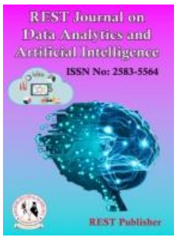
DOI: http://doi.org/10.46632/jdaai/1/2/6

REST Journal on Data Analytics and Artificial Intelligence

Vol: 1(2), 2022

REST Publisher; ISSN: 2583-5564

Website: http://restpublisher.com/journals/jdaai/


REST Journal on Data Analytics and Artificial Intelligence

ISSN No: 2583-5564

REST Publisher

# Detecting of Flow Timing Known Attacks and Protection in VoIP Networks

***Sugin lal G, Blessy R**

*Bharathiar University, Coimbatore, India.*

*Corresponding Author Email: *g.suginlal@gmail.com*

***Abstract:*** *Voice over Internet Protocol is a technology that use internet to make and receive telephone calls, voice is been turned into digital data packets that is been transmitted over the Internet. VoIP providers permit you to call anywhere at a flat rate for a fixed number of minutes, Call charges remain low over any distance. Economical, the simplicity is the properties that make maximum subscribers for VoIP Phone Service over conventional modes. At this paper, we make a center of attention on attacks that happen in VoIP, Here the attacks are happen by traffic analysis in the packet delivery phase. Two important contributions that are made. By means of the shortest route for routing voice flow makes the network at risk to flow based traffic analysis attack, as a contribution we derive new timing attack. Then, we develop a realistic technique to achieve experimental, customizable k-anonymity and randomness on voice over internet protocol networks. It provides solution for new timing attack with protected VoIP, thereby improving the quality of voice in VoIP.*

***Keywords:*** *VoIP, k-anonymity, Randomness protocol, Timing Attack*

## 1. INTRODUCTION

In general, the VoIP Phone Service makes the best suited system. The process of VoIP Phone Service constitutes conversion of analog signals into digital ones and sending them via broadband internet connection. The user is directly linked with the service provider. Several advantages over VoIP phone user as compared to traditional services, with reduced cost being the benefit. One of the most tempting features of VoIP Phone Service constitutes its insensitivity towards the distance over which a call is made. VoIP Phone Service is totally irrespective of the distance involved and this feature renders it a highly suited service for long distance calls for the Call charges remain low over any distance. Consistently low over any distance. Highly economical, the simplicity is the properties that make maximum subscribers opt for VoIP Phone Service over conventional modes. VoIP Phone Service doesn’t require any complicated infrastructure, moderately an Analog Telephone Adapter is provided by the VoIP Phone Service provider at the time of subscription that converts the analog signals into digital signals through a convertor. Digital signals are compress through codec and ultimately lead to the segmentation of signals. Signals are stored in the form of voice packets that are transferred by voice communication protocol. The next process comprises the decoding of the voice packets on the other end. While decoding, the sequence of events takes place in exactly reverse order where the voice de-capsulated and are decompressed by the codec resulting in the formation of digital signals. Thus formed digital signals are converted into analog signals for the listener to listen the original voice generated; In VoIP two major protocols RSP and real-time transport protocol (RTP) for packet delivery. In order to satisfy QoS requirements a common solution used in peer-peer Voice over internet protocol networks is to use a route setup protocol that sets up the shortest route on the VoIP network from a caller src to a destination dst. Real-time Transport Protocol carries voice traffic between the caller and the receiver along an established bidirectional voice circuit.

Preserving the anonymity in Voice over internet protocol networks is a difficult problem. Here, we center on attacks that challenge to infer VoIP call using traffic analysis in the packet delivery phase. Two important contributions. Using the shortest route for routing voice packet flows makes network at risk to flow based traffic analysis attack, as a contribution we derive new timing attack. Then, we develop realistic techniques to achieve quantifiable, customizable k-anonymity and randomness on voice over internet protocol networks. The following portion of this paper are organized as follows: we present a reference model for a VoIP network followed by flow based traffic analysis attack and provides a more concrete definition of k-anonymity and describes an efficient

AARSP. we have developed a new flow analysis attack i.e. Flow timing known attack and We Introduce **randomness** protocol to defend against timing attack. We sketch an implementation of our proposal and present experimental results that quantify the latency and throughput of Randomness protocol. We present related work and finally concluded.

