Following Skype Signaling Footsteps

Dario Rossi [1], Marco Mellia [2], Michela Meo [2]

[1]*ENST Telecom Paris, France*
dario.rossi@enst.fr

[2]*Politecnico di Torino, Italy*
firstname.lastname@polito.it

***Abstract*— Skype is beyond any doubt *the* VoIP application in the current Internet. Its amazing success drawn the attention of telecom operators and the research community, both interested in knowing its internal mechanisms, characterizing its traffic, understanding its users' behavior. One of the most peculiar characteristics of Skype is that it relies on a P2P infrastructure for the exchange of signaling information that is distributed between active peers. Leveraging on the use of an accurate Skype classification engine that we recently proposed, we carry on an experimental study of Skype signaling based on extensive passive measurements collected from our campus LAN. In particular, we focus on the signaling traffic in the attempt of inferring some interesting properties of the overlay maintenance and, possibly, some hints about its structure.**

Our results show that, despite the signaling bandwidth used by normal peers is exiguous, it may however constitute a very significant portion of the total traffic generated by a Skype client – since, in order to guarantee reachability, Skype application is running most of the time even if no active call is in progress. Skype performs peer discovery and refresh by using a large number of single packets probes – which may be as effective for the purpose of the overlay maintenance as costly from the viewpoint of statefull layer-4 network devices. At the same time, single packet probes constitute only a minor portion of the signaling traffic: therefore, we dig into further details the traffic exchanged among more stable peers in the attempt of learning how the peer selection mechanism works.

I. Introduction

The last few years witnessed VoIP telephony gaining a tremendous popularity, as testified by the increasing number of operators that are offering VoIP-based phone services. Skype [1] is beyond doubt the most amazing example of this new phenomenon: developed in 2002 by the creators of KaZaa, it recently reached over 170 millions of users, and accounts for more than 4.4% of total VoIP traffic [2]. Being the most popular and successful VoIP application, Skype is attracting the attention of the research community and of the telecom operator as well.

One of the most interesting peculiarities of Skype is that it relies on a P2P infrastructure to exchange signaling information in a distributed fashion with the twofold benefit of making the system highly scalable and robust. The natural question is then how costly is the P2P overlay maintenance as well as the signaling overhead needed to exchange information about the users' reachability in a distributed fashion. The objective of this paper is to provide an answer to this question. To the best of our knowledge, this work is the first deep investigation of Skype signaling traffic: indeed, the study of Skype traffic and mechanisms is made very complex by the fact that protocols are proprietary, by the extensive use of cryptography, obfuscation and anti reverse-engineering techniques [4], and the implementation of a number of techniques to circumvent NAT and firewall limitations [3].

By exploiting our previous work, in which we devised a methodology that successfully tackles the problem of Skype traffic identification [8], this work aims at contributing to the understanding of Skype. We follow the same methodology, which does rely on protocol ignorance, since Skype proprietary design and adoption of cryptography mechanisms make it almost impossible to decode it. We propose a simple classification of Skype signaling traffic, isolating different components of the signaling activity that pertain to different tasks (such as network discovery, contact list refresh and overlay maintenance). Our results show that, despite the signaling bandwidth used by normal peers is exiguous, it may however constitute a very significant portion of the total traffic generated by a Skype client. Also, we observe that Skype performs peer discovery and refresh by using a large number of single packets probes – which may be as effective for the purpose of the overlay maintenance as costly from the viewpoint of statefull layer-4 network devices. At the same time, the bulk of the signaling traffic is carried by a relatively small number of longer flows, exchanged with more stable contacts. We therefore dig into further details the traffic exchanged among such peers, in the attempt of guessing how the peer selection mechanism works: apparently, the selection is driven by both the network latency and the user preference.

Despite the attention of the research community and Telecom operators versus Skype is steadily increasing [4], [3], [5], [6], [7], [8], all previous papers but [3] completely ignore Skype signaling traffic, being the focus different than ours. [3] focuses indeed on the login phase, and how Skype traverses NAT and firewalls. Our aim is instead to provide quantitative insights on the amount and characterization of Skype signaling traffic. Moreover, we evaluate the cost of the typical P2P mechanisms, such as network discovery, overlay maintenance, distributed diffusion of information.

