Toward an Analytical Approach to Anonymous Wireless Networking

Parvathinathan Venkitasubramaniam, Ting He, Lang Tong, and Stephen B. Wicker

Abstract

Transmissions in a wireless network are susceptible to unauthorized traffic analysis by eavesdroppers. Although cryptography can protect the contents of communication, the transmission times of packets alone can provide significant networking information. This article focuses on analytical approaches to anonymous networking for the prevention of timing based traffic analysis. In particular, we propose an analytical measure for anonymity, and develop provably anonymous countermeasures for wireless ad hoc and sensor networks, where traffic is subjected to tight constraints on medium access and latency. A key objective is to bridge a long standing gap between the information theoretic approach to secrecy in communication and a more pragmatic approach of Chaum Mixing used for anonymity in Internet applications. The efficacy of the proposed approach is demonstrated using an orthogonal transmitter directed signaling network.

Keywords— Traffic analysis, Anonymity, Mixing, Equivocation, Rate-Distortion.

I. Introduction

As wireless networks increasingly dominate our means of communication, the need for security and privacy has gained significant prominence. Owing to the unprotected communication medium, wireless networks are vulnerable to unauthorized retrieval of networking information. For example, by merely observing packet transmission times of different nodes, a passive eavesdropper can decipher source-destination pairs and paths of traffic flow in a network. Retrieval of such information, known as *traffic*

The authors are with the Department of Electrical and Computer Engineering, Cornell University, Ithaca NY 14853 (e-mail: {pv45,th255,lt35,sbw11}@cornell.edu).

This work is supported in part by the National Science Foundation under award CCF-0635070, the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program DAAD19-01-2-0011, and TRUST (The Team for Research in Ubiquitous Secure Technology) sponsored by the National Science Foundation under award CCF-0424422.

analysis, is a violation of user privacy. Further, it also provides crucial information for the jamming of network traffic and launching of a denial-of-service attack.

In emerging wireless technologies such as ad hoc and sensor networks, traffic analysis can be particularly damaging. For example in sensor networks, even without knowledge of source destination pairs, the direction of data flow alone can provide critical information such as event location, access points, etc. Further, since nodes are deployed in the open with limited or no physical protection, the network is susceptible to active means of traffic analysis such as node capturing or packet insertion.

The design of protective measures against traffic analysis depends on the nature of information available to the adversary. Apart from the node transmission schedules obtained through eavesdropping, an adversary may also have access to the public network protocols and signaling strategies used by the network. While the contents of communication can be secured using cryptography, hiding the act of communication requires a fundamental redesign of networking protocols. The challenge in designing protocols that are resilient to traffic analysis is to hide the routing information without violating networking constraints. In this regard, the wireless medium presents its own advantages and disadvantages. On the one hand, wireless transmissions make it difficult for an eavesdropper to ascertain the sender-receiver pair of an encrypted transmission, especially when different streams are multiplexed at a single node. On the other hand, the shared wireless medium is band-limited and susceptible to fading and interference, thereby constraining the network designer.

