda_R(1 - \lambda_B)}$.

In other words, no buffer is needed for $\lambda_R \geq \frac{2\lambda_B}{1 + \lambda_B}$, but, as rates get closer, for $\lambda_B < \lambda_R < \frac{2\lambda_B}{1 + \lambda_B}$, a buffer of size m^* for the red flow is needed. The optimal threshold m^* is depicted in Figure 6. Note that the singular case of $\lambda_R = \lambda_B = \lambda$ ($\rho = 1$) is not stable. By allowing a small drop rate of $\epsilon\lambda$ for each flow, where $0 < \epsilon \ll 1$, one buffer for each flow can be considered, and the thresholds and the average queue size can be expressed as functions of ϵ.

Proof of Proposition 3: The steady state distribution for the Markov chain representing the double input-double output Mix is given by

$$\pi_{0,y} = \pi_{0,0}\rho^y, \ y = 1, 2, \cdots$$

$$\pi_{x,0} = \pi_{0,0}\rho^{-x}\prod_{i=0}^{x-1}(1 - \delta_i), \ x = 1, 2, \cdots$$

where

$$\pi_{0,0} = \left(\frac{1}{1-\rho} + \sum_{x=1}^{\infty}\rho^{-x}\prod_{i=0}^{x-1}(1 - \delta_i) \right)^{-1},$$

and

$$\rho = \frac{\lambda_B(1 - \lambda_R)}{\lambda_R(1 - \lambda_B)}.$$

Recall that, by assumption, $\lambda_R > \lambda_B$, and therefore $0 \leq \rho < 1$. The average queue length is

$$\begin{aligned} \bar{L} &= \sum_{y=0}^{\infty} y\pi_{0,y} + \sum_{x=1}^{\infty} x\pi_{x,0} \\ &= \pi_{0,0}\left[\frac{\rho}{(1-\rho)^2} + \sum_{x=1}^{\infty} x\rho^{-x}\prod_{i=0}^{x-1}(1 - \delta_i) \right]. \end{aligned}$$

Note that for any nonnegative integer j, and for fixed values of δ_is, $i \neq j$, $\bar{L}$ is a linear fractional function of δ_j. More formally,

$$\bar{L}(\delta_j) = \frac{A_j + (1 - \delta_j)B_j}{A'_j + (1 - \delta_j)B'_j},$$

where

$$A'_j = \frac{1}{1-\rho} + \sum_{x=1}^{j}\rho^{-x}\prod_{i=0}^{x-1}(1 - \delta_i),$$

$$A_j = \frac{\rho}{(1-\rho)^2} + \sum_{x=1}^{j}x\rho^{-x}\prod_{i=0}^{x-1}(1 - \delta_i),$$

$$B'_j = \frac{\prod_{i=0}^{j-1}(1 - \delta_i)}{\rho^{j+1}}\left[1 + \sum_{x=1}^{\infty}\rho^{-x}\prod_{i=j+1}^{x+j}(1 - \delta_i) \right],$$

and

$$B_j = \frac{\prod_{i=0}^{j-1}(1 - \delta_i)}{\rho^{j+1}}\left[j+1 + \sum_{x=1}^{\infty}(j+x+1)\rho^{-x}\prod_{i=j+1}^{x+j}(1 - \delta_i) \right].$$

Therefore, $\partial\bar{L}/\partial\delta_j$ is either positive or negative, independent of δ_j, and consequently, the optimal δ_j to minimize $\bar{L}$ is either 0 or 1, i.e., $\delta_j^* \in \{0, 1\}$ for all j. But, all of the δ_js cannot be zero, otherwise the system will not be stable ($\bar{L} = \infty$). Define m to be the smallest j such that $\delta_j^* = 1$. Then $\delta_x = 0$ for all $0 \leq x \leq m-1$, and $\delta_m = 1$ which yields a threshold policy with threshold m. Therefore the threshold policy is the optimal policy.

