A novel mechanism for anonymizing GSM calls using a resource based SIP community network[⋆]

Ioannis Psaroudakis, Vasilios Katos, and Pavlos S. Efraimidis

Information Security and Incident Response Unit
Department of Electrical and Computer Engineering
Democritus University of Thrace
University Campus, Xanthi 67100, Greece
{jpsaroud}@duth.gr
{vkatos,pefraimi}@ee.duth.gr
http://isir.ee.duth.gr/

Abstract. Considering the wide spread adoption of smartphones in mobile communications and the well established resource sharing use in the networking community, we present a novel mechanism to achieve anonymity in the Global System for Mobile Communications (GSM). We propose a Voice over Internet Protocol (VoIP) infrastructure using the Session Initiation Protocol (SIP) where a smartphone registers on a SIP Registrar and can start GSM conversation through another smartphone acting as a GSM gateway, by using a SIP Intermediate without an extra cost. The testbed that we developed for empirical evaluation revealed no significant QoS degradation.

Keywords: privacy; SIP; smartphone; GSM anonymity

1 Introduction and motivation

Resource sharing in community networks is a well established concept since the dawn of the Internet. This has recently evolved through peer to peer networking, to grid computing and finally to cloud computing services, as the benefits of the collective paradigm are non disputable.

In the meantime, the wide adoption and commercial success of mobile networks due to the advances of wireless communications has resulted to smartphone being the most preferred device for communicating through a variety of platforms including email, social networking, messaging and so on.

Calls in the Global System for Mobile Communications (GSM) are very well regulated. Users are bound to a mobile number according to a regulatory framework and carriers are obliged to keep logs of their telephony conversations for a period of up to two years (Data Retention Directive 2006/24/EC). Carriers

[⋆] A preliminary version of this work has been presented at the 27th IFIP International Information Security and Privacy Conference, Springer IFIP AICT, Greece, June 2012 offer location based services because they are able to know and track the phone's location. The GSMs encryption A5/1 algorithm is suffering from a number of vulnerabilities and some carriers have even preinstalled rootkits (Carrier IQ [1]) on the smartphones for debugging purposes as they claim. However the lack of privacy is profound as the parties that offer the infrastructure, software, and operating system are sharing information regarding the users location, preferences and behavior.

In this paper we argue that certain privacy goals could be achieved by the active participation and collaboration of a community of users. We focus on the Voice Over Internet Protocol (VoIP) and mobile communications and present a proof of concept for performing telephone calls on a mobile network with caller anonymity. The motivation behind the proposed framework is based on the problem of providing caller anonymity where a caller's GSM provider may be malicious and all other participants and nodes of the infrastructure are honest but curious.

There is a number of examples where such a service would be really useful. Totalitarian regimes and countries with limited civilian rights and such environments call for privacy enhancing technologies, Tor[1] being one of the most popular. Government members or big firm executives are often victims of mobile phone eavesdropping. Soldiers out of approach could form an ad hoc wireless network and one of them acting as the Registrar can help others to communicate through a voice network.

In addition to privacy, a new value added service is created as the participants may also enjoy financial gain due to the (mobile phone) flat rate contract sharing of the particular advantages.

It should be noted that in the context of this paper, caller anonymity relates to the caller id and the call metadata; the underlying audio stream will be susceptible to passive eavesdropping by the callee's provider. This paper is structured as follows. Section 2 presents the related work on which our proposed scheme draws upon. In Section 3 we present the proposed scheme and in Section 4 we report on some preliminary findings after applying parts of the scheme on our testbed. Section 5 presents the conclusions.

2 Related work

In our proposed scheme we make use of the Session Initiation Protocol (SIP) as the underlaying protocol for the VoIP infrastructure. Requirements and specifications for offering caller anonymity over SIP are defined in RFC3323 [2] for three use cases relating to withholding the identity from the intermediary parties, the final destination(s), or both.

Furthermore RFC3325 describes private extensions to the SIP that enable a network of trusted SIP servers to assert the identity of authenticated users, and the application of existing privacy mechanisms to the identity problem.

[1] https://www.torproject.org/

This is achieved by inserting a new header in SIP protocol named P-Preferred-Identity [3]. However as RFC states the use of these extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information which is not our case.

In [5], a finer granularity to the anonymity specifications in a SIP context by distinguishing the communicating intermediaries on the caller or callee providers was added. In our proposed solution, there is a need to further elaborate on this definition as the underlying communication environment involves two types of infrastructures (namely the VoIP and the GSM environment). The principle behind our proposed scheme is similar to that of crowds [4]. However the main difference is that in crowds anonymity is achieved by routing communication randomly within a group of similar users whereas in our proposition we do not allow direct communication between users and traffic is routed through special SIP protocol capable entities.

Quality of Service (QoS) is a critical factor that needs to be considered when designing and deploying any kind of telephony communication. A prevalent QoS feature for telephone communications is the delay [12], both while establishing a session and, most importantly, during the actual session for the voice stream. Other constraints include the guaranteed ordered arrival of the messages and the unambiguity of the service agreements. These parameters affect significantly the choice of the appropriate privacy enhancing technology. In [5] the authors present the main categories of PETs and conclude that a large number of technologies cannot be integrated with a VoIP solution like SIP due to their negative impact on the QoS attributes. For instance, Onion Routing [10] and Mixes [11] exhibit high call delays, whereas Hordes [18], DC-Nets and pMixes [17] may be more suitable but the latter has scalability issues as the underlying computational cost is in $O(n^2)$. In addition, many technologies were not designed or implemented with a view to be applied in VoIP communications (Onion Routing for example) and as such they do not inherently support UDP which makes them suitable only for the call initiation phases. Authors in [6] have proposed the PrivaSIP1 and PrivaSIP2 protocols that are used to hide the Caller and Callee IDs from intermediate untrusted SIP Proxies. They assume that both Caller's and Callee's SIP Registrars have RSA capabilities. They use the public key of the SIP Registrar in order to encrypt partial information in the "From" and the "To" SIP headers respectively. In [7] the authors have extended their work to use AES and elliptic curves. In case of the AES algorithm the key is derived from the user's credentials. Our approach has the same result in the untrusted network and it consumes less computational power as we replace every header with the "Anonymous" keyword except from the "To" header that carries the destination GSM phone number. However authentication between the SIP user agent and the SIP Registrar is considered to lie within a trusted environment. Finally authors in [8] adopt the MIST technique in a SIP environment achieving in simulation low latency responses from their peers but the implementation is tested only under special and limited conditions, such as within a 30 second duration call window. In addition, there is limited literature with respect to the quality of the audio in the RTP stream.

Although users are familiar with the idea of sharing their computer resources, this is not the case when it comes to sharing their smartphones. As new applications are developed phone sharing is expected to be a common issue in the near future. An example of such application is *xycall* [2] which *provides new means to optimize communication in a peer-group and subsequently lower telephone bill in the process.*

3 The proposed scheme

The main idea behind the proposed scheme rests on the assumption that a participant (or smartphone owner) is voluntarily willing to offer her equipment for other users to make calls. This setting leads to two advantages. First, the carrier would not be able to establish the identity of the real caller. Second, there could be no charge at all if the offering person has a flat rate contract with the carrier. Clearly the success of the proposed scheme relies on ease of use, reliability and level of participation in accordance to Metcalfe's Law [13].