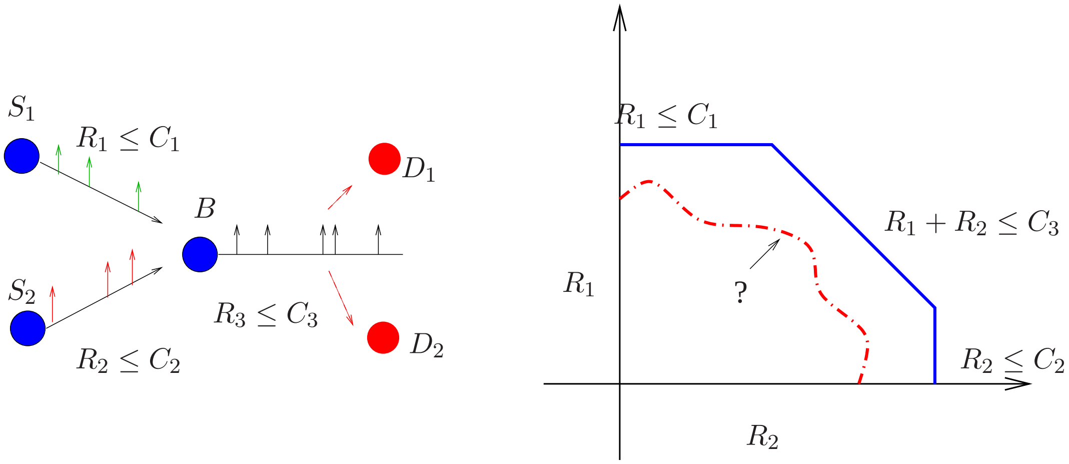


Fig. 1. Achievable Rate Region for Two Hop Relay: Outer Region: The transmission rates of the nodes S_1, S_2 are bounded by C_1, C_2 respectively. The sum rate of relayed packets from S_1, S_2 are bounded by C_3 to maintain stability at the relay. Inner Region: Unknown relay rate region when transmission schedules are independent

As a motivating example, consider a multiaccess relay as shown in Figure 1, where node B forwards packets received from nodes S_1 and S_2 (to D_1 and D_2 respectively) subject to a strict delay constraint for every packet. Assuming all nodes transmit on orthogonal channels, if the transmission rate of each node is bounded, then the rates of packets that can be relayed successfully fall into a pentagonal region as shown in Figure 1. Rates in this region are achieved if the relay forwards every received packet after a small processing delay. It is easy to see that such a strategy would result in the transmission schedules of the source nodes and the relay to be highly correlated; an eavesdropper would be able to use the correlation to detect the relaying operation of B. In addition to the medium access requirements, if the schedules of all nodes are forced to be statistically independent, an eavesdropper would not detect any correlation across schedules, thus effectively hiding the relay operation. When the schedules are statistically independent, however, the strict delay constraint would result in dropped packets, and therefore, lower rates of relayed packets.

The multiaccess relay of Figure 1 represents a basic component in wireless networking, and hiding the relay operation is a key step towards designing anonymous network protocols. The example highlights that providing *anonymity* in networking would result in a reduced network performance. This raises some interesting and important questions. Can we define a provable, and if possible, quantifiable notion of anonymity in wireless networks? How do we design protocols that guarantee a specified level of anonymity? What are the trade-offs between achievable network performance and the guaranteed level of anonymity?

In this article, we present an analytical framework to addressing these questions. In particular, the presented approach aims to combine the analytical strength of information theoretic secrecy and the proven applicability of anonymous protocols for the Internet, to develop rigorous analytical foundations for anonymous wireless networking.

The rest of this article is organized as follows. In Section II, the idea of Chaum Mixing and its applicability in wireless networks are described. The analytical model for measuring anonymity is presented in Section III. The idea of covert relaying to guarantee anonymity is described in Section IV. In Section V, the duality of this problem with information theoretic rate-distortion, and the resulting trade-off between network performance and anonymity are presented. Conclusions and relevant discussions are provided in Section VI.

II. Anonymity in Internet Protocols: Mixing

Anonymous protocols for Internet applications such as email or browsing use the well known concept of Mixing [1], pioneered by Chaum. A Mix is a special router or a proxy server, that collects packets from multiple users, and transmits them after re-encryption and length padding. This ensures that by comparing contents or packet lengths, it is impossible to match an incoming and outgoing packet at a Mix. Further, packets received from multiple sources are transmitted in batches, so that an eavesdropper is unable to identify the source of a packet using the arrival and departure times. Since a single Mix stands a chance of being compromised, a (possibly random) sequence of Mixes are interposed between source and destination terminals to protect against active means of gaining information. The key idea is to perform encryption for multiple Mix servers in layers such that, each Mix can only reveal the address of the subsequent Mix in the path, and an eavesdropper can not determine the source-destination pairing unless all the Mixes are compromised.

