Towards Anonymous Mobile Community Services

Konstantinos P. Demestichas[1,*], Evgenia F. Adamopoulou[1], John G. Markoulidakis[2], and Michael E. Theologou[1]

[1] *School of Electrical and Computer Engineering, National Technical University of Athens*
9 Iroon Polytechniou Str., Zographou GR-157 73, Athens, Greece

[2] *Vodafone-Panafon Greece, R&D Department*
1-3 Tzavella Str., Halandri GR-152 31, Greece

***Abstract*--In the current market conditions, network operators are in search of novel value-added services that will increase their revenue. This paper introduces the innovative concept of Anonymous Mobile Community (AMC) services and thoroughly defines and describes a robust platform targeted for their deployment. AMC services take advantage of the terminals' capabilities to collect information and deliver it to the network. In this context, terminals are enabled to form communities that serve as sources of information. In these communities, the anonymity and privacy of the end-users are respected and guarded. Several examples of promising AMC services are presented and categorized. An indicative example application is the provision of real-time information regarding road-traffic conditions, based on the location and speed of mobile terminals. A system aiming at the provision of diverse AMC services is proposed, and its requirements, architecture and functionality are described in detail. The related scalability issues and business models are carefully outlined, and a use case scenario as well as trial results are presented.**

***Index Terms*--Anonymity and Privacy, Mobile Value-Added Services, Terminal-Collected Data, User Communities.**

1 Introduction

In the Beyond 3G (B3G) scenery, network operators strive to increase their networks' usage as well as their revenues. This is especially true for those operators that invested significant funds in order to acquire a 3G license, without achieving a complete payoff within the expected timeline. To that end, they are keen on introducing a great number of value-added services, with a view to generating additional income. At the same time, in today's complex social environment, users need to learn and access various kinds of information on a regular basis.

By combining these two trends, a whole new set of innovative value-added services that bring

Manuscript received November 21, 2007.
* Corresponding author. Tel. +30 210 772 1493.
E-mail addresses: cdemest@cn.ntua.gr, eadam@cn.ntua.gr, Yannis.Markoulidakis@vodafone.com, theolog@cs.ntua.gr.

information closer to the end-user, while ensuring in parallel his anonymity, can be defined and deployed. In this paper, a novel group of promising services, called *Anonymous Mobile Community (AMC) services*, together with a system capable of delivering them to the end-user, are presented.

An AMC is a group of terminals that, by definition, has the following characteristics:

- *Community*: The terminals' users are willing to cooperate with one another and share information about a common purpose.
- *Mobility*: The users are mobile, which enables the dynamic collection of information from locations of interest.
- *Anonymity*: Information exchange is done anonymously, respecting the users' privacy.

AMC services are services that rely on the formation of AMCs. Their basic concept lies in (a) allowing the end-users to form cooperative communities, and (b) exploiting the capability of mobile terminals to collect information and deliver it to the network (whenever requested) for further exploitation. Two types of information can be collected: (i) manually produced information (i.e., the users' textual input), and (ii) automatically generated information, such as a terminal's location, speed, etc. The second case is of greater interest, since it enables the transparent and unobtrusive provision of several AMC services (e.g., road-traffic information service).

Hence, in a typical AMC service delivery process, a terminal can request for impersonalized information that resides in a community of terminals. The network can receive this request, acknowledge it, and query the appropriate community of terminals, in order to collect the necessary data, process them, and produce a response to the requesting terminal.

A crucial point is that the extraction of information from the community of terminals must

respect user anonymity and privacy, making the users more eager to participate in communities and exchange information. This requirement imposes that the collected data are not associated with the identity of the user from whom they have been gathered. Anonymity is also desirable for the requesting user, which means that a user must be able to make a service request without exposing his identity. An initial approach for the AMC system's functional architecture is given in Figure 1(a). A thorough approach can be found in Section 5.

Figure 1(b) depicts the AMC functional reference model, according to which the AMC system's functionality is organized into the following layers:

- *Data Collection Layer*: This layer is responsible for collecting the required data and presenting them to the Service Enabling Layer. The AMC-enabled terminals monitor their environment, as well as their own status (e.g., location), and are able to respond to appropriate queries. The responses are then aggregated at the network side. The following is an indicative list of parameters that can be retrieved from current mobile terminals:
    - Location: this may correspond either to a set of network-related measurements (received signal level from neighboring cells) or to GPS-positioning information (if a GPS receiver is present), which is by far more accurate.
    - Velocity (through GPS)
    - Time (timestamp)
    - Perceived signal strength
    - Temperature (retrieved either from the battery's sensor or from an integrated temperature sensor)
    - User input (i.e., a text response-message composed by the user)

- Binary or text file

- *Service Enabling Layer*: This layer enables diverse applications to access the data provided by the Data Collection Layer in a consistent and efficient manner. By separating this layer from the Applications Layer, complex services can be developed more easily, since the Service Enabling Layer provides a level of abstraction from the data extraction procedures.
- *Applications Layer*: This layer caters to providing specific services to the end-users. The same set of data can be processed in different ways, with a view to offering different services.

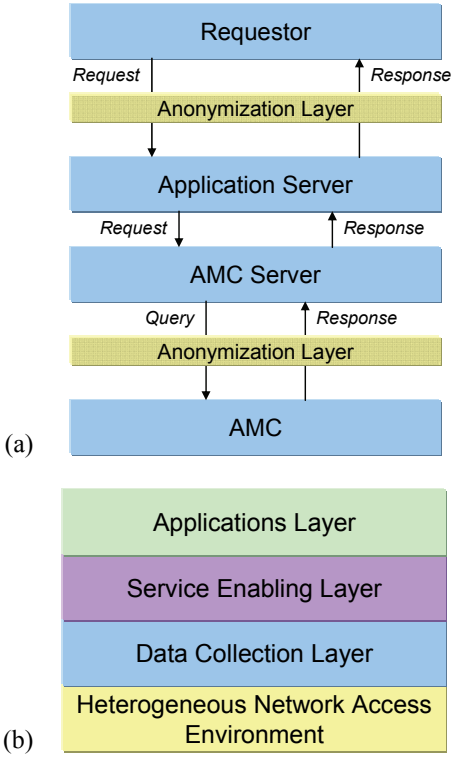

Figure 1: (a) Simplified AMC functional architecture; (b) AMC reference model

The remainder of this paper is structured as follows: Section 2 outlines some interesting related work that can be found in the literature. Section 3 presents a set of potential AMC services and

classifies them according to specific criteria. Section 0 deals with the basic requirements that an AMC system has to fulfill. Section 5 offers an in depth description of the proposed AMC system's architecture and functionality. The architecture's most essential components are detailed, and some significant functional aspects are considered. Section 6 copes with scalability issues, while Section 7 refers to appropriate business models that can be employed for the successful deployment of AMC services. Section 8 illustrates a representative use case scenario along with the corresponding information flow. Section 9 presents some significant trial results. Finally, Section 10 concludes the paper, making references to future work.

2 Related Work

In today's market, a considerable number of mobile value-added services have been introduced, including the purchase of ring-tones, wallpapers, games and videos, chatting, prize competitions, informative services, such as live scores, and so forth. A relatively new area of value-added services is that of location-based services (LBSs) [3][8][15]. User and fleet tracking, navigation, location-based advertising and billing are indicative examples of this advanced type of services [8]. Although location inference also plays an integral part in AMC services, the latter are more innovative compared to conventional LBSs, in terms of enabling user cooperation and ensuring user anonymity.