The requirements and issues for a practical solution are summarized with the following questions:

1. How can one discover users willing to offer their phones as SIP-GSM relays?
2. How can one discover the call destinations every user can offer, that is, with which providers do they have an flat rate contract?
3. How are the participating users protected by other, malicious participants? In a resource sharing setting there may be a number of attacks aiming to exploit an honest users contract.
4. How do I communicate with them?

Throughout the scheme the following roles and entities are identified:

- *Caller*: This role refers to the main beneficiary of the infrastructure which is the user that wishes to make a call to a user (callee) with a selective preservation of her anonymity. Alice will be caller in our examples.
- *Callee*: The user that accepts a call. Bob will have this role.
- *SIP-to-GSM gateway*: The user that acts as a VoIP to GSM gateway and shares her GSM service for a certain call session instance. In our scheme, Carol will have this role.
- *SIP Registrar*: The registrars maintain the user SIP accounts and act as back-to-back user agents [20]. We assume the trusted entities Registrar A (for Alice) and Registrar C (for Carol).
- *SIP Intermediate*: Act as intermediaries on the communication path providing call routing. We assume a single SIP Intermediate entity in one of the scenarios.

[2] http://www.xycall.com/

- *GSM Carrier*: This role offers the GSM mobile phone service. We assume the entities GSM carrier A, C and B, for Alice, Carol and Bob respectively. GSM Carrier A is assumed to be malicious and all other entities are assumed to be honest but curious.

Definition 1. Honest-But-Curious (HBC): *An honest-but-curious party (adversary) [14] follows the prescribed protocol properly, but may keep intermediate computation results, e.g. messages exchanged, and try to deduce additional information from them other than the protocol result.*

Definition 2. Malicious Model: *A malicious entity has no by default restrictions on what actions it can take; the entity may behave arbitrarily. It may for example submit any value as input to the protocol or even abandon the protocol at any step. See the definition given in [15] or the more detailed treatment in [16].*

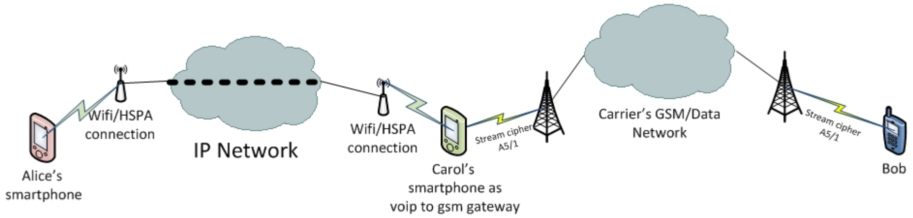


Fig. 1. The basic communication scenario

3.1 The anonymous communication scenario

Alice wants to communicate with Bob using her smartphone whilst maintaining her anonymity from her carrier which is GSM Carrier A and Bobs carrier which is GSM Carrier B and Carols carrier which is GSM Carrier C. More importantly, the GSM carrier of Alice should not learn anything about this phone call.

Alice knows that a community of VoIP and GSM users is willing to help by sharing their phone and credits from their contracts. The easiest way is to communicate with some appropriate member (Carol) of the community by using the Internet infrastructure. Carol's device must be able to communicate with Alice using the Internet through her Wireless Internet (WiFi) or High Speed Packet Access (HSPA) connection and at the same time to call Bob using the GSM connection; that is, Carol has to act as a bridge between these two connections (Fig. 1).

This particular operation fulfilled by Carol (i.e., her smartphone) is a so-called a SIP-to-GSM gateway operation and it is the core function for the service. The operation has to take place without any actions taken from Carol apart from her declaration of consent to lend her resources. This suggests a user registration phase which is outlined later in this section.

We must note that when Alice is accessing the network by a HSPA connection an encrypted tunnel must be used. This is necessary to avoid a side channel attack by Alice 's carrier.

We define the following privacy requirements:

P1 *Caller anonymity in the GSM network.* Alice's identity should be hidden from GSM carriers A, B and C.

P2 *Mutual anonymity between the caller and the gateway.* Alice should not know that her call is routed through Carol and vice versa.

P3 *SIP-to-GSM gateway privacy.* The gateway's personal information, including its contracts and capabilities should only be available to SIP Registrar C and GSM carrier C.

P4 *SIP Registrar privacy.* There should be no leakage of the information maintained by the SIP registrars A and C.

The main entities, the important information items and the scope of each item, that is, which entities have access to each item, are shown in Fig. 2.

Although in principle the caller's anonymity in the GSM environment can be trivially offered due to the apparent "incompatibility" of the two networks, the caller's identity could be discovered from the actual voice stream which Bob's and Alice's GSM carriers B and C have access to. In general terms, this is considered as a probabilistic side channel, since the probability of identifying the caller from the available audio data is not necessarily equal to one. Since audio data under current regulations is not stored by carriers, the disclosure of Alice identity has to take place only during active calls.

The call metadata stored in the carriers' logfiles will not contribute to any evidence revealing Alice's identity. Furthermore, mutual anonymity is also required between the caller and the gateway. Anonymity of the caller is required because in the opposite case if Carol (the gateway) is malicious or a passive eavesdropper or (even worse) belongs to the GSM carrier, then she will have access to both the caller and the callee information. Therefore, P1 depends on P2.

P3 is probably the most important requirement. All information provided by the gateway needs to be protected as in the opposite case a curious participant (e.g. another SIP Registrar) may collect valuable data and generate statistics over the users and their contracts, which then can be used for personal gain. P3 also depends upon P4. Since the SIP Registrar maintains user information, if P4 is not offered, a curious participant may query a particular Registrar and construct aggregate and statistical information about the users hosted by that Registrar.

3.2 User registration

Each end user of the service will have two distinct roles, namely the Caller (which will be using the SIP functionality), or the SIP2GSM gateway mentioned above. We will refer to them as endpoint users of the SIP infrastructure.

Scope Data Item	GSM Carrier A	Alice	Reg A	Intermediate	Reg C	Carol	GSM Carrier C	GSM Carrier B	Bob
GSM carrier A	🟩	🟩							
Alice's Identity	P1	🟩	🟩 P3			P2	P1	P1	🟩
Registrar A		🟩 P3	🟩	🟩					
Intermediate			🟩	🟩	🟩				
Registrar C				🟩	🟩	🟩			
Carol's name (gateway)		P2			🟩 P3	🟩 P3	🟩 P3	🟩	
Carol's capabilities					🟩 P3	🟩 P3	🟩 P3		
GSM Carrier C						🟩	🟩	🟩	🟩
Registrar A Users records			🟩 P4						
Registrar C Users records					🟩 P4				
GSM Carrier B			🟩	🟩	🟩	🟩	🟩	🟩	🟩
Bob's phone number		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Voice data	P1	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Fig. 2. The scope of each information item. Note that GSM Carrier A (apparently) knows Alice but is not aware that she is making a phone call to a GSM phone. We also assume that Honest-but-Curious users will not collaborate/share information. Every green cell indicates that in our solution the corresponding data item (row) is visible to the respective entity (column). The privacy requirements in cells indicate that the corresponding data item should (P3,P4) or not (P1,P2) be visible to the respective entity.

