Hindawi Publishing Corporation
Advances in Multimedia
Volume 2011, Article ID 706164, 14 pages
doi:10.1155/2011/706164

Research Article

Mobile Music Distribution: A Multichannel Approach

Marco Furini

Communication and Economics Department, University of Modena and Reggio Emilia, Via Allegri 9, 42100 Reggio Emilia, Italy

Correspondence should be addressed to Marco Furini, marco.furini@unimore.it

Received 6 June 2011; Revised 1 August 2011; Accepted 19 September 2011

Academic Editor: T. Turletti

In contrast to what is happening in the Internet-based scenario, the music market in the mobile scenario is far from being considered a large success. Several studies state that excessive downloading time and high cost are the main burdens. Motivated by the growth of social and mobile applications, in this paper we propose an approach that aims at reducing both the downloading time and the cost to get digital music when acquired in the mobile scenario. The proposed architecture exploits the usage of personal communication technologies embedded in cellphones (e.g., Bluetooth and Wi-Fi) to couple the current distribution model (mainly based on 3G networks), so as to provide a multichannel distribution model where users are free to redistribute digital music. The architecture includes a license-based security mechanism that prevents unauthorized usage of digital music, and makes use of an incentive mechanism to stimulate and reward the music distribution among customers. By analyzing pros and cons of the music distribution chain, results show that the proposed architecture might help in reducing both the downloading time and the cost to get digital music when acquired in the mobile scenario. Therefore, it might be helpful to the success of the mobile music scenario.

1. Introduction

The presence of several online music stores, as well as the capability of several devices (e.g., iPods, cellphones, and in-car and home entertainment systems) to play digital music, is an index of the popularity and of the success of digital music. Today, customers can acquire and download digital music with few clicks, and research reports estimate that the digital music market accounted for 29 percent of record companies' trade revenues in 2010 [1].

Several studies in economic, social, and technological fields investigated the reason of this success: low prices, high-speed residential Net access (e.g., DSL) with flat rate plans, large availability of attractive and cool portable music devices, and an access to an (almost) unlimited music catalog are commonly seen as the key factors that set the success of digital music.

Long time has passed since record labels were reluctant, for piracy reasons, to the idea of releasing music for the download scenario. Today, record labels, along with mobile phone producers and cellphone network operators, are attempting to create a ubiquitous and mobile e-music market, with the goal of creating an additional source of income (mobile phone producers hope to refill the market with new cellphones equipped with features more suitable to digital music, whereas cellphone network operators see in digital music distribution an opportunity to recover the huge investments made on building the 3G network infrastructure).

Preliminary analysis of the mobile music market shows that, despite the attractiveness of a ubiquitous scenario where consumers can buy music when and where they want, people prefer buying digital music using residential Net access, and only later they transfer the acquired songs over their mobile music devices. In fact, in the mobile world, the strong power of Telcos on their customers and the high price of the data traffic establish a burden for the diffusion of the digital entertainment contents in the mobile scenario [2]. For instance, when buying music in a mobile scenario, user may be informed of the cost of the song, but not of the cost of data transfer. Therefore, users usually do not have an idea of the total cost of the purchase and this influences the consumption behavior [3, 4]. Analysis showed that there are two main burdens that limit the success of the mobile music market: longer downloading time and higher cost than the ones of the residential Net access [2–6]. In fact, although digital communication transfer data rates on mobile phones are increasing, even using high-speed 3G network the achieved transfer data rate is much slower than the one achieved with residential Net access; not to mention that in many areas (e.g., rural zone) high-speed 3G networks are not available. Moreover, it is to note that the usage of cellphone networks plays an important role in the price paid by customers to acquire and download music in the mobile scenario. In fact, although flat-rate data plans are beginning to appear in the mobile scenario, most cellphone network operators apply a pay-per-bit business model, causing consumers to pay, for a song, around twice the price paid if downloaded at home via a residential Net access. This is a burden for the success of the mobile music market. In fact, as analyzed in [6], price significantly influences purchase decisions as high price is the key inhibitor of purchase willingness. Potential purchasers may purchase online music only when they perceive an adequate monetary price and price remains a very important determinant of willingness to make continued purchase decision for purchasers [6]. Needless to say, to make the mobile music market a success, it is necessary to reduce both the total cost (i.e., song price plus cost of the data traffic) to get e-music and the downloading time, so as to make the mobile scenario a real alternative to the Internet-based scenario [7].

Motivated by the success and the increasing usage of social mobile applications (e.g., Foursquare, http://www.foursquare.com/, Gowalla, http://www.gowalla.com/) [8], in this paper we propose MoMu (Mobile Music), an architecture for multichannel music distribution in the mobile scenario. The creation of a multichannel distribution scenario is seen as a fundamental step to allow music players to capitalize in the mobile digital environment [2]. In particular, our proposal is designed to reduce both the downloading time and the cost to get digital music in the mobile scenario. Note that our proposal does not demand or require the vendor to change the song price (which is and still remains a business decision), but MoMu aims at reducing the total cost (composed of the song price plus the cost of the data traffic) paid by the user. To this aim, MoMu integrates the usage of the (expensive and relatively slow) cellphone network technologies with the usage of (free-of-charge and high-speed) personal area networks built upon personal communication technologies (e.g., Bluetooth and WiFi) provided in many cellphones and uses an incentive mechanism to stimulate and reward the distribution of music among MoMu members. In essence, MoMu aims at creating a scenario where MoMu members use personal communication technologies to share digital music and use the cellphone network only when strictly necessary. In this way, MoMu aims at reducing both the downloading time and the price to get digital music in the mobile scenario. It is worth noting that, since sharing of digital music can lead to copyright problems, MoMu is provided with a license-based security mechanism that protects music against unauthorized usage.

To evaluate the effects that the MoMu multichannel approach might have on the mobile music scenario, we first analyze the security mechanism, focusing on the security achieved to protect music contents from unauthorized usage and on its introduced overhead. Then, we analyze whether MoMu is effective in reducing both the downloading time and the cost to get digital music in the mobile scenario. Finally, we analyze pros and cons of using MoMu with respect to the digital music distribution chain: customers, cellphone producers, cellphone network operators, and content owners. Results show that MoMu can reduce both the downloading time and the cost to get digital music when acquired in the mobile scenario and might bring benefits to all the entities involved. Therefore, MoMu might contribute to the growing and to the success of the mobile music scenario.

The remainder of this paper is organized as follows In Section 2 we briefly review proposals related to wireless music distribution; Section 3 presents details of the MoMu architecture, whereas in Section 4 we analyze the security achieved by MoMu when protecting digital contents and we also present the introduced computational overhead. Section 5 shows results obtained from analyzing both the downloading time and the cost to get e-music when MoMu is used in a mobile scenario. Conclusions are drawn in Section 6.

2. Related Works

In the literature, different studies analyzed the distribution of music contents in the mobile scenario with respect to different points of view (e.g., sociological, business, and engineering). In the following, we briefly review proposals related to distribution strategy and security aspects, as these studies are more related to the MoMu approach.

Grech and Luukkainen [7] proposed a multichannel wireless distribution with the idea of exploiting synergies between music and radio broadcasting. In essence, the proposed mechanism works as follows: a customer can acquire and download over the mobile device the music he/she is listening to at the radio channel. The evaluation shows that the mechanism stimulates customers to acquire digital music in the mobile scenario. Ghini et al. [9] propose the creation of a seamless music delivery service, by combining different network technologies (in a transparent way for the consumer), so that even in the presence of horizontal and vertical handoffs, the download of digital music can be done. Roccetti et al. [10] propose a mechanism for distributing digital music over mobile devices, focusing on the availability and on the responsiveness of the distribution service. The mechanism uses a software redundancy to replicate the music catalog over different web servers in order to increase the performance of the music distribution system. Tanaka [11] considered the mobile network as a mean to support a system for collaborative musical creation. Kubek and Nutzel [12] and Stanek [13] analyzed the sharing of music contents among users in a mobile scenario and proposed a personal file sharing mechanism built over the Bluetooth technology.

Cervi et al. [14] studied the possibility of using a P2P approach in a mobile scenario. Schmidt [15] analyzed the sharing of digital goods among customers and concluded that the sharing can be really attractive for the digital economy.