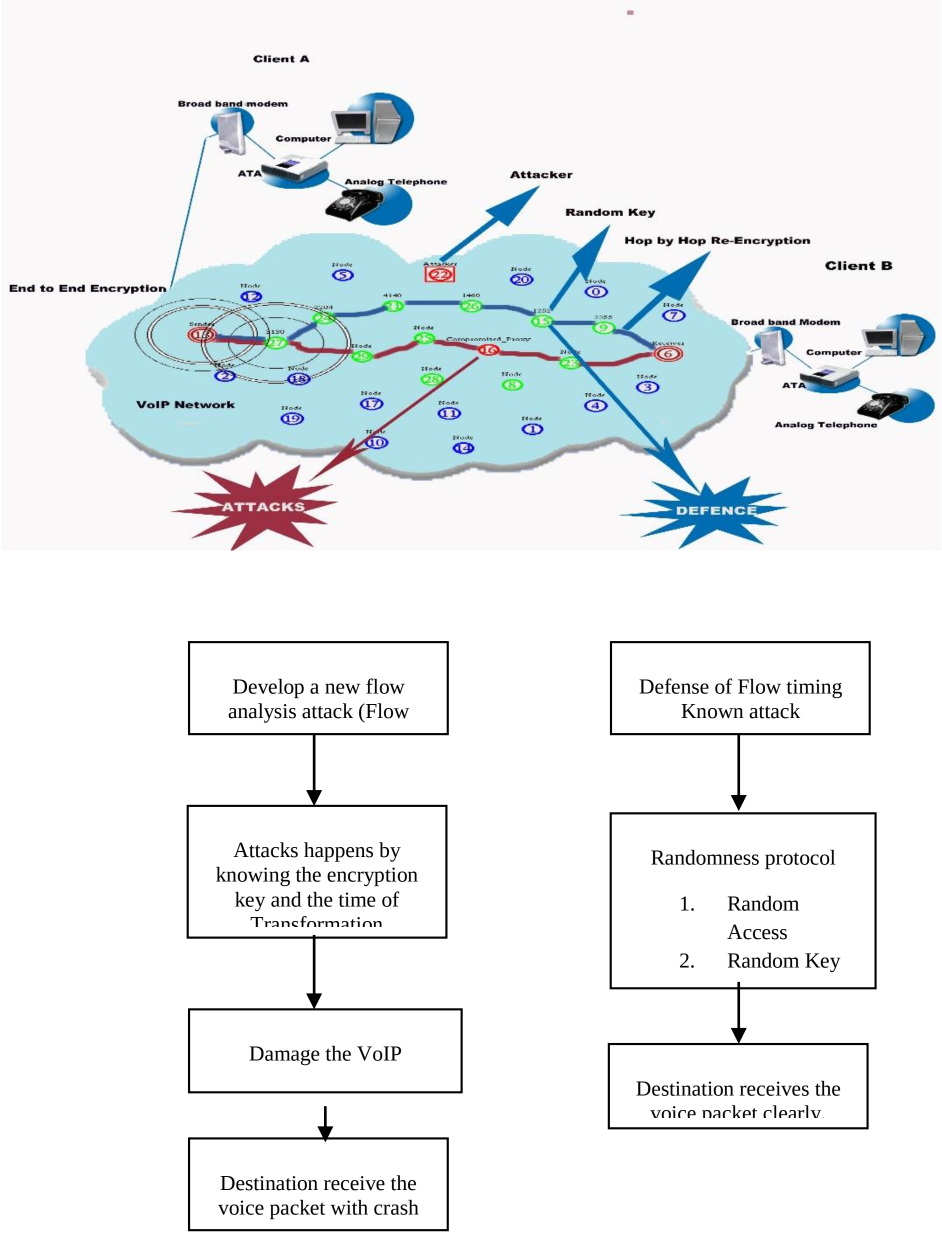


**FIGURE 1.** Architecture Diagram

***Route Setup:*** In this section, we describe a commonly used shortest route setup protocol in peer-to-peer Voice over internet protocol networks. Four steps that operates protocol initSearch (initiates a route setup by src), process Search (process route setup request at some node), process Result (process results of a route setup request at some node), and finSearch (concludes the route setup). One should note that flow based traffic analysis attack exploit only the property and are independent of the concrete route setup protocol. .

initSearch. A VoIP client src initiates a route setup for a destination dst by broadcasting search (searched, sipurl = dst.sipurl, ts = curTime) to all nodes p € ngh(src), where ngh(src) denotes the neighbours of node src in the VoIP network. VoIP client is identified by a URL (say, sip:lal@example.com). The searchId is a long randomly chosen unique identifier and ts denotes the time stamp at which the search request was initiated.