II. Skype Overview

In this section, we introduce some necessary notions about Skype behavior.

Skype offers end users several (free) services: i) voice communication, ii) video communication, iii) file transfer and iv) chat services. The communication between users is established using a traditional end-to-end IP paradigm, but Skype can also route calls through a supernode to ease the traversal of symmetric NATs and firewalls. Voice calls can also be directed toward the PSTN using Skypein/Skypeout service, in which case a fee is applied.

The main difference between most VoIP services and Skype is that –except for user's authentication which is performed under a classical client-server architecture, by the means of public key mechanisms–, the latter operates on a P2P model. After the user (and the client) has been authenticated, all further signaling is performed on the P2P network, so that Skype user's informations (e.g. contact list, status, preferences, etc.) are entirely decentralized and distributed among nodes. This allows the service to scale very easily to large sizes, avoiding a costly centralized infrastructure. Peers in the P2P architecture can be normal nodes or supernodes. The latter ones are selected among peers with large computational power and good connectivity (considering bandwidth, uptime and absence of firewalls), so that they take part to the decentralized information distribution system which is based on a DHT.

From a protocol perspective, Skype uses a proprietary solution which is difficult to reverse engineer due to extensive use of both cryptography and obfuscation techniques [4], [3]. Though Skype may rely on either TCP or UDP at the transport layer, both signaling and communication data are preferentially carried over UDP. A single random port is selected during application installation, and it is never changed (unless forced by the user). When a UDP communication is impossible, Skype falls back to TCP, listening to the same random port, and port 80 and 443 which are normally left open by network administrators to allow Web browsing. We introduce the following definitions:

- A Skype *client* is identified by its socket address, i.e. the (IP address, UDP/TCP port) pair.
- A Skype *flow* is the bidirectional set of packets having the same tuple (IP source and destination addresses, UDP/TCP source and destination ports, IP protocol type). A flow starts when a packet with a given flow tuple is first observed, while it is ended by either an *inactivity timeout* (set to 200s as later discussed) or, in case of TCP, by observing the tear-down sequence if present. We further refer to the *sender* and *receiver* monodirectional flows to distinguish among the stream of packets coming from the same source and going to the same destination.

III. Measurement Results

This study is based on our previous work [8], which proposes an accurate Skype classification engine that detects Skype traffic, namely voice, video and signaling flows.

We report results that were collected by passively monitoring the campus access link at Politecnico di Torino for more than a month, starting from April the 22nd 2007. More than 7000 different hosts were used by both students and staff members which account to about 50000 people. We present a subset of those results, namely the first week where we observed about 3000 voice/videocalls and monitored Skype peer signaling activity. About 1700 monitored internal clients contacted nearly 305000 external peers, exchanging 496000 flows for a total of 33 millions of packets.

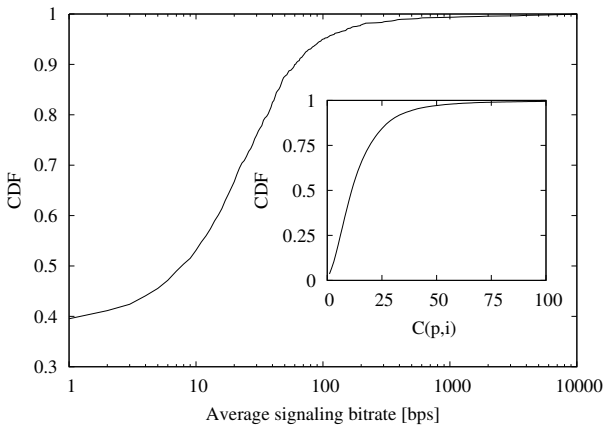

Fig. 1. Signaling bitrate (outset) and flows per time unit (inset) distributions

A. On the Signaling Overhead

We first consider the "overhead" that Skype signaling introduces in the network. The average signaling bitrate, evaluated as the total signaling message bits transmitted by a client during its whole lifetime, is very low. Outset plot of Fig. 1 reports the Cumulative Distribution Function (CDF) of the average signaling bitrate. It can be seen that the consumed signaling bandwidth is less than 100bps in 95% of cases, while only very few nodes generate more than 1 kbps of average signaling bitrate (they are possibly supernodes).