Next, we find the optimal threshold m^*. The stationary distribution of a threshold policy with threshold m is given by

$$\begin{aligned} \pi_{0,y} &= \pi_{0,0}\rho^y, \ y = 1, 2, \cdots \\ \pi_{x,0} &= \pi_{0,0}(1/\rho)^x, \ x = 1, 2, \cdots, m \end{aligned}$$

where $\pi_{0,0} = (1 - \rho)\rho^m$. Therefore, $\pi_{m,0} = 1 - \rho$, and the average packet-drop rate, P_{drop}, is given by

$$P_{drop} = \pi_{m,0}\lambda_R(1 - \lambda_B) = \lambda_R - \lambda_B$$

which is independent of the threshold m. The average queue length is given by

$$\bar{L}(m) = \sum_{y=1}^{\infty} y\pi_{0,y} + \sum_{x=0}^{m} x\pi_{x,0}$$
$$= \left(2\rho^{m+1} + m(1-\rho) - \rho\right)/(1-\rho). \quad (34)$$

Note that $\bar{L}(m)$, as a continuous function of m, is strictly convex over $m \in [0,\infty)$ for any fixed $0 \le \rho < 1$; therefore, it has a unique minimizer m^* which is either zero or the solution of $\frac{\partial \bar{L}}{\partial m} = 0$. Since we seek the smallest integer-valued m^*, the convexity implies that m^* is zero if

$$\bar{L}(0) \le \bar{L}(1),$$

or it's a positive integer m^* satisfying

$$\bar{L}(m^*) < \bar{L}(m^* - 1),$$

and

$$\bar{L}(m^*) \le \bar{L}(m^* + 1).$$

Then by using (34), it follows that $m^* = 0$ if $\rho \le \frac{1}{2}$, and for $\rho > \frac{1}{2}$, it satisfies

$$2\rho^{m^*} > 1,$$

and

$$2\rho^{m^*+1} \le 1,$$

which yields

$$m^* = \lceil -\frac{1}{\log \rho} \rceil - 1.$$

This concludes the proof. ■

Remark 3. *As far as the average queue size is concerned, it does not matter which packet is dropped when $\delta_x = 1$. However, in order to get a better delay performance for those packets that are not dropped, it is better to accept the new arrival and drop the head-of-the line packet.*

IV. CONCLUSIONS

The definition of anonymity and the optimal mixing strategy for a router in an anonymous network depend on its functionality. In the case of a double input-single output Mix, an eavesdropper knows the next hop of every packet but the router attempts to hide the identity of the packet at the output link so as to make it harder for the eavesdropper to follow the path of a flow further downstream. On the other hand, when there are two inputs, two outputs and only two flows, even revealing the identity of one packet at the output compromises that portion of both flow's route. For the first case, the optimal mixing strategy was found to achieve the maximum anonymity under a per-packet latency constraint. For the second case, the maximum throughput strategies with perfect anonymity were found for a per-packet latency constraint and for minimum average queue size. Our results in this paper represent a first attempt at theoretically characterizing optimal mixing strategies in two fundamental cases. Further research is needed to find optimal mixing strategies under more general constraints or for the multiple input-multiple output Mix.

APPENDIX A

Proof of Lemma 3: Taking the derivative of g respect to ξ yields

$$g'(\xi) = (p^* - d^*) + (p^{*\prime} - d^{*\prime})\xi + d^{*\prime}\frac{d}{dd^*}\mathcal{H}(d^*)$$
$$-p^{*\prime}\frac{d}{dp^*}\mathcal{H}(p^*) - d^{*\prime},$$

but

$$\frac{d}{dd^*}\mathcal{H}(d^*) = \log\frac{1-d^*}{d^*} = 1 + \xi$$

and

$$\frac{d}{dp^*}\mathcal{H}(p^*) = \log\frac{1-p^*}{p^*} = \xi,$$

therefore

$$g'(\xi) = (p^* - d^*)$$

which is always nonnegative for all values of ξ. Similarly for $f(\xi)$, we have

$$f'(\xi) = (r^* + p^*) + (p^{*\prime} + r^{*\prime})\xi + r^{*\prime}\frac{d}{dr^*}\mathcal{H}(r^*)$$
$$- p^{*\prime}\frac{d}{dp^*}\mathcal{H}(p^*) - r^{*\prime} - 1,$$

but

$$\frac{d}{dr^*}\mathcal{H}(r^*) = \log\frac{1-r^*}{r^*} = 1 - \xi,$$

and, as we saw,

$$\frac{d}{dp^*}\mathcal{H}(p^*) = \xi,$$

therefore

$$f'(\xi) = r^* + p^* - 1$$
$$= \frac{1}{1+2^{1-\xi}} + \frac{1}{1+2^{\xi}} - 1$$
$$= \frac{2^{\xi}}{2^{\xi}+2} + \frac{1}{1+2^{\xi}} - 1$$
$$\le \frac{2^{\xi}}{1+2^{\xi}} + \frac{1}{1+2^{\xi}} - 1$$
$$= 0. \quad (35)$$