The formation of virtual communities firstly appeared as a phenomenon in the Internet. Internet users are keen on creating groups and interacting with each other. They create forums, help-desks, blogs and relay-chat hubs, where they exchange opinions and information. Virtual communities can also affect e-commerce. In [10], a number of significant issues are addressed by relevant papers, including ways in which community members contribute value in the form of content, reviews and recommendations [2], ways in which a community may influence product

development [9], business models that integrate communities' influential role [7][9], motivations for participating in communities [12], and leisure time coordination for groups of mobile users [13]. The majority of the above-mentioned contributions are Internet-oriented. Even in cases where mobility is a possibility, there is lack of an appropriate framework capable of exploiting terminal-collected data, ensuring anonymity and integrating several diverse services under a common umbrella.

The issue of anonymity has also emerged from Internet-based communications. As malicious parties that intend to harm user data integrity and track user habits grow in number, solutions that provide a degree of safety and anonymity have appeared. Most of these solutions are targeted for web browsing, such as the Anonymizer [1] and SafeWeb [14] products, but location privacy, as well as database security solutions, exist as well (see [11] and references therein). An interesting class of anonymization approaches, such as the one presented in [11], aims at reducing the accuracy of sensitive data (e.g., location estimations), in order to render them practically anonymous. Such approaches can complement the proposed AMC framework, with a view to further enhancing anonymity and privacy (also see Section 5.8).

3 AMC SERVICES – CLASSIFICATION

The formation of an AMC can be based on different criteria, such as the proximity of users to a certain area, the sharing of same interests or even same characteristics, including age, nationality, gender, profession, etc. The services provided through the formation of AMCs may vary in both their general scope and their specific attributes. However, they can all be provisioned through the same mechanism.

The categorization of the AMC services can rely on a number of different characteristics:

- *Triggering Type*: The provision of an AMC service may either be event-based or user-

triggered. Event-based triggering involves context-awareness, which implies that when a specific situation occurs or a specific requirement or condition is met (e.g., day of week, time of day, location) the service is automatically provided, without the user's intervention. A user-triggered case is exactly the opposite, and involves the explicit triggering of the service from the user's part.

- *Response Type*: The response from each queried AMC member, within the context of a specific AMC service, may either involve the member's interaction or not. In the first case, the queried user has to explicitly produce a response for the query (e.g., by answering a question via an SMS). In the second case, the response is generated automatically from the software modules on his mobile terminal.
- *Content Creation Mechanism*: This classification refers to the mechanism applied for the creation of the exchanged content. Two different cases can be distinguished, namely content creation with user interaction or automatically. In the first case, the user explicitly creates the content that is to be shared among the AMC members, (e.g., by stating his opinion, or composing and publishing an article), whereas in the second case the content is automatically created by the terminal's monitoring modules (e.g., positioning monitoring, received signal strength monitoring).
- *Real-time/Non real-time provisioning*: This classification refers to the time period that the content is created. In detail, the content may be formed at the time of the request, or it may have been formed some time in the past and reside in a database.

Table I presents a concise description of potential AMC services. For instance, the 'Clubbing Information' AMC service enables users who are interested in clubbing to get informed about the quality and popularity of clubs. Some of the queries that a service requestor may issue are the

following:

- Which is the most popular club at this moment? I.e., where has the majority of the clubbing community members gathered?
- Which are the most popular clubs for the past week/month? This can automatically be calculated based on the AMC members' locations and time spent in each location, during the past week/month.
- What do the other community members think about club A?
- What is the average grade of club A for the past two weeks?

Table II depicts the characteristics of each of the services presented in Table I. The services of Table I represent some indicative examples; nonetheless, the possibilities are endless, and the deployment of even more services is feasible through the exploitation of the proposed AMC system.

TABLE I: DESCRIPTION OF POTENTIAL AMC SERVICES

No.	Service	Description
1	Traffic Information	Informs a user about the current traffic conditions in an area of his choice. The information is derived from the location and velocity of fellow drivers.
2	Clubbing Information	Informs a user about the quality and popularity of clubs, based on where other people went and how much time they have spent.
3	Library Information	Informs a user about what other people think about a certain book, helping him to determine if it is worth borrowing.
4	File-sharing	Enables users to share files (e.g., songs, ring-tones, pictures, etc.) through their mobile devices, anonymously.
5	Wiki-Guide	Serves as a city guide, through which users can get informed about monuments and other places of interest, thanks to other people's input.
6	Weather	Informs a user about the weather conditions, e.g. the temperature or level of humidity, in an area of his choice. Terminals that cooperate with sensors can be exploited for the provision of this service.

TABLE II: OVERVIEW OF CHARACTERISTICS OF THE AMC SERVICES OF TABLE I (✓ = YES, × = NO)

	Triggering		Response Type		Content Creation Mechanism		Real-time	
	Event-based	*User-triggered*	*With User Interaction*	*Automatic*	*With User Interaction*	*Automatic*	*Yes*	*No*
Traffic Information	✓	✓	×	✓	×	✓	✓	×
Clubbing Information	✓	✓	×	✓	✓	✓	✓	✓
Library Information	×	✓	✓	✓	✓	×	✓	✓
File-sharing	×	✓	×	✓	✓	×	✓	×
Wiki-Guide	✓	✓	×	✓	✓	×	×	✓
Weather	✓	✓	✓	✓	✓	✓	✓	✓

4 SYSTEM REQUIREMENTS

A system targeted for the provision of AMC services has to comply with the following requirements:

- *Anonymity*: This is the most central requirement and refers to the anonymity of both the service requestor and the queried users.
- *Interoperability*: Data collection from the community of terminals must be feasible regardless of the underlying wireless access network. This means that the AMC system must be capable of operating in a completely heterogeneous environment. In addition, different applications must be able to access the required data in a standardized manner.
- *Ease of integration*: The deployment of the AMC system must not call for any modifications in the current infrastructure of today's wireless access systems.
- *Extendibility*: The AMC system must be capable of easily integrating new features and additional, possibly diverse in nature, applications.

5 System Architecture and Functionality

5.1 Overview

The provision of the AMC services calls for the development of a robust system that fully complies with the requirements of Section 0. The present section is dedicated to the detailed description of the proposed system.

Concerning the terminal side, the requirements are minimum, in order to allow for ease of deployment. Nonetheless, an AMC-enabled terminal must have a software module installed, encompassing the following functionality:

- *Monitoring capability*: Terminals anyhow collect various measurements during their operation. An AMC-enabled terminal is capable of storing this information in a registry and presenting it to the network whenever triggered. Thanks to this capability, the AMC-enabled terminals implement the Monitoring & Data Collection Layer with regard to the reference model of Figure 1(b).
- *Query serving capability*: An AMC-enabled terminal is capable of receiving requests from the AMC network system and responding by sending back the required information.

The AMC terminal software module can be installed at the mobile terminal in three possible ways:

- It may be pre-installed by the mobile phone manufacturer;
- It may be installed at an authorized shop, probably owned by the mobile network operator;
- It may be downloaded over-the-air (OTA). In this way, it can be installed or updated dynamically.

