Journal of Computer Applications (JCA)
ISSN: 0974-1925, Volume IV, Issue 4, 2011

ANOMALY PROTECTION USING BATCHING STRATEGIES

M. Renukadevi [a,*], N. Bhaskar [b,1], R. Prabu [c,2]

***Abstract* - Traffic analysis is typically countered by the use of intermediary nodes, whose role is to perturb the traffic flow and thus confuse an external observer. Such intermediaries are called mixes. We address attacks that exploit the timing behaviour of TCP and other protocols and applications in low-latency anonymity networks. Intermediaries delay and reroute exchanged messages, reorder them, pad their size, or perform other operations such a mix network to handle mail traffic. Mixes have been used in many anonymous communication systems and are supposed to provide counter measures to defeat traffic analysis attacks. There are many attacks that occur in the networks such as Sinkhole attacks, Wormhole attacks, and flow correlation attacks and so on. We focus on a particular class of traffic analysis attacks, known as flow correlation attacks, by which an adversary attempts to analyse the network traffic and correlate the traffic of a flow over an input link with that over an output link. Flow-correlation attacks attempt to reduce the anonymity degree by estimating the path of flows through the mix network. Two classes of correlation methods are considered, namely time-domain methods and frequency-domain methods. In the time domain, statistical information about rate distributions is collected and used to identify the traffic dependency. In the frequency domain, it identifies traffic similarities by comparing the Fourier spectra of timing data. The empirical results provided in this paper give an indication to designers of Mix networks about appropriate configurations and mechanisms to be used to counter flow-correlation attacks.**

***Index Terms* - Mix, anonymity, flow-correlation attack, intermediaries node, security.**

I. INTRODUCTION

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

Manuscript received, 22-Oct-2011.
M. Renukadevi [a,*],
Department of Computer Science and Engineering,
S.A.Engineering College, Chennai.
E-mail: cserenukadevi13@gmail.com
N. Bhaskar [b,1],
Department of Information Technology,
Dr. Rangarajan Dr. Sakunthala engineering, Chennai.
E-mail: itbhaskaran@gmail.com
R. Prabu [c,2], Assistant Professor,
Department of Information Technology,
Dr. Rangarajan Dr. Sakunthala engineering, Chennai.
E-mail: dprpit@gmail.com

Most traditional communications media including telephone, music, film, and television are reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP) and IPTV. It has being identified that encryption alone does not provide security for a user, since traffic analysis can easily uncover information about the participants in a distributed application.

The anonymity of the system is attacked either by exchange of packets or via the encryption. Due to this the anonymity of the user is reduced. Therefore a efficient encryption can be used to prevent packet content inspection. Generally traffic occurs in a congested network where the anonymity and privacy of user is completely destroyed. Traffic analysis is typically countered by the use of intermediary nodes, whose role is to perturb the traffic flow and thus confuse an external observer. Such intermediaries (often called mixes) delay and reroute exchanged messages, reorder them, pad their size, or perform other operations.

In the previous researching papers the anonymity of the system is ruined by various kinds of attacks that occur in the network. Some of the attacks that occur in the network such as Sink-Hole attack, Worm-Hole attack and Flow-Correlation attack. In this paper, we focus on a particular type of attack called as Flow-Correlation attack whose role is to reduce the anonymity of the user in a congested network. In general, flow correlation attacks attempts to reduce the anonymity of the user, correlation analyzes the traffic on a set of links inside the network and reduce the security and helps the adversary identify the path of a flow and consequently reveal other critical information related to the flow.

The congestion will occur due to the bottlenecks occurs in the network. So that the network is not efficient and secured to send the data since the data might be lost. To overcome this, an Intermediate node is used to send the data in a secured manner over the network. The role of the Intermediate node is to perturb the traffic flow and thus confuse an external observer. In this paper, we focus on secured algorithms and some techniques known as Batching and recording techniques to improve the anonymity of the users in the network. Batching strategies are designed to prevent not only simple timing analysis attacks, but also powerful trickle attacks, flood attacks, and many other forms of attacks. Major contributions are summarized as follows:

- Two classes of correlation methods
- Detection rate
- Batching

II. BACKGROUND

Zhenghao Zhang [1] this paper uses simultaneous Multiple Packet Transmission (MPT) to improve the downlink performance of wireless networks. With MPT, the sender can send two compatible packets simultaneously to two distinct receivers and can double the throughput in the ideal case. This paper formalize the problem of finding a schedule to send out buffered packets in minimum time as finding a maximum matching problem in a graph.There are some limits for arrival rate that can allow in a network.