Process Search. Let suppose p receives search (searchId; sipurl; ts) from its neighbour q. If p has seen searchId , then the search request is dropped. If not, p checks if sipurl is the URL of a VoIP client linked to p. If true, (searchId; p) to q. p broadcasts search (searchId, sipurl; ts) to all ṕ Є ngh(p) –{q} and caches the search identifier <searched, sipurl, q> in its recently seen list. Note that ṕ has no knowledge of where the search request is initiated.

Process result let suppose p recives Result (searchId; q) from q. Note that p has no knowledge as to where the search result was started. p recently seen search queries to locate <searchId, sipurl, prev>. p adds a routing entry <sipurl, q> and forwards result(searched, p) to prev.

finSearch. When src receives result (searchId, q) from q, it adds a routing entry <dst, q> to its Routing table.

The route setup protocol establishes the shortest overlay network route between src and dst. This observation follows from the following facts: 1) the first search request that reaches a node p must have travelled along the shortest route from src to p, and 2) in process Search, a node p records the neighbor q through which it received the first search request. This shortest route from src to p is via q. Setting p = dst shows that the route setup procedure in process Result builds the shortest VoIP network path from src to dst. After a successful route setup, the client’s src and dst exchange an end-to-end media encryption key and switch to the delivery phase. The delivery phase additionally uses the randomness that the destination client access the packets randomly then the level of encryption use the random key for encryption technique we use AES algorithm. The description here serves as a basis for our Randomness protocol.

## 2. PREVIOUS WORK

***Flow Analysis Attack:*** The paper effectively highlights the growing vulnerability of SIP-based VoIP networks to DDoS attacks due to the transition from PSTN to NGN. It clearly outlines the research focus on employing machine learning techniques for robust DDoS detection. The emphasis on the importance of the paper's findings for cybersecurity professionals is commendable [1]. The paper effectively highlights the growing vulnerability of SIP-based VoIP networks to DDoS attacks due to the increasing popularity of VoIP services. The proposed research to compare existing detection mechanisms and develop a new attack detection scheme is valuable. A clear focus on user awareness is commendable [2]. The paper effectively highlights the vulnerability of VoIP services to security threats and the limitations of existing IP-based security solutions. The proposed VoIP-aware attack detection scheme, with its focus on both DoS and SPAM detection, is promising. The inclusion of experimental results to validate the scheme is a strong point [3]. In this section, we describe flow based traffic analysis attack on voice over internet protocol networks [6]. These attacks exploit the nature of the voice flows to identify pairs of callers and receivers on the voice over internet protocol network. Parallel to other security models for VoIP networks, the physical network infrastructure is owned by an un-trusted third party. For this reason, the VoIP service must route voice flows on the un-trusted network in a way that preserves the identities of callers and receivers from the un trusted network. We assume that the un trusted network service provider (adversary) is aware of the VoIP network topology [19] and the flow rates on all links in the VoIP network [15], [4]. The network service provider can obtain VoIP topology and flow information using traffic analysis or using various measurement-based approaches (such as expanding ring search on the network topology) [23]. We experimentally show that the attack can be very effective even when only one-third of the links are monitored by the adversary.

We represent the VoIP network topology as a weighted graph G =<V, E>, where V is the set of nodes and E V × V is the set of undirected edges. The weight of an edge e =(p, q) is the latency between the nodes p and q. We assume that the adversary can observe the network and thus know nf(p →q) the number of voice flows between two nodes p and q on the VoIP network such that (p, q) Є E.

To illustrate the effectiveness of our flow based traffic analysis attack, we use a synthetic network topology with 1,024 nodes. The topology is constructed using the GT-ITM topology generator [9] and our experiments were performed on NS-2 [10], [11]. GT-ITM models network geography and the small-world phenomenon (power law graph with parameter ¼ 2:1). The topology generator assigns node-to-node round trip times varying from 24 to 150 ms with a mean of 74 ms and is within 20 percent error margin from real-world latency measurements. The average route()latency between any two nodes in the network is 170ms,while the worst-case route latency in 225 ms. Our experiment over NS-2 use a bursty packet delay model wherein 20 percent of the packets incur an additional delay of up to 44 percent of average one-way latency [23]. In practice, the total cost of framing, decoding, and hop-by-hop re encryption amounts to about 1.4 ms per voice packet on commodity hardware. In our simulations, we adjust link latencies to reflect the cost of routing VoIP packets.