At the network side, appropriate mechanisms have to cater for service enabling, service

provisioning and anonymity. These are explained in detail in the subsections that follow. Some important additional functional issues are also studied, namely the user registration process, the security of communication channels, as well as ways to further enhance anonymity.

5.2 Network Architecture

In this subsection, the network architecture targeted for the provision of AMC services is defined. Open interfaces are used among the various entities, in order to facilitate the inter-working of different access networks and technologies, as well as to assist in the incorporation of additional functionality. Furthermore, the architecture integrates the necessary privacy and security mechanisms. Figure 2 depicts the network architecture deployed for the provision of AMC services.

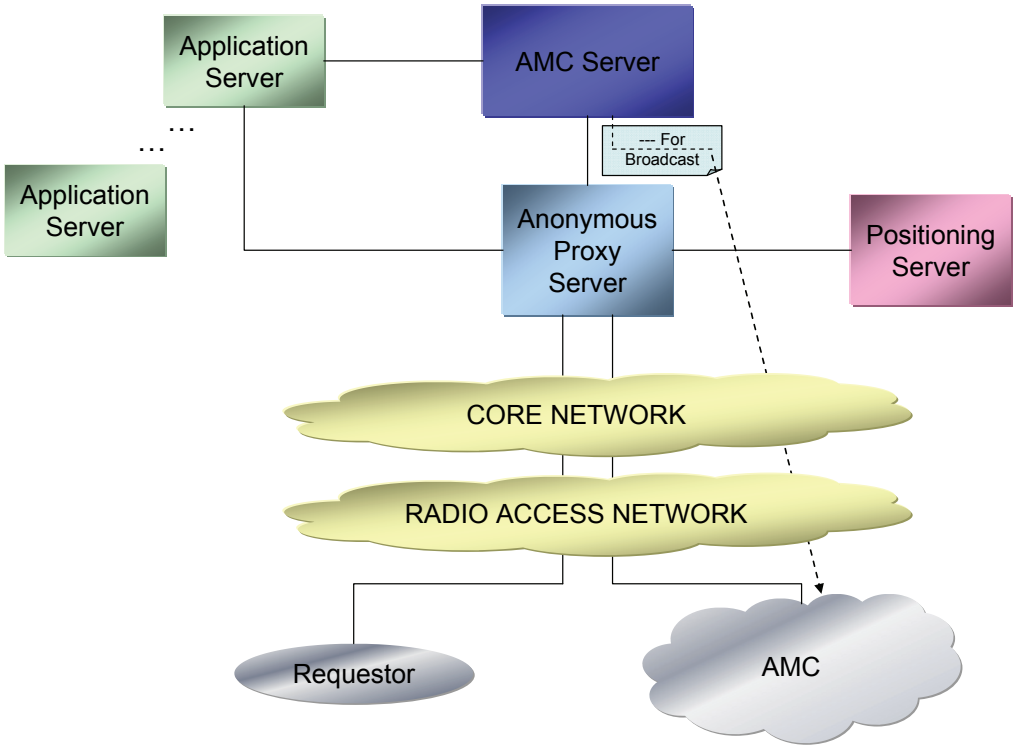

Figure 2: AMC network architecture

The main objective of this architecture is to provide a large degree of functionality without

compromising user anonymity. The main entities comprising this architecture are presented in what follows:

- *AMC Server*: This entity holds the primary role in AMC service provisioning. It encompasses functionality enabling it to receive and process requests, query and manage the AMCs, cooperate with other servers, if necessary, and finally provide the data collected from the AMCs.
- *Application Servers*: Each application server may be owned either by the network operator itself or by a third-party service provider. An application server is responsible for accepting and processing requests originating from its subscribers, issuing them to the AMC Server, collecting the data extracted by this server, and finally providing the end user with the final response.
- *Anonymous Proxy Server*: The presence of an Anonymous Proxy Server is necessary for ensuring the anonymity of both the service requestor and the queried AMC members. The real identity of each subscribed user (i.e., the International Mobile Subscriber Identity – IMSI), together with an alias or pseudonym, are kept within this entity. The server is responsible for substituting the real identity with the corresponding alias, or vice versa, before forwarding a message.
- *Positioning Server*: The AMC Server has to communicate with the Positioning Server, when positioning information is requested to be provided (e.g., for location-based services).
- *Requestor*: This is the entity that requests the provision of a specific AMC service. The requestor is typically a member of an AMC.
- *AMC Members*: These are the owners of mobile terminals that have registered and

formed an anonymous mobile community. Several AMCs may exist, each one covering different needs or location areas.

5.3 AMC Server's Functional Architecture

This server is the heart of the AMC service provisioning system. It encompasses the basic functionality for the provision of advanced anonymous services and can be regarded as the service enabler (Service Enabling Layer). Figure 3 depicts the functional architecture of the AMC Server.

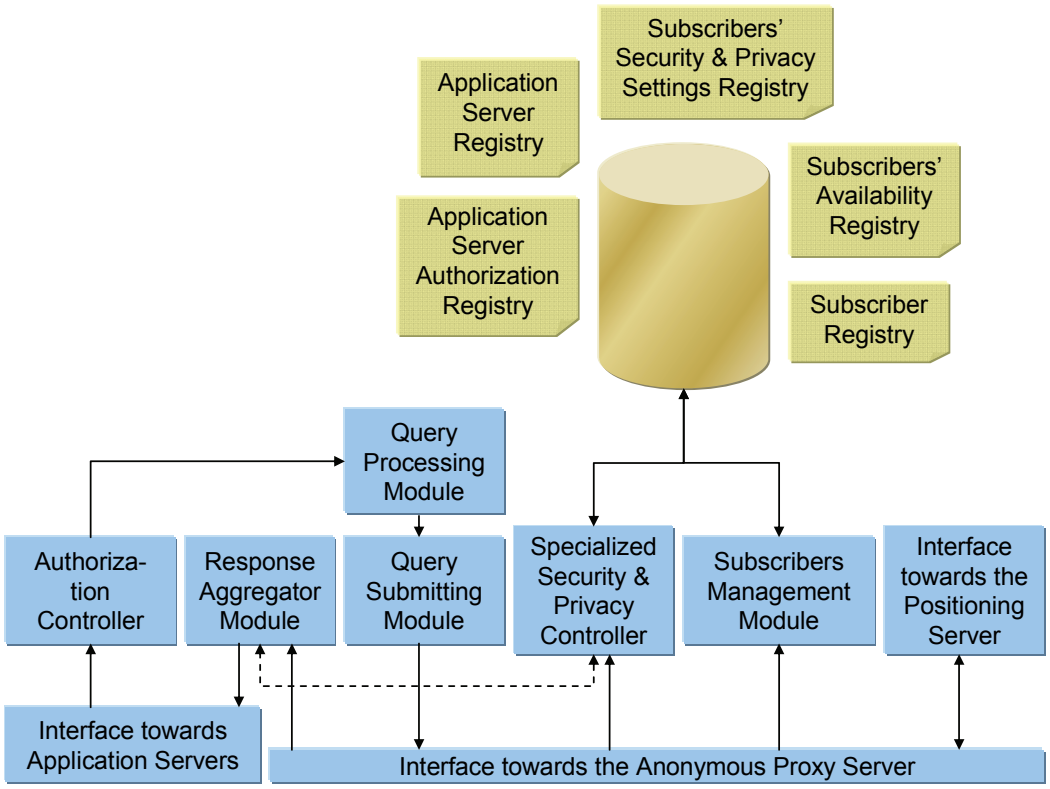

Figure 3: AMC Server's functional architecture

As illustrated in this figure, the functional architecture consists of the following components:

- *Interface towards Application Servers*: This interface enables the connection and data exchange between the AMC Server and third-party application servers. This interface should be open and well defined, in order to facilitate the interoperability with different

application servers. The implementation of this interface follows the web services paradigm, which is ideal for supporting interoperable machine-to-machine interaction over a network.