Hence, $f(\xi)$ is a decreasing function. ■

REFERENCES

[1] http://www.onion-router.net
[2] http://www.torproject.org
[3] D. Chaum, Untraceable electronic mail, return addresses and digital pseudonyms, *Communications of the ACM*, vol. 24, no. 2, pp. 84-88, February 1981.
[4] D. Kesdogan, J. Egner, and R. Buschkes, Stop-and-go MIXes providing probabilistic security in an open system, *Second International Workshop on Information Hiding*, Lecture Notes in Computer Science, Springer-Verlag, pp. 83-98, April 1998.
[5] A. Pfitzmann, B. Pfitzmann, and M. Waidner, ISDN-MIXes: Untraceable communication with very small bandwidth overhead, *Proceedings of the GI/ITG Conference: Communication in Distributed Systems, Informatik-Fachberichte*, vol. 267, (Mannheim, Germany), pp. 451-463, February 1991.
[6] C. Gulcu and G. Tsudik, Mixing e-mail with babel, *Proceedings of the Symposium on Network and Distributed System Security*, pp. 2-19, February 1996.
[7] M. K. Reiter and A. D. Rubin, Crowds: anonymity for web transactions, *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66-92, 1998.

[8] O. Berthold, H. Federrath, and S. Kopsell, Web MIXes: A system for anonymous and unobservable Internet access, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pp. 115-129. Springer-Verlag, LNCS 2009, July 2000.

[9] M. Rennhard and B. Plattner, Introducing morphmix: Peer-to-peer based anonymous internet usage with collusion detection, *Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002)*, November 2002.

[10] U. Moller, L. Cottrell, P. Palfrader, and L. Sassaman, Mixmaster Protocol, Version 2. Draft, July 2003.

[11] G. Danezis, R. Dingledine, and N. Mathewson, Mixminion: Design of a type III anonymous remailer protocol, *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2003.

[12] A. Beimel and S. Dolev, Buses for anonymous message delivery, *Journal of Cryptology*, vol. 16, no. 1, pp. 25- 39, 2003.

[13] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, 1949.

[14] C. Diaz, S. Seys, J. Claessens, and B. Preneel, Towards measuring anonymity, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, Springer-Verlag, April 2002.

[15] A. Serjantov and G. Danezis, Towards an information theoretic metric for anonymity, *Privacy Enhancing Technologies*, 2002.

[16] C. Diaz and A. Serjantov, Generalising Mixes, *Proceedings of Privacy Enhancing Technologies (PET 2003)*, 2003.

[17] C. Diaz and B. Preneel, Reasoning about the anonymity provided by pool Mixes that generate dummy traffic, *Proceedings of Information Hiding (IH'04)*, 2004.

[18] P. Venkitasubramaniam and V. Anantharam, On the anonymity of Chaum mixes, *2008 IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008.

[19] P. Venkitasubramaniam, T. He and L. Tong, Anonymous networking amidst eavesdroppers, *IEEE Transactions on Information Theory: Special Issue on Information-Theoretic Security*, Vol. 54, No 6, pp. 2770-2784, June 2008.

[20] T. Cover and J. Thomas, Elements of Information Theory, *New York: Wiley*, 1991.

[21] D. P. Bertsekas, Dynamic Programming and Optimal Control (1), *Athena Scientific*, 1995.

[22] V. Vasilevich, Elements of combinatorial and differential topology, *Graduate Studies in Mathematics*, V. 74, 2006.

[23] S. A. Lippman, Semi-Markov decision processes with unbounded rewards, *Management Science*, vol. 19, No. 7, pp. 717-731, March 1973.

[24] L. Sennott, Average cost optimal stationary policies in infitie state Markov decision processes with unbounded costs, *Operations Research*, Vol. 37, No. 4, pp. 626-633, August 1989.

[25] P. R. Kumar and P. Varaiya, Stochastic systems: estimation, identification and adaptive control, *Prentice-Hall*, 1986.