We generate voice traffic based on call volume and call hold time distribution obtained from a large enterprise with 973 subscribers (averaged over a month). The call volume is specified in Erlangs [21]. if the mean arrival rate of new calls is per unit time and the mean call holding time (duration of voice session) is h, then the traffic in Erlangs is A ¼ h; for example, if total phone use in a given area per hour is 180 min, this represents 180=60 ¼ 3 Erlangs. We use G.729A audio codec for generating audio traffic. The (src, dst) pair information for each call was not made available. We have experimented under two settings: first, we assume that for a given VoIP call, the (src, dst) pair is chosen randomly from the VoIP network; second, we assume that 80 percent of the calls are made between nodes that are in the same network geography (e.g., same autonomous system). Any prior information (such as 80 percent of call volume is limited to local network geography) can be used by the adversary to further enhance the efficacy of flow based traffic analysis attack. Finally, we note that all results reported in this paper have been averaged over seven independent runs.

***VoIP Privacy Using k-Anonymity:*** In this section, we develop a k-anonymity approach to protect the identity of a receiver from flow analysis active attack like Compromised Proxies.

*1) Compromised Proxies:*

The adversary could actively compromise some of the nodes in the VoIP proxy.

Some of the observation based passive attacks [6] that are involved for the below active attack.

2) *Naive Tracing Algorithm:*

Considering the nature of voice paths leads us to conclude the possible receiver.

3) *Statistical Tracing:*

We handle such uncertainties in network link latencies by using a construction of top-k algorithm.

4) *Distance Prior and Hop Count Prior:*

Find top-m probability receivers by using previous Distance and Hop Count.

*5) AARSP: Anonymity-Aware Rout Setup Protocol:*

In this section, we summarize our ideas behind AARSP [3].

AARSP accepts an anonymity parameter k as an input for the route setup protocol, on a per-client per-call basis. AARSP modifies the basic route setup protocol.

## 3. PROPOSED WORK

***Timing Known Attack:*** Timing attacks can break systems which are often considered to be un-break-able. We have developed flow based traffic analysis attack Named as **Flow Timing known Attack.** Attacker when they know the encryption key and the timing of transformation the **Flow Timing known Attack accrue.** Flow Timing known Attack [5] has low possibility in VoIP but more **injure.** The attacker hopes to correctly guess the packet sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may in fact originate from some compromised node controlled by the attacker. One possible way for this to occur is for the attacker to listen to the conversation occurring between the trusted hosts, and then to issue packets using the same source IP address. By monitoring the traffic before an attack is mounted, the compromised node can figure out the correct sequence number. After the IP address and the correct sequence number are known, it is basically a race between the attacker and the trusted host to get the correct packet sent. One common way for the attacker to send it first is to launch another attack on the trusted host, such as a Denial-of-Service attack. Once the attacker has control over the connection, it is able to send counterfeit packets without getting a response. ***Algorithm*** **Step 1:** if known of time for voice transformation Calculate the K-th packet timing. **Step 2:** Find his to the Destination. **Step 3:** Transfer the K-th duplicate packet to the destination with Level of encryption. **Step 4:** Destination receive the K-th duplicate packet and rejected tubule that is original packets. *E. Defence for Flow Timing Known Attack.* Here in this paper we have introduced a new Randomness protocol for the defence of flow timing knows attack here the protocol has two parts such as **Random Access** and **Random Key.** It is clear that we need an algorithm to generate random keys (Rnk), a Random Access (Rna), an encryption (Enc) algorithm. A triplet (Rnk, Rna, Enc) of algorithms, a message space M and a key space K, is called a symmetric key encryption scheme if: **a**. The Random key-generation algorithm: Rnk is an algorithm that returns a key K, denoted by k ← Rnk, such that k €K. **b.** The Random access algorithm: Rna is an algorithm that takes a key k and a voice-data m €M, and outputs a cipher data c ← Rna (m). **c**. The Encryption algorithm: Enc is an algorithm that takes a key k and cipher data c and outputs a voice-data m. In this paper we are discussing about the encryption method using Random key generation at each level. *Random Key* Here we generate Random Key using random key Generation Algorithm; Computer cryptography uses integers for keys. In some cases keys are randomly generated using random number generator [17] key lengths of 128 bits.