In addition to the distribution strategy, different studies investigated the security aspect in mobile music distribution. Briefly stated, such proposals (e.g., [16–19]) suggest using security techniques (e.g., encryption and watermarking) to set up a mechanism (a.k.a. Digital Right Management- (DRM-) mechanism) that protects digital music from unauthorized usage in the mobile scenario. However, DRMs seem to have added more obstacles to nontechnological users than security to the process of distributing music. In fact, current DRMs admit no final and provable strong solution (see [20] for a history of cracks in several DRMs designed to protect digital goods). For this reason, an increasing number of music sellers (e.g., iTunes and Amazon) are selling DRM-free music. However, it is worth noting that the release of DRM-free music does not mean the end of music protection. For instance, while on the one side EMI Music offers DRM-free music within the iTunes catalog, on the other side they highlight that [21] "*EMI Music will continue to employ DRM as appropriate to enable innovative digital models such as subscription services (where users pay a monthly fee for unlimited access to music), super-distribution (allowing fans to share music with their friends) and time-limited downloads (such as those offered by ad-supported services).*" Therefore, DRM is still a competitive tool especially when dealing with music distribution among customers.

MoMu differs from the above approaches as it is a complete architecture designed to securely distribute digital music in the mobile scenario: it integrates the current distribution approach with a distribution model based on sharing among customers so as to provide a multichannel distribution service. MoMu is provided with a security mechanism that protects digital music from unauthorized usage and is equipped with an incentive mechanism that stimulates MoMu members to redistribute music by giving a financial reward to those who actively participate in the redistribution of digital music.

3. The MoMu Multichannel Distribution Model

In this section we present MoMu (Mobile Music), an architecture designed to distribute digital music in the mobile scenario using a multichannel approach. MoMu integrates the current distribution model (based on 3G networks) with a distribution based on personal wireless communication technologies like Bluetooth and Wi-Fi. These technologies allow direct communications from one device to another without the involvement of an access point. In the current mobile scenario, Bluetooth and Wi-Fi are very popular thanks to their massive usage in portable game consoles, digital cameras, and other consumer electronics devices. The Wi-Fi transmission distance range typically varies from 32 to 95 meters (depending on the version), whereas Bluetooth technology is not dependent on the specification, but on the capabilities of the device (e.g., a minimum distance of 10 meters is required for a Bluetooth device [22]). The motivation behind the proposal is to reduce both the downloading time and the cost to get digital music in the mobile scenario. Before presenting details of the proposal, let us depict a possible MoMu scenario.

Alice is registered with a MoMu server and is now part of the MoMu community. As a member, she has an advanced e-music player installed on her cellphone. Using such player, Alice can browse the MoMu catalog of music and can buy and download digital music directly with her cellphone. To pay, Alice uses the cellphone billing system. Once downloaded, Alice can play out the acquired e-music and can also redistribute it within the MoMu community. Today, Alice decides to share the song she just acquired with her neighbor Bob, who is also a MoMu member. Alice uses the cellphone communication technologies to scan for Bob's device, and when found, she sends him the song. Since Bob is a MoMu member, he also has an advanced e-music player installed on his cellphone. When contacted from another MoMu member, the advanced player shows Bob some information about the song. If Bob is interested in receiving the song, the actual download begins; otherwise, it does not. Here, we suppose that Bob wants to download the song Alice is sending to him. Since the song is locked, Bob has to buy the license. Therefore, the player asks Bob if he wants to buy the license file. If so, the player uses the cellphone network to contact the MoMu server in order to acquire the song license. The license is produced on the fly and delivered to Bob's player using the cellphone network. Once the license has been fully downloaded, the player uses the license information to unlock the song, so that the song can be played out. From now on, Bob can redistribute the song (which remains protected against piracy) to other MoMu members.

Although simple, the scenario just described highlights the potentiality of a multichannel approach. To build such system, it is necessary to well define the architecture and the functionalities of its components, as well as it is mandatory to design a security mechanism that prevents unauthorized usage of digital music. Further, to stimulate users' cooperation, we present an incentive mechanism and a reward policy that may contribute to the success of the proposed architecture.

3.1. System Architecture. MoMu is designed to reduce both the downloading time and the cost to get e-music when acquired in the mobile scenario. To achieve both goals, MoMu is based on a multichannel approach and is provided with an incentive mechanism and a reward policy that stimulate music redistribution among MoMu members. It is worth noting that MoMu is not meant to replace the current distribution model, mainly based on 3G networks, but is designed to integrate it with additional communication technologies. With respect to Figure 1, the MoMu architecture is composed of the following: a MoMu server that has access to music contents (e.g., provided by

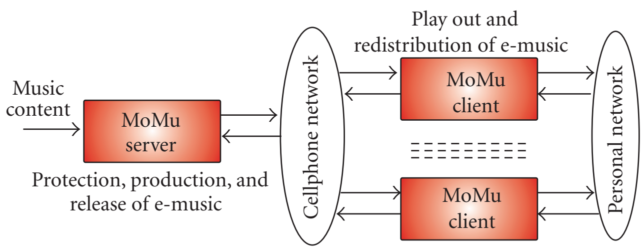


Figure 1: MoMu architecture: the cellphone network distribution is coupled with personal network built upon (free-of-charge) personal wireless communication technologies like Bluetooth and Wi-Fi.

record labels) and is in charge of protecting, producing, and releasing e-music to consumers using the cellphone network; a MoMu client that may acquire (from the MoMu server using a cellphone network), play out and redistribute (to other MoMu members using personal communication technologies like Bluetooth or Wi-Fi) e-music. Note that, without loss of generality, the MoMu architecture might be expanded with a license server that performs all the necessary tasks related to license production/release. In this paper, for the sake of simplicity, we suppose that all the operations related to license production/release are performed by the MoMu server.

In essence, MoMu creates a multichannel distribution model by integrating the cellphone network with personal area networks. As mentioned, the reason behind the integration is to limit the usage of the (expensive and slow speed) cellphone networks, in favor of the (free-of-charge and high-speed) personal area networks, so as to reduce both the downloading time and the price paid to acquire music in the mobile scenario.

In the following we present details of such architecture.

3.2. MoMu Server. The server is in charge of three main tasks: protection, production, and release/distribution of digital music. Protection is achieved with a security mechanism that uses standard techniques (encryption and watermarking) to defend contents from unauthorized usage (a play out is said to be authorized when the song license is acquired). The security mechanism is license based, which means that digital music can be unlocked only with a license file that is produced and released by the MoMu server. The mechanism is designed in such a way that a locked song is produced *once-for all*, whereas the license that unlocks the song is produced *ad hoc* for any requests.

Figure 2 outlines the security mechanism. The server generates an encryption key (say α) and uses such key to encrypt the song file, or a portion of it (e.g., the first 30 seconds may be left in clear for commercial purposes) with a symmetric encryption technique. In this way, the same key is used to lock and unlock the content. To keep the α key secret to unauthorized users or software, the security mechanism uses a watermarking technique to spread the α key inside the song file without compromising the media content [23]. Locations where the α key is stored are decided using another key, the so-called watermarking key (WKey), which will be available in the license file. Therefore, a music song cannot be unlocked without its license file.

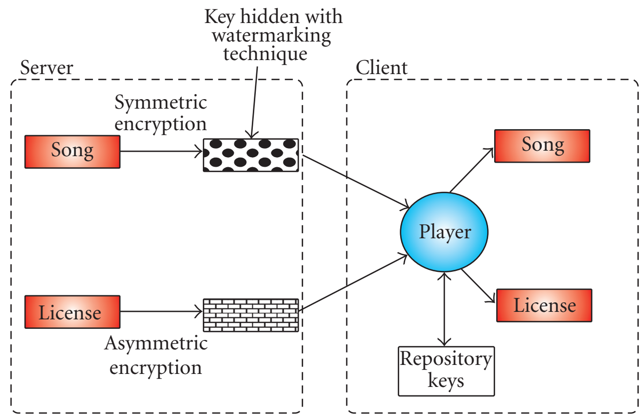


Figure 2: Details of the security mechanism employed in MoMu. The server release encrypted e-music and watermark the necessary keys into the e-music file. At the client side, the player decrypts e-music using a license file.

The license file is protected against unauthorized usage using an asymmetric technique. This technique uses two separate keys (a public key used by the server to encrypt the file and a private key used by the client to decrypt the file) to lock and unlock the content. In this way, the unlocking procedure can be done only by who owns the private key and license sharing is useless as the license is bound to a specific MoMu member (license is produced ad hoc for any request). Note that every MoMu member owns a private key, assigned when signed up for the MoMu service. It is worth mentioning that the private key is stored in the device repository key, which is accessible only to the MoMu player (i.e., the private key is kept secret to the user).

In summary, the key to unlock the song is the same for all the MoMu members (the song is produced once and for all), but to find where the α key is hidden the watermarking key is necessary. To get this key it is mandatory to unlock the license file, and, since a license file is produced with an asymmetric technique, a private key is necessary to unlock the license.