Since the signaling bitrate is exiguous, its relative importance vanishes if weighed on the ground of VoIP call traffic: e.g., for about 5% of the Skype clients, signaling accounts only for 5% of the total (i.e., including voice and video calls) Skype traffic. At the same time, since clients may be left running for long periods without VoIP services being actively used, the signaling traffic portion is dominating in 80% of the cases, reaching more than the 99% of the traffic generated by a Skype client.

Finally, let $C(p, i)$ be the number of different peers contacted by peer p considering the i-th time interval of 5 minutes since the start of peer p activity. Distribution of $C(p, i)$ over all internal peers, i.e., peers in our campus, and over whole measurement intervals is shown in the inset of Fig. 1: a peer contacts about 16 other peers on average, and no more than 30 in 90% of cases. Still, $C(p, i)$ can grow larger than 75 in 1% of the cases, which may constitute a burden for some layer-4 devices that keep per flow state (e.g., a entry in a NAT table, a lookup in a firewall ACL table). Moreover, it has to be stressed that, as will be discussed later and shown in Fig. 3, many signaling flows are single-packet probes that creates new temporary soft-state entries, rarely used later on.

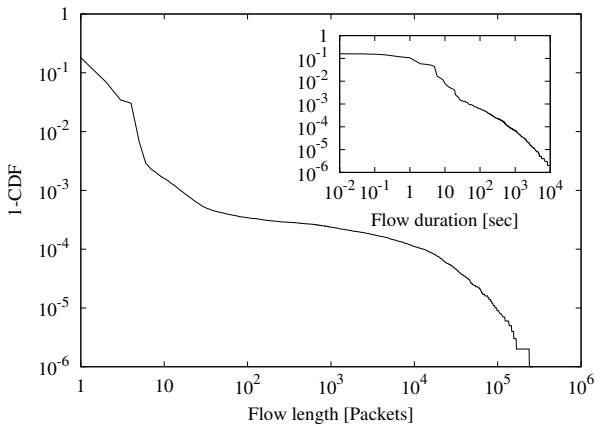

Fig. 2. Distribution of the signaling flow size (outset) and duration (inset)

B. Signaling Flow Classification

We are now interested in observing the signaling traffic a Skype client exchange. In particular, we look at measurements at the transport (flow) layer. The *semantic* of the signaling activity cannot be inferred from purely passive measurement, but the *form* of signaling activity can be further differentiated. Let us observe the *source* signaling flow length (in packets) and duration (in seconds) complementary distribution function (1-CDF) reported in Fig. 2, where both axis are in log-scale: about 80% of the signaling flows consists of single packet probes, and 99% of the flows is shorter than 6 packets. At the same time, some persistent signaling activity is present transferring a few MBytes of information over several thousand packets and lasting for hours, as the tails of Fig. 2 show: indeed, the single-packet probes account for less than 5% of the total bytes.

Consider now the schematic representation of the typical Skype signaling activity depicted in Fig. 3. Let p be the observed peer. We select two of them, namely the most active peer p_1 that does not perform any voice call (left plot in the figure) and a randomly picked peer p_2 having both signaling and voice flows (right plot). Each dot in the picture corresponds to a packet in the trace: the x-axis represents the packet arrival time since the first packet observed for that client. Y-axis reports an ID that uniquely identifies a peer that exchanged a packet with peer p. Positive IDs are used for peers that received a packet from p, negative IDs for peers that sent a packet to p. The range of the y-values corresponds to the number of different Skype peers with whom the selected peer is exchanging packets. The figure shows that p_1 has contacted (was contacted by) about 1100 other peers, whereas p_2 by about 450.