Since the original solution proposed by Chaum, there have been several improvements to the batching strategies of Mixes to handle different types of traffic analysis attacks [2]. While the Mix based solutions are useful for Internet applications such as anonymous remailers and web browsing, a study of flow correlation attacks [3] showed that when long streams of packets with buffer or latency constraints are forwarded through Mixes, it is possible to correlate incoming and outgoing streams almost perfectly. Constraints on delay and buffer size are critical in network applications, such as media transmission, or in sensor networks, where each sensor node cannot store packets indefinitely. The authors in [3] proposed that allowing Mixes to transmit dummy messages may overcome these weaknesses. However, dummy transmissions have not been optimally designed to maximize performance in terms of throughput or latency, which is crucial in bandwidth constrained wireless networks. Our intent is to use ideas such as Mixing and dummy transmissions to develop strategies for a wireless network setting; the challenge lies in maximizing network performance under the constraints on bandwidth, latency and anonymity.

III. An Information Theoretic Measure of Anonymity

The first step towards an analytical model for this problem is to define a quantifiable measure of anonymity. In the context of Mix networks, anonymity has been measured using the *anonymity set* of an observed packet, which contains all possible source-destination pairs for that packet. A similar notion of *sender anonymity* was provided by the General Packet Radio Service (GPRS) standard until very recently. The service allowed a mobile user to exchange data packets with a predefined host that can be addressed by the supported interworking protocols. Since all user packets go through a GPRS Gateway

Source Node (GGSN), the sender's identity remains anonymous. The anonymity here is measured by the size of the sender anonymity set (set of all possible senders). Although the anonymity set serves as a good model in Internet applications, for networks such as wireless adhoc or sensor networks, it is equally important to protect the routes of data flow as it is to hide the source destination information. Further, it is imperative that streams of packets are considered, and anonymity provided, not only for individual packets, but for the information flows.

Our analytical model for anonymity derives its motivation from the information theoretic approach to secrecy. Parallel to cryptography, secrecy in communication has been studied extensively from an information theoretic perspective using the idea of equivocation. Equivocation, proposed by Shannon [4], measures the uncertainty of a transmitted message with respect to an eavesdropper's observation. It has been used to measure secrecy in point-to-point communication models such as wiretapped channel [5] and broadcast channel [6]; the goal was to maximize the reliable rate of communication to an intended receiver, while guaranteeing a level of secrecy (equivocation) with respect to the eavesdropper. For these channels, the authors characterized the inverse relationship between communication rate and equivocation.

While previous applications of equivocation have been restricted to secrecy of transmitted messages, we use it to quantify the anonymity of the *routes* in a network. Consider a network, where V represents the set of nodes. During any network operation, let some subset of nodes in V communicate using a fixed set of routes. This set of routes S, which we refer to as a *network session*, is an ordered subset of $2^{\mathcal{V}}$, and represents the information that we wish to hide from the eavesdropper.

During any network session, each node transmits packets at arbitrary times, which can be represented as a point process, say $\mathcal{Y}_A$ for node A. In a wireless network, if packet headers are encrypted, detection of a transmitted packet may not directly reveal the identity of the transmitting or receiving node. However, if the eavesdroppers are positioned such that the received power level can be used to estimate the location of the transmitter, or alternatively, if the underlying physical layer utilizes an orthogonal transmitter directed signaling model, the eavesdropper would obtain the point processes individually for each transmitting node. Since it is not possible to identify the locations of eavesdroppers, we assume every node is monitored; the set of point processes $\mathcal{Y} = \{\mathcal{Y}_A : A \in \mathcal{V}\}$ represents the eavesdroppers complete observation.