In addition to music content protection, the MoMu server is also in charge of ensuring the integrity of the data song so as to avoid any possible alteration (e.g., malicious information like wrong song title). To this aim, the security mechanism uses a hash function H to compute the song digest (i.e., $\mathrm{SD} = H(E_\alpha(\text{song}))$) and watermarks it inside the digital music file.

To be as more general as possible, MoMu does not bind the production, protection, and the distribution of digital music to specific technologies. Therefore, the encoding format is completely transparent to the MoMu architecture, that is, any encoding format like MP3, AAC, or WMA, just to name a few, can be used. Similarly, the protection is supposed to be achieved using the more appropriate technologies (e.g., RSA, DES, IDEA, AES, and Blowfish), and the distribution of e-music is done through the fastest networking technology available at the user side (e.g., GPRS

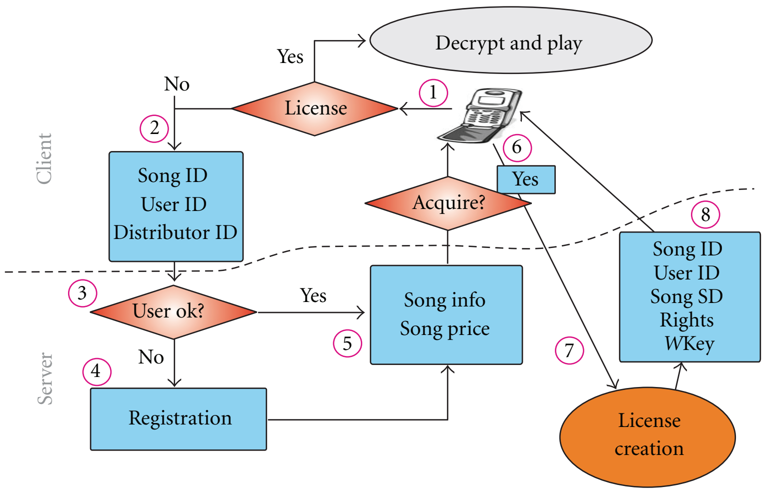


FIGURE 3: License file acquisition.

or 3G when operating in the cellphone network, Bluetooth or Wi-Fi when transmitting in the personal area network).

3.3. MoMu Client. A MoMu client is in charge of unlocking and playing digital music, as well as of distributing e-music to other MoMu members. Before detailing the way MoMu unlocks and distributes e-music, it is worth mentioning that to become a MoMu member it is necessary to sign up for the service. The sign-up procedure is required to gather device and user information. Once the registration succeeded, a MoMu client is identified with a unique user identifier (UID), and the server sends to the client the advanced e-music player as well as the private key (this one will be stored into the device repository keys).

To increase security, we assume that the advanced e-music player is bound by standard techniques to the client's hardware device. In mobile devices, this is typically achieved by exploiting some unique device identifiers like the International Mobile Entity Identification (IMEI) in mobile phones. As a result of this assumption, the player can only run in the client's device and it does not work in any other clients' device.

The redistribution of digital music towards other MoMu members is handled by the advanced MoMu player, which uses personal communication technologies to scan for other MoMu members and to transfer e-music. In particular, the player performs an air scanning to look for other MoMu members in the nearby; when a MoMu member is discovered, the players on the two clients begin a handshaking procedure that investigates whether the contacted MoMu member is interested in receiving the song or not. To this aim, the two players exchange information (e.g., song ID, song title, song author, and user ID), and the actual song transfer begins only if the contacted MoMu member is interested. In this way the downloading of undesired songs is avoided. Note that the selection of what networking technology (e.g., Wi-Fi or Bluetooth) has to be used is completely transparent to the user and is managed by the advanced e-music player provided to each MoMu member.

The unlocking of digital music depends on the way e-music has been downloaded. If downloaded from another MoMu member, the player needs to contact the MoMu server in order to acquire the license.

Figure 3 shows details of this scenario: when the player tries to play out the digital song, it finds out that the song is locked (1); therefore, the MoMu member needs to acquire the license song. Here, without loss of generality, we suppose that the MoMu server is also in charge of releasing licenses. To acquire the license of a song, the following steps are necessary:

(a) the player sends to the server the song ID, the distributor ID (the ID of the MoMu member that distributed the song), and the user ID (2);

(b) the server checks whether the user is subject to some country restriction. Indeed, in the entertainment scenario, the delivery of contents might be subject to country-dependent policies. With respect to the music scenario, this is particularly true for streaming distribution where, due to license constraints, the service might be available only in some countries. For instance, Pandora is available only in USA whereas Spotify is available in just eight countries. Although MoMu is designed for the download service, to be as more general as possible, we consider the country check also in the MoMu architecture. Note that the server can easily perform this task by checking the cellphone network provider used by the user (3) and also checks if the user has already signed up for the service (4). If not, a registration procedure is mandatory (5); otherwise, the server sends back some information about the song (e.g., Song Title and Song Author) and the song price (6);

(c) the player asks the user if he/she wants to proceed with the license acquisition. If so (7), the server is contacted and the license is created (8) and is sent back to the client (9).

Once the license has been downloaded, the unlocking procedure may begin and the player performs the following steps:

(1) retrieve the private key from the repository and decrypts the license file;

(2) check for the song integrity by comparing the song digest (SD) value embedded inside the license file against the SD value watermarked inside the e-music file. If the integrity check fails, the play out cannot begin;

(3) use the *W*Key to locate and retrieve the α key;

(4) unlock the song file and begin the play out.

Note that the previous steps are performed also when e-music is downloaded directly from the MoMu server.

Before concluding, we mention a possible annoying drawback: song integrity is checked once the song has been completely downloaded. If the check fails, the MoMu member retrieved useless data. To minimize the reception of useless data, one can think of splitting the song into several segments. For instance, in P2P networks a single file is composed of several chunks with limited size (e.g., 512 KB or 1024 MB). This approach is reasonable in the residential scenario where bandwidth is more precious than computational power, but in a mobile scenario computational power is very important as it may be limited and it greatly affects battery life. A possible and practical solution might see the player to keep track of members who distribute "wrong" songs and ban them (automatically or manually) in future operations.

3.4. Incentive Mechanism and Reward Policy. The proposed MoMu architecture aims at ameliorating two main burdens that restrain users from acquiring music in the mobile scenario: long downloading time and high cost to get digital music. As previously described, MoMu exploits personal wireless communication technologies to reduce both the downloading time and the usage of the expensive cellphone network. However, since the MoMu idea relies on customers' distribution, it is necessary to stimulate MoMu members in being e-music distributors. In fact, several studies of cooperative systems (e.g., P2P networks), where the process of sharing/distributing resources is critical for the success of the system, highlight that users tend to use system resources while giving back little (or no) resources.

In the literature, the lack of cooperation, known as *the free-riders problem*, is addressed with incentive mechanisms, which aim at stimulating users' cooperation. Roughly, incentive mechanisms fall into two categories: reputation systems, where users are punished/rewarded based on the observed behavior (e.g., [24–26]), and payment mechanisms, where a fee is given back in return for service (e.g., [27–29]).

MoMu is provided with a payment-based mechanism that stimulates customers' cooperation by financially compensating customers who successfully distribute a song. Note that here, a successful distribution means that the song has been delivered to another MoMu member and this one acquired the song license. In essence, MoMu introduces an additional financial cost to the license price, in such a way that this additional cost can be partially or totally recouped by redistributing the song to other customers. Paradoxically, to reduce the cost to get e-music, MoMu introduces a (small) additional financial fee, but our findings suggest that not only customers can fully recover the additional financial cost, but they can also have additional incomes if the redistribution mechanism takes place. To clarify, let us denote the parameters that usually participate in the price paid by users to get a digital song: C_L (cost of the license), C_{LT} (cost of receiving the license data), C_{ST} (cost of receiving the song data), and C_I (additional cost introduced by MoMu).

The price paid to get a song is defined as $P = C_L + C_{LT} + C_{ST} + C_I$. Note that, C_L is the same for all customers (e.g., 99 cents in the Apple iTunes Music Store), determined by a business decision taken by the music store, whereas C_{LT}, C_{ST}, and C_I might differ from customer to customer, according to the technology used to download a song. For instance, in the fixed Internet with DSL residential flat rate plans, C_{LT} and C_{ST} are negligible. Conversely, in the mobile scenario, C_{LT} and C_{ST} awfully affect the price paid by users to get a song.

MoMu may cause C_{ST} to be negligible also in the mobile scenario. In fact, the multichannel approach allows members to download digital music from other MoMu members. The side effect of MoMu is that it introduces the additional C_I cost as it has to stimulate music sharing/distribution among users. It is important to point out that, although the C_I cost is collected by the music store, it is meant to be shared among customers that helped in distributing the song. Note that $0 \leq C_I \ll C_{ST}$; otherwise, it would be more convenient to download the song using the cellphone network, and we already mentioned the problems of such distribution strategy.