- *Authorization Controller*: This module is responsible for checking whether the application server communicating with the AMC Server and asking for specific information is authorized to receive the latter or not. This is achieved by referring to a specific registry, namely the Application Server Authorization Registry, where a list of the registered Application Servers, along with the access rights of each one, resides.
- *Query Processing Module*: When a query is requested from an Application Server, it has to be processed by the AMC Server, before it is issued. The functionality of this module is twofold: Firstly, a subgroup of the members of the AMC to which the query is related is formed. This subgroup serves as target for the query that is to be performed. It can be formed, based on criteria like location, preferences match, availability, etc. Secondly, after the target AMC subgroup has been determined, this module decides upon the type of the query that will be issued. This decision often depends on the size of the target AMC subgroup, as well as the type of the requested information. More specifically, this module may decide to either broadcast (e.g., to a whole cell or group of cells) or multicast a query message, in the form of an SMS, an MMS or a WAP push message. The decision depends on the scarcity of the members of the target AMC subgroup (e.g., whether most of the members reside in different cells or not).
- *Query Submitting Module*: This module is responsible for taking the appropriate action in order to submit the query. A query is issued in either of the following forms, depending on the decision of the previous module: (a) broadcast message; or (b) multicast message.

Queries of type (b) are directed through the Anonymous Proxy Server, which replaces the alias identity of each target AMC subgroup member with the real identity (i.e., the IMSI). In contrast, queries of type (a) need no knowledge of the target members' IMSIs, and can be based solely on the knowledge of the identities of the cells where the target members reside. The latter can be extracted by contacting the Positioning Server, through the Anonymous Proxy Server.

- *Interface towards the Anonymous Proxy Server*: This interface is of primary importance for ensuring anonymity. The AMC Server is unaware of the AMC members' real identities, and this is why most communication is tunneled through the Anonymous Proxy Server. The implementation of this interface is also web-based.
- *Interface towards the Positioning Server*: Communication between the AMC Server and the Positioning Server is required when, for the provision of a specific AMC service, knowledge of the position of a certain number of mobile terminals is necessary, e.g. in the context of location-based services. In this case, the Positioning Server must acknowledge the real identities of the users involved. For this reason, the Anonymous Proxy Server intervenes in the communication path with the AMC Server, which consequently remains unaware of the real identities. The communication between the AMC Server and the Anonymous Proxy Server, as well as the communication between the Anonymous Proxy Server and the Positioning Server, are both web-based.
- *Subscribers Management Module*: This module is responsible for handling and keeping up-to-date: (a) user registration and user availability information, and (b) settings related to security and privacy. Therefore, it utilizes three specialized registries, namely (a) the Subscriber Registry, (b) the Subscriber Availability Registry, and (c) the Subscribers'

Security and Privacy Settings Registry. Information indicating the Application Servers to which each user is subscribed is held in the first registry. Information about users' availability, as well as settings reflecting their availability preferences (e.g., time of day), are stored in the second registry. User-specific security and privacy settings are kept in the third registry. The latter registry is optional; however, it empowers the users with the ability to specify even more stringent security and privacy requirements. Every user is provided with the ability to change his registration and availability status at will, as well as to edit both his availability settings and his security and privacy settings, whenever wanted.

- *Specialized Security and Privacy Controller*: This module is responsible for checking the data collected from each member of the target AMC subgroup, in order to decide upon their conformity with the user-specific security and privacy settings, which are kept in the Subscribers' Security and Privacy Settings Module. If any piece of the collected data does not comply with these settings, it has to be either processed (e.g., in the case of positioning information, the spatial resolution may have to be reduced -Section 5.8-) or discarded, before it is relayed back to the requesting Application Server. This module is optional, yet it provides an additional layer of security and privacy, which can prove to be useful for users who tend to be particularly concerned about their anonymity.
- *Response Aggregator Module*: After a query has been issued by the Query Submitting Module, the Response Aggregator Module undertakes the task of awaiting and gathering the responses from the members of the AMC subgroup. Subsequently, it cooperates with the Specialized Security and Privacy Controller, in order to render the collected raw data fully compliant with the subscribers' supplementary privacy features. Finally, it relays

the responses back to the cooperating Application Server, through the relevant interface.

The AMC Server holds information about the cooperating Application Servers and the corresponding AMCs. This dictates the need to encompass a database containing several registries, as described below:

- *Application Server Registry*: This registry holds general information about each cooperating Application Server, including a general description, the IP address, contact information, as well as a valid public key certificate. A generic format for this registry is depicted in Figure 4(a).
- *Application Server Authorization Registry*: This registry holds authorization settings for each of the Application Servers included in the aforementioned registry. In more detail, it determines the access rights for each function/operation offered by the AMC Server towards external application servers. According to its type, an Application Server may be restricted from accessing certain types of data and/or issuing certain types of queries. A generic format for this registry is depicted in Figure 4(b).
- *Subscriber Registry*: This registry contains the aliases/pseudonyms of all users that are subscribed to the service provided by at least one Application Server. This means that these users are members of at least one AMC. The registry indicates whether a user has registered for a specific AMC service or not. Each Application Server also retains a registry of its subscribers, which must actually be an exact copy of the relevant section of the AMC Server's Subscriber Registry. A generic format for this registry is depicted in Figure 4(c).

(a)

Application Server	Description	Static IP Address	Contact	Digital Certificate

App. Server 1`	Application server providing clubbing information	147.102.7.1	admin@aps1.com	…
…	…	…	…	…
App. Server N	…	…	…	…

(b)

Function	**App. Server 1**	**…**	**App. Server N**
Velocity	authorized	…	not authorized
Temperature	authorized	…	authorized
…	…	…	…
Pop-up Messages	not authorized	…	not authorized

(c)

User Alias	**App. Server 1**	**…**	**App. Server N**
usr1265	true	…	false
usr6858	true	…	true
…	…	…	…
g12jt78	true	…	false

(d)

User Alias	**App. Server 1**			**…**	**App. Server N**
	Spatial Resolution	...	*Temporal Resolution*	…	…
usr1265	low	…	high	…	…
…	…	…	…	…	…
g12jt78	high	…	high	…	…

(e)

User Alias	**App. Server 1**				**…**	**App. Server N**
	Status	*Context 1*	...	*Context M*	…	…
usr1265	available	available	…	not available	…	…
…	…	…	…	…	…	…
g12jt78	not available	available	…	not available	…	…

Figure 4: Typical structures of the AMC Server's registries: (a) Application Server Registry; (b) Application Server Authorization Registry; (c) Subscriber Registry; (d) Subscribers' Security and Privacy Settings Registry; (e) Subscriber Availability Registry

- *Subscribers' Security and Privacy Settings Registry*: Thanks to this registry, users are able to specify different security and privacy settings for each Application Server. This is an optional, nonetheless significantly useful, component, as it takes into account the heterogeneity of the various Application Servers. A generic format for this registry is depicted in Figure 4(d).