In accordance with the definition of equivocation, the anonymity of a network session can be defined using the conditional uncertainty of the session with respect to eavesdroppers' observation. We model the network session as an iid random variable $S \sim p(S)$, and use the normalized equivocation,

$$\alpha_s = \frac{H(S|\mathcal{Y})}{H(S)},$$

to measure anonymity. The normalization is required because the eavesdropper is assumed to have knowledge of the prior distribution $p(S)$. The maximum value of $\alpha_s = 1$, in which case the schedules have *perfect anonymity*; the observed $\mathcal{Y}$ provides the eavesdropper no additional information about the session S. When $\alpha_s < 1$, the physical interpretation of anonymity comes from Fano's Inequality [7]; the *error probability* of the eavesdropper in decoding the session correctly is lower bounded by equivocation.

The fundamental design problem is, given a session S, what is the optimal scheduling strategy $\mathcal{Y}$, such that anonymity $\alpha_s \geq \alpha$ is guaranteed. An optimal scheduling strategy is defined as the distribution $q(\mathcal{Y}|S)$ that maximizes the performance metric in consideration, such as network throughput, latency or energy efficiency.

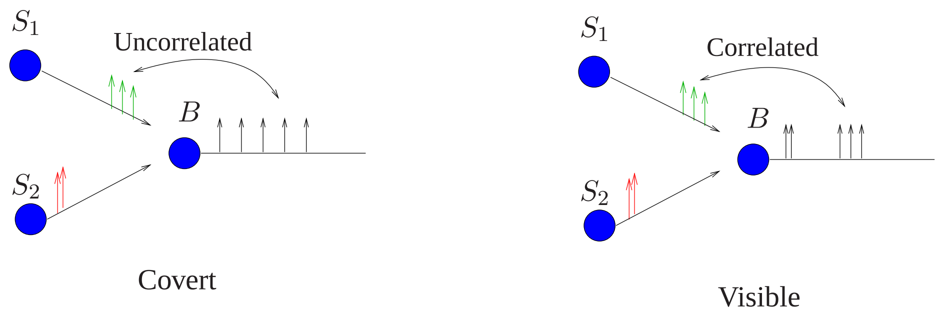
Note that this analytical model assumes that eavesdroppers do not use active means of gaining inference such as compromising nodes. In the event of active compromising of nodes, the model can be modified to account for the additional *side information* available to the adversary; side information would correspond to the unknown set of compromised nodes.

IV. Providing Anonymity

The Mix network approach to providing anonymity, as discussed in Section II, does not provide the required solution under the constraints of wireless networks. An alternative is the idea of traffic cover, where, irrespective of the active routes, the transmission schedules of all nodes are fixed and periodic. If a node does not have packets to transmit, it transmits dummy packets at those times. The fixed scheduling, analyzed in [8], provides complete anonymity to the routes at all times. However, it does not consider the constraints on traffic latency or stability. Furthermore, the fixed scheduling strategy requires synchronization across all nodes and a constant network topology, which is not practical in energy constrained wireless networks.

The approach we propose shares some traits with the ideas of Mixing and traffic cover, but considers strict network constraints on medium access and delay, and is adaptive to the network session. Specifically, depending on the routes in each session, we divide the set of relays into two categories (see Figure 2), *covert* and *visible*, which are described as follows.

Covert Relays: A relay B (as shown in Figure 2) is *covert*, if its outgoing transmission schedule is statistically independent of the transmission schedules of all nodes occurring previously in the paths



Covert

Visible

Fig. 2. Visible and Covert Relaying

that contain B. When a relay is covert, it would be impossible for an eavesdropper to correlate the transmission schedule of any preceding node in a path and that of the relay B. In effect, the relaying operation of B is hidden. However, owing to constraints on delay and bandwidth, the independence in transmission schedules would result in dropped packets or require dummy packet transmissions.

Visible Relays: A *visible* relay B generates its schedule depending on the arrival times of packets at B. For every received packet, the relay forwards the packet after a processing delay. It is evident that the schedules of streams transmitted by a preceding node in the path and the relay would be highly correlated, and the eavesdropper can detect the relaying operation.