The way the additional financial cost is redistributed among members, the so-called *reward policy*, is very important as it is the factor that stimulates users' cooperation. Roughly, as described in [30], the reward policy can be either single or multiple: the single-reward policy gives back the entire additional financial cost to who successfully distributed the e-song, whereas a multireward policy splits the additional financial cost among all the members that participated in the redistribution of the e-song (beginning from the one who acquired the song from the MoMu server).

Figure 4 highlights the difference between the two reward policies. Here, we suppose a scenario where Alice (A) buys a song from the MoMu server and redistributes the song to Janel (J). Janel acquires the license and redistributes the song to Lucy, who buys the license and redistributes the song to Sam (S).

If the system applies a single reward policy, when Janel acquires the license song, the additional C_I cost is given back only to Alice. Similarly, when Lucy acquires the license song, the additional C_I cost is given back only to Janel. Lucy gets back the additional cost C_I only when Sam acquires the license song.

Conversely, if the system applies a multireward policy, the amount C_I is shared among all the members who cooperated in the song distribution, from the one who originally bought the song through the cellphone network to the one who just

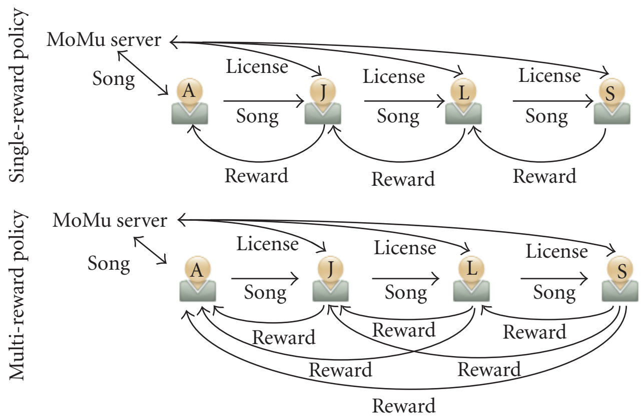


Figure 4: Difference between a single- and a multireward policy. In the single-reward policy the additional financial cost is given back to who successfully distributed the song; in the multireward policy the additional financial cost is split among all the members that successfully distributed the song.

distributed the song. With respect to Figure 4, when Janel acquires the license song, the additional C_I cost is given back only to Alice, but when Lucy acquires the license song, the additional C_I cost is split between Alice and Janel. When Sam acquires the license song, the additional cost C_I is split among Alice, Janel, and Lucy.

From the system point of view, the single-reward policy is very simple to implement, as it simply requires the mobile music store to know who distributes the song. This is possible during the license acquisition procedure (with respect to Figure 4, when Janel acquires the license, the player tells the music store that the song has been received from Alice). Since each mobile customer is uniquely identified (a sign-up procedure is always required to access a music store), the implementation of the single-reward policy is very easy. However, this policy presents a fairness issue: the reward given to a member does not consider if this member bought the song from the expensive cellphone network or if it has received the song from another member using one of the free-of-charge communication technologies. This is quite unfair, as the one who originally distributes the song pays more than the ones who simply redistribute the song. Hence, members may avoid the direct song acquisition from the cellphone network and may wait for the song from other MoMu members. As a result, the single reward policy may slow down the popularity of the mobile music scenario.

Although more complex to handle, the multireward policy can be more fair, as the reward is split among all the members that participated in the song distribution. For this reason, MoMu is provided with a multireward policy that equally distributes revenues along the distribution path (if N is the path length, then each member receives C_I/N). However, it is to note that other reward policies may be considered without affecting the MoMu architecture (as the reward policy is implemented at the server side).

By providing a financial compensation, MoMu members are stimulated to redistribute music files, and hence the multichannel strategy can take place.

4. MoMu Evaluation

In this section we evaluate MoMu from the security point of view, as security is a fundamental feature of distribution systems where users may participate in content redistribution. To this aim, we first analyze different types of users that may use MoMu and then we investigate and highlight different levels of security that MoMu can achieve. Secondly, we analyze the overhead of the security mechanism focusing on workload and on battery consumption. In the next section we complete the MoMu evaluation by investigating whether MoMu meets its goal (reduction of downloading time and of the total cost paid to get digital music over a mobile device) or not.

4.1. Users Typology. As in any other cooperative system, MoMu members may involve different types of users, from rational to selfish to malicious, all with different objectives [31]. Therefore, MoMu has to take care of every possible behavior that may compromise the success of the multichannel approach. In particular, in addition to rational and honest users, the following types of users have to be considered:

(i) *Selfish Users*. A selfish user tends to use resources while giving back few or none of them. This means that the redistribution of e-music among MoMu members will not take place.

(ii) *Malicious Users*. A malicious user tries to block (or disturb) other MoMu members' devices by performing e-music spam send requests (i.e., by trying to distribute thousands of songs at the same time, with the results that other MoMu members have to reply to several proposals or have to switch off the application in order not to be bothered).

(iii) *Dishonest Users*. A dishonest user tries to share, play out, distribute, and modify music songs in different ways with respect to the authorized ones.

To deal with selfish users, MoMu uses an incentive mechanism that stimulates and rewards cooperative users. In Section 3.4 we described this users' behavior and how an incentive mechanism can deal with them.

To discourage malicious users, the advanced MoMu player should be customized so as to allow MoMu members to specify a threshold on the maximum number of requests that another MoMu member can issue in a specific time window. In addition to the threshold, the advanced MoMu player should be able to operate either in PUSH or in POP mode. The PUSH mode is the approach described in Section 3.3, whereas a POP mode could operate in the following way: instead of asking a MoMu member if he/she is interested in downloading a song (i.e., the PUSH mode), a MoMu member specifies what song(s) he/she is interested in.

To protect contents from unauthorized modifications from dishonest users, MoMu uses a security mechanism that provides different levels of security as described in the following.

4.2. Security. Content protection is an important feature when dealing with entertainment contents, as its goal is to avoid unauthorized usage. To this aim, we provide MoMu with a security mechanism based on classic security tools like encryption, watermarking, and hash function so as to ensure that a song can be played out only upon license acquisition and also to guarantee the integrity of a music file.

We mentioned that content protection mechanisms admit no final and provably strong solution, as shown by the history of cracks developed for popular DRMs (see, e.g., [20]). It is worth recalling here that the weak point of most DRMs is that they run on a device that is commonly considered an untrusted environment as it is under the user's control. In fact, in order to be played out, the music content must be in the clear; if a user may access music content in the clear, unauthorized usage or distribution may happen. Therefore, content protection is effective as long as the user cannot retrieve the key from the player/content and cannot capture the unencrypted data while the player plays it out.

To avoid key retrieval, the DRM software must run at kernel level and its integrity should be preferably checked by some secure hardware components. These are the fundamentals upon which all DRMs depend on. To avoid capture of protected data, it is necessary to authenticate also the hardware that handles music contents in the clear [32]. However, although the absence of a provable strong solution, it is important to point out that, nowadays, DRMs are the only mechanisms employed to protect digital contents against unauthorized usage and that a mobile phone can be an interesting environment for developing secure DRM. In fact, as pointed out by Messerges and Dabbish [17], unlike the PC environment, a mobile device is identified through a unique and unchangeable number (i.e., the International Mobile Equipment Identification, IMEI) and also a subscriber's service account can be identified through the International Mobile Subscriber Identity (IMSI). By making available these information to the application layer, a more secure DRM system can result.

The MoMu security mechanism aims at avoiding the following operations on digital music: (i) unauthorized sharing, (ii) unauthorized play out, (iii) unauthorized distribution, and (iv) unauthorized content alteration.

Before analyzing the levels of security achieved by MoMu, we state the security assumptions under which our proposal works.

(A1) We assume a dishonest user with polynomially bounded probabilistic computational power;

(A2) We assume the existence of cryptographically secure hash functions and of secure symmetric/asymmetric encryption schemes. By these assumptions it is computationally unfeasible to break the mentioned cryptographic schemes, and therefore security properties that are based on such schemes have the highest security level.

(A3) We assume statistically invisible, robust, and tamper-resistant watermarking schemes. Since a dishonest user that can read watermarked data can change it at leisure, this assumption implies confidentiality of watermarked data. Properties that are based on such schemes attain an intermediate security level.

(A4) We assume that software is protected to the best of the state of the art: only a dishonest user skilled in reverse engineering might be able to break the protection. Properties that rest on this assumption have the lowest security level.

As mentioned, the MoMu security mechanism is designed to achieve four different goals. In the following we investigate whether those goals are met or not.