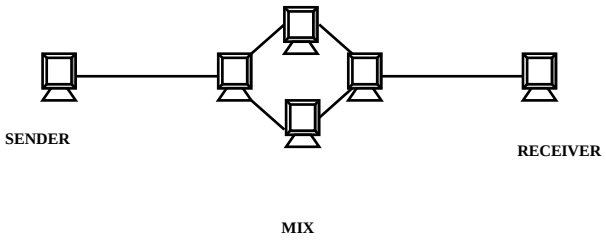
For anonymous e-mail applications, Chaum [2] proposed using relay servers, called mixes, which encrypt and reroute messages. An

encryption for a user is provided by using an encryption method. Onion Routing [3] is used for providing encryption in an anonymity networks. An encrypted message is similar to an onion constructed by a sender, who sends the onion to the first mix. The steps used in the Onion routing are as follow:

- Using its private key, the first mix peels off the first layer, which is encrypted using the public key of the first mix.
- Inside the first layer are the second mix's address and the rest of the onion, which is encrypted with the second mix's public key.
- After getting the second mix's address, the first mix forwards the peeled onion to the second mix. This process repeats all the way to the receiver.
- The core part of the onion is the receiver's address and the real message to be sent to the receiver by the last mix.

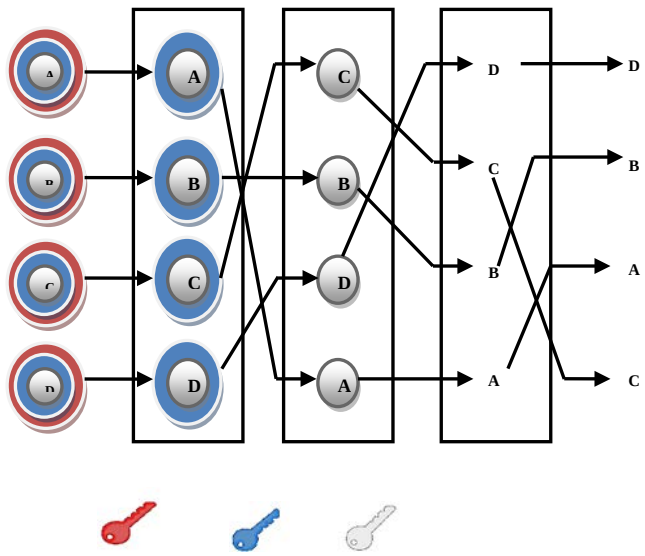
Suh[4] Characterize and detect the Skype-related traffic. This paper focuses on characterizing and detecting relayed traffic generated by Skype, a popular voice over IP application that uses relays. Skype is an Internet service that uses voice over Internet protocol (VOIP) technology to allow people from all over the world to communicate. Call quality from Skype may suffer if you have a slower-than-average Internet connection. Customers may also experience interference during calls if using a Skype WIFI or cordless phone from other devices such as routers, microwave ovens or even Bluetooth-enabled devices that operate at the same frequency. Yuanchao Lu [5] paper focus on traffic analysis on encrypted Voice over IP (VOIP) calls at the network level and the application level.

Ye Zhu [6] model the effectiveness of single mixes or of mix networks in terms of information leakage and measure it in terms of covert channel capacity. The relationship between the anonymity degree and information leakage is described. There are different methods to build an anonymity service using mixes. A peer-to-peer mix network is one of best mix network which provides a better anonymity for the users in many situations. Crowds [7], Tarzan [8], Morph Mix [9], and P5 [10] belong to this category.The possibility of a lone flow along an input link of a mix is analysed by the Sewell [11] . If the rate of this lone input flow matches with to the rate of a flow out of the mix, this pair of input flow and outflow flow are correlated. In [12], Wright et al. analyze passive logging attacks on anonymous communication networks. Danezis's attack [13] discuss on continuous time mix. Correlation-based traffic analysis schemes are applicable beyond anonymity networks. For example, traffic analysis has been successfully applied to identify and locate stepping stones [14], [15], [16]. Most of these traffic analysis approaches are timing based.



