Volume 3, Issue 6, June-2016, pp. 332-335 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Source Anonymity using multiple mixes in Packet Scheduling

[1]Mrs.S.Suganyadevi MCA., [2]Mrs.Dr.V.Anuratha MCA., M.Phil., Ph.D.,

[1]Pursuing M.Phil. (Computer Science) from Sree Saraswathi Thyagaraja College, Pollachi.

Email: suganyanadhan@gmail.com

[2]HOD - PG Computer Science, Sree Saraswathi Thyagaraja College, Pollachi.

Email: mailanuvinu@yahoo.co.in

Abstract:-Secret communication, where users converse without revealing the personalities of communicating parties or the trails of data stream is critical in data networks. On the Internet, Chaum mixes, intermediate nodes, or proxy servers, which use coated encryption and packet shuffling techniques to hide source identities, are used to provide anonymity to network users. In this analysis, an information theoretic structure is developed to study the maximum anonymity possible by packet shuffling when the merges are memory restricted—in other words, they can store a finite number of packets. Network of mixes over receiving packet sources from an eavesdropper's perspective as the measure of secrecy, the maximum achievable secrecy of a single mix with buffer size *b* (packets which contains the source and destination details of itself) serving for achieving multiple mixes (network of mixes). By obtaining network of mixes the source anonymity is achieved successfully. For a general multiuser system, the maximum anonymity as buffer size $b \to \infty$ is shown to approach the entropy of the source arrival probabilities at a convergence rate no less significant than $1/b^2$. When the arrival probabilities of the general multiuser system can be expressed as a rational portion $k/2^n$ for some fixed n, this union rate is shown to be achievable. The secrecy analysis is extended to a common network of mixes linking the sources to multi destination, where the source secrecy achievable on the target link is shown to be lower enclosed by a weighted sum of the secrecy achievable by each individual mix.

Keywords - Anonymity, mixing, buffer, entropy.

1. INTRODUCTION

Information hiding in networks extends beyond the protection of communicated data; hiding the identities of communicating parties is equally critical. Knowledge of source-destination pairs or routes of information flow, obtained through traffic analysis in a network, also provides crucial information for an adversary to jam a particular flow, deploy black holes or launch other sophisticated attacks. More generally, this work takes an important step in identifying the relationship of anonymity to fairness in the landscape of different metrics of evaluating scheduling strategies. We have used Poisson processes to model packet arrivals [1]. One of the

earliest uses of traffic analysis occurred in World War II [2], when the US Army established a Traffic Intelligence group (OP-G-20) on Corregidor Island [3]. More specifically transmission timing analysis has been a critical concern in the design and analysis network protocols [4], [5]. Presently, anonymous communication on the Internet can be facilitated through the use of Chaum mixes [6]. subsequent to Chaum's original design, many batching strategies have been designed to deal with resource and QoS constraints, such as Timed-dynamic Pool mixes [7], STOP-and-GO mixes [8], red-green-black mixes [9], the maximum achievable anonymity under memory constraints has not been studied rigorously and several fundamental questions remain to be answered.

1.1 RELATED WORK

Information-theoretic measures, based on Shannon's equivocation have been proposed previously to measure the anonymity provided by mixes. In [10], the authors proposed Shannon entropy of the anonymity set (set of plausible sources of an observed packet) to quantify anonymity, using which the performance of different mixing systems were compared numerically.

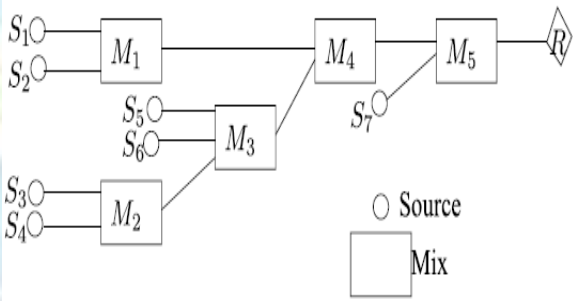
Recent signal processing approaches have demonstrated fundamental tradeoffs between privacy and delay in the timing side channel analysis as well.

2. PROBLEM SETUP

We consider the problem of hiding sources of packets transmitted to a particular destination node in a network. Such a system can be modeled as a single-destination network; a 3−tupleM= (G,B,Λ), where G is the graph.

That describes the network topology, B is the set of buffer sizes and Λ is the set of arrival rates. G = (V,E) is an in-tree directed graph, wherever the group of nodes V can be separated into a group of leaf nodes S = {S_1, . . . , S_s } denoting the sources, a set of transitional nodes M = {M_1, . . . , M_m} representing the mixes, and the root node R that represents the final destination. With no loss of simplification, we let Mm ∈ M be the only node in the graph connected to R.3 we partition the set of edges as E = E_s U E_m U E_r where

E_s = {(A, B) ∈ E : A ∈ S} (Source Edges),
E_m = {(A, B) ∈ E : A, B ∈ M} (Intermediate Edges),
E_r = {(Mm, R)} (Destination Edge).
Mix: For a mix Mi ∈M, let Emi ={(A, M_i) : (A, M_i) ∈ E} denote the set of incoming links to M_i. Mix M_i ∈ M observes only the set of incoming streams {Xe(t) : e ∈ Emi }.
All packets on any particular stream X_{A,M_i} (t) have identical headers due to layered encryption.
νM1 (AM2, νM2 (AM3, νM3 (· · · νMk (AR, νR(X)))) · · ·)).