(i) *Sharing.* A dishonest user has a song and has free access to the player for which the song has been released. He/she wants to play out the song on another client's advanced player. The security level rests on assumption A4: indeed, the dishonest user can successfully share song if he/she can capture the audio as it is decrypted by the software player (he/she can legitimately make her personal unencrypted copy of the audio stream). Similarly, if he/she wants to embed the watermarking keys in the audio file, he/she must learn the destination player's watermarking key, and this can be obtained with suitable reverse engineering techniques. Also, in this case, the security level is the one of assumption A4.

(ii) *Play Out.* A dishonest user has a music file, but he/she does not have access to the player for which it was released. The security level rests on assumption A3, and therefore the security level is the one of assumption A3.

(iii) *Distribution.* A dishonest user has an authorized music file and has free access to the player for which it was released. The goal of the dishonest user is to make the music file available to other MoMu members by developing an alternative music player. The dishonest user should capture the music content as decrypted by the software player and reuse it in the player he/she writes for distribution. Since he/she has access to the software player for which the music song was released, this is a reverse engineering problem, and therefore the security level is the one of assumption A4.

(iv) *Alteration.* A dishonest user has a music file and wants to modify its content before sending it to another MoMu member. We assume that he/she has no access to the MoMu member's player. To succeed the dishonest user needs to embed a new SD value, with no knowledge of the watermarking key (recall that we assume that he/she has no access to the software player on which it will be reproduced). Therefore, the security level is the one of A3. Conversely, a MoMu member can verify the music integrity in a strong way, meaning that it should be computationally unfeasible to alter the content of the music file. Therefore, since this control is based on a hash function, the security level is the one of assumption A2.

When speaking about security of digital contents, it is worth recalling that the use of hiding schemes like watermarking is subject of a never-ending debate [33]. For instance, Schonberg and Kirovski [34] claim that the development of secure watermarking techniques is not possible with current technologies, but He and Hu [35] are much more optimistic about the security of watermarking techniques.

Far from trying to settle the dispute, we simply note that watermarking techniques are largely used by current DRM systems and that if the watermarking scheme is statistically invisible (users should not take advantage by comparing different watermarked copies), robust (it cannot be removed by simple manipulation of the audio file: for instance, compression or digital-analog-digital conversions), and tamper resistant (it should be impossible to alter/identify/remove the watermark as well as to insert a valid watermark for an unauthorized person), extracting and altering a watermark would be hard with no knowledge of the watermarking key [36]. In particular, different studies (e.g., [37–39]) showed that robustness implies the *secrecy* of the watermark (see, e.g., [40]) (i.e., it is hard to read the watermark without knowledge of the watermarking key).

4.2.1. Overhead of the Security Mechanism. Security operations (e.g., decryption) use complex mathematical operations that can be problematic to mobile devices with limited processing power. For this reason, we analyze the decryption processing cost in relation to entry-level PDAs (processors speed that ranges between 126 and 624 MHz) and cellphones (processors speed around 200 MHz) (e.g., the Nokia Xpress Music cellphone is equipped with a 369 MHz/434 MHz processor, whereas the Apple A4 processor used in iPad and iPhone can operate at a clock frequency of 1 GHz as described at http://www.eetimes.com/electronics-news/4200451/Apple-s-A4-dissected-discussed—and-tantalizing), in order to investigate the feasibility of our approach.

MoMu encrypts music with a symmetric technique. Ravi et al. [41] showed that a 206 MHz SA-1110 processor can sustain a decryption rate of 1.8 Mbps, when fully dedicated to the task, and a decryption rate of 180 kbps when only 10% of the computational resource is dedicated. Therefore, the decryption workload can be sustained by common PDAs and cellphones (e.g., Apple iTunes releases e-music encoded at 128 kbps).

MoMu encrypts the license file with an asymmetric technique, which uses more intensive mathematical operations than a symmetric one. A study performed in [42] showed that an asymmetric decryption takes 2.63 ms for 1 KB of data, using a 100 MHz processor. Again, since this file is usually very small (around 2–4 KB), portable devices can sustain the decrypting of the license file without causing an excessive delay to the content material play out.

The impact of security operations on battery life is another important aspect to investigate as energy consumption of such operations can be very high. Karri and Mishra [43] investigated this aspect, and they considered the energy consumption of a wireless handheld (Symbol PPT2800 PocketPC) while transmitting 64 KB of data over a secure wireless session that employs 3 DES for bulk data encryption and SHA for message authentication. The study highlights significant variations in the energy consumption of various symmetric ciphers with AES and IDEA that consume less than Blowfish. In general 21% of the overall energy consumption is spent on security processing. Raghunathan et al. [44] show another detailed analysis on energy consumption when cryptographic algorithms are used. In essence, they show that a wireless device (iPAQ 3870 PDA) consumes only 1.21 μJ/byte if AES is used as a symmetric cipher.

It is worth noting that a precise estimation of how many resources a security mechanism will consume is not possible in general since it depends on the specific cryptographic techniques used, not to mention that many DRM systems employ obfuscation techniques to increase the security level. Note that code obfuscation is employed at the end host which is usually an untrusted environment, and therefore the code to be run on it is obfuscated to protect the secrets it carries. Here, we simply note that the "old" iPod 3rd generation (processor type PP5002 and speed of 90 MHz ($\times 2$) and the current Apple iPod touch 4th generation (processor speed that is estimated to run around 750 MHz to 800 MHz [45])) performed decryption and ran obfuscated code [46].

5. Experimental Scenario

In this section we complete the MoMu evaluation by investigating whether MoMu meets its goal (reduction of downloading time and of the total cost paid by users to get digital music over a mobile device).

The analysis has been carried out with the following procedure: we considered a song of 4 MB (a common size in the digital music scenario), and we downloaded it using different networking technologies, different cellphone networks (Italian providers TIM and Wind), and different cellphone devices (Nokia N90 and Nokia 6230). In such a scenario, we performed several downloads in different day times (office hours, evening, and night), and we measured the time necessary to download it. In a second analysis we applied MoMu to the above scenario in order to investigate how MoMu might affect the downloading time and the cost paid by users to get digital music on their mobile devices.

5.1. Scenario without Using MoMu. As mentioned, the first experimental scenario investigated the downloading time of digital music when MoMu in not used. In particular, we analyzed the time necessary to get a music song on a mobile phone by first using cellphone network technologies and then by using personal communication technologies.

5.1.1. Usage of Cellphone Network Technologies. We considered two different technologies: GPRS and 3G-UMTS. We investigated the performance of the former technology using a Nokia 6230 cellphone (equipped with GPRS connection class 10, a connection with a higher transfer rate in the GPRS family). During the experiments we noticed that the real transfer rate only occasionally went above 50 kbps (against the theoretical 170 kbps). With such transfer rate the time necessary to download a 4 MB song is around 940 seconds. Using a Nokia N90 cellphone and the 3G UMTS technology, we performed several downloads without changing the device position while downloading. The data transfer rate showed an average download rate of 312 Kbps (a max of 440 kbps was reached), which leads to a downloading time of 102 seconds to get a 4 MB song. Again, the actual transfer data rate is far from the theoretical one (144 kbps, 384 kbps, or 2 Mbps depending on the usage (vehicular, pedestrian, or fixed).

5.1.2. Usage of Personal Area Network Technologies. We considered two different personal area network technologies: Bluetooth and Wi-Fi. The former technology is theoretically capable of achieving a transfer speed of 3.0 Mbps, whereas the Wi-Fi technology is theoretically capable of achieving a transfer speed of 54 Mbps. Unfortunately, practice is different from theory.

In particular, for the Bluetooth technology we experienced an effective transfer data rate that ranged from 723 kbps to 2.1 Mbps. With such data rates, a song of 4 MB may require up to 44 seconds to be downloaded. Note that, for the sake of completeness, it is worth mentioning that Bluetooth requires a connection set-up phase before beginning the data transfer and a study [47] showed that an average connection set-up time between two Bluetooth devices requires around 1100 ms. Therefore, the downloading of a 4 MB song may require up to 45 seconds. The effective transfer data rate of the Wi-Fi technology varied a lot, and in our experimental scenario we experienced a maximum downloading time of 16 seconds for a song of 4 MB and an average downloading time of 5 seconds.

5.2. Scenario Using MoMu. A second experimental scenario investigated how MoMu affects the downloading time and the cost paid by users to get digital music on their mobile device.