From the figure we can make three observations. First, the number of contacted peers exhibits an almost linear growth over time, hinting to P2P network discovery being carried on during most of the peer lifetime. This part of the signaling activity is mainly carried out by the transmission of a single packet, to which (most of the times) some kind of acknowledgment follows. The fact that p knows the address and port of valid (but previously un-contacted) Skype peers means that the above information is carried by some signaling messages. Since some of the unknown contacted peers may have gone offline before p actually probes them, the positive and negative ID ranges are not exactly symmetrical. Second, some of the peers are contacted on a regular basis: in the activity plot, horizontal patterns state that the same peer is periodically contacted during p lifetime. Finally, a periodic information refreshment can be distinguished in the form of vertical patterns (clearly visible in the right-hand side of Fig. 3 at about every hour).

These observations suggest the existence of different types of signaling flows, which we classify depending on their *length* and *periodicity* as:

- **One-Time Probe**: any packet sent toward an unknown peer, to which a single reply packet possibly follows, but *no further packet* is exchanged between the peer pair; for the sake of brevity, in the following we refer to one-time probe simply as probe;
- **Heartbeat**: a sequence of periodically exchanged one-time probes, separated by a time gap larger than the inactivity timeout, so that they are identified as different flows
- **Dialog**: any *source* flow constituted by more than a packets.

In Fig. 3 heartbeats and dialogs can be easily recognized as dotted horizontal patterns and solid horizontal segments respectively. The periodic information refreshment, responsible for the vertical patterns, involves both heartbeats toward already known peers, as well as discovery probes toward new peers.

Notice that the above definitions are sensitive to the setting of the end-of-flow inactivity timer, e.g., by setting the timeout to infinity heartbeats are turned into dialogs. However, we experimentally verified that the results are only very marginally affected by the choice of the inactivity timer, as far as it is up to a few minutes. Results reported in this paper are derived setting the timer to 200 s. This choice is justified by the fact that the largest regular inter-packet-gap that we ever observed was 180 s.

For the sake of simplicity, in what follows we distinguish signaling traffic depending on the kind of signaling activity in:

- **Probe** traffic, which is associated to probe flows;
- **Non-probe** traffic, which is associated to heartbeats and dialog flows.

C. Signaling Flow Characterization

We now analyze and characterize signaling traffic based on the proposed flow classification. We start by focusing on internal peers, and investigate the kind of generated flows[1]. Tab. I summarizes the amount of traffic due to peers that exchange i) only probe flow (label as 'probe' in the table),

[1]We have to restrict our attention to internal peers, since we do not have access to all the traffic generated by external peers.