(A)

Simple decryption mix net. Messages are encrypted under a sequence of public keys. Each mix node removes a layer of encryption using its own private key. The node shuffles the message order, and transmits the result to the next node.



(B) Figure 1. (a) Mix network (b) Mix network with authentication

The rest of the paper is organized as follows: section 2 first reviews the related work; section 3 introduces the methodology concerned in the paper; section 4 describes the batching strategies and algorithms used; section 5 describes the results analysis. The conclusion of the paper is discussed in section 6.

III. METHODOLOGY

A mix-network as a cryptographic primitive that provides anonymity. A mix-network takes as input a number of cipher texts and outputs a random shuffle of the corresponding plaintexts. Mixes were proposed by Chaum [2] in 1981. The mix takes a number of input messages, and outputs them in such a way that it is infeasible to link an output to the corresponding input (or an input to the corresponding output).Common applications of mix-nets are electronic voting and anonymous network traffic.

Claudia Diaz [17] presents an analysis of mixes and dummy traffic policies, which are building blocks of anonymous services. Mixes are a basic building block for anonymous applications. In order to increase the anonymity of a mix system, mixes are usually combined in a mix network. This way, the fact that some mixes are corrupted or controlled by an attacker does not break the anonymity of the users (the anonymity of a message is guaranteed even if only one of the mixes in the path of the message is honest). Also, the reliability of the system is improved, because the failure of a mix does not lead to a denial of service. The disadvantages in mix network, is that the adversary node can easily reconstruct the path of the connection by combining measurements and results of flow correlation either at the network boundaries or within the network. The attack in more detail, Fig 2 shows a diagrammatic representation which the adversary may use to perform flow correlation. The flow correlation attack can be discovered by four techniques.

- Data collection
- Flow pattern vector extraction
- Distance function selection
- Flow correlation

This section discusses the traffic analysis methodologies that may be deployed by an adversary. Recall the objective of the adversary's is to correlate an incoming flow to an output link at a Mix. This is known as flow-correlation attacks, where an adversary may disclose the communication relationship between a sender and a receiver by measuring the similarity between the sender's outbound

flow and the receiver's inbound flow. Various techniques have been used to disclose the user anonymity of an user. They are as follow:

Technique 1: Collection of Data

The adversary is able to collect information about all the packets on both input and output links (assumption). For each collected packet, the arrival time is recorded and also all the packets are encrypted and padded to the same size. The arrival times of packets at input link "i" form a time series.

$$\mathbf{A_i = \{ (a_{i,1}) ,\ldots.. (a_{i,r}) \}}$$

Where $a_{i,k}$ is the k^{th} packet's arrival time at input link "i" and "r" is the size of the sample collected during a given sampling interval. Similarly, the arrival times of packets at output link j form a time series.

$$\mathbf{B_j = \{ (a_{j,1}) ,\ldots.. (a_{i,s}) \}}$$

Where $b_{j,k}$ is the k^{th} packet's arrival time at output link "j", and "s" is the size of the sample collected during a given sampling interval. The packets come out from mixes in batches.