5.2.1. Downloading Time. We first investigated how the multichannel distribution strategy affects the downloading time. Initially, 3G network was coupled with personal area networks built upon Wi-Fi technology. We considered a scenario where a MoMu member has only one friend and we varied the probability of successfully distributing a song to this friend. Figure 5 shows the average downloading time in the multichannel distribution scenario. The highest values are the downloading time through cellphone network technologies. It can be noticed that even with low probability of successfully redistributing e-music and with a limited length of the distribution chain (friends of friends who acquired e-music), the reduction of the downloading time is considerable.

Figure 6 presents results obtained from performing a similar analysis, but using Bluetooth instead of the Wi-Fi technology. Again, we considered a scenario where a MoMu member has only one friend and we varied the probability of successfully distributing a song to this friend. Figure 6

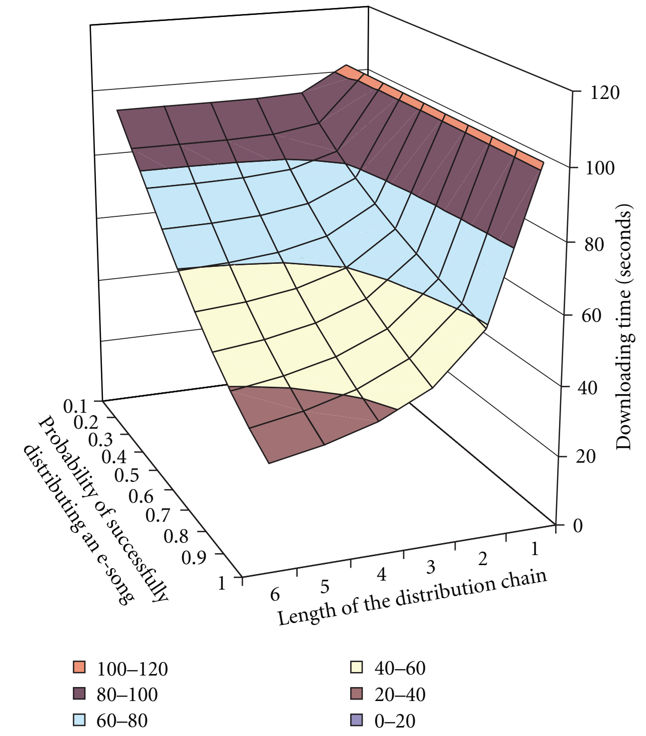


FIGURE 5: Downloading time (average) in a multichannel distribution strategy by coupling the Wi-Fi personal communication technology with 3G cellphone networks.

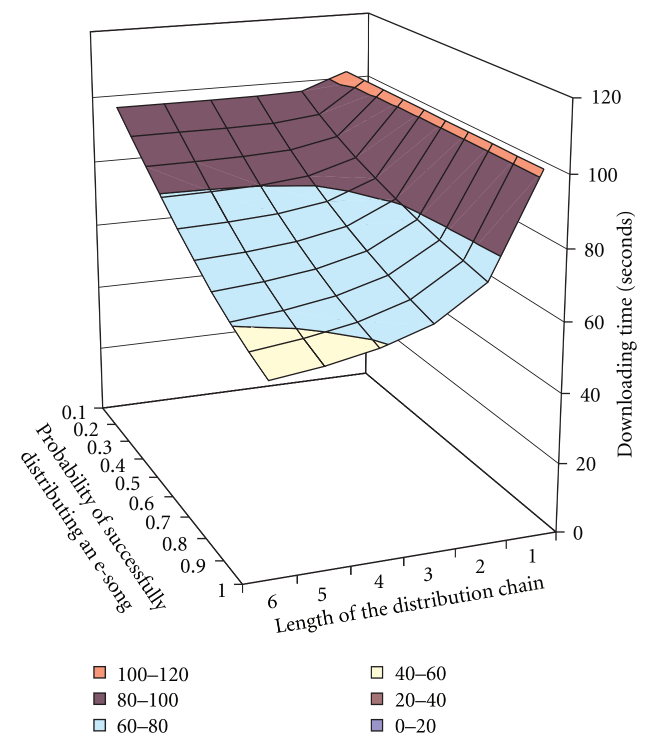
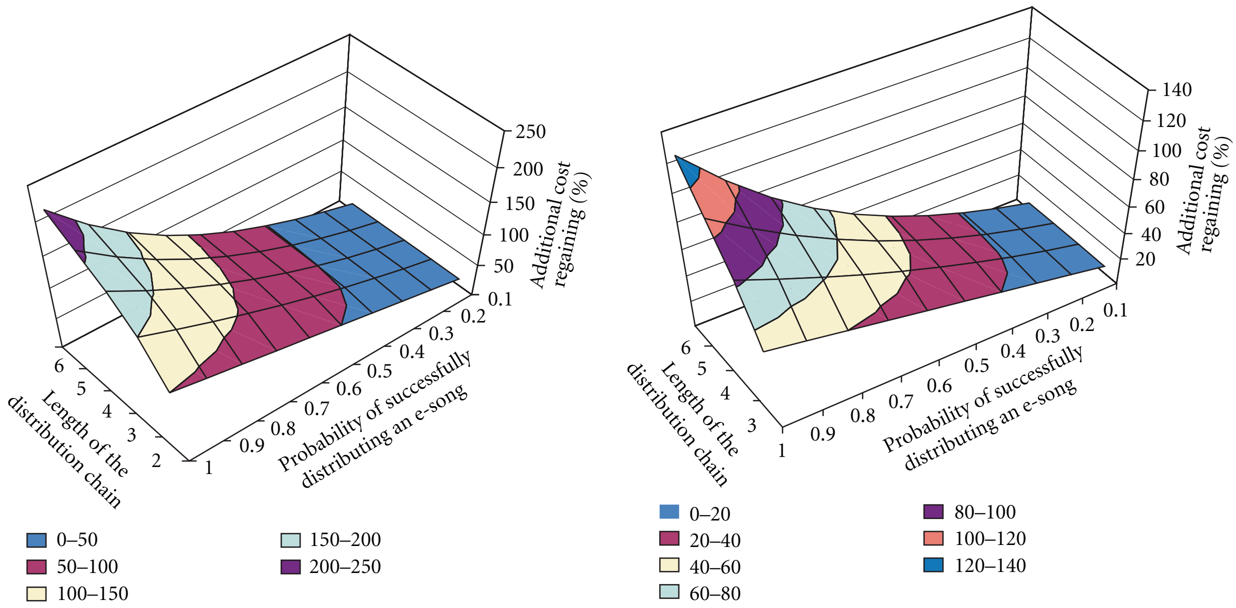


FIGURE 6: Average downloading time in a multichannel distribution strategy by coupling the Bluetooth personal communication technology with 3G cellphone networks.



(a) (b)

FIGURE 7: Additional cost regaining for the first (a) and second (b) members in the distribution chain by supposing only one friend per member.

shows the average downloading time in the multichannel distribution scenario. It can be noticed that also in this case the reduction of the downloading time is considerable.

5.2.2. Cost to Get Digital Music on the Mobile Device. The reduction of the cost paid by users to get digital music on the mobile device is the other important goal of the MoMu architecture.

As early described, the cost paid by users to get a song is given by the cost of the license (C_T), the cost of the license transfer (C_{LT}), and the cost of the song transfer (C_{ST}). These costs are determined by music stores and network operators and cannot be changed by anyone else. Therefore, the cost paid by users when MoMu is not employed can be defined as $\text{COST}_{\text{no\_MoMu}} = C_L + C_{LT} + C_{ST}$. When using MoMu, an addition cost (C_I) is introduced and shared among users using a specific reward policy. Therefore, if MoMu is employed, the cost paid to get a song can be defined as $\text{COST}_{\text{MoMu}} = C_L + C_{LT} + C_{ST} + C_I - C_{\text{reward}}$, where C_{reward} is the amount of money a user receives thanks to the employed reward policy.

The first investigated scenario supposed that any MoMu member had just one friend and we analyzed the rewards of the first and of the second members in the distribution chain. Note that the first member is the one who acquires the song from the MoMu server, whereas the second member is the one who gets the song from the first member. During the experiments, we varied the probability of successfully distributing an e-song and we also varied the length of the distribution chain.

Figure 7(a) shows the reward of the first member, whereas Figure 7(b) depicts the reward of the second member. It can be noticed that the first member can easily regain the additional cost introduced by MoMu and can also achieve an extra profit from redistributing the song (i.e., $C_{\text{reward}} > C_I$). The second member does not achieve the same profit of the first member, but it is worth recalling here that the first member acquired the music song from the MoMu server, and therefore he/she paid the song much more than the second member (who received the song via the free-of-charge personal communication technologies, and hence $C_{ST} = 0$). It is also important to highlight that such results are obtained while supposing just one friend per member.