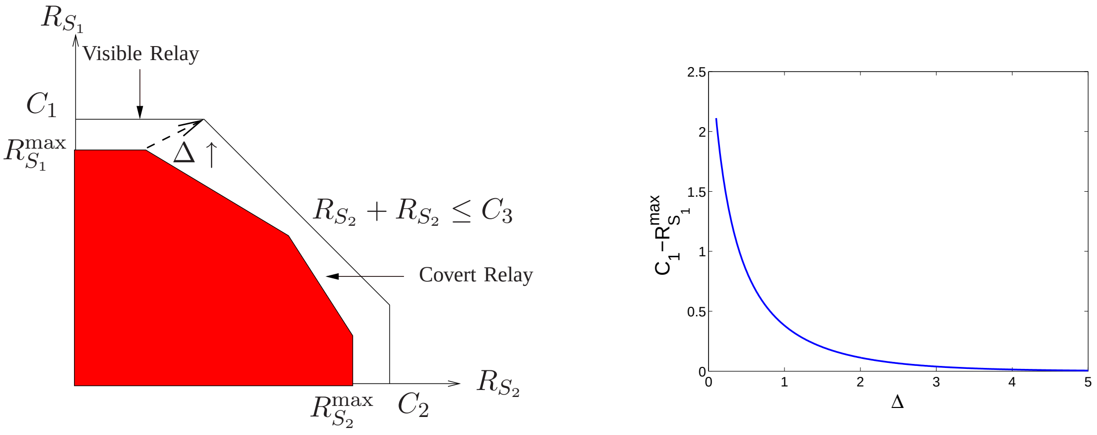
A covert relay that forwards packets from multiple sources plays the role of a Mix, by completely decorrelating the incoming and outgoing schedules. In addition, due to the wireless medium and encrypted headers, the independence in schedules would ensure that an eavesdropper is unable to decipher which routes contain the covert relay, even using long streams of packets. However, due to dummy transmissions and possible packet drops by the covert relay, the achievable relay rates would be lower than the visible relay.

This approach entails two fundamental design issues: optimal scheduling and relaying strategies for a covert relay, and optimal choice of covert relays. The choice of covert relays is dependent on the routes of a session and the required level of anonymity, which will be explained in Section V. In the remainder of this section, we discuss covert relaying in more detail.

A. Covert Relaying

One approach to generate independent schedules at a covert relay would be to derive a queuing discipline that forwards packets within the required delay constraints, and yet results in a statistically independent outgoing schedule. Such a strategy would, however, be vulnerable to active inference techniques such as packet insertion or flooding attacks [2]. We propose an alternative strategy, where a random transmission schedule is generated apriori by the relay, and a subset of arrived packets are chosen to be forwarded, so that the delay constraints are satisfied with minimum packet drops.

In [9], we had designed covert relays with strict delay constraints, where each received packet needs to be relayed within Δ time units, or otherwise dropped. For an orthogonal transmitter directed signaling at the physical layer with Poisson transmission schedules, we developed relaying strategies and characterized the set of achievable rates for an $m \times 1$ multiaccess relay. The rate region for a 2×1 relay (example in Section I) is illustrated in Figure 3.a). It is evident that independent Poisson schedules result in a non-zero packet drop rate for a strict delay constraint, as illustrated in the figure ($R_{S_1}^{\max} < C_{S_1}$). However, the rate region converges to that of a visible relay as $\Delta \to \infty$. This can be seen from Figure 3.b), which plots the difference in the maximum relay rate for S_1 when B is covert and visible, as a function of Δ.



(a)

(b)

Fig. 3. a) 2×1 Relay rate region. b) Difference between maximum relay rate for S_1 for a covert and visible relay, when $C_{S_1} = C_{S_2} = 3, C_B = 4$.

A key element in the optimal relaying strategies is the Bounded Greedy Match (BGM) algorithm, proposed in [10], in the context of chaff insertion for stepping stone attacks. For any pair of point processes, the BGM algorithm guarantees that packets are relayed within strict delay constraints with least possible packet drops. Combining this idea with prioritizing multiple source nodes, time-sharing and forward error correction, the region in Figure 3 was characterized in [9].