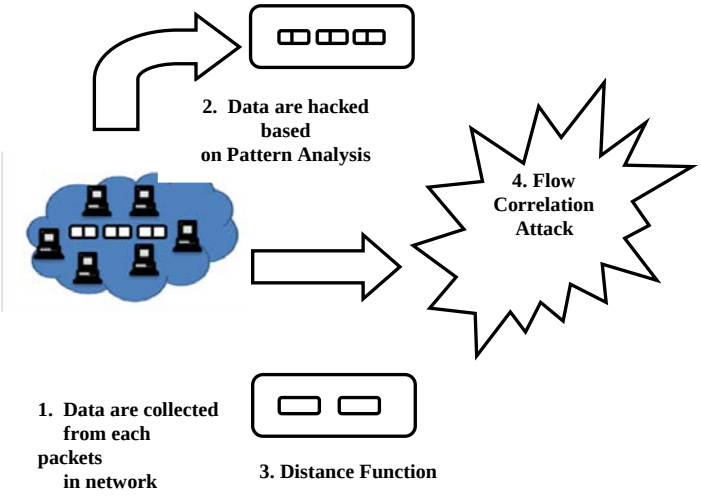


Figure 2. Techniques in Flow-correlation

Technique 2: Extraction of Flow Pattern Vector

The aim of the adversary is to analyse the time series A_is and B_js in order to determine "Similarity" between an input flow and an output flow of the mix. A direct analysis over these time series will not be effective. They need to be transformed into so-called pattern vectors. The time series A_i is transformed into pattern vector.

$$\mathbf{X_i = \{(x_{i,1}) ,\ldots.. , (x_{i,q})\}}$$

And time series B_j is transformed into pattern vector

$$\mathbf{Y_j = \{(y_{i,1}) ,\ldots.. , (y_{i,q})\}}$$

Technique 3: Selection of Distance Function

We define the distance function $d(X_i,Y_j)$,which measures the "distance" between an input flow at input link "i" and the traffic at output link "j". The smaller the distance, the more likely the flow on an input link is correlated to the corresponding flow on the output link.

Technique 4: Flow Correlation

Once the distance function has been defined between an input flow and an output link, it can be easily carry out the correlation analysis by selecting the output link whose traffic has the minimum distance to input flow pattern vector X_i. This paper focuses on preventing Flow-correlation attack from the adversary node. The Flow-correlation attack can be overcome by using the Intermediate node. This intermediate node performs the batching and the reordering techniques for providing security to the data via a congested network.

IV. BATCHING STRATEGIES AND ALGORITHM

Batching strategies are designed to prevent powerful trickle attacks, flood attacks, and many other forms of attacks. It is also used to prevent simple timing analysis attacks. Table 1 show the seven batching strategies. They are as follow:

Table 1
Batching Strategies [18]
(a) GLOSSARY

n	queue size
m	threshold to control the packet sending
t	timer's period if a timer is used
f	the minimum number of packets left in the pool for pool Mixes
P	a fraction only used in Timed Dynamic-Pool Mix

Batching Strategies can be achieved by using the reordering techniques. In this proposed scheme, the attacks focus on the traffic characteristics. As reordering does not significantly change packet interarrival times for mixes that use batching, these attacks are unaffected by reordering. Thus, these results are applicable to systems that use any kind of reordering methods. More precisely, reordering are in all cases caused by packets being delayed by the batcher, and can therefore be handled by modifying the batching algorithm accordingly.

(b) Algorithm

Strategy Index	Name	Adjustable Parameters	Algorithm
S0	Simple Proxy	*none*	no batching or reordering
S1	Threshold Mix	< *rn* >	if *n* = ra, send n packets
S2	Timed Mix	< ***t*** >	if timer times out, send n packets
S3	Threshold Or Timed Mix	< **m, *t*** >	if timer times out, send n packets; elseif *n* = *m* {send n packets; reset the timer}
S_4	Threshold and Timed Mix	< *m,t* >	if (timer times out) and *(n* > ra), send *n* packets
S5	Threshold Pool Mix	< *m , f* >	if *n* = *m* + /, send **m** randomly chosen packets
S6	Timed Pool Mix	< ***t , f*** >	if (timer times out) and *(n* > *f)* , send *n* — *f* randomly chosen packets
S7	Timed Dynamic-Pool Mix	< *m , t , f , p* >	if (timer times out) and **(n** > ra + /), send **max**(1, *[p(n* — *f)\)* randomly chosen packets

Any of the batching strategies can be implemented in two ways:

- Link-Based Batching
- Mix-Based Batching

Link-Based Batching: In this method, separate queue is allocated for each output link. Depending on its destination a newly arrived packet is put into a queue. Once a batch is ready from a particular queue (per the batching strategy), the packets are taken out of the queue and transmitted over the corresponding link.