- *Subscriber Availability Registry*: This registry indicates the availability of each registered user, for every particular AMC service, and is especially useful in cases where a user is temporarily unavailable, yet wishes to remain registered. This registry is accessed by the Query Processing Module, before the formation of a target AMC subgroup. It also holds information about the events (contexts, e.g. locations, time) in which a user should be considered unavailable by the system. A generic format for this registry is depicted in Figure 4(e).

5.4 Application Server's Functional Architecture

An Application Server is the entity responsible for implementing the application logic that lies behind an AMC service (Applications Layer). Various Application Servers may be deployed from different parties, each one exploiting the AMC Server's functionality in its own way. Figure 5 depicts the functional architecture of a typical Application Server cooperating with the AMC Server.

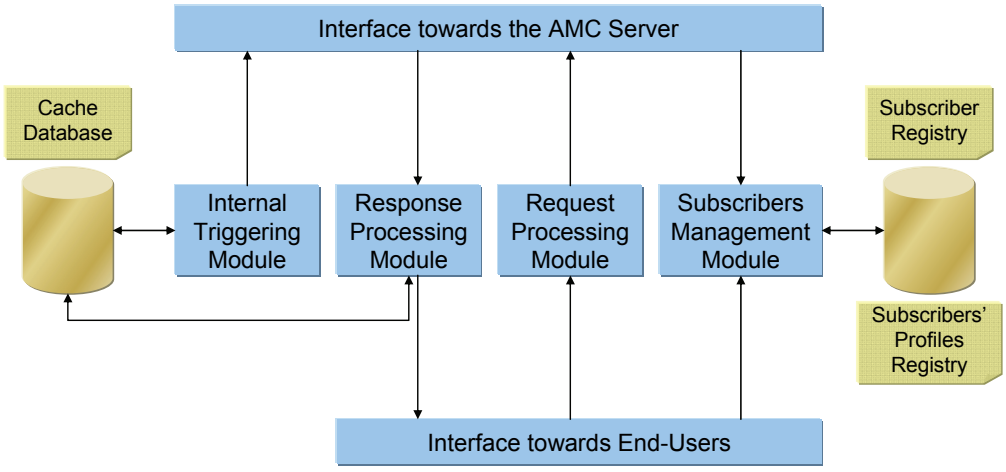

Figure 5: The functional architecture of a typical Application Server in the AMC context

As illustrated in this figure, the functional architecture consists of the following components:

- *Interface towards the AMC Server*: This interface facilitates the communication and data exchange between the Application Server and the AMC Server. It should be open and well-defined, in order to ensure interoperability. Its implementation follows the web services paradigm.
- *Interface towards End-Users*: This interface enables the Application Server to receive requests from its subscribers, and deliver the appropriate responses to them. All communication between an Application Server and the end-users should pass through the Anonymous Proxy Server, in order to ensure anonymity.
- *Subscriber Registry*: This registry contains the aliases/pseudonyms of all users that are subscribed to the specific service provided by the Application Server. These users form the Application Server's AMC.
- *Subscribers' Profiles Registry*: This registry contains a set of preferences for each subscribed user. Users have edited these preferences themselves, in order to enable the personalization of the AMC service offered by the Application Server. The set of parameters comprising a user profile may differ from one Application Server to another. For instance, with regard to a service related to Music, a suitable user-profile parameter would be the preferred type of music.
- *Subscribers Management Module*: The role of this module is twofold: Firstly, it is responsible for communicating with the AMC Server, in order to keep the Application Server's Subscriber Registry up-to-date. Secondly, it is delegated to handle the end-users' profiles, by updating the relevant records in the Subscribers' Profiles Registry, according to the input received from the end-users.
- *Request Processing Module*: This module is responsible for processing the requests

originating from the end-users. It identifies the type and parameters of each request, which is a necessary step before issuing an appropriate query to the AMC Server. It also checks a request's similarity to previous requests, in order to determine whether an appropriate query may be addressed to the local cache database, instead of querying the remote AMC Server, with a view to avoiding unnecessary network load and delay.

- *Response Processing Module*: This module handles the raw data collected from the AMC Server and conducts the main volume of processing, in order to produce a useful for the end-user result. Indicative examples of functions performed by this module are the statistical processing of raw data and the construction of relevant graphical representations.
- *Cache Database*: This database holds passed information regarding the queries to and the answers from the AMC Server. Its purpose is to serve future requests that are similar to passed ones, so as to reduce network load and delays.
- *Internal Triggering Module*: An Application Server might need to enrich the data contained in its Cache Database, in order to be able to offer enhanced services to its subscribers. Therefore, it would be valuable to equip the Application Server with the ability to issue queries to the AMC Server on its own, without an end-user's prior request. The Internal Triggering Module is responsible for triggering such an information gathering process, whenever it finds it appropriate.

Finally, an Application Server might maintain additional information in one or more databases, according to the purpose it serves. For instance, an Application Server that offers a 'Restaurant Information Service' might hold restaurant locations in a database.

5.5 Anonymous Proxy Server's Functionality

The Anonymous Proxy Server's purpose is to fulfill the most central requirement of AMC services, i.e. the anonymity. It complements the AMC Server's functionality in implementing the reference model's Service Enabling Layer.

A proxy server allows clients to make indirect network connections to other network services. A client connects to the proxy server, and then requests a connection, file, or other resource available on a different server.

The Anonymous Proxy Server hides the end-user's real identity by replacing it with an alias. The Anonymous Proxy Server is the only entity that knows and holds the mapping of real identities to aliases. For this reason, it maintains a secure registry, namely the Alias Registry, containing the mapping of aliases to real identities. When an end-user connects to the Anonymous Proxy Server, the latter looks up in the Alias Registry, in order to find the corresponding alias, then replaces the real identity with the alias and forwards the user's request to the destination server (either the AMC Server or an Application Server). Regarding the terminal side, the AMC software module has to be configured with the Proxy's address, so as to direct all AMC communication through the Proxy, which guarantees anonymity.

Concerning its connectivity, the Anonymous Proxy Server is able to communicate will all the other servers of the architecture through web-based message exchange. Towards the end-users, the Anonymous Proxy Server is able to send/receive SMS/MMS/WAP push messages. It is also capable of accepting web-services connections, which is useful in case the AMC terminals wish to answer a query using web services and not a conventional SMS/MMS mechanism.

5.6 Registration Process

The process followed when a user registers, for the first time, to the AMC Server is of

particular interest. The user connects to the AMC Server through the Anonymous Proxy Server. The latter executes a search in the Alias Registry, but finds no relevant record. It acknowledges that the user wants to register to the AMC Server, so it generates a temporary alias, on behalf of the user, and forwards his request to the AMC Server. If the user registers successfully for one or more AMC services, the AMC Server caters to notifying the Anonymous Proxy Server for this event. Upon the reception of this notification, the Anonymous Proxy Server grants a permanent alias and adds a relevant record to the Alias Registry. The Subscriber Registry of the AMC Server is notified about the new permanent alias.