Poisson point processes are a particular scheduling distribution and are generally suboptimal. An interesting open problem is to characterize the optimal distribution of transmission schedules that maximizes the achievable rates for a covert relay. The optimal distribution would vary depending on the medium access channel and the nature of delay constraints for the traffic. As mentioned earlier, for a transmitter directed signaling system with an average delay constraint, Poisson schedules can be optimal. Similarly, for a strict delay constraint, if the minimum allowed interpacket delay is much smaller compared to the delay bound, it can be shown that for high transmission rates, a periodic schedule [8] is optimal.

Independent scheduling for covert relays is a specific technique for providing anonymity to routes in a network. The broad idea of hiding the relaying operation of nodes is quite general, and also an attractive solution owing to its distributed nature. Each node decorrelates its incoming and outgoing schedules independent of the other nodes in the path. Further, the relaying strategies we proposed to maximize relay rates do not require the relay node to have apriori knowledge of the source nodes schedules; the decision to forward or drop a packet is made only after the packet has arrived at a relay [9]. The discussion in this article is centered around orthogonal channels for packet transmissions with strict delay constraints. For a general physical layer model the multiple access relay can be viewed as a network of queues, where each source node maintains an independent queue and incoming packets constitute the arrival processes. Combining ideas from classical multiaccess communication and techniques such as Mixing and independent scheduling, we believe that relaying strategies can be designed for a general multiaccess relay model.

V. Throughput-Anonymity Tradeoff

As is evident from the discussion and the presented results in Section IV, every covert relay incurs a loss in performance, either in terms of rates of relayed packets or the induced delay in transmissions. Therefore, it is not possible to make all relays covert, especially in a large network. The challenge is, therefore, to optimize the choice of relays depending on the required level of anonymity, such that network performance is maximized. A key insight into this optimization comes from a duality with information theoretic rate distortion.

The duality between anonymous networking and rate-distortion is not tied to the idea of covert relaying, and can be explained using a general intuition. The objective of the rate-distortion problem is to generate a fixed number of codewords for a set of source sequences, such that the corresponding reconstruction sequences have minimum distortion with respect to the original sequences. The idea is to divide the set of source sequences into partitions such that for each partition there exists a reconstruction sequence which is minimally distorted from each sequence in that partition. The compression rate determines the total number of allowed partitions. In the anonymous networking setup, the key idea is to divide the set of all possible network sessions into partitions such that, for each partition, there exists a scheduling strategy that would make the sessions within that partition indistinguishable to an eavesdropper. The level of anonymity required determines the number of partitions and the optimal scheduling strategy plays the role of the reconstruction sequence by minimizing the performance loss across sessions within a partition.

In [11], we had considered the special case of orthogonal transmitter directed signaling for strict delay constrained traffic, and characterized the relationship between throughput and anonymity by proving this duality. Specifically, in any session S, the set of covert relays $B \subset \mathcal{V}$ was chosen randomly using a conditional distribution $q(B|S)$. Since the adversary is unable to correlate schedules at the covert relays, he observes a set of broken paths, denoted by $\hat{S}$ (which is a function of (S, B)). The covert relays cause a reduction in throughput denoted by $d(S, \hat{S})$, which is evaluated by adding the packet loss at each covert relay in the set B, which are in turn obtained using the analysis of covert relays (Section IV-A). For this model, we optimized the conditional distribution $q(B|S)$ and showed that the throughput and anonymity are related directly through the distortion-rate function [7].