Mix-Based Batching: In this method, a single queue is allocated for the entire mix. Selected batching strategy is applied to this queue. That is, once a batch is ready (per the batching strategy), the packets are taken out the queue and transmitted over links based on the packets' destination. These two methods has its own advantages

and disadvantages. The control of link-based batching is distributed inside the mix and hence may have good efficiency. On the other hand, mix-based batching uses only one queue and hence is easier to manage. We consider both methods in this paper. The effectiveness of continuous mixes [19], have been recently described. We discuss in detail how to extend our work to larger and complicated mix networks in [20].

In this paper, we assume that the adversary uses a classical timing analysis attack [21], [22] which is popularly known as flow-correlation attacks. The adversary cannot correlate (based on packet timing, content, or size) a packet on an input link to another packet on the output link. Packet correlation based on packet timing is prevented by batching, and correlation based on content and packet size is prevented by encryption and packet padding, respectively. In previous research papers they use AES encryption algorithm an d shortest path algorithm for analyzing the traffic in the network. The shortest path problem is the problem of finding a path between two vertices (or nodes) such that the sum of the weights of its constituent edges is minimized. Shortest path algorithms are applied to automatically find directions between physical locations, such as driving directions on web mapping websites like Mapquest or Google Maps. The Shortest path algorithm is used in this paper to find the intermediate system from the end-systems. Then the batching algorithm is used for sending the data's in a security manner.

A. Architecture

It alludes to the overall structure of the system and the ways in which that structure provides conceptual integrity for a system. In a broader sense however components can be generalized to represent major system elements and their interaction.

This paper generally used to overcome the overhead that occurs in the congested network. The confidential file cannot be send via the congested network. To overcome this Intermediate node is selected from a congested network to send the confidential files in a secure manner via the congested network. An intermediate node is selected based on the shortest-path algorithm. It will clear from the Fig 3 that the user (server) playing a vital role in sending the data in a confidential matter. The adversary can easily identify the data from a congested node and reduce the anonymity of a user. To avoid this certain nodes are selected from the congested network based on the shortest path algorithm. The database contains speed of each node and based on their speed a secured intermediate node is selected.

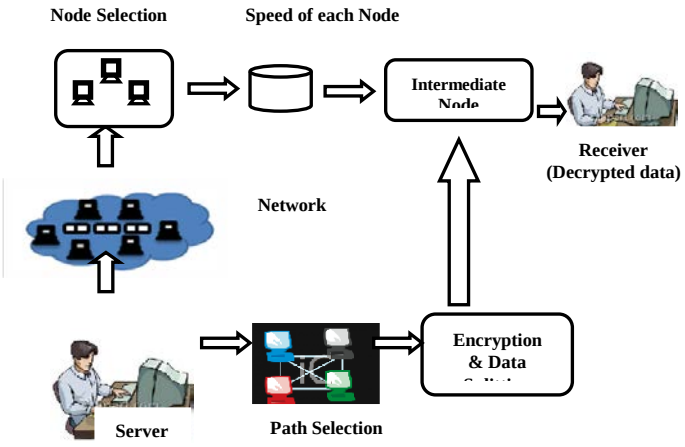


Figure 3. Architecture

A best path is selected by the user to send the encrypted data via the intermediate node. To improve the performance of anonymity users, the data are encrypted using the RSA algorithm. RSA offers a wide range of strong two-factor authentication solutions to help organizations assure user identities and meet compliance requirements.

B. RSA Algorithm

RSA is an encryption algorithm. It is widely used for encrypting important messages or digitally signing documents for e-commerce and is included as part of Web browsers by Netscape and Microsoft. The encryption algorithm was developed by Ron Rivest, Adi, Shamir and Len Adleman (R , S and A) at the Massachussets Institute of Technology (MIT) in 1977[23]. RSA encrypts on the principle of a private key and a public key. Users who wish to encrypt data first encrypt the message using a private key. This encrypted message can only be decrypted using a public key, which has already been distributed to the recipients of the message. The primary advantage of RSA comes from the fact that while it is easy to multiply two huge prime numbers together to obtain the product, it is computationally difficult to do the reverse. RSA is still the most widely used encryption algorithm. However while other standards such as DES are faster to decrypt, RSA remains an industry favourite for encrypting data with many believing it's 2048 bit key encryption is virtually unbreakable.