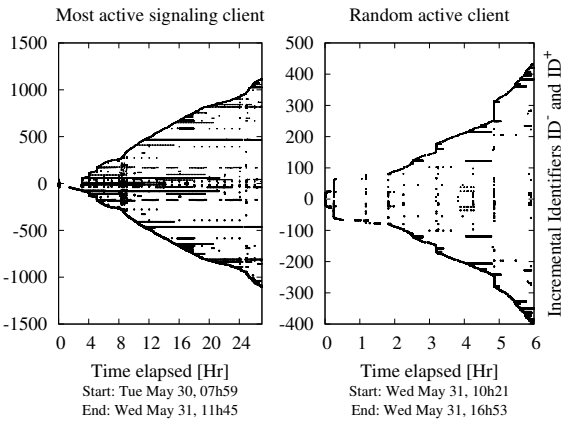

Fig. 3. Pictorial representation of Skype signaling activity

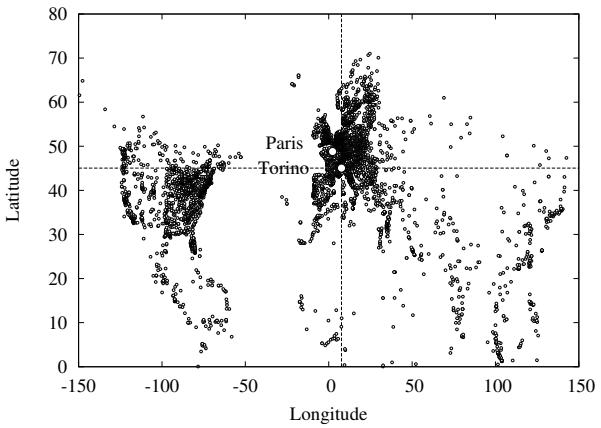

Fig. 5. Peer geolocation

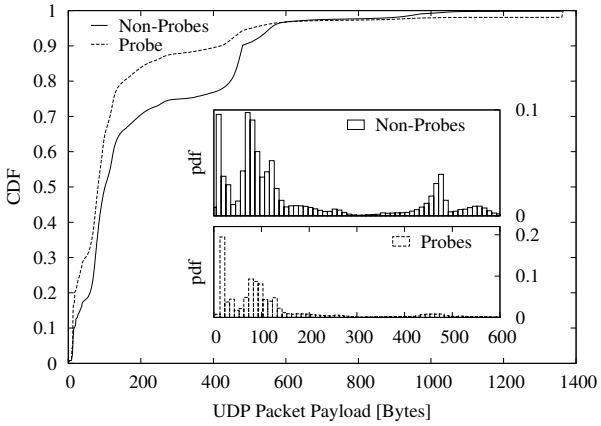

Fig. 4. Probe versus Non-Probe traffic packet size distribution

TABLE I
PER-SOURCE SIGNALING TRAFFIC CLASSIFICATION

Level	Probe%	Heartbeat%	Dialog%	Mix%	Total No.
Peers	51.2	15.8	25.1	8.0	390126
Flows	8.0	26.3	6.2	59.5	2505622
Packets	1.0	3.1	12.6	83.3	18274451

ii) only heartbeats flow, iii) only dialog flows or iv) a mix of heartbeat and dialog flows. Results are reported considering the peer level, the flow level and the packet level. Clients generates one-time probes in more than 50% of contacted peers. But only 8% of all observed flows are one-time probes, accounting for just 1% of signaling packets. On the contrary, dialogs represent the only signaling activity with one fourth of the peers, accounting for a relatively modest percentage of flows (6.2%), but corresponding a large number of packets (12.6%). Finally, a mixture of heartbeats and dialogs is exchanged with about 8% of the peers, which builds the bulk of the signaling activity in terms of flows (59.5%) and packets (83%). These results confirm that probe and non-probe traffic correspond to different kinds of signaling activity (possibly network discovery and network maintenance).

Another consequence of the different nature of probe and non-probe traffic is that flows carry a different amount of information, as testified by the distribution of the UDP payload size reported in Fig. 4. It shows that probe traffic has typically smaller packet size than non-probe traffic. Though it is not possible from purely passive techniques and without a reverse engineer of the protocol to state ground truth about Skype signaling, it is possible to conjecture that: i) network discovery, carried out by means of probes, is a continuous activity; ii) heartbeats are used to continuously ping contacts and friends, and to notify them of changes of the availability status; iii) dialogs may be used to maintain the overlay, during call setup, to update user information, etc.

IV. INSIGHTS INTO SKYPE SIGNALING

A. On the Geolocation of Peers

We now consider the geographical location of Skype peers. In the dataset we consider, we observed 304,690 external peers, corresponding to 263,886 different IP addresses. We queried the geographical location of the above addresses using HostIP [9], a public, open and free IP address database.

The geolocation is available in Fig. 5, which constitutes the subset of about 10k peers (out of the about 264k queries) for which longitude and latitude information were available. From the picture, it is easy to recognize the shape of the different continents, especially the European and North American ones, and a white landmark helps in locating the cities of Paris and Torino.

Further details on the geolocation of the whole Skype peer dataset is given in Tab. II. The table reports a breakdown, considering probe versus non-probe traffic, of the peers per continent (left), per European country (center) and per Italian city (right). Continents are sorted alphabetically, and the whole breakdown is reported; breakdown by countries and cities, instead, limitedly reports the 10 preferred locations, ranking them by increasing level of preference from top to bottom, i.e., most active locations are at the bottom. Uncertain items are labeled with UNKNOWN in the table. Elements in bold represent those that are geographically close to the measurement point, i.e., the Politecnico di Torino campus.