Theorem 1: (Throughput-Anonymity Tradeoff) If $R(0)$ is the throughput achievable with zero anonymity, then throughput $R(\alpha)$ is achievable with anonymity α if

$$R(0) - R(\alpha) \geq D\left(H(S)(1-\alpha)\right),$$

where $D(R)$ is the *Distortion-Rate* function defined as

$$D(R) = \min_{q(\hat{\mathbf{S}}|\mathbf{S}):I(\mathbf{S};\hat{\mathbf{S}})\leq R} \mathbb{E}(d(\mathbf{S}, \hat{\mathbf{S}})). \tag{1}$$

In Theorem 1, the level of anonymity α directly corresponds to the rate of compression, and the performance loss function $d(S, \hat{S})$ plays the role of distortion. Therefore, obtaining the distortion-rate function is equivalent to obtaining the optimal throughput anonymity relation. The consequences of this duality, however, extend beyond the characterization of the optimal throughput. Rate distortion is a field that has been studied for many decades, and the numerous models and techniques developed therein, could serve to design strategies for anonymous networking. For example, applying the result of Theorem 1, the Blahut-Arimoto algorithm provides an efficient iterative technique to obtain the optimal conditional distribution of covert relays $q(B|S)$ and the throughput function $R(\alpha)$.

A. Example

Consider the example of a switching network, as shown in Figure 4.a). During any network session, each source S_i picks a distinct destination D_i, and for each pair S_i, D_i there is a fixed path through the intermediate relays. There are 24 possible sessions (source-destination pairings) which are assumed equiprobable.

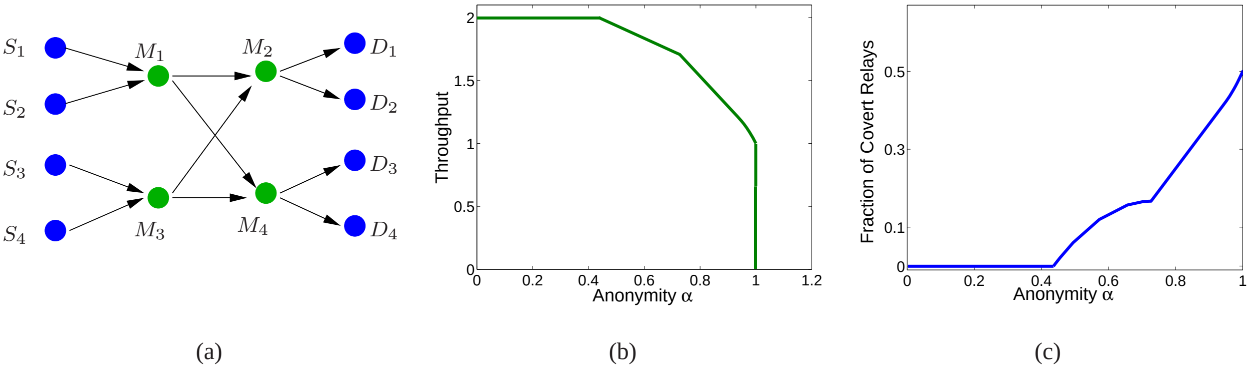


Fig. 4. a)Switching Network: Sources $\{S_i\}$ transmit packets to destinations $\{D_i\}$ through relays $\{M_i\}$ b) Throughput vs Anonymity. c) Fraction of covert relays vs Anonymity.

For this setup, Figure 4 plots the throughput-anonymity region and the fraction of covert relays, when all nodes have identical transmission rate constraints. As can be seen from Figure 4.b), the throughput is a convex function of the anonymity level, which is a property of the rate-distortion function. Intuitively, it can be attributed to the average nature of the metrics, namely equivocation and throughput. Note that the maximum throughput is achievable with non-zero anonymity. This is a virtue of transmitter directed signaling; encrypted headers would ensure that final destination nodes are not inferable to the eavesdropper. Figure 4.c) shows the relation between average number of covert relays and the level of anonymity. As can be seen, it is not necessary to make all relays covert to obtain maximum anonymity (in this case, it is sufficient to make relays M_2, M_4 covert for $\alpha = 1$).