The RSA is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. It is mainly used for providing security for the participant (users).

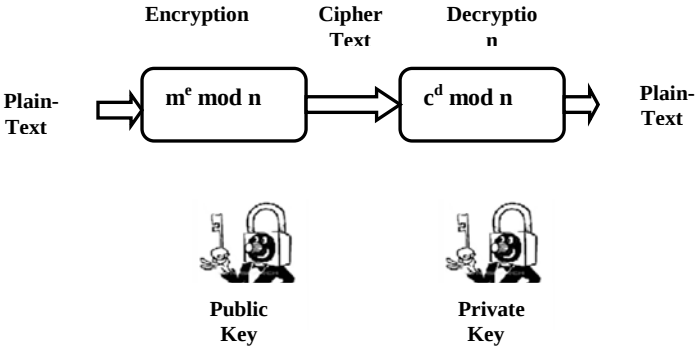


Figure 4. Authentication provided in RSA Algorithm

The RSA scheme is a block cipher in which the plaintext and cipher text are integers between and n-1 for some n. A typical size for n is 1024 bits, or 309 decimal digits. Encryption and Decryption are the two main concepts of RSA whereas the plaintext block is declared as M and cipher text block as C, such as

$$c = m^e \bmod n$$
$$m = c^d \bmod n$$

Both the sender and receiver must know the value of n. The value of 'e' is known to the sender, and only the receiver knows the value of d. This RSA algorithm must satisfy the following requirements:

- It is possible to find values of e, d, n such that m^{ed} mod n = M for all M < n.
- It is relatively easy to calculate mod m^e mod n and c^d mod n for all values of M < n.
- It is infeasible to determine d given e and n.

C. Steps in RSA Algorithm

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a **public key** and a **private key.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

- **Choose two distinct prime numbers *p* and *q*.**

For security purposes, the integers *p* and *q* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.

- **Compute *n* = *pq*.**

n is used as the modulus for both the public and private keys

- **Compute $\varphi(n) = (p-1)(q-1)$,** where φ is Euler's totient function.
- **Choose an integer *e*,** such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n)) = 1$, i.e. *e* and φ(*n*) are coprime.
- **Determine $d = e^{-1} \bmod \varphi(n)$**; i.e. *d* is the multiplicative inverse of *e* mod φ(*n*).

This is often computed using the extended Euclidean algorithm. *d* is kept as the private key exponent.

The **public key** consists of the modulus *n* and the public (or encryption) exponent *e*. The **private key** consists of the private (or decryption) exponent *d* which must be kept secret.

Encryption

Alice transmits her public key (*n*,*e*) to Bob and keeps the private key secret. Bob then wishes to send message **M** to Alice. He first turns **M** into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text *c* corresponding to

$$c = m^e \pmod n$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits *c* to Alice.

Decryption

Alice can recover *m* from *c* by using her private key exponent *d* via computing

$$m = c^d \pmod n.$$

Given *m*, she can recover the original message **M** by reversing the padding scheme.

V. Result Analysis

This paper raised the issues of the traffic that occurs in network whose role is to reduce the anonymity of the user which is famously known as Flow Correlation Attack. This Flow correlation attacks dropped the packets from the network using the inbound and outbound link of the packets to collect all the information from it. Such packet loss can occur in overloaded networks or in wireless settings where environmental interference can cause packets to be dropped. Based on the threat model and known strategies in existing mix networks, this paper performs extensive experiments to analyse the performance of mixes. The Flow Correlation Attacks can be overcome by using the Intermediate Node and efficient cryptographic algorithms. Such a security concern has not been addressed in the design of the Mix networks. The scheme used in this paper is effective by providing the intermediates by using the Shortest-path algorithm and also by providing batching and reordering techniques. This paper also provides security to a user by using cryptographic algorithm such as RSA algorithm. Due to this even the adversary cannot hack the data.

We use detection rate as a measure of the ability of the mix to protect anonymity. Detection rate here is defined as the ratio of the number of correct detections to the number of attempts. While the detection rate measures the effectiveness of the mix (the lower the detection rate, the more effective the mix), we measure its efficiency in terms of QOS perceived by the applications. The batching and reordering functions is performed by using the Mix control module which is then integrated into Linux's firewall system[24] using Netfilter; we use a set of firewall rules to specify which traffic should be protected.