Furthermore, for security reasons, the Anonymous Proxy Server can renew the aliases in its registry on a regular basis, and then again notify the AMC Server about the changes. In its turn, the AMC Server notifies the Application Servers, so that they synchronize their Subscriber Registries with its own (Section 5.8).

5.7 Communication Security

The presence of the Anonymous Proxy Server in the center of the proposed AMC system ensures anonymity. Besides this, however, in order for the system to be secure in its entirety, the information channels between the different parties need also be secured. For the communication with the end-users on the Radio Access Interface, the security framework [4]-[6] of current 3G systems is sufficient. However, the communication between the different network servers within the architecture is web-based, thus appropriate security measures need also be taken. In this direction, public-key cryptography combined with the HTTPS protocol can be utilized.

In the AMC architecture, each server belonging to the architecture needs to have a valid public-key certificate and distribute it to the other servers. Once installed to one of the other servers, this certificate can be used to encrypt information addressed to the server which the

certificate refers to. This mechanism renders the communication among the servers of the architecture secure. The certificate of the Anonymous Proxy Server also needs to be installed on the terminals of the AMC members, since this will enable them to open secure, over HTTPS, connections with the proxy server.

5.8 Enhanced Anonymity vs. Quality of Answers

As has been presented, in the AMC architecture, the mechanism that safeguards users' privacy is the mapping of their 'true' identifier to an alias (pseudonym). In this approach, although a significant degree of anonymity is accomplished, nonetheless the tracking of a unique user footprint is still possible. In order to overcome this problem and enhance the users' anonymity, two solutions can be adopted:

(a) A protocol responsible for regularly renewing the assigned pseudonyms: According to this solution, the Anonymous Proxy Server substitutes the already existing pseudonyms that are stored in its database with new ones, on a regular basis. Subsequently, it notifies (over secure HTTPS) the AMC Server about the changes, which, in turn, is responsible for informing (over HTTPS) the various third-party Application Servers. Through this communication procedure, all servers synchronize their registries with the updated, valid aliases. The adoption of this solution renders the tracking of a user's footprint a rather difficult task, since the random aliases change frequently and are, thus, hard to monitor.

(b) Reduction of the accuracy of sensitive data: Another notion that may be applied, as briefly indicated in Section 2, is the reduction of the accuracy of some parts of the shared user data, especially the positioning information. The latter can be accomplished in two ways: either through the employment of less accurate positioning techniques (such as cell-id, for example, instead of GPS), or through the addition of random noise to the positioning estimates, which

decreases spectral resolution. Temporal resolution can also be decreased through the same approach. Such a task can be assigned to the AMC Server's Specialized Security and Privacy Controller, as briefly discussed in Section 5.3. An interesting issue associated to this solution is the possible impact that this may have on the quality and usefulness of the collected answers. However, several classes of AMC applications, including the File-sharing, Environmental (Weather) and Wiki-based applications, are not affected by the decreased location accuracy, since they only require rough location estimations or even none at all. For example, the cell-id information is adequate for the Weather application (see Section 3). On the other hand, there are some classes of AMC applications, such as the provision of (vehicular) Traffic Information, that are indeed affected by the issue in question, since they require positioning information as accurate as possible. In order to provide this kind of applications, a stronger user affirmation should normally be requested. Further to this, a way to compensate for the inevitably increased user exposure in such cases is to maintain the collected sensitive data for shorter periods of time in the cache databases.

6 Scalability Issues

A system is scalable if it is able to provide the required services, for a wide range of load levels, at an acceptable level, without need for architectural changes. AMC scalability issues are mostly related to traffic requirements at the radio access network.

To that end, in order to decrease the network load, the AMC system has two options at its disposal: (a) the AMC Server may reduce the size of the AMC subgroup that is to be queried; and (b) the Application Server may increase the number of requests that are serviced via queries to the local cache databases. In both cases, the quality of service may remain practically the same if a representative subgroup of members is selected or if a similar query had recently been

issued.

Apart from this, the network servers of the AMC architecture must be capable of handling and servicing multiple requests, which is anyhow a typical requirement for most commercial servers. Lastly, the communication links between the architecture's connected servers must be of sufficient bandwidth, in order to efficiently serve the message exchange.

7 BUSINESS MODELS

To ensure a service's sustainability, appropriate business models have to be considered before service deployment. In the case of AMC services, the most robust business model would be for the network operator to become a 'payment aggregator', using the mobile telephone bill to charge users for the AMC services. In this way, users will get a single bill, regardless of the number of AMC services they use.

For this to be achieved, the network operator's billing (charging) system has to be used. For value-added services, the logging of chargeable events is not a complex task [15]. The problem usually lies in feeding this information to the main billing system (where the bill is created and sent to the user). To that end, application servers are provided with an interface towards the network operator's billing system. How the interface works is dependent on the architecture, but, in principle, the application server must be able to create a record in the billing Customer Data Record (CDR) database. The application servers offering AMC services will have to interface the billing database through the Anonymous Proxy Server.

Concerning the generation of network traffic, the most realistic scenario is not to charge the queried users for explicitly or implicitly answering the queries. This will have the positive effect of not discouraging the community members to respond to queries.

Regarding service requests, charging can be either demand-based or could be confined to a

standard subscription fee. In the first case, the registered user is charged a transaction sum whenever he makes a request to the corresponding application server. In the second case, there is a standard subscription cost for registering to a specific AMC service. A combination of the two approaches can also be applied, e.g. in case a user exceeds a predefined number of service requests.

A revenue-sharing model will also have to exist between the network operator and each application server. In this way, the network operator will be recompensed for allowing the third-party service providers to use its network. Another interesting aspect that has to be accounted for is the application of a penalty system for community members that do not seem willing to serve as query-targets. Thus, members who tend to issue requests without, at the same time, permitting other users' queries to be answered should be penalized.

Finally, sponsors can prove to be valuable sources of supplementary revenues for both the third-party service providers and the network operator. In this context, users may be requested to agree on receiving a certain number of advertisements or offers at their mobile terminals (e.g., via SMS). Advertisements may also be location-based, which will certainly render them more attractive. However, anonymity constraints must again be satisfied at all costs.

8 Use Case Scenario – Information Flow

Consider an environmental AMC service, which allows subscribers to learn information about the weather conditions (temperature) in the areas of their interest. Assuming that every member of the corresponding AMC has in his possession a mobile terminal capable of measuring the temperature of its physical surrounding, a requestor (who must also be a member of the AMC) may ask anonymously for the temperature in his desired area and get an appropriate reply, by querying members of the AMC who happen to be in that area. Figure 6 depicts the information

flow for this indicative use case scenario.