Figure 8 presents a similar investigation, but in this analysis we supposed that every MoMu member has three friends. In this scenario, the first member achieves very easily an extra profit (up to seven times the additional cost introduced by MoMu), and also the second member can easily regain the additional cost introduced by MoMu and can easily achieve an extra profit.

It is important to point out that, although we supposed a very limited number of friends, the additional cost introduced by MoMu can be easily regained by MoMu members that successfully redistribute digital music ($C_{\text{reward}} = C_I$). Furthermore, the experiments showed that it is possible to easily achieve an extra-profit ($C_{\text{reward}} > C_I$) for the first members of the distribution chain, and therefore this might stimulate users in acquiring and redistributing e-music. In summary, experiments showed that it is very likely that $\text{COST}_{\text{no\_MoMu}} > \text{COST}_{\text{MoMu}}$, which means that MoMu is effective in reducing the cost paid by users to get digital music on their mobile device.

5.2.3. Effects on the Music Chain. The distribution of music in a mobile scenario involves many players, and the most

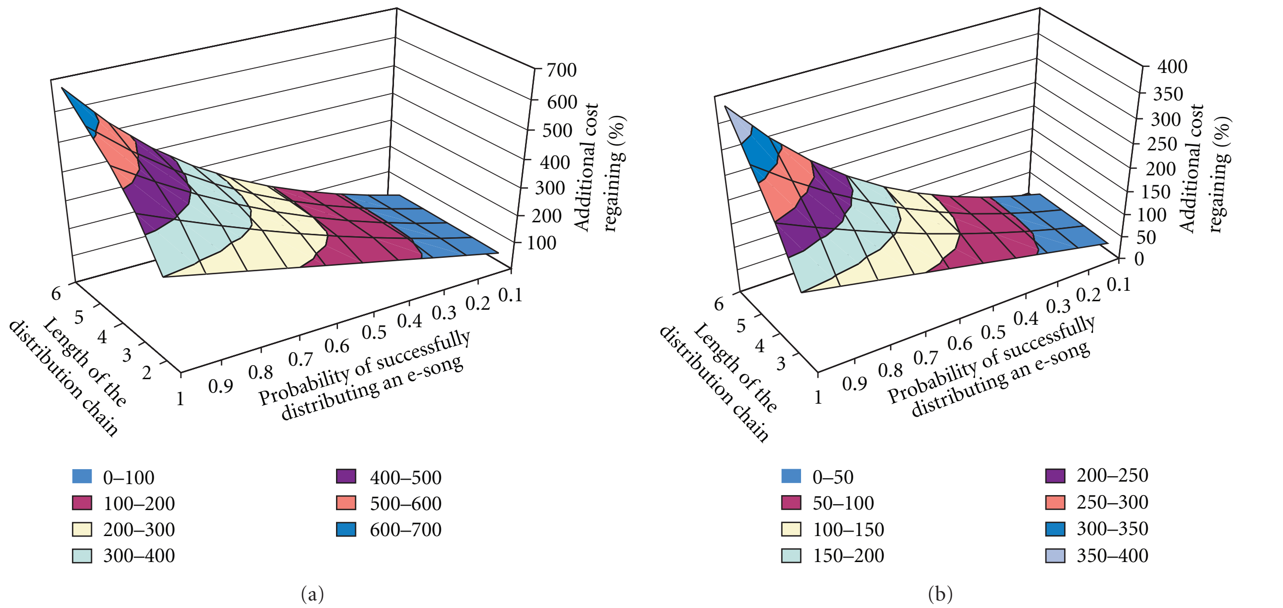


Figure 8: Additional cost regaining for the first (a) and second (b) members in the distribution chain by supposing three friend per member.

significant obstacle in building a successful multichannel strategy is the conflict between different channel players [2]. In fact, a multichannel strategy may be seen as a zero sum game: if one channel player gains, another will not. Here, we discuss possible consequences that MoMu may cause to the players involved in the mobile music distribution. Note that the following are just brief outlines as a detailed analysis of the effects that a multichannel distribution may cause on cellphone industries, network operators, and content owners goes beyond the scope of this paper.

Cellphone Industry. The worldwide mobile phone market grew 19.8% in the first quarter of 2011 fueled by high smartphone growth [48]. These devices are usually employed not only to call someone, but also they allow us to extend our office and our living room. Indeed, the availability of several applications that can run on such devices has brought a new wave in the cellphone industry.

Therefore, the cellphone industry is craving mobile applications that require devices with advanced capabilities (e.g., high storage capacity and wireless communication technologies) as users will likely ask for novel devices. Looking at the different mobile application stores, it is easy to note that the most downloaded applications are the ones with multimedia and social features. Since MoMu has these features, we believe it might benefit the market of the cellphone industry.

Cellphone Network Operators. The main difference introduced by MoMu is that there will be less usage of the cellphone network, as music files will likely be transferred through personal communication technologies. Since most network operators apply a pay-per-bit model, they seem penalized by the multichannel distribution strategy.

Indeed, it is worth recalling that MoMu aims at creating a successful mobile music scenario by reducing long downloading time and high cost of digital music. In such a scenario, customers are forced to use the cellphone network to acquire the license. Moreover, it is worth mentioning that a number of customers will continue to get music files through the cellphone network, as the incentive mechanism and the reward policy give commissions to members who redistribute music to other members. We showed that members may receive higher revenues if they are in the first part of the distribution chain. Therefore, it is likely that MoMu will raise a competition among friends to download a popular hit. A successful mobile music scenario will likely bring benefits to cellphone network operators as recently shown by the success of multimedia and social mobile applications that largely increased mobile data traffic [49].

Content Owners. MoMu might help content owners to expand their market as it might stimulate unplanned purchases. In fact, music is an experience good and, as what happens with any other goods, is subject to the *impulse buying* phenomenon, which is an unplanned and immediate decision to purchase a product or a service. Such decision causes people to feel better. No wonder, the impulse buying is a phenomenon largely exploited in marketing [50, 51].

If we look at the MoMu scenario, we notice that a MoMu member receives a song from another MoMu member. While observing the song title or the song author, the MoMu member enters into the impulse buying process and he/she is stimulated to acquire the song license immediately after the reception of song. As a result, MoMu might stimulate unplanned purchases, and therefore it might help content owners to expand their market.

6. Conclusions

This paper presented MoMu, a multichannel distribution architecture designed to reduce both the downloading time and the price paid by users to get digital music when acquired in the mobile scenario. By exploiting the usage of personal communication wireless technologies and by coupling them with the current distribution model based on cellphone networks, MoMu allows members to freely redistribute digital music among friends. A license-based security mechanism, an incentive mechanism, and a reward policy complete the architecture.

The evaluation showed that MoMu can achieve different levels of security, and the experimental scenario highlighted that the proposed architecture can reduce both the downloading time and the price paid by users to get digital music when acquired in the mobile scenario. A brief overview of possible effects that a multichannel approach may have on the music chain showed that MoMu may introduce a win-win strategy for all the entities involved in the digital music chain (from e-music fans to cellphone operators, from cellphone producers to content owners). Therefore, the proposed approach might be helpful to the success of the mobile music scenario.

References

[1] IFPI, “The digital music report 2011. Research report,” International Federation of the Phonographic Industry, 2011, http://www.ifpi.org/content/section_resources/dmr2011.html.

[2] E. Furregoni, A. Rangone, F. M. Renga, and M. Valsecchi, “The mobile digital contents distribution scenario,” in *Proceedings of the 6th IEEE International Conference on the Management of Mobile Business (ICMB ’07)*, IEEE Computer Society, Toronto, Canada, 2007.

[3] A. Kaikkonen, “Full or tailored mobile web—where and how do people browse on their mobiles?” in *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, ACM Press, Yilan, Taiwan, September 2008.

[4] V. Roto, R. Geisler, A. Kaikkonen, A. Popescu, and E. Vartiainen, “Data traffic costs and mobile browsing user experience,” in *Proceedings of the 4th MobEA Workshop on Empowering the Mobile Web*, pp. 1–6, May 2006.

[5] P. Vlachos, A. Vrechopoulos, and G. Doukidis, “Exploring consumer attitudes towards mobile music services,” *International Journal on Media Management*, vol. 5, no. 2, pp. 138–148, 2003.

[6] C. W. Chu and H. P. Lu, “Factors influencing online music purchase intention in Taiwan,” *Internet Research*, vol. 17, no. 2, pp. 139–155, 2007.

[7] S. Grech and S. Luukkainen, “Towards music download and radio broadcast convergence in mobile communications networks,” in *Proceedings of the*, vol. 2005, pp. 218–224, Pomona, Calif, USA, 2005.

[8] M. R. Ebling and R. Caceres, “Gaming and augmented reality come to location-based services,” *IEEE Pervasive Computing*, vol. 9, no. 1, pp. 5–6, 2010.