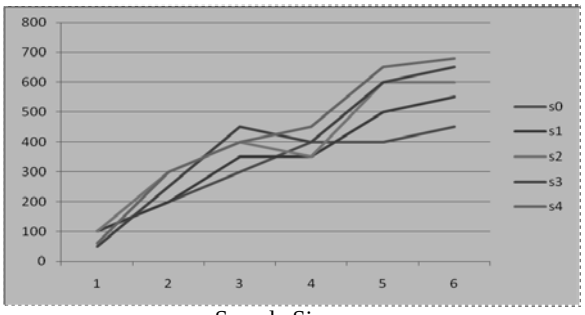


Figure 5. Detection rate for link-based batching

VI. Conclusion

We have analyzed mix networks in terms of their effectiveness in providing anonymity and quality-of-service. Various methods used in mix networks were considered: seven different packet batching strategies and two implementation schemes, namely the link-based batching scheme and mix based batching scheme. We found that mix networks that use traditional batching strategies, regardless of the implementation scheme, are vulnerable under flow-correlation attacks. By using statistical analysis, an adversary can accurately determine the output link used by traffic that comes to an input flow of a mix. The detection rate can be as high as 100 percent as long as enough data are available. This is true even if heavy cross traffic exists. The data collected in this paper should give designers guidelines for the development and operation of mix networks. The failure of traditional mix batching strategies directly leads us to the formulation of a new packet control method for mixes in order to overcome their vulnerability to flow-correlation attacks. Appropriate output control can achieve a guaranteed low detection rate while maintaining high throughput for normal payload traffic. Our claim is validated by extensive performance data collected from experiments.

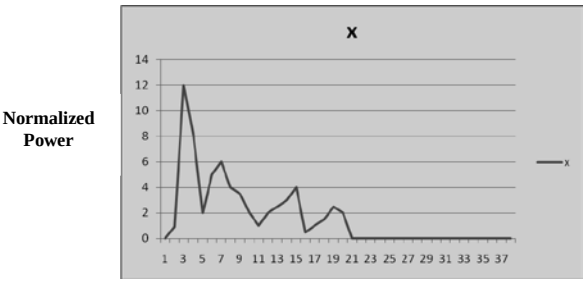


Figure 6. Power spectrum of an FTP flow

References

[1] Zhenghao Zhang; Yuanyuan Yang "Enhancing Downlink Performance In Wireless Networks by Simultaneous Multiple Packet Transmission", IEEE conference paper on parallel and distributed systems,2006.

[2] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-90, Feb.1981.

[3] P.F. Syverson, D.M. Goldschlag, and M.G. Reed, "Anonymous Connections and Onion Routing," Proc. IEEE Symp. Security and Privacy, pp. 44-54, 1997