Assume a working system that users want to get access to its services. Endpoint users must first obtain an account from a trusted SIP Registrar. A typical registration process may involve visiting a website run by the SIP Registrar and filling in an on-line application form with the necessary information for the service to operate successfully. This application should consist of the following five sections:

User Registration Application Form

Section A1: "Personal Data"

- Username (e.g. email address) and a password for accessing their account when they sign on and for updating their profile data.
- A valid email address to send a verification email in order to enable the service.
- Credentials for the SIP network. The username and password created here will be used when endpoint users set up their smartphone sip2gsm application along with the SIP client program in order to be authenticated by the SIP Registrar.

Section A2: "Network/Sharing Resources"

- GSM Carrier contract to share.
- UDP port to use for sip2gsm application.

Section A3: "Policy Data"

- Whitelist/blacklist for subscribers that endpoint users wish to or do not allow to be called from their device.
- Time-schedule. A time table of the availability of their resources.
- Max call duration.

Section A4: "Security"

- The endpoint users should have the option to create a certificate signed by the Trusted SIP Registrar Certificate Authority to support Transport Layer Security (TLS) in case that encryption is needed for the SIP signalling or the audio stream.

Section A5: "License Agreement"

- In this section the endpoint user is informed about the service levels and that the application is offered as a public service.

Following the endpoint user registration, the data provided will allow the SIP Registrar to create:

1. A SIP account for the SIP client application.
2. A SIP account for the sip2gsm operation.
3. The outgoing trunk for the specific carrier that is shared.

It is worth noting here the importance of the Section A2 parameters that the user is declaring because on these values relies on the whole operation. Each smartphone establishes two concurrent IP connections with the trusted SIP Registrar. The first connection is used by the SIP client application so as the smartphone is capable to make a call and the second connection is necessary for the sip2gsm application in order to forward the call to the GSM network. Fig. 3.

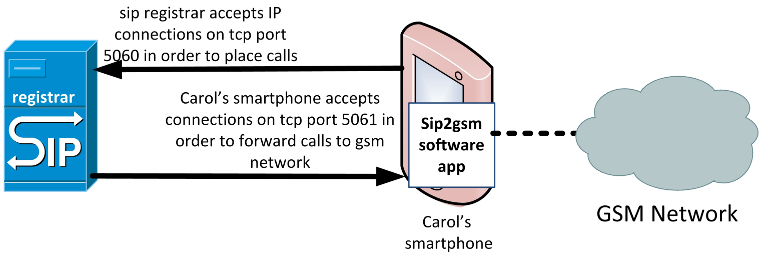

sip registrar accepts IP connections on tcp port 5060 in order to place calls
registrar
SIP
Carol's smartphone accepts connections on tcp port 5061 in order to forward calls to gsm network
Sip2gsm software app
Carol's smartphone
GSM Network

Fig. 3. Two concurrent IP connections for each smartphone.

In addition the SIP Registrar will update the outbound route for the specific carrier with the new trunk member when the endpoint user is in service. This operation will be continuously updated as endpoint users are expected to continuously enter and leave the network.

SIP registrars are assumed to be trusted and to act as agents on behalf of the users. As back-to-back user agents, the registrars operate between the end points of the voice session during the phone calls. The general privacy assumption here is that the user may trust its Registrar but should not be obliged to trust other registrars or SIP Intermediates. It is the user's Registrar's responsibility to protect the user's personal data including her capabilities from curious or even malicious participants who could try to collect statistics on user carrier contract data.

3.3 Trusted SIP Registrar and SIP Intermediates

As noted above a user trusts a SIP Registrar for providing their data and obtaining an account. Every SIP Registrar in turn needs to be affiliated with at least one SIP Intermediate server. The process is described below.

The affiliation is initiated with the SIP Registrar administrator who will provide the following data to the SIP Intermediate server during the application process:

SIP Registrar Application Form

Section R1: "Personal Data"

- Username (the email address of the administrator) and a password for accessing their account when they sign on to update their profile data.
- A valid email address where verification email will be send in order to enable the service.
- Credentials for the SIP network. The username and password created here will be used when administrators build their trunks to the SIP Intermediate server in order to be authenticated by the SIP service.

Section R2: "Network/Sharing Resources"

- GSM Carriers that trusted SIP registrars can route calls to.
- UDP port to use for sip2sip peering.
- Landline numbers that trusted SIP registrars can route calls to.

Section R3: "Policy Data"

- Whitelist/blacklist for subscribers that SIP Registrar does or not accepts calls.
- Time-schedule. A time table of the availability of their resources

Section R4: "security"

- Enable encryption or not (TLS)

Section R5: "License Agreement"

- In this section the SIP Registrar Administrator is informed on the service levels and liabilities of the SIP Intermediate offered as a public service.

Following the data provided by the administrator, the SIP Intermediate will create:

1. A SIP account for SIP Registrar peering.
2. New trunks for the carrier networks that SIP Registrars can route calls to.

Lastly, the SIP Intermediate Server will update the outbound route directory for the specific carriers that the new trunk member can serve. This update operation will be regularly performed as trunks are expected to continuously enter and leave the network. The operation of the outbound route directory of the SIP Intermediate Server is similar to the routing table of a router.

3.4 Baseline case: mutually trusted registrars

We initially setup a testbed consisting of two registrars. In the baseline scenario we assumed that the registrars are mutually trusted in the sense that the gateway's Registrar will have knowledge of the caller's Registrar (but not the caller's ID as there is no reason to disclose this piece of information). This setting is presented in Fig. 4 whereas the corresponding communication messages and sequence are presented in the diagram in Fig. 5.