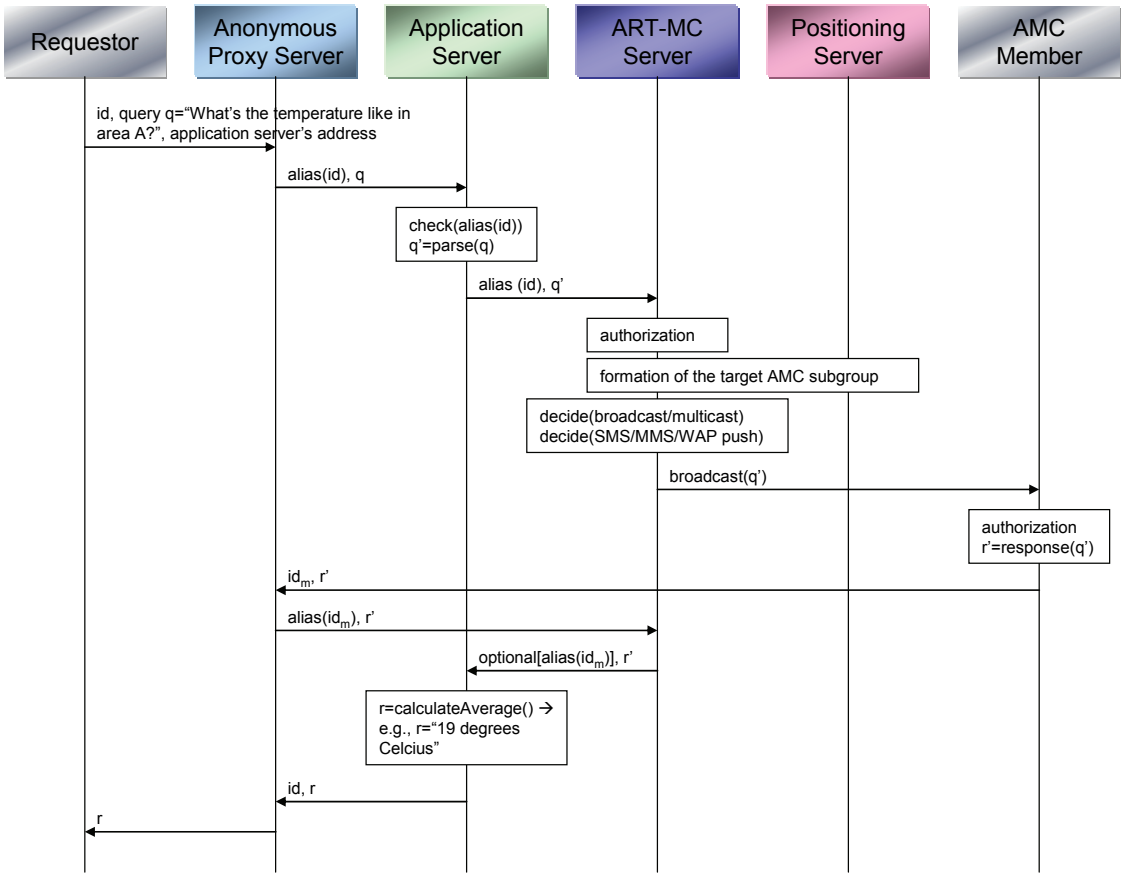

Figure 6: Typical AMC information flow

As illustrated in this figure, the requesting mobile terminal asks for the current temperature conditions in a specific area. The query is directed to the Anonymous Proxy Server, which immediately replaces the Requestor's real id (IMSI) with the corresponding alias. Then, the query is forwarded to the Application Server. The latter checks to determine if the received alias id is included in its Subscriber Registry, then its Request Processing Module parses the request, in order to issue an appropriate query to the AMC Server. Subsequently, the AMC Server checks to verify if the communicating Application Server has access right to the information requested in the query. If so, it proceeds with the formation of the AMC subgroup which will serve as query target (Query Processing Module). For this reason, it communicates with the Positioning Server, in order to include in the subgroup only those subscribed members that are in the region

of interest. Thereafter, the Query Submitting Module decides upon the query's issuing method (broadcast/multicast, SMS/MMS/WAP push message), taking under consideration the size and scarcity of the subgroup. Assuming that 'broadcast', through e.g. SMS, is chosen, there is no need for the Anonymous Proxy to intervene. Each AMC member subscribed to this service receives this notification and the appropriate response is generated by their client. The AMC Server collects the replies through the Anonymous Proxy Server, optionally checks their compliance with the records of the Subscribers' Security and Privacy Settings Registry, and delivers them back to the Application Server. The latter processes the received raw data, by e.g. averaging the temperature values, and produces the final response, which is lastly provided to the Requestor through the intervention of the Anonymous Proxy Server.

9 TRIAL RESULTS

In order to evaluate the usability and performance of the AMC services, the architecture of Section 5.2 was developed and a sample of 30 end-users was selected for participation in the conduction of trials. The test group consisted of students from the School of Electrical and Computer Engineering of the National Technical University of Athens, Vodafone-Panafon employees, and members of the research team of the Institute of Communication and Computer Systems, Computer Network Laboratories, Greece. The users were requested to evaluate the File-sharing service and each user participated with his/her own Java-enabled mobile phone (thus, a variety of mobile devices were used in the testing process, including different brands, as well as different models of the same brand). At the end of the 10-day trial period, the users were given questionnaires and were asked to fill in their responses to the provided questions. The trial results are summarized in Figure 7. Trial results for other AMC services, besides File-sharing, as well as additional, secondary details can also be found in [16]. The following conclusions can be

drawn based on the trial results:

- Concerning the application's User Interface at the terminal side, the vast majority of the respondents found it very easy to use. The interface provided for searching for a file was found to be practical. The two registration interfaces (Web-based and terminal) were found to be almost equally useful.
- The system proved to be absolutely robust, since no wrong responses were encountered during the trial operation. The responses were found to match the users' requests to a great extent. The service proved to be available whenever requested by the test users.
- The average time that the users had to wait in order to receive a response was mostly judged as really short (47%) or acceptable (by an equal 47%). This time was affected by the size of the requested file, since the file transfers were conducted over GPRS (or 3G whenever available). This explains why 40% of the users gave a 'yes' but not a firm 'yes' to the question regarding the suitability of the application for fast (i.e., near real-time) use.
- The users found the application quite interesting and half of them stated that they would be willing to share more than ten (10) files in a potential commercial deployment.
- The terminal application was fully robust, with no crashes occurring on the test users' mobile phones. All users enjoyed the use of the application either partly or a lot, and all of them found the concept to be valuable. A division of file types into categories (e.g. music, videos and pictures) was suggested as an improvement. The vast majority would most probably like to take part in a file-sharing anonymous community in the future. The preferred billing method for this application was "being rewarded on answering a query".