[4] Suh, K.; Figueiredo, D. R.; Kurose, J.; Towsley, D. "Characterizing and detecting Skype-relayed traffic", IEEE conference paper on parallel and distributed systems, 2006.
[5] Yuanchao Lu; Ye Zhu, "Correlation-Based Traffic Analysis on Encrypted VoIP Traffic", IEEE journal on parallel and distributed systems, 2010
[6] Ye Zhu; Bettati, R. "Anonymity vs. Information Leakage in Anonymity System", Distributed computing Systems, ICDCS 2005. Proceedings. 25th IEEE International Conference on 10 June 2005.
[7] M.K. Reiter and A.D. Rubin, "Crowds: Anonymity for Web Transactions," ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998.
[8] M.J. Freedman and R. Morris, "Tarzan: A Peer-to-Peer Anonymizing Network Layer," Proc. Ninth ACM Conf. Computer and Comm. Security, pp. 193-206, 2002.
[9] M. Rennhard and B. Plattner, "Introducing MorphMix: Peer-to-Peer Based Anonymous Internet Usage with Collusion Detection,"Proc. ACM Workshop Privacy in the Electronic Soc. (WPES '02),pp. 91-102, 2002.
[10] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "p5: A Protocol for Scalable Anonymous Communication" Proc. IEEE Symp. Security and Privacy, pp. 58-70, May 2002.
[11] A. Serjantov and P. Sewell, "Passive Attack Analysis for Connection-Based Anonymity Systems," Proc. European Symp. Research in Computer Security(ESORICS '03), pp. 116-131, Oct. 2003.
[12] M. Wright, M. Adler, B.N. Levine, and C. Shields, "Defending Anonymous Communications against Passive Logging Attacks," Proc. IEEE Symp. Security and Privacy (SP '03), pp. 28-41, May 2003
[13] G. Danezis, "The Traffic Analysis of Continuous - Time Mixes," Proc. Privacy Enhancing Technologies Workshop (PET '04), pp. 35-50, May 2004.
[14] Y. Zhang and V. Paxson, "Detecting Stepping Stones," Proc. Ninth Conf. USENIX Security Symp. (SSYM '00), pp. 13-13, 2000.
[15] X. Wang and D.S. Reeves, "Robust Correlation of Encrypted Attack Traffic through Stepping Stones by Manipulation of Interpacket Delays," Proc. 10th ACM Conf. Computer and Comm. Security (CCS '03), pp. 20-29, 2003.
[16] Y.J. Pyun, Y.H. Park, X. Wang, D.S. Reeves, and P. Ning, "Tracing Traffic through Intermediate Hosts that Repacketize Flows," Proc. 26th IEEE INFOCOM '07, pp. 634-642, May 2007.
[17] Claudia Diaz, Bart Preneel "TAXONOMY OF MIXES AND DUMMY TRAFFIC" Towards measuring anonymity.
[18] A. Serjantov, R. Dingledine, and P. Syverson, "From a Trickle to a Flood: Active Attacks on Several Mix Types," Proc. Information Hiding Workshop (IH '02), F. Petitcolas, ed., pp. 36-52, Oct. 2002
[19] Y. Zhu, X. Fu, and R. Bettati, "On the Effectiveness of Continuous - Time Mixes under Flow Correlation Attacks," Technical Report TR2005-2-6, Texas A&M Univ. Computer Science, 2005.
[20] Y. Zhu, X. Fu, R. Bettati, and W. Zhao, "Anonymity Analysis of Mix Networks against Flow-Correlation Attacks," Proc. IEEE GLOBECOM '05, vol. 3, pp. 1801-1805, 2005.
[21] X. Fu, B. Graham, R. Bettati, W. Zhao, and D. Xuan, "Analytical and Empirical Analysis of Countermeasures to Traffic Analysis Attacks," Proc. 32nd Int'l Conf. Parallel Processing (ICPP '03), pp. 483-492, Oct. 2003. [22] D.X. Song, D. Wagner, and X. Tian, "Timing Analysis of Keystrokes and Timing Attacks on SSH," Proc. 10th USENIX Security Symp., pp. 337-352, 2001.
[23] W.Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall, 1999.
[24] Netfilter.org, "Netfilter," http://netfilter.samba.org/, 2003.

BIOGRAPHY

Ms.M.Renukadevi was born in Chennai, India, in 1988. She has received B.Tech degree (Information Technology) from Anna University, Chennai, India, in 2009 and currently pursuing M.E degree (Computer Science Engineering) in S.A.Engineering College Affiliated with Anna University, Chennai, India. Her areas of interests are Image Processing, Software Engineering and Data Mining.

Mr.N.Bhaskar was born in Salem, India, in 1984. He has received B.Tech degree (Information Technology) from Anna University, Chennai, India, in 2005, and currently pursuing M.Tech degree (Information Technology) in Vel Tech Multi Tech Dr.Ranagarajan Dr.Sakunthala Engneering College, Affiliated with,Anna University, Chennai, India. His areas of interests are Networking, Data Mining and Software Engineering.

Mr.R.Prabu was born in Erode, India, in 1983. He has received B.Tech degree (Information Technology) from Periyar University, Salem, India, in 2004. He has received M.Tech degree (Information Technology) in Sathyabama University, Chennai, India, in 2008. He is currently employed at Vel Tech Multi Tech Dr.Ranagarajan Dr.Sakunthala Engneering College, Chennai, India. His areas of interests are Networking, Data Mining and Software Engineering