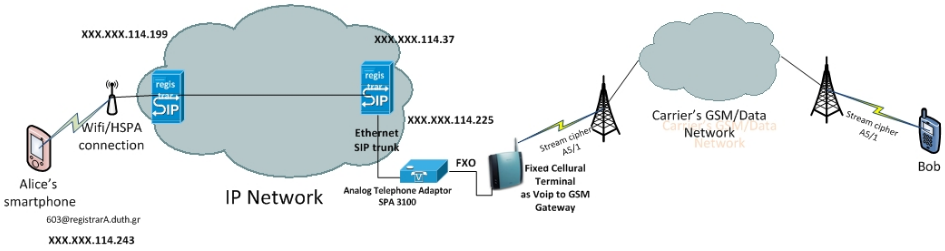


Fig. 4. Mutually trusted registrars

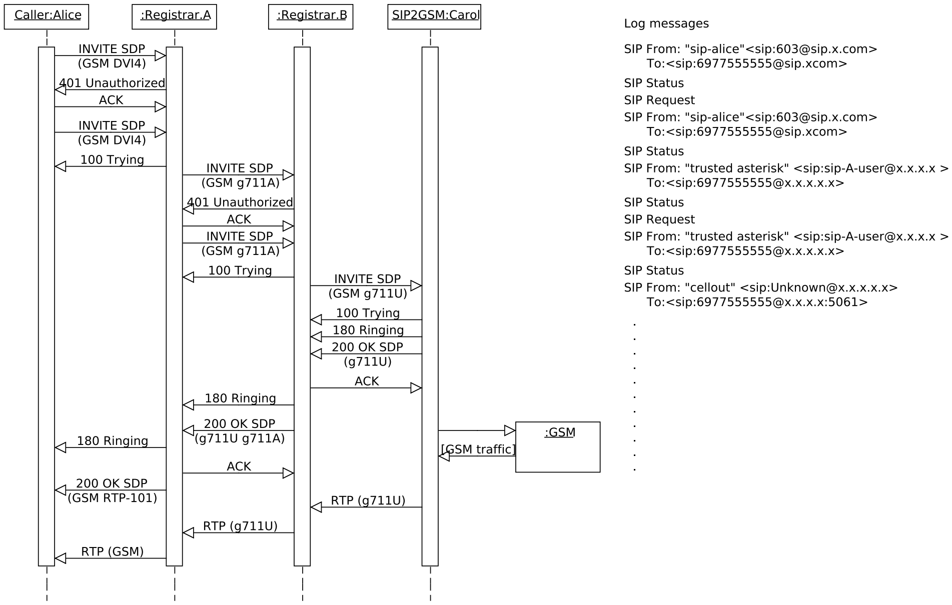
The `401 Unauthorized` message is noteworthy; this is triggered because the first `SIP INVITE` is unauthenticated and is part of the connection process flow. The sequence of two `SIP INVITE` messages can be utilised for intrusion detection purposes, as this pattern describes a legitimate request.

In terms of the stated privacy requirements, the above setting can partially meet P1 through P3. This can be achieved if the capabilities discovery process is executed between the registrars and without disclosing the caller's and gateway's identity. For example, Alice, maintaining a contract with Carrier A wishes to call a user who is with Carrier B. Alice's Registrar will issue a request "`Who has flat rates with carrier B?`" and will receive an answer from Carol's Registrar of a type "`I have a user(s) with a contract with B`". Carol's Registrar could also create a temporary pseudonym of Carol to assist future identification of the resource and speed up the subsequent process steps.

Due to the presence of direct communication between registrars, requirement P4 cannot be met unless some sophisticated cryptographic protocol is used. What follows in the next section is a proposal for achieving Registrar privacy and further strengthening P3.

3.5 Private VoIP to GSM gateway discovery

A fully developed version of our system will have to address additional privacy issues that arise in auxiliary functions of the system. An example is the gateway discovery procedure discussed earlier. If the SIP Registrar A is trusted (as we assumed earlier) then the privacy of Alice is preserved while requesting to use the platform for a call to Bob. Similarly, if the Registrar C of Carol is trusted then Carol can safely advertise her readiness to act as SIP-to-GSM gateway for specific GSM carriers. The above scheme can be further improved by adding a SIP Intermediate server to it. However, in all these cases, privacy relies on assumptions about the participating entities and/or the introduction of a SIP Intermediate. A challenging requirement would be to solve the same problem for Honest-but-Curious or even Malicious entities, by applying advanced cryptographic techniques. For example, in [21] the authors present a cryptographic protocol for privacy-preserving service discovery in ubiquitous computing en-



```
Log messages
SIP From: "sip-alice"<sip:603@sip.x.com>
      To:<sip:6977555555@sip.xcom>
SIP Status
SIP Request
SIP From: "sip-alice"<sip:603@sip.x.com>
      To:<sip:6977555555@sip.xcom>
SIP Status
SIP From: "trusted asterisk" <sip:sip-A-user@x.x.x.x >
      To:<sip:6977555555@x.x.x.x.x>
SIP Status
SIP Request
SIP From: "trusted asterisk" <sip:sip-A-user@x.x.x.x >
      To:<sip:6977555555@x.x.x.x.x>
SIP Status
SIP From: "cellout" <sip:Unknown@x.x.x.x.x>
      To:<sip:6977555555@x.x.x.x:5061>
  .
  .
  .
  .
  .
  .
  .
  .
  .
  .
  .
```

Fig. 5. VoIP to GSM call sequence

vironments. We are currently examining a similar service for the needs of our application.

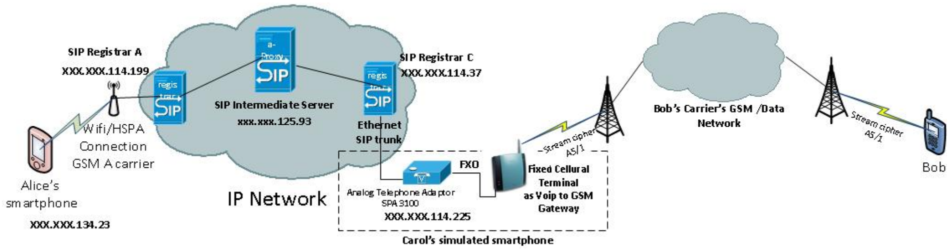


Fig. 6. The testbed environment

3.6 Testbed develpment

We implemented the proposed framework and conducted a series of experiments. We used two CentOS servers with Asterisk [3] software as SIP Registrar entities,

[3] Asterisk is a popular software implementation of a telephone private branch exchange (PBX).

a third Asterisk server as the SIP Intermediate Server and a VoIP Analog Telephony Adaptor (Linksys SPA3000) with Fixed Cellural Terminal from Ericsson as VoIP-to-GSM gateway (Fig. 6) simulating the application to be developed for smartphones. The initial caller (Alice) was an Android smartphone running the CSipSimple SIP application.

The main difference between the new framework and the one we presented in our earlier work [22] is the replacement of the TekSIP Proxy Server with another Asterisk server as SIP Intermediate. This choice gives us the ability to manipulate SIP Headers in order to eliminate information leakage regarding identity and to significantly improve performance.

The RFC3323 [2] states that SIP entities (intermediates or proxies) add headers on their own that they could reveal information about the originator of a message; for example, a Via[4] header might reveal the service provider through whom the user sends requests, which might in turn strongly hint at the user's identity to some recipients. RFC states also that the following SIP headers, when generated by a user agent, can directly or indirectly reveal identity information about the originator of a message: From, Contact, Reply-To, Via, Call-Info, User-Agent, Organization, Server, Subject, Call-ID, In-Reply-To and Warning. The same may occur during the authentication procedure.

Since we use trusted SIP registrars that act as back to back user agents it is safer to strip off this kind of information before forwarding the message to SIP intermadiate server than expecting from each user agent not to reveal such information. In particular special modifications were taken into the SIP Registrars and the SIP Intermediate Server's configurations files to accomplish that.

For the data collection we used a 2960G Gigabit Cisco switch with port monitoring enabled. For analyzing the SIP negotiation (Fig. 7) we used the voip telephony analysis tool from Wireshark software[5].

From the call flow and the SIP request methods it can be seen that Bob is unaware of the initial caller. None of the entities has full knowledge of the path of communication. If we look carefully at SIP headers of the second (authorized) SIP INVITE request in (Fig. 7) identity information regarding Alice has been revealed. Below is the full listing of the SIP INVITE request.