TABLE II

PEER GEOLOCATION: BREAKDOWN BY CONTINENT, EUROPEAN COUNTRY AND ITALIAN CITY

	Continent Breakdown			
	Non-Probe		Probe	
Continent	%	#	%	#
Africa	1.84	946	2.24	4763
America NO	23.09	11857	11.88	25246
America SO	2.98	1530	2.69	5709
Asia	12.15	6241	11.66	24777
Europe	**38.16**	**19598**	**45.38**	**96444**
Oceania	0.76	391	0.72	1520
UNKNOWN	21.02	10795	25.44	54069
TOT	100	51358	100	212528

European Union Countries Breakdown			
Non-Probe		Probe	
822	Finland	3655	Belgium
1099	Poland	4068	Sweden
1170	Belgium	4110	Bulgaria
1212	UNKNOWN	5159	Netherlands
1298	Sweden	5171	Spain
1349	Netherlands	**7130**	**Italy**
1743	**Italy**	9492	France
2004	Germany	11072	Poland
2327	France	13584	Germany

Italian Cities Breakdown			
Non-Probe		Probe	
18	**Moncalieri**	54	Napoli
19	Firenze	58	Padova
20	Napoli	71	Bologna
20	Bari	72	Firenze
38	Bologna	99	Bari
81	Roma	**208**	**Torino**
93	Milano	290	Milano
139	**Torino**	365	Roma
1055	UNKNOWN	4722	UNKNOWN

There are two important considerations that can be drawn from Tab. II. First, probing mechanism tends to privilege nearby hosts: indeed, nearly half of the probed IPs (45%) are located in Europe, nearly four times as much as in North America (12%). This means that the probing mechanism tends to discover network hosts that are geographically close. Second, the geographical location is much less important for non-probe traffic: indeed, while the percentage of peers that are located in Europe actually decreases (38%) with respect to probe traffic, the percentage of North American peers nearly doubles (23%). Considering that users resort to Skype to lower communication fees and to keep contacts with other faraway users, we are not surprised that non-probe traffic is more spread out. Indeed, the relationship among users forces Skype peer selection when considering non-probe traffic. On the contrary, the peer discovery mechanisms implemented by the one-time probes is driven by the physical properties of the underlying network.

B. On the Peer Selection Criterion

Fig. 6 shows the distribution of the Round Trip Time (RTT) between two peers, measured as the time elapsed between the packet probe going out from the campus LAN and the probe response packet (if any). For non-probe traffic, the first sent-received packet pair is used to estimate the RTT. This measurement takes into account both the network and application latency.

The information in the picture confirms our previous intuition: the latency of probing traffic is lower than that of non-probing traffic. Given Torino location, RTT smaller than 100ms are typical of nodes within the European Union, while RTT larger than 100ms are typical of nodes outside it. Measurement results allow us to conjecture that the probing mechanism is *latency driven*: Skype client probes for peers based on the information received by other peers so that low latency peers are more likely selected than high latency ones. Conversely, the peer selection mechanism is *preference driven*, where the preference criterion is dependent on the user relationships with others.

We now investigate the degree of "clustering" of the Skype overlay network. To this purpose, we define, for a given peer p, the *popularity* as the number of peers that *contacted* it; i.e., an internal (external) peer has a popularity x whenever it had

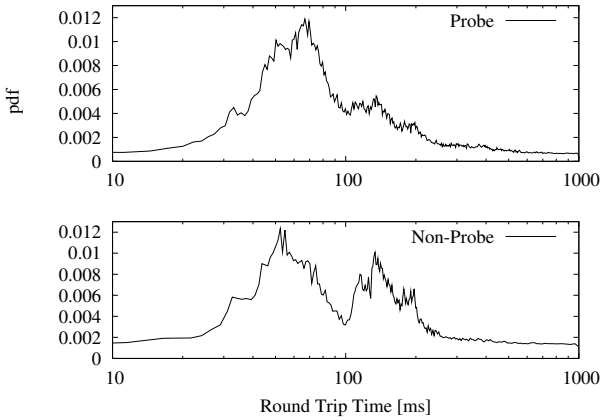

Fig. 6. Probe versus non-probe traffic round trip time distribution

been contacted by x external (internal) peers. The popularity distribution is depicted in Fig. 7 considering probe and non-probe traffic separately. From earlier considerations, non-probe traffic popularity pertains to the degree of clustering of users at Politecnico di Torino. Conversely, probe popularity may help revealing super-peers that are probed more frequently that random peers. Interestingly, this can be clearly noticed by looking at the external flows directed toward internal peers (right plot of Fig. 7). Indeed, for probe traffic, popularity is 1 in about 65% of the cases, i.e., the internal peer has been contacted by a single external peer. The CDF then increases until a popularity of 10. It keeps constant afterwards until the popularity achieves much higher values (100 or more). This hints to the internal peer being a super-node, in which case it attracts many signaling traffic from external peers; the phenomenon is similar for probe traffic.