A Mix Network: $E_s = \{(S_1, M_1), (S_2, M_1), (S_3, M_2), (S_4, M_2), (S_5, M_3), (S_6, M_3), (S_7, M_5)\}, E_m = \{(M_1, M_4), (M_2, M_3), (M_3, M_4), (M_4, M_5)\}. n_1 = 2,\ n_2 = 2, n_3 = 3, n_4 = 2, n_5 = 2, s = 7, s_1 = 2, s_2 = 2, s_3 = 4, s_4 = 6, s_5 = 7.$

The mix M_i may collect up to bi packets beyond which, any further arrival mandates an immediate departure; in other words no packets can be dropped. Since mixes cannot drop any packets or create new packets, the average packet transmission rates on the outgoing link of any mix are a deterministic function of the topology and Λ.

3. ANONYMITY OF A SINGLE MIX

In this section, we analyze the anonymity of a single Chaum mix serving two users; this system is represented by the 3−tuple M1 = (G1, b, (λ1, λ2)) where G1 is as shown in Figure 3. For this simple system, we will derive the optimal mixing strategy, and characterize the achievable anonymity as a function of the buffer size b. prior to describing the results; we will present two key reductions to the class of possible mixing strategies that simplifies the analysis without losing generality.
Consider a modified version of this strategy, say ψ , described as follows. If at time t, there was no arrival point on any incoming stream, and strategy ψ chooses to transmit a packet stored in its buffer, then strategy ψ also chooses (at time t)

the identical packet to transmit from its buffer, but does not transmit the packet immediately. When arrival rate of both users are equal is

$A(b) = 1 + \log_2(\cos(\pi/b+3))$

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

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

Theorem 1 represents the first closed form characterization of the maximum anonymity of a buffer limited Chaum mix, and provides the optimal strategy to achieve the maximum anonymity. When q = 0.5, the resulting series of nonlinear equations are hard to solve, and consequently a single letter characterization is as yet unknown. However, numerical analysis and algebraic reduction can be used in some special cases. For instance, when b = 1, and q = 1 n where n ∈ N, then anonymity A(1) = −q log2(1 − t)

where t is the unique solution of polynomial xn−1 + x −1 = 0 which lies in (0, 1).

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

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

We study the anonymity of a mix network and characterize a lower bound on the anonymity of a mix network as a weighted sum of anonymities of individual mixes.

4. POSSIBLE ANONYMITY IN A NETWORK OF MIXES

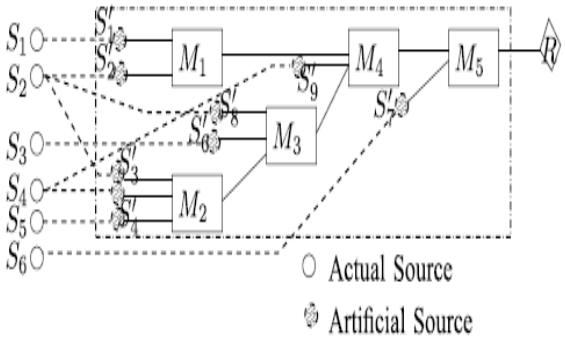
The layered encryption ensures that each mix in the system is only aware of the immediate preceding and immediate succeeding node of any packet that arrives to it.

In a general mix network M = (*G*, B,), let M_i= (G_i, b_i, i) denote a single mix sub-network containing only mix M_i with buffer size b_i and the number of sources equal to the number of incoming links to mix M_i in M, where each source in M_i transmits according to an independent.

Poisson process with a rate is equal to the arrival rate λe on the corresponding incoming link e ∈ E_{Mi} in M. If ψ_i denotes the strategy used by mix M_i in the sub network M_i , then, there exists $\psi \in \psi(M)$ such that:

$$A^{\Psi}(\mathcal{M}) \geq \sum_{i=1}^{m} \frac{\lambda^i}{\lambda} A^{\Psi_i}(\mathcal{M}_i)$$

We assume that given Λ i , each individual process XSi ,Mj is an independent Poisson process with rate λi, j .



Two Stage Analysis of Single Destination Network with Multipath.