[4] The Via header is used to record the SIP route taken by a request and is used to route a response back to the originator.

[5] Wireshark is a free and open-source network packet analyzer.

```
Session Initiation Protocol
    Request-Line: INVITE SIP:6977xxxxxx@xxx.xxx.duth.gr SIP/2.0
        Method: INVITE
        Request-URI: SIP:6977xxxxxx@xxx.xxx.duth.gr
            Request-URI User Part: 6977xxxxxx
            Request-URI Host Part: xxx.xxx.duth.gr
        [Resent Packet: False]
    Message Header
        Via: SIP/2.0/UDP xxx.xxx.134.23:60500;rport;
branch=z9hG4bKPjMkNs9jzvJ2NFDbVYcl86o2MsngtkuRrH
            Transport: UDP
            Sent-by Address: xxx.xxx.134.23
            Sent-by port: 60500
            RPort: rport
            Branch: z9hG4bKPjMkNs9jzvJ2NFDbVYcl86o2MsngtkuRrH
   Max-Forwards: 70
   From: <SIP:604@xxx.xxx.duth.gr>;tag=KmMGFHZqxgOvEiItn-JEkU47eyXhqmzq
            SIP from address: SIP:604@xxx.xxx.duth.gr
                SIP from address User Part: 604
                SIP from address Host Part: xxx.xxx.duth.gr
            SIP tag: KmMGFHZqxgOvEiItn-JEkU47eyXhqmzq
        To: <SIP:6977xxxxxx@xxx.xxx.duth.gr>
            SIP to address: SIP:6977xxxxxx@xxx.xxx.duth.gr
                SIP to address User Part: 6977xxxxxx
                SIP to address Host Part: xxx.xxx.duth.gr
        Contact: <SIP:604@xxx.xxx.134.23:60500;ob>
            Contact-URI: SIP:604@xxx.xxx.134.23:60500;ob
                Contactt-URI User Part: 604
                Contact-URI Host Part: xxx.xxx.134.23
            ... ommitted for brevity
            User-Agent: CSipSimple r1108 / E10i
        Authorization: Digest username="604",  realm="Asterisk",
nonce="1be6b04e",  uri="SIP:6977xxxxxx@xxx.xxx.duth.gr",
response="cbb7187f375ee94ec625cae946c4be41", algorithm=MD5
            Authentication Scheme: Digest
            username="604"
           realm="Asterisk"
            nonce="1be6b04e"
            uri="SIP:6977xxxxxx@xxx.xxx.duth.gr"
            response="cbb7187f375ee94ec625cae946c4be41"
            algorithm=MD5
        Content-Type: application/sdp
        Content-Length: 367
    Message Body
        Session Description Protocol
            Session Description Protocol Version (v): 0
            Owner/Creator, Session Id (o): - 3551550501 3551550501
IN IP4 xxx.xxx.134.23
                Owner Username: -
                Session ID: 3551550501
                Session Version: 3551550501
                Owner Network Type: IN
                Owner Address Type: IP4
                Owner Address: xxx.xxx.134.23
            Session Name (s): pjmedia
            Connection Information (c): IN IP4 xxx.xxx.134.23
                Connection Network Type: IN
                Connection Address Type: IP4
                Connection Address: xxx.xxx.134.23, lines ommitted.
```

It is worth mentioning that we have three major disclosures regarding Alice. We can learn the username and the userid that she uses when registering to Registrar A which is “604”. Both dataitems are reported in several fields in many SIP headers but especially in *Authorization: Digest username=“604”*. We can also learn the application she is using to make phone calls. This information is in header *User-Agent: CSipSimple r1108 / E10i-7*. The name of the application is *CSipSimple* with revision r1108. Even more interesting is the fact that we can learn the make and model number of smartphone *E10i-7* that Alice is using. That model number leads us to the commercial name “Sony Ericsson Xperia X10 mini”. From Session Description Protocol (SDP) and Session Name header we can learn that the application is using the “pjmedia”[6] media stack for the audio stream. Finally from the Authorization header and the realm value we can learn that Alice’s Registrar is based on Asterisk PBX software.

We proceeded to the appropriate modifications in Registrar’s A configuration so as to block any information leakage regarding Alice and the server itself. All packets that are sent from Registrar A to the SIP Intermediate are sanitized of sensitive information. Even better all possible values that can reveal identity information has been removed or replaced with “Anonymous” keyword or “anonymous.invalid” domain as RFC 3323 suggests. This can be seen in detail in the following listing which refers to the SIP INVITE method from Registrar A to SIP Intermediate.

[6] http://www.pjsip.org/pjmedia/docs/html/

```
Session Initiation Protocol
    Request-Line: INVITE SIP:6977xxxxxx@xxx.xxx.125.93 SIP/2.0
        Method: INVITE
        Request-URI: SIP:6977xxxxxx@xxx.xxx.125.93
            Request-URI User Part: 6977xxxxxx
            Request-URI Host Part: xxx.xxx.125.93
        [Resent Packet: False]
    Message Header
        Via: SIP/2.0/UDP xxx.xxx.114.199:5060;branch=z9hG4bK7f15f6cb
            Transport: UDP
            Sent-by Address: xxx.xxx.114.199
            Sent-by port: 5060
            Branch: z9hG4bK7f15f6cb
        Max-Forwards: 70
        From: "Anonymous" <SIP:Anonymous@anonymous.invalid>;tag=as6fe34fdf
            SIP Display info: "Anonymous"
            SIP from address: SIP:Anonymous@anonymous.invalid
                SIP from address User Part: Anonymous
                SIP from address Host Part: anonymous.invalid
            SIP tag: as6fe34fdf
        To: <SIP:6977xxxxxx@xxx.xxx.125.93>
            SIP to address: SIP:6977xxxxxx@xxx.xxx.125.93
                SIP to address User Part: 6977xxxxxx
                SIP to address Host Part: xxx.xxx.125.93
        Contact: <SIP:Anonymous@xxx.xxx.114.199:5060>
            Contact-URI: SIP:Anonymous@xxx.xxx.114.199:5060
                Contactt-URI User Part: Anonymous
                Contact-URI Host Part: xxx.xxx.114.199
                Contact-URI Host Port: 5060
        Call-ID: 10362e2467bc0bfc77e2a11d1a39c048@anonymous.invalid
        CSeq: 102 INVITE
            Sequence Number: 102
            Method: INVITE
        User-Agent: Anonymous
        Date: Tue, 17 Jul 2012 21:48:23 GMT
        Allow: ... ommitted for brevity
        Session Description Protocol
            Session Description Protocol Version (v): 0
       Owner/Creator, Session Id (o): Anonymous 372877586 372877586
IN IP4 xxx.xxx.114.199
```

```
              Owner Username: Anonymous
              Session ID: 372877586
              Session Version: 372877586
              Owner Network Type: IN
              Owner Address Type: IP4
              Owner Address: xxx.xxx.114.199
Session Name (s): Anonymous
          Connection Information (c): IN IP4 xxx.xxx.114.199
              Connection Network Type: IN
              Connection Address Type: IP4
              Connection Address: xxx.xxx.114.199
          Bandwidth Information (b): .... ommitted for brevity
```

Alike SIP Invite requests are produced from SIP Intermediate Server as well as Registrar C.