B. Discussion

The model for network sessions used in this article, assumes independent and static observations by eavesdroppers. This may not apply to the scenario where an eavesdropper monitors the network for long periods of time. In that case, one would need a stochastic model to account for session changes, depending on when nodes start or stop communication. In this regard, if we use a Markovian model for sessions, we believe that, as an extension of the duality, techniques in causal source coding [12] would apply to the schedule design.

In the results presented thus far, we had considered the special case of strict delay constrained traffic, and optimized the network throughput. Imposing a delay constraint at each relay is restrictive in a multihop network, and the ideal metric to constrain is the end-to-end delay. This throws up some interesting questions: For a fixed end-to-end delay constraint, how does one allocate delays at each (covert) relay in the route? If the throughput requirement was fixed, how does the optimal end-to-end delay vary with anonymity? The analytical approach presented in this article strongly suggest that these questions can be answered in a fundamental theoretical way.

From a practical standpoint, the translation of the theoretical results to implementable solutions also requires a decentralized relay selection strategy. One approach to address decentralization is to investigate message passing for distributed decision systems, where in every session, the nodes exchange minimum amount of information so that the decision to remain covert or visible can be made optimally. Alternatively, each relay could make an independent decision to be covert depending on the local information available without message exchanges. Since each relay would only possess partial information about the session, this would result in lower network performance [13].

VI. Conclusions

The main contribution in this article is the analytical approach to anonymous wireless networking. To the best of our knowledge, ours is the first analytical model designed to measure the secrecy of *routes* in an eavesdropped wireless network. The preliminary results obtained so far clearly demonstrate the potential for analytical methods to addressing the scheduling design. Further, our results also present clear connections to classical information theoretic problems such as wiretapped channel communication and rate-distortion, which are well studied in literature and provide applicable techniques.

This article primarily deals with fixed set of routes between source destination pairs. In many situations, using a fixed set of routes may not provide sufficient anonymity, especially when the adversary obtains side information by compromising nodes. In that case, the anonymity can be improved by randomizing the routes between source-destination pairs. The goal is to design a collection of routes for every session such that, revealing an unknown subset of links does not provide sufficient information about the session. This problem is analogous to coding for wiretap II channels [14], where channel codes are designed so that, revealing an unknown subset of bits does not provide sufficient information about the transmitted message.

References

[1] D. Chaum, “Untraceable electronic mail, return addresses and digital pseudonyms,” *Communications of the ACM*, vol. 24, pp. 84–88, February 1981.

[2] 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.

[3] Y. Zhu, X. Fu, B. Graham, R.Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in *Proceedings of Privacy Enhancing Technologies workshop*, May 26-28 2004.

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

[5] A. Wyner, "The wiretap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, 1975.

[6] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Information Theory*, vol. 24, pp. 339–348, May 1978.

[7] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[8] B.Radosavljevic and B. Hajek, "Hiding traffic flow in communication networks," in *Military Communications Conference*, 1992.

[9] P. Venkitasubramaniam, T. He, and L. Tong, "Relay Secrecy in Wireless Networks with Eavesdroppers," in *Proc. of 2006 Allerton Conference on Communication, Control and Computing*, (Monticello, IL), Sep. 2006.

[10] A. Blum, D. Song, and S. Venkataraman, "Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds," in *Conference of Recent Advance in Intrusion Detection (RAID)*, (Sophia Antipolis, French Riviera, France), September 2004.

[11] P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous Networking amidst Eavesdroppers," *Submitted to IEEE Transactions on Information Theory: Special Issue on Information-Thoeretic Security*, Feb. 2007.

[12] D. Neuhoff and L. Gilbert, "Causal Source Codes," *IEEE Trans. on Information Theory*, vol. 28, pp. 701–713, Sep. 1982.

[13] P. Venkitasubramaniam and L. Tong, "Throughput-Anonymity Trade-off in Wireless Networks with Latency Constraints," in *submitted to IEEE INFOCOM 2008*, July, 2008.

[14] L.H.Ozarow and A.D.Wyner, "Wiretap Channel II," *Bell Laboratories Technical Journal*, pp. 2135–2146, 1984.