[9] V. Ghini, P. Salomoni, and G. Pau, “Always-best-served music distribution for nomadic users over heterogeneous networks,” *IEEE Communications Magazine*, vol. 43, no. 5, pp. 69–74, 2005.

[10] M. Roccetti, P. Salomoni, V. Ghini, S. Ferretti, and S. Cacciaguerra, “Delivering music over the wireless internet: from song distribution to interactive karaoke on UMTS devices,” in *Wireless Internet Handbook: Technologies, Standards, and Application*, pp. 537–565, 2003.

[11] A. Tanaka, “Mobile music making,” in *Proceedings of the 2004 International Conference on New Interfaces for Musical Expression (NIME ’04)*, pp. 154–156, National University of Singapore, Hamamatsu, Japan, 2004.

[12] M. Kubek and J. Nutzel, “A mobile peer-to-peer application for distributed recommendation and re-sale of music,” in *Proceeding of the 2nd International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS ’06)*, pp. 93–98, Leeds, UK, 2006.

[13] G. Stanek, *Bluetella: a java application for new mobile phones*, Semester thesis, ETH Zurich, Zurich, Switzerland, 2003, TIK-SA-2003.19.

[14] E. Cervi, C. E. Palazzi, and A. Bujari, “P2P file sharing on mobile phones: design and implementation of a prototype,” in *Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT ’09)*, pp. 136–140, Beijing, China, August 2009.

[15] A. U. Schmidt, “On the superdistribution of digital goods,” in *Proceedings of the 3rd International Conference on Communications and Networking in China, ChinaCom 2008*, pp. 1337–1344, Hangzhou, China, August 2008.

[16] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, “Digital rights management for content distribution,” in *Proceedings of the 1ST Australasian Information Security Workshop Conference on ACSW Frontiers (ACSW Frontiers ’03)*, pp. 49–58, Australian Computer Society, Darlinghurst, Australia, 2003.

[17] T. S. Messerges and E. A. Dabbish, “Digital rights management in a 3G mobile phone and beyond,” in *Proceedings of the 3rd ACM Workshop on Digital Rights Management (DRM ’03)*, pp. 27–38, Association for Computing Machinery, New York, NY, USA, October 2003.

[18] L. Egidi and M. Furini, “Bringing multimedia contents into MP3 files,” *IEEE Communications Magazine*, vol. 43, no. 5, pp. 90–97, 2005.

[19] Z. Yan, *Digital Rights Management for Mobile Multimedia book chapter of Multimedia Communication Security: Recent Advances*, Nova Science, 2008.

[20] N. Anderson, *Hacking Digital Rights Management*, 2006.

[21] R. MacManus, “Emi music drm-free: what it means for the online music industry,” *ReadWriteWeb*, 2007.

[22] Bluetooth Basics, *A look at the Basics of Bluetooth Wireless Technology*, 2011.

[23] S. Cheng, H. Yu, and Z. Xiong, “Enhanced spread spectrum watermarking of MPEG-2 AAC audio,” in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’02)*, vol. 4, pp. 3728–3731, Orlando, Fla, USA, May 2002.

[24] R. Dingledine and P. Syverson, “Reliable mix cascade networks through reputation,” in *Proceedings of the 6th International Financial Cryptography Conference (FC ’02)*, Southampton, Bermuda, March 2002.

[25] T. H.-T. Hu, K. Wongrujira, and A. Seneviratne, “Reputation in peer-to-peer networks,” in *Proceedings of the IEEE International Conference on Communications (ICC ’04)*, pp. 1411–1415, Paris, France, June 2004.

[26] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Reputation systems,” *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[27] K. C. Almeroth and A. Garyfalos, "Coupons: wide scale information distribution for wireless ad hoc networks," in *Proceedings of the IEEE Global Telecommunications Conference (Globecom) Global Internet and Next Generation Networks Symposium*, pp. 1655–1659, Dallas, Tex, USA, December 2004.

[28] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile Ad Hoc networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.

[29] N. B. Salem, M. Jakobsson, L. Buttyán, and J. P. Hubaux, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '03)*, pp. 13–24, Annapolis, Md, USA, June 2003.

[30] M. Furini and M. Montangero, "The impact of incentive mechanisms in multi-channel mobile music distribution," *Multimedia Tools and Applications*, vol. 37, no. 3, pp. 365–382, 2008.

[31] H. V. Zhao, W. S. Lin, and K. J. R. Liu, "Behavior modeling and forensics for multimedia social networks: a case study in multimedia fingerprinting," *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 118–139, 2009.

[32] Digital rights management (drm), http://msdn.microsoft .com/en-us/library/cc838192(v=vs.95).aspx.

[33] G. Tardos, "Capacity of collusion secure fingerprinting: a tradeoff between rate and efficiency," in *Proceedings of the 12th international conference on Information hiding (IH '10)*, pp. 81–85, Springer-Verlag, Alberta, Canada, 2010.

[34] D. Schonberg and D. Kirovski, "Fingerprinting and forensic analysis of multimedia," in *Proceedings of the 12th annual ACM international conference on Multimedia (MULTIMEDIA '04)*, pp. 788–795, ACM Press, New York, NY, USA, 2004.

[35] S. He and M. Hu, "Performance study of ecc-based collusion-resistant multimedia fingerprinting," in *Proceedings of the 38th Conferences on Information Sciences and Systems*, pp. 827–832, Princeton, NJ, USA, March 2004.

[36] I. Cox, M. Miller, and J. Bloom, *In Digital Watermarking*, Morgan Kaufmann, San Fransisco, Calif, USA, 2001.

[37] X. Luo, J. Zhang, R. Perdisci, and W. Lee, "On the secrecy of spread-spectrum ow watermarks," in *Proceedings of the 15th European Conference on Research in computer security (ESORICS '10)*, pp. 232–248, Springer-Verlag, Athens, Greece, 2010.

[38] X. Li and H. H. Yu, "Transparent and robust audio data hiding in subband domain," in *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '00)*, p. 74, IEEE Computer Society, Washington, DC, USA, 2000.

[39] X. Li and H. Yu, "Transparent and robust audio data hiding in cepstrum domain," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '00)*, pp. 397–402, Piscataway, NJ, USA, 2000.

[40] J. Seok, J. Hong, and J. Kim, "A novel audio watermarking algorithm for copyright protection of digital audio," *ETRI Journal*, vol. 24, no. 3, pp. 181–189, 2002.

[41] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: design challenges," *ACM Transactions on Embedded Computing Systems*, vol. 3, no. 3, pp. 461–491, 2004.

[42] C. Mclvor, M. McLoone, and J. V. McCanny, "Fast montgomery modular multiplication and rsa cryptographic processor architectures," in *Proceedings of the 37th Asilomar Conference on Signals, Systems and Computers*, pp. 379–384, Pacific Grove, Calif, USA, November 2003.

[43] R. Karri and P. Mishra, "Minimizing energy consumption of secure wireless session with QoS constraints," in *Proceedings of the International Conference On Communication*, pp. 2053–2057, IEEE Computer Society, Washington, DC, USA, 2002.

[44] A. Raghunathan, N. R. Potlapally, S. Ravi, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the ACM International Symposium on Low Power Electronics and Design (ISLPED '03)*, ACM Press, 2003.

[45] EveryiPod.com. Apple ipod touch (4th gen/facetime) 8, 32, 64 gb specs, http://www.everymac.com/systems/apple/ipod/ specs/ipod-touch-4th-gen-4g-facetime-specs.html.

[46] EveryiPod.com. Apple ipod 3rd gen (15/20/40) 15, 20, 40 gb specs, http://www.everymac.com/systems/apple/ipod/specs/ ipod-touch-3g-specs.html.

[47] S. Schlott, F. Kargl, S. Ribhegge, and M. Weber, "Bluetooth-based ad-hoc networks for voice trasmission," in *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*, IEEE Press, Big Island, Hawaii, USA, 2002.

[48] International Data Corporation, "Worldwide mobile phone market grew nearly 20% in the first quarter; smartphones and vendors outside the top 5 keys to growth," http://www.idc .com/getdoc.jsp?containerId=prUS22808211.

[49] CISCO, "Cisco visual networking index: Global mobile data traffic forecast update, 2010–2015," http://www.cisco.com/ en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/ white_paper_c11-520862.html.

[50] C. J. Cobb and W. D. Hoyer, "Planned versus impulse purchase behavior," *Journal of Retailing*, vol. 62, no. 4, pp. 384–409, 1986.

[51] D. Rook, "The buying impulse," *Journal of Consumer research*, vol. 14, no. 2, pp. 189–199, 1987.