3.7 Performance evaluation

Telephony applications require real time audio streaming and are tightly coupled with QoS network parameters. We therefore need to investigate whether the proposed solution with the added security controls will not have negative impact on the user acceptance.

We performed a stress test to our framework with varying number of concurrent connections using the sipp[7] application. We ran a number of incremental concurrent calls with each call having duration of 20 secs. The tests stopped when we reached the total number of 100 calls. From the results (Fig. 8) in can be seen that the call on the SIP side, with one SIP Intermediate the majority of the calls can be established within a period of 400 ms wich is less than the 500 ms delay (Fig. 9) we achieved in the previous testbed [22]. It is noteworthy that it was now possible to reach the number of 60 concurrent (in previous test we reached 50 concurrent) calls before the system started dropping calls at 10 percent rate.

In all experiments the SIP transaction delay compared to the GSM call establishment delay which is in the order of 8-12 seconds, is insignificant.

In the following graphs we can see the resources impact of such SIP infrastructure to the computer system that hosted Registrar A. It is very clear that the proposed scheme is mainly CPU intensive (Fig. 10) while disk (Fig. 11), network (Fig. 13) and memory (Fig. 12) usage is less affected.

4 Concluding remarks and areas for future research

We have described a framework for providing caller anonymity from their GSM carriers by utilizing a resource based community of VoIP infrastructure that

[7] http://sipp.sourceforge.net/. SIPp is a free Open Source test tool / traffic generator for the SIP protocol.

used SIP as a means to identify the issues and explore possible design and implementation alternatives. Following our empirical investigation, we concluded that adding such an infrastructure to a GSM network will not cause any significant delays in the call establishment, as the bottleneck remains on the GSM side.

Currently, one of the weaknesses the proposed framework has is the ability to perform eavesdropping on the SIP network since it lacks encryption. This ongoing area of research is twofold requiring effective encryption algorithms but also suitable ones in terms of network efficiency, systems load and quality of service.

Another area of research is in the development of a protocol so that each affiliated Registrar advertises its network routing capabilities to the affiliated SIP Intermediate in a dynamic way. Framework parameters must be tuned accordingly such as registration intervals, audio codecs to be used and SIP OPTIONS method update interval to succeed in optimizing performance.

This community based resource scheme can be expanded with resources such home PSTN lines with flat rates or even home wireless access points. Accountability issues may arise with large number of community members offering their resources and mechanisms such as SIPA+ [23] may apply.

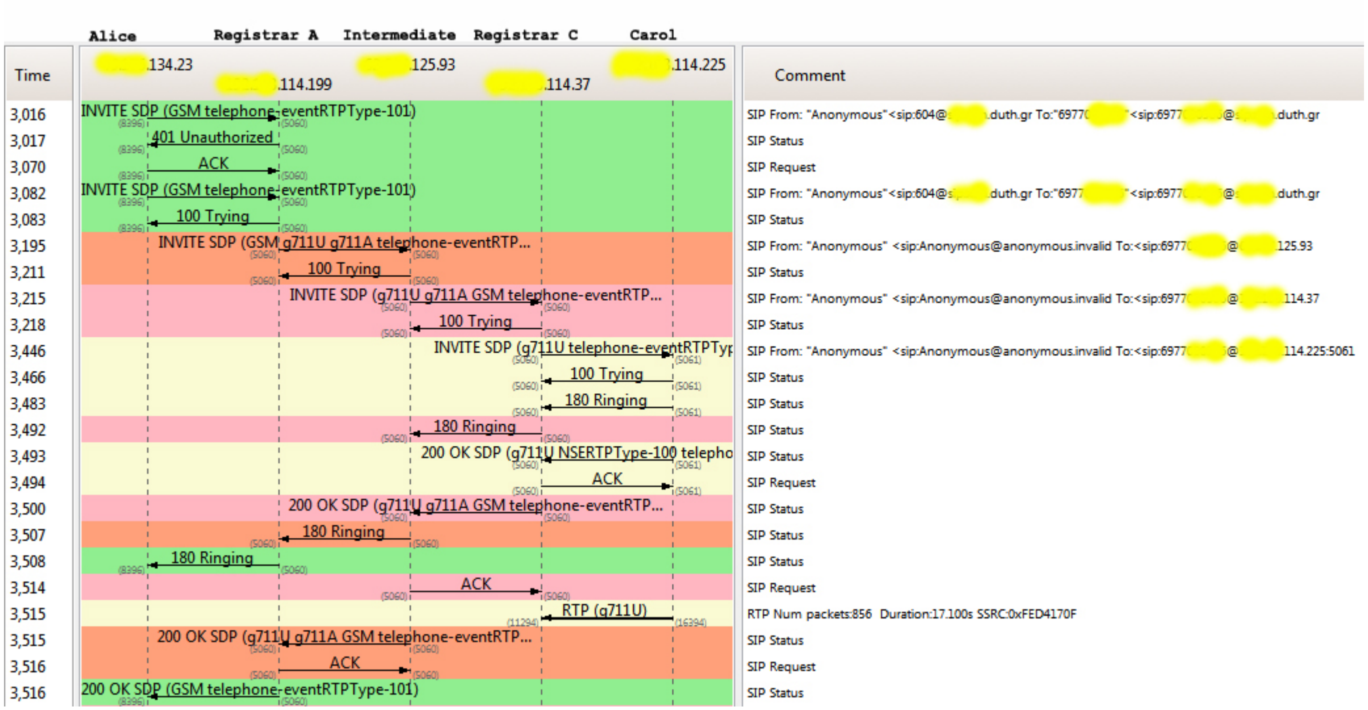
As this proposed solution is defined over a novel configuration of a heterogeneous network, further security analysis of relevant threat vectors and corresponding countermeasures must be conducted. For example, a VoIP bot running on the proposed infrastructure could make excessive resource allocation and as such an antispam over Internet Telephony mechanism must be deployed [19]. Lastly, legal issues must be looked into when offering such a service in public and their compliance to the respective legislation and the related directives like the Data Protection Directive (95/46/EC), the ePrivacy Directive (2002/58/EC), the regulatory framework on electronics communications by the Citizen's Rights Directive (2009/136/EC) and finally the Data Retention Directive (2006/24/EC).

Acknowledgments This work was performed in the framework of and partially funded by the GSRT/CO-OPERATION/SPHINX Project (09SYN-72-419) (http://sphinx.vtrip.net)

References

1. Eckhart T.: Carrier IQ. `http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/` (2011)
2. Peterson, J.: A Privacy Mechanism for the Session Initiation Protocol (SIP). `http://cabernet.tools.ietf.org/html/rfc3323` (2002)
3. C. Jennings, J. Peterson, M. Watson: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks. `http://www.ietf.org/rfc/rfc3325.txt` (2002)
4. Reiter, M., Rubin, A.: Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1(1), 66–92 (1998).

