Spam Detection in IP Telephony

One of the most prominent problems with today’s messaging systems is the high percentage of spam content clogging the systems. The problem is likely to become more serious with the rapidly becoming popular Voice-over-IP (VoIP) technology replacing traditional switch based telephone networks. Spam in Internet Telephony (SPIT) is not only more annoying and disruptive than generic E-Mail spam, but also more expensive to the service provider. The fact that it has to be analysed and filtered in real-time makes the problem more difficult. In this project, we design a SPIT detection server to analyse call feedbacks and calculate spam ratings. We also develop an application for Google Android platform which acts as the link between the user and server.

Spam in Internet Telephony (SPIT) can be defined as unsolicited bulk calls that result in media sessions, where the content delivered to a phone or voice terminal may include voice, images or video. There are several kinds of SPIT, i.e. advertisement, telephone poll and telemarketing. VoIP usage has grown rapidly over the past few years with the introduction of services like Skype, Vonage and VoIP.com. It is estimated that approximately 25% of the people in Europe have abandoned traditional Public Switched Telephone Network (PSTN) service in favour of VoIP. At the same time, it is also attracting a greater number of spammers. This is primarily due to the lower costs per call and ease of opening peering interfaces. It allows the spammer to make automated tools to deliver the bulk messages. Advertisers who flood these services with spam messages cause a huge reduction in the bandwidth and possible failure of the service all together. The load on network resources by SPIT is up to 10 times more as compared to E-Mail spam. Moreover SPIT is potentially more annoying and obtrusive because phone calls happen in real time and require immediate response.

The fundamental criteria for any SPIT protection is that the spam call should be identified before the user’s phone rings. Everytime the phone rings it disturbs the user’s current activity and potentially blocks the receiver’s line and clog server bandwith. A second criteria relates to maintenance of the protection technique. It should be simple and transparent to use, and require minimal configuration at a very low cost. At the same time cost incurred to the spammer should be as high as possible. Ultimately, the number of false positives and false negatives should be as small as possible, preferable even zero. Because each time we make a false deduction the user pays the price, and in case of false positive the price is substantially high.

SPIT possesses several inherent characteristics which make it much more difficult to detect as compared to generic E-Mail spam. The call handling decisions must be made in Real-Time, before the actual session starts i.e. during the signaling/protocol exchange. A legitimate call cannot be deferred by more than a few seconds or redirected to a Voice Mail. Analysing Call Data (media sessions) for identifying SPIT is
impractical, and may also be illegal in some cases. The session data comprises of audio or video signals which are much harder to analyse compared to plain text in case of E-Mails.

In first part of the project, we developed the application for Google Android platform. The application resides on the mobile and serves two main purposes. First, it displays the user a spam rating for every incoming call and on the basis of user settings it can either drop the call, redirect it to Voice Mail or do nothing. Second, it collects feedback from the user about whether the call was spam or not and sends it to our central server.

In the second part, we set up a server to coordinate with all the mobile devices. The server receives feedbacks from the mobile phones and calculates spam ratings for each call. The spam ratings are calculated from a combination of heuristics including the call feedback and network analysis for connection between caller & callee. As a result we have a dynamic database of Spam Ratings which continuously changes itself according to feedback from the user and calling patterns of users.

A major challenge in developing the whole system was to make it secure, robust and deny access to unauthorised users. This was achieved by authenticating all requests using the IMEI (International Mobile Equipment Identity) and phone number of the user. We want to make sure the requests are genuine and sent from a mobile device rather than an automated script. On the application side we tried to make the whole interface as simple and less intrusive as possible, to make it less annoying.

The system is still being developed and improved, so that it can be launched for beta testing soon. Once it is up and running, it will be very interesting to study how well it performs in the real world and how effective it is in curbing spam calls.

Naveen Kumar Sharma
under the guidance of
Dr. Yashar Ganjali
University of Toronto