***Random Access:***

Here instead of sending the packet in a correct sequence we send the voice packet in a mixed randomly ordered and we set the random access of the destination so the destination access the packets randomly for the dynamic accessing the random number access Algorithm is Used. *Advanced Encryption Standard* Encryption is one of the essential security technologies for computer data, and it will go a long way toward securing VOIP. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. An encryption algorithm along with a key is used in the encryption and decryption of data. Advanced Encryption Standard (AES), is one of the most popular algorithms used in symmetric key cryptography. AES [16] is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. It has been analyzed extensively and is now used widely world wide enough to protect classified information up to the TOP SECRET level, which is the highest security level and defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public. AES supports key sizes of 128 bits, 192 bits and 256 bits and will serve as a replacement for the Data Encryption Standard which has a key size of 56 bits. In addition to the increased security that comes with larger key sizes, AES can encrypt data much faster than Triple-DES, a DES enhancement that which essentially encrypts a message or document three times.

***AES Algorithm***

AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.

AES operates on a 4×4 array of bytes termed the state. For encryption, each round of AES (except the last round) consists of four stages:

***Add Round Key*** — each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

***Sub Bytes*** — a non-linear substitution step where each byte is replaced with another according to a lookup table.

***Shift Rows*** — a transposition step where each row of the state is shifted cyclically a certain number of steps.

***Mix Columns*** — a mixing operation which operates on the columns of the state, combining the four bytes in each column using a linear transformation.

The final round replaces the Mix Columns stage with another instance of Add Round Key.

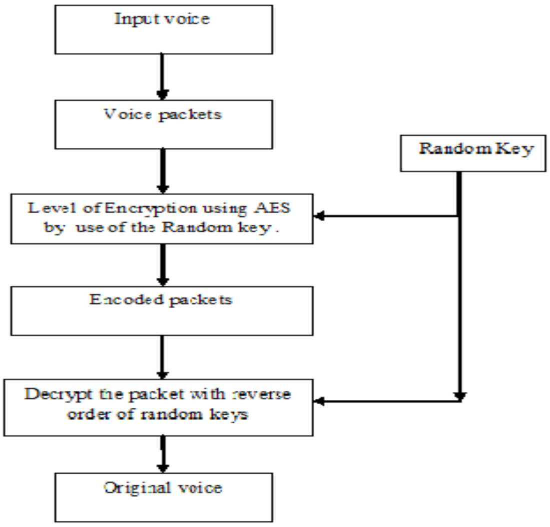

Input voice
Voice packets
Random Key
Level of Encryption using AES by use of the Random key.
Encoded packets
Decrypt the packet with reverse order of random keys
Original voice