5. Kazatzopoulos, L., Delakouridis, C., Marias, G.F.: Providing anonymity services in SIP. In: 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (2008)
6. Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, PrivaSIP: Ad-hoc identity privacy in SIP, Computer Standards and Interfaces, Volume 33, Issue 3, pp. 301–314 (2011)
7. Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, Elisavet Konstantinou, A framework for identity privacy in SIP, Journal of Network and Computer Applications, pp. 16–28 (2010)
8. Iraklis Leontiadis, Constantinos Delakouridis, Leonidas Kazatzopoulos, and Giannis F. Marias. 2012. ANOSIP: anonymizing the SIP protocol. In Proceedings of the First Workshop on Measurement, Privacy, and Mobility, New York (2012)
9. Khavari, K., Tizghadam, A., Fadaie, F., Abji, N., Farha, R.: Unstructured Peer-to-Peer Session over IP using SIP. In: 2006 IEEE International Performance Computing and Communications Conference, pp. 441–448 (2006)
10. Reed, M G, Syverson, P F, Goldschlag, D M.:Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications. 16(4), 482–494 (1998)
11. Chaum, D. L.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90 (1981)
12. Stier, M., Eick, E., Koerner, E.: A Practical Approach to SIP, QoS and AAA Integration. Integration The VLSI Journal (2006)
13. Metcalfe, R.: Metcalfe's Law. IEEE Spectrum, 17(40), 53 (1995)
14. A. Acquisti and S. Gritzalis and C. Lambrinoudakis and S. De Capitani di Vimercati", Digital privacy, Auerbach Publications, Taylor & Francis Group, 2008
15. Kissner, Lea and Song, Dawn, Privacy-Preserving Set Operations, Advances in Cryptology - CRYPTO '05, Lecture Notes in Computer Science, Shoup, Victor, Springer Berlin / Heidelberg, pp 241-257, volume 3621, 2005
16. Goldreich, O., The Foundations of Cryptography, Cambridge University Press, 2004
17. Melchor, C. A., Deswarte, Y.: From DC-Nets to pMIXes: Multiple Variants for Anonymous Communications. In: Fifth IEEE International Symposium on Network Computing and Applications, IEEE Computer Society Washington, DC, USA pp.163–172 (2006)
18. Levine, B. N., Shields, C.: Hordes: A multicast-based protocol for anonymity. Journal of Computer Security, 10(3), 213–240 (2002)
19. Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., Ehlert, S.: SPIDER: A platform for managing SIP-based Spam over Internet Telephony (SPIT). Journal of Computer Security 19(5): 835–867 (2011)
20. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: SIP: Session Initiation Protocol. RFC 3261, http://tools.ietf.org/html/rfc3261 (2002)
21. Kim, J., Baek, J., Kim, K., Zhou, J.: A privacy-preserving secure service discovery protocol for ubiquitous computing environments. EuroPKI 2010, 45–60 (2011)
22. Psaroudakis I., Katos V., Efraimidis P.: A framework for anonymizing GSM calls over a smartphone VoIP network. Proc. of the 27th IFIP International Information Security and Privacy Conference, Springer IFIP AICT, Greece, June 2012, pp. 543-548.
23. Alexandros Tsakountakis, Georgios Kambourakis, Stefanos Gritzalis:SIPA: generic and secure accounting for SIP, Security and Communication Networks, Volume 5, Issue 9, pages 1006–1027, September 2012.



Time		Comment
3,016	INVITE SDP (GSM telephone-eventRTPType-101)	SIP From: "Anonymous"<sip:604@[redacted].duth.gr To:"6977[redacted]"<sip:6977[redacted]@[redacted].duth.gr
3,017	401 Unauthorized	SIP Status
3,070	ACK	SIP Request
3,082	INVITE SDP (GSM telephone-eventRTPType-101)	SIP From: "Anonymous"<sip:604@[redacted].duth.gr To:"6977[redacted]"<sip:6977[redacted]@[redacted].duth.gr
3,083	100 Trying	SIP Status
3,195	INVITE SDP (GSM g711U g711A telephone-eventRTP...	SIP From: "Anonymous" <sip:Anonymous@anonymous.invalid To:<sip:6977[redacted]@[redacted]125.93
3,211	100 Trying	SIP Status
3,215	INVITE SDP (g711U g711A GSM telephone-eventRTP...	SIP From: "Anonymous" <sip:Anonymous@anonymous.invalid To:<sip:6977[redacted]@[redacted]114.37
3,218	100 Trying	SIP Status
3,446	INVITE SDP (g711U telephone-eventRTPTyp	SIP From: "Anonymous" <sip:Anonymous@anonymous.invalid To:<sip:6977[redacted]@[redacted]114.225:5061
3,466	100 Trying	SIP Status
3,483	180 Ringing	SIP Status
3,492	180 Ringing	SIP Status
3,493	200 OK SDP (g711U NSERTPType-100 telepho	SIP Status
3,494	ACK	SIP Request
3,500	200 OK SDP (g711U g711A GSM telephone-eventRTP...	SIP Status
3,507	180 Ringing	SIP Status
3,508	180 Ringing	SIP Status
3,514	ACK	SIP Request
3,515	RTP (g711U)	RTP Num packets:856 Duration:17.100s SSRC:0xFED4170F
3,515	200 OK SDP (g711U g711A GSM telephone-eventRTP...	SIP Status
3,516	ACK	SIP Request
3,516	200 OK SDP (GSM telephone-eventRTPType-101)	SIP Status

Fig. 7. The anonymised SIP flow

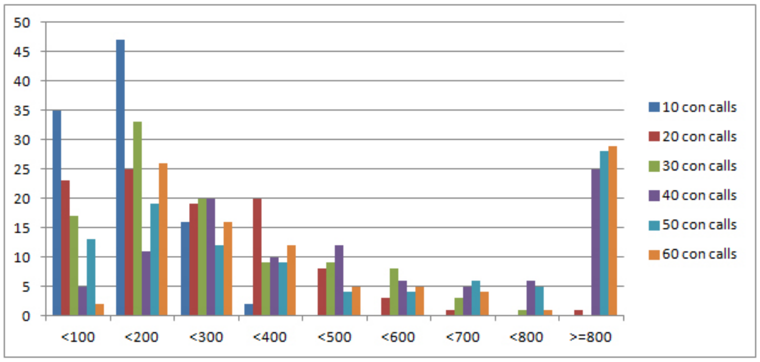


Fig. 8. Response Time Repartition for 100 calls using Asterisk as SIP Intermediate