Conversely, in the case of traffic directed toward external peers, the phenomenon is no longer visible since the number of internal clients is much smaller (1700) with respect to the external clients (305000).

V. CONCLUSIONS

In this paper we have investigated Skype signaling traffic by means of passive measurement, providing insights into Skype signaling mechanisms, that enlighten the cost and complexity of managing a P2P infrastructure. In particular, we have

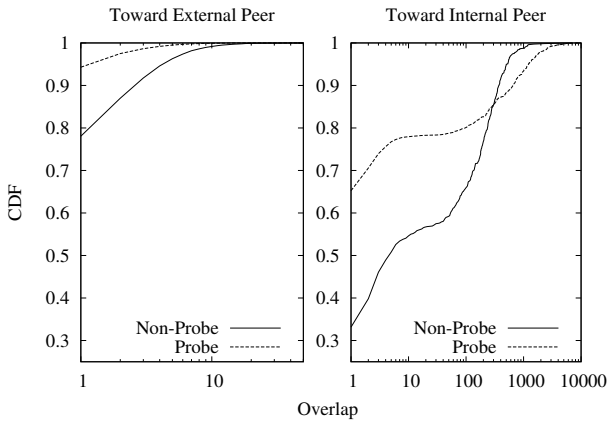

Fig. 7. Peer popularity toward external (left) and internal (right) peers

observed that Skype signaling traffic can be distinguished in: i) probe traffic flows, composed of a pair of packets exchanged between two peers, which are used to discover new nodes; ii) periodic heartbeats flows, that are used to exchange information about the status of peers of interest in the user's contact network, iii) long dialog flows, carrying most signaling information, that support the overlay network maintenance.

Our results provided empirical evidence of the fact that Skype prefers to flood the network with short single-probe toward many hosts – which may be as effective for the purpose of the overlay maintenance as costly from the viewpoint of stateful layer-4 network devices.

Moreover, Skype performs network discovery by accounting for geographical peer location (i.e., in terms of latency), while the overlay network is also influenced by the user network of contacts so that it is affected by peer geographical location in a different way.

ACKNOWLEDGEMENT

The Italian team was funded by the Italian Ministry of University, Education and Research (MIUR) through the PRIN project MIMOSA.

REFERENCES

[1] Skype web site, `http://www.skype.com`
[2] "International carriers' traffic grows despite Skype popularity", TeleGeography Report and Database. available on line `http://www.telegeography.com/`, Dec. 2006.
[3] S. A., Baset, H. Schulzrinne, "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol." *IEEE Infocom'06*, Barcelona, Spain, Apr. 2006.
[4] P. Biondi, F. Desclaux, "Silver Needle in the Skype." *Black Hat Europe'06*, Amsterdam, the Netherlands, Mar. 2006.
[5] S. Guha, N. Daswani and R. Jain, "An Experimental Study of the Skype Peer-to-Peer VoIP System", *5th International Workshop on Peer-to-Peer Systems*, Santa Barbara, CA, Feb. 2006.
[6] K. Ta Chen, C. Y. Huang, P. Huang, C. L. Lei "Quantifying Skype User Satisfaction", *ACM Sigcomm'06*, Pisa, Italy, Sep. 2006.
[7] K. Suh, D. R. Figueiredo, J. Kurose, D. Towsley, "Characterizing and detecting relayed traffic: A case study using Skype.", *IEEE Infocom'06*, Barcelona, Spain, Apr. 2006.
[8] D.Bonfiglio, M.Mellia, M. Meo, D.Rossi, P.Tofanelli, "Revealing Skype Traffic: when randomness plays with you", *ACM Sigcomm'07*, Kyoto, Japan, Aug. 2006.
[9] `http://www.hostip.info`