5. ASYMPTOTIC ANONYMITY

In any network, the achievable entropy rate of sources of departing packets cannot exceed the prior entropy rate of the arrival processes owing to the finite buffer size restriction .the packets are containing the source and destination information. For instance, if in a single mix system M_1 with buffer size b, the arrival rates are given by $\lambda_1, \ldots, \lambda s$, then for any mixing strategy ψ

$A\psi(M1) \leq - s \; E\, j=1\; \lambda i/\lambda \log(\lambda i/\lambda)$

A. Lower Bound on Rate of Convergence

As observed in (14), the optimal Convergence rate of anonymity with buffer size in a two user equal rate system is O(1b2). In the following theorem, we prove that in any multiuser system with unequal arrival rates, the convergence rate of the anonymity of a Chaum mix is no better than O(1/ b2).**Aψ(M1) ≤ hs (q1, . . . , qs) − Ω (1/ b2)**

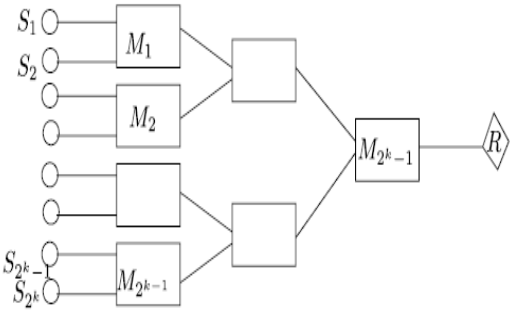
B. Upper Bound on the Convergence Rate

For a two source equal rate mix, the maximum achievable anonymity as a function of the buffer size is given by:

A(b) = 1 + log (cos (π b + 3))= 1 − O(1/ b2)

In combination with this Theorem, we can prove that this convergence rate is achievable for a range

of multiuser systems. In particular, consider a binary tree single destination Network all mixes have equal buffer size b.



Binary Tree Mix Network: All sources transmit at equal rates.

6. CONCLUSION

Using an information theoretic measure of anonymity, we designed scheduling and relaying strategies to maximize anonymity in arbitrary single destination networks of mixes. We restricted our attention to passive eavesdroppers. In addition to observing transmission times, an adversary can compromise a fraction of nodes to reveal additional portions of routes, the anonymity are restricted the eavesdropper. Network of mixes over receiving packet sources from an eavesdropper's perspective as the measure of secrecy, the maximum achievable secrecy of a single mix with buffer size *b* (packets) serving for achieving multiple mixes (network of mixes). By obtaining network of mixes the source anonymity is achieved successfully.

REFERENCES

[1] Abhishek Mishra ; ECE Department, Lehigh University, ; Parv Venkitasubramaniam "Anonymity and Fairness in Packet Scheduling: A Quantitative Tradeoff" DOI: 10.1109/CISS.2012.6310742

[2] N. West, The SIGINT Secrets: The Signals Intelligence War, 1900 to Today. New York, NY, USA: William Marrow, 1988.

[3] U. S. Navy, "Military study, communication intelligence research activities," Dept. Navy Library, Washington Navy Yard, Washington, DC, USA, Tech. Rep. SRH-151, Jun. 1937.

[4] A. Back, U. Möller, and A. Stiglic, "Traffic analysis attacks and tradeoffs in anonymity providing systems," in Proc.
4th Int. Inf. Hiding Workshop, Pittsburg, PA, USA, Apr. 2001, pp. 245–257.

[5] J.-F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in Proc. Int. Workshop Designing Privacy Enhancing Technol., Design Issues Anonymity Unobservability, LNCS vol. 2009. 2001, pp. 10–29.

[6] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. ACM, vol. 24, no. 2, pp. 84–88, Feb. 1981.

[7] C. Díaz and A. Serjantov, "Generalising mixes," in Proc. 3rd Int. Workshop Privacy Enhancing Technol., 2003, pp. 18–31.

[8] D. Kesdogan, J. Egner, and R. Büschkes, "Stop-and-go-MIXes providing probabilistic anonymity in an open system," in Proc. 2nd Int. Workshop Inf. Hiding (IH), vol. 1525. Portland, OR, USA, Apr. 1998, pp. 83–98.

[9] G. Danezis and L. Sassaman, "Heartbeat traffic to counter (n-1) attacks: Red-green-black mixes," in Proc. ACM Workshop Privacy Electron. Soc., 2003, pp. 89–93.

[10] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, 1949.

ABOUT THE AUTHOR

S.Suganyadevi MCA., is pursuing M.Phil. (Computer Science) degree in Sree Saraswathi Thyagaraja College (STC), Pollachi. Under the guidance of Dr.V.Anuratha, Assistant Professor in MCA, STC, Pollachi, Tamilnadu, India.

Dr.V.Anuratha did her UG graduation in Computer Science at PSG CAS, Coimbatore. She did her MCA at Madras University, M.Phil at Manonmaniam Sundaranar University, Tirunelveli, Ph.D in the area of Wireless Area Networks through Mother Teresa University, Kodaikanal. Her area of interest is Wireless Networks, Cloud Computing and MANET. She have guided more than 20 M.Phil Research scholars and currently guiding 6 Ph.D Scholars in the area of Computer Science. She have published more than 10 research papers in reputed journals.