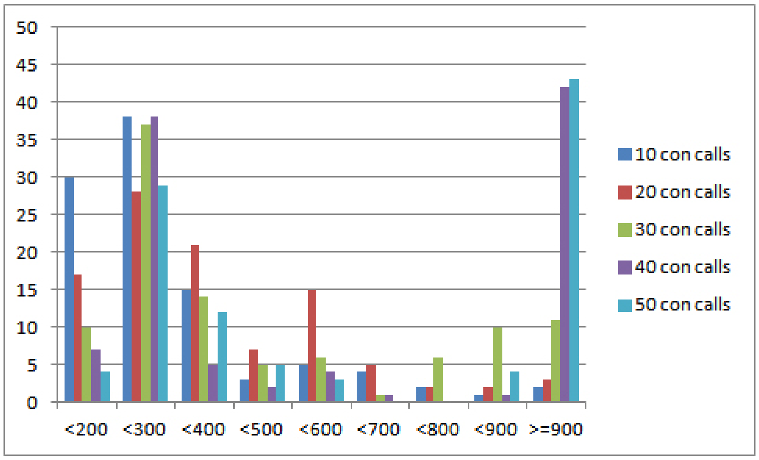


Fig. 9. Response Time Repartition for 100 calls using TekSIP Proxy

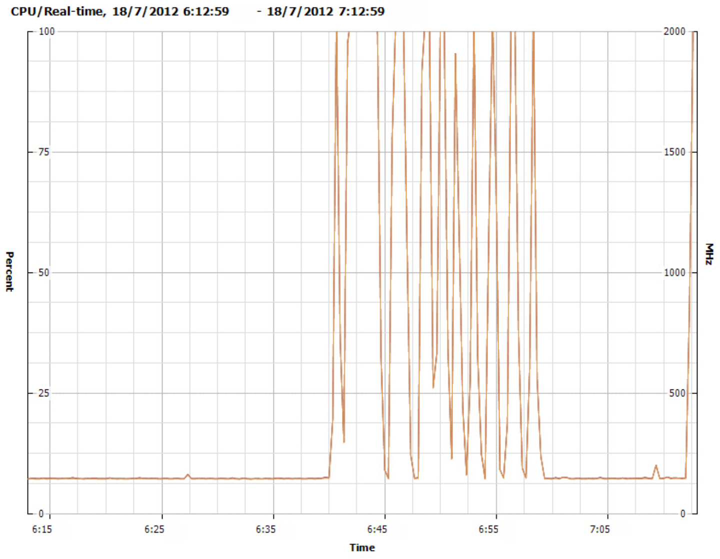


Fig. 10. Registar A - Very significant increase in CPU utilization during stress tests

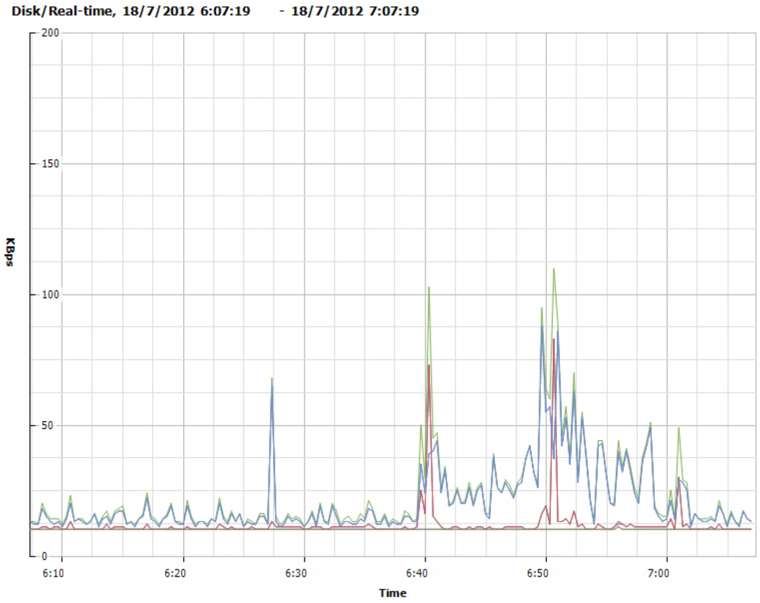
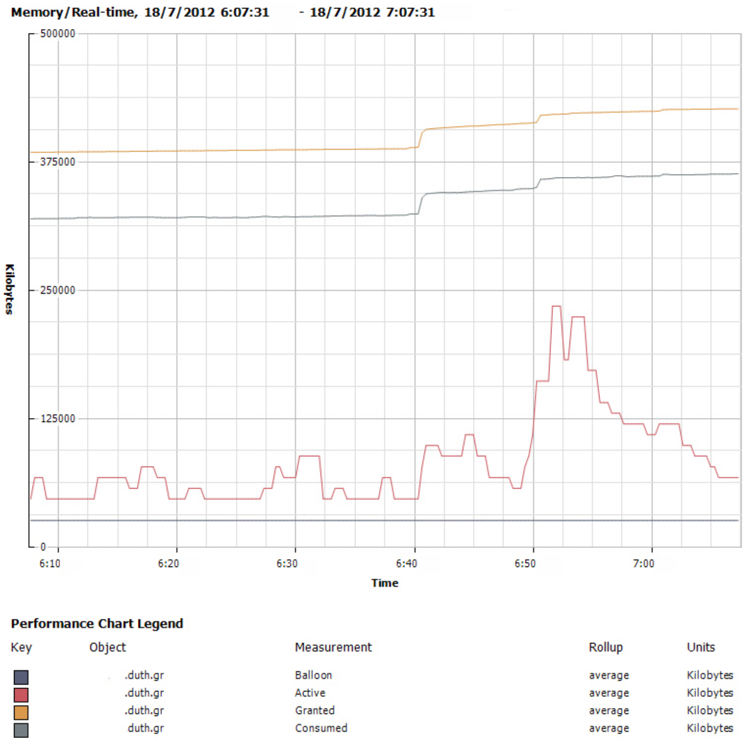


Fig. 11. Registar A - Small increase in disk usage during stress tests



Performance Chart Legend

Key	Object	Measurement	Rollup	Units
■	.duth.gr	Balloon	average	Kilobytes
🟥	.duth.gr	Active	average	Kilobytes
🟧	.duth.gr	Granted	average	Kilobytes
■	duth.gr	Consumed	average	Kilobytes

Fig. 12. Registar A - Small increase in memory usage during tests

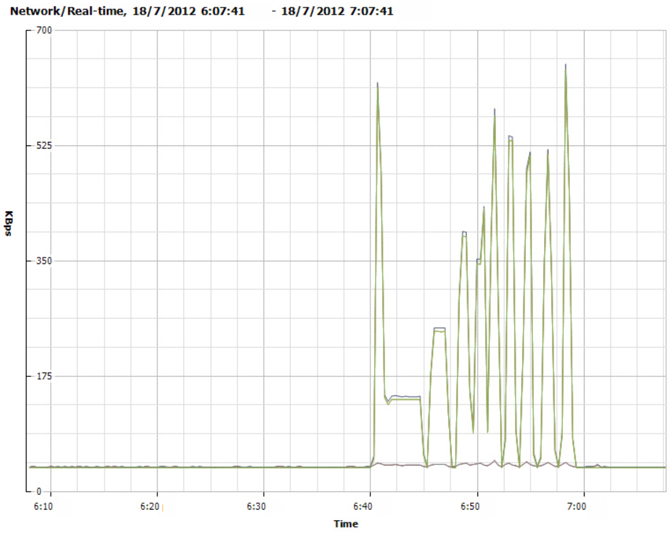


Fig. 13. Registar A - Significant increase in network utilization during stress tests