**FIGURE 2.** Encrypt and Decrypt using Random Key

## 4. SIMULATIONS, RESULTS & DISCUSSIONS

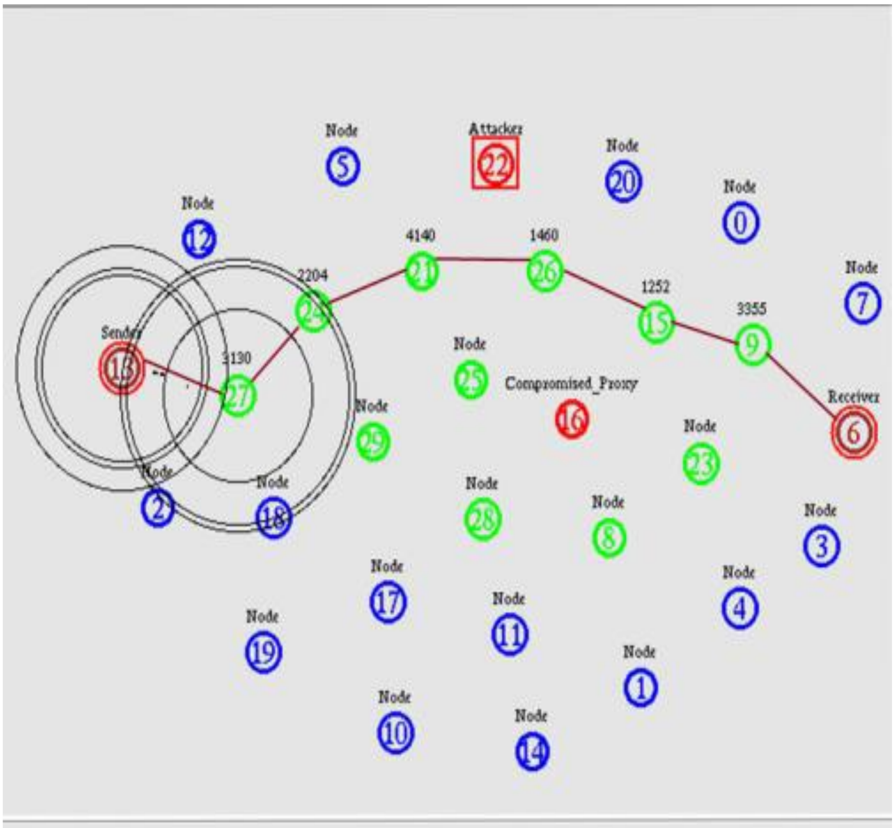


**FIGURE 3.** VoIP Scenario for Randomness protocol

The above VoIP Scenario consist of 30 nodes and the sender sends voice packet through a Anonymity Aware Route Setup Protocol, Here the packets are been send randomly with a hop by hope re-encryption using random key at each node.

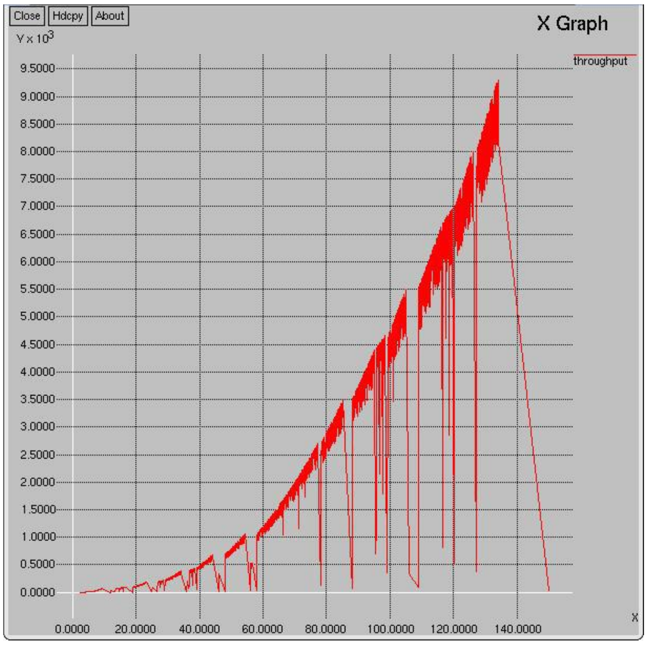


**FIGURE 4.** Throughput for VoIP using Randomness protocol

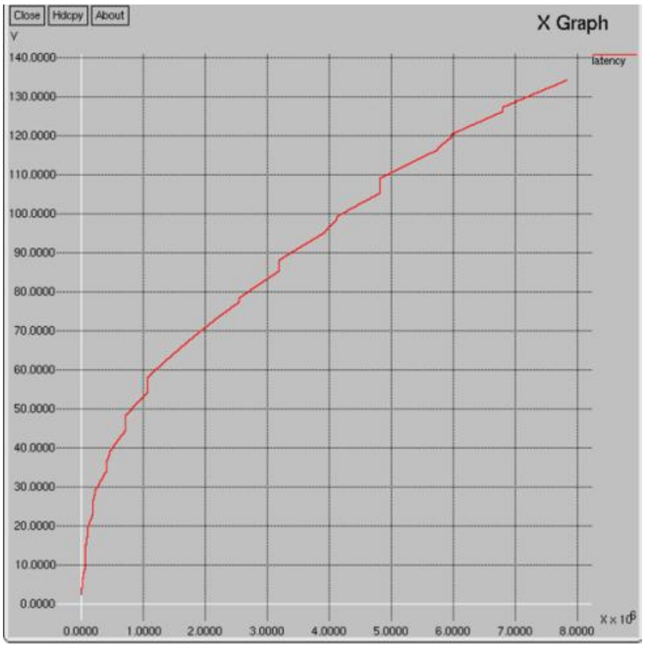


**FIGURE 5.** Latency for VoIP using Randomness protocol

## 5. CONCLUSION

In this paper, we have addressed the problem of providing privacy guarantees in peer-to-peer VoIP networks. Our process three stage. First, we have developed flow based traffic analysis attack that allows an adversary (external observer) to identify a small and accurate set of candidate receivers even when all the nodes in the network are honest. We have used network flow analysis and statistical inference to study the efficacy of such an attack. Second, we have developed mixing-based techniques to provide a guaranteed level of anonymity for VoIP clients. We have developed an AARSP that allows clients to specify personalized privacy requirements for their voice calls (on a per-client per-call basis) using a quantifiable k-anonymity metric. Finally, We Introduce randomness to defend against timing attack that is to break the tight correlation of timing and distance. Here by use of Random Search Algorithm we find Best anonymity and worst QOS. Then do Tradeoff between anonymity and QOS.