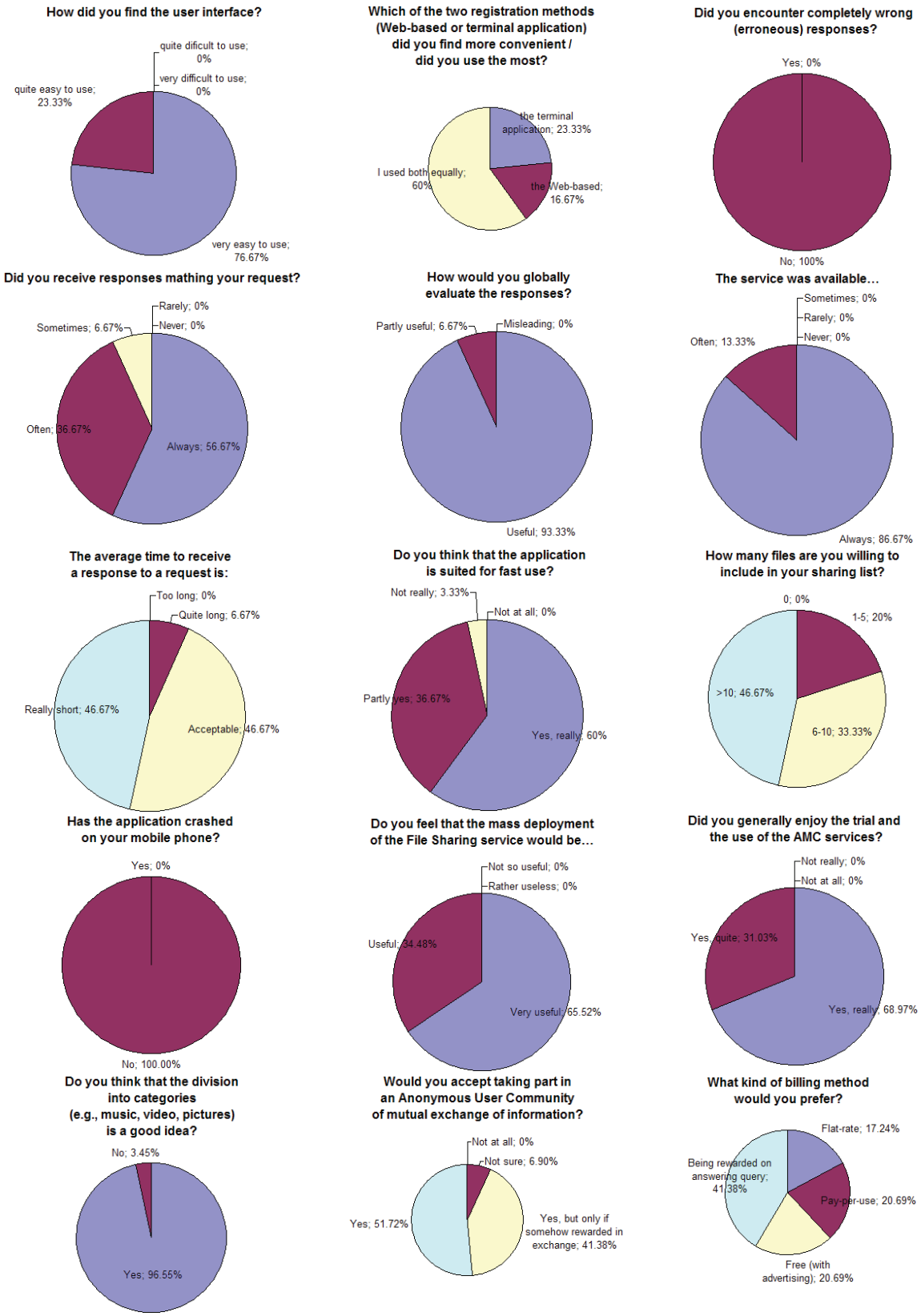

Figure 7: Answers provided by the test users after trials of the File Sharing service

10 Concluding Remarks – Future Work

In this paper, the concept of Anonymous Mobile Community (AMC) services, which take advantage of the terminals' capabilities to collect information and deliver it to the network, was introduced. In this context, terminals are enabled to form communities that serve as sources of information. In these communities, the anonymity and privacy of the end-users are respected and guarded.

Several examples of promising AMC services were presented and a systematic classification was attempted. A system capable of delivering diverse AMC services to the end-users was described in detail, focusing on its architecture and requirements. The related scalability issues and the appropriate business models were also investigated. Finally, the information flow of a use case scenario was examined.

Future plans include the commercial deployment of a group of AMC services. Towards this goal, the scalability issues will be studied more thoroughly and the end-user experience will be monitored and enhanced. Our target is the full commercial deployment of an AMC system, capable of self-adjusting to environmental conditions, including network congestion, without noticeably deteriorating the provided quality of service.

Acknowledgement

The work presented herein is conducted in the framework of Ph.D. research performed by K. Demestichas and E. Adamopoulou, under the supervision of Prof. M. Theologou. The work is also supported in part by the European Commission, under the Sixth Framework Program, in the context of the IST project MOTIVE (FP6-IST-27659).

References

[1] Anonymizer website, 5694 Mission Center Road #426, San Diego, CA 92108-4380, US, http://www.anonymizer.com, 2000.

[2] B. Nonnecke, D. Andrews, and J. Preece, "Non-public and public online community participation: Needs, attitudes and behavior", *Special Issue on Virtual Communities in E-commerce, Electronic Commerce Research*, Springer, Vol. 6, No. 1, pp. 7-20, Jan. 2006.
[3] D. Mohapatra and S. B. Suma, "Survey of location based wireless services", *in IEEE International Conference on Personal Wireless Communications (ICPWC 2005)*, pp. 358-362, Jan. 2005.
[4] ETSI TS 133 102 V7.0.0 (2005-12): Universal Mobile Telecommunications System (UMTS), 3G Security, "Security architecture", 3GPP TS 33.102, version 7.0.0, Release 7, December 2005.
[5] ETSI TS 133 103 V4.2.0 (2001-09): Universal Mobile Telecommunications System (UMTS), 3G Security, "Integration Guidelines", 3GPP TS 33.103, version 4.2.0, Release 4, September 2001.
[6] ETSI TS 133 120 V4.0.0 (2001-03): Universal Mobile Telecommunications System (UMTS), 3G Security, "Security Principles and Objectives", 3GPP TS 33.120, version 4.0.0, Release 4, March 2001.
[7] I. MacInnes, "Property rights, legal issues, and business models in virtual world communities", *Special Issue on Virtual Communities in E-commerce, Electronic Commerce Research*, Springer, Vol. 6, No. 1, pp. 39-56, Jan. 2006.
[8] J. Corhonen, "Introduction to 3G Mobile Communications", Second Edition, *Artec House Inc.*, Mobile Communication Series, Boston, London, ISBN: 1-58053-507-0, 2003.
[9] J. Füller, M. Bartl, H. Ernst, and H. Mühlbacher, "Community based innovation: How to integrate members of virtual communities into new product development", *Special Issue on Virtual Communities in E-commerce, Electronic Commerce Research*, Springer, Vol. 6, No. 1, pp. 57-73, Jan. 2006.
[10] M. Ginsburg and P. Schubert guest eds., "Virtual Communities in E-Commerce", *Special Issue in Electronic Commerce Research*, Springer, Vol. 6, No. 1, Jan. 2006.
[11] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", *in Proceedings of the MobiSys 2003*, pp. 31-42, 2003.
[12] P. Grace-Farfaglia, Ad Dekkers, B. Sundararajan, L. Peters, and S.-H. Park, "Multinational web uses and gratifications: Measuring the social impact of online community participation across national boundaries", *Special Issue on Virtual Communities in E-commerce, Electronic Commerce Research*, Springer, Vol. 6, No. 1, pp. 75-101, Jan. 2006.
[13] P. Schubert and J. F. Hampe, "Mobile communities: How viable are their business models? An exemplary investigation of the leisure industry", *Special Issue on Virtual Communities in E-commerce, Electronic Commerce Research*, Springer, Vol. 6, No. 1, pp. 103-121, Jan. 2006.
[14] SafeWeb website, Symantec Corporation, US, http://www.safeweb.com.
[15] T. D'Roza and G. Bilchev, "An overview of location-based services", *BT Technology Journal*, Kluwer Academic Publishers, Vol. 21, No. 1, pp. 20-27, Jan. 2003.
[16] FP6-IST4 27659 Project MOTIVE, "Deliv. 5.1: Trial Results and Analysis", Nov. 31, 2006.