## REFERENCE

[1]. Amita Chauhan, Nitish Mahajan, Harish Kumar, Sakshi Kaushal, Analysis of DDoS Attacks in Heterogeneous VoIP Networks: A Survey, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-6S3, April 2019.

[2]. R. Safoine, S. Mounir and A. Farchi, "Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks," 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), Rabat, Morocco, 2018, pp. 1-5, doi: 10.1109/ICMCS.2018.8525878.

[3]. Lee, J., Cho, K., Lee, C. et al. VoIP-aware network attack detection based on statistics and behavior of SIP traffic. Peer-to-Peer Netw. Appl. 8, 872–880 (2015). https://doi.org/10.1007/s12083-014-0289-8

[4]. G. Perng, M.K. Reiter, and C. Wang, M2: Multicasting Mixes for Efficient and Anonymous Communication, Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2006.

[5]. V. Shmatikov and M.H. Wang, Timing Analysis in Low Latency Mix Networks: Attacks and Defenses,Proc. 11th European Symp. Research in Computer Security (ESORICS), 2006.

[6]. M. Srivatsa, A. Iyengar, and L. Liu, Privacy in VOIP Networks: A k-Anonymity Approach,Technical Report IBM Research RC24625, 2008.

[7]. X.Wang,S. Chen, and S. Jajodia, Tracking Anonymous Peer-to- Peer VoIP Calls on the Internet, Proc. 12th ACM Conf. Computer and Comm. Security (CCS), 2005.

[8]. A. Blum, D. Song, and S. Venkataraman, Detection of Interactive Stepping Stones: Algorithms and Confidence bounds,Proc. Seventh Symp. Recent Advances in Intrusion Detection (RAID), 2004

[9]. GT-ITM: Georgia, Tech Internetwork Topology Models http://www.cc.gatech.edu/projects/gtitm/, 2010.

[10]. The Network Simulator NS-2 http://www.isi.edu/nsnam/ns/, 2010.

[11]. The Network Simulator NS-2: Topology generation, http://www.isi.edu/nsnam/ns/ns-topogen.html, 2010.

[12]. Phex Client, http://www.phex.org, 2010.

[13]. Skype the Global Internet Telephone Company, http://www.skype.com, 2010.

[14]. Telegeography Research, http://www.telegeography.com,2010.

[15]. A. Back, I. Goldberg, and A. Shostack Freedom 2.1 Security Issues and Analysis, Zero KnowledgeSystems, Inc., White Paper, 2001.

[16]. P.Arul, Dr.A.Shanmugam Genarate a key for AES using biometric over VoIP Network security jatit.org/volumes/research papers/Vol5No2/2Vol5No2.pdf 2005.

[17]. Random Number Generator Algorithm. http://www.cryptosys.net/rng_algorithms.html

[18]. M.J. Freedman and R. Morris, Tarzan: A Peer-to-Peer Anonymiz-ing Network Layer, Proc. Ninth ACM Conf. Computer and Comm.Security (CCS), 2002.

[19]. D. Goldschlag, M. Reed, and P. Syverson, Onion Routing for Anonymous and Private Internet Connections, Comm. ACM,vol. 42, no. 2, 1999.

[20]. S. Saroiu, P.K. Gummadi, and S.D. Gribble, A Measurement Study of Peer-to-Peer File Sharing Systems,Proc. Multimedia Computing and Networks (MMCN) Conf., 2002.

[21]. Eclipse. Aspectj Compiler, http://eclipse.org/aspectj, 2010.

[22]. FBI. Letter to FCC, http: / /www .askcalea .com /docs /20040128.jper.letter.pdf, 2009.

[23]. K. Gummadi, R. Gummadi, S. Gribble, S. Ratnasamy, S. Shenker,and I. Stoica, The Impact of DHT Routing Geometry on Resilience and Proximity,Proc. ACM SIGCOMM, 2003.