Using financial incentives to enable legal media distribution in ad-hoc peer-to-peer networks: An introduction to FluidMedia

Christophe Gouguenheim, Salil Pradhan, Cyril Brignone,
John Recker, Bill Serra, Kan Zhang
Mobile and Media Systems Laboratory
HP Laboratories Palo Alto
HPL-2004-15
February 2nd , 2004*

Email: salil.pradhan@hp.com

media sharing, peer-to-peer network, digital right management, copyright, incentive

Can the media industry profitably use peer-to-peer networks to increase their market? We propose a novel media distribution system called FluidMedia that potentially answers this question. FluidMedia provides a framework within which users can trade in media copyrights legally and remunerate the media provider for these. Furthermore, users are actually encouraged to engage in such trade through economic incentives.

* Internal Accession Date Only Approved for External Publication
© Copyright Information Hewlett-Packard Company 2004

1. Introduction

The exponential growth of peer-to-peer (P2P) networks since Napster emerged in 1999 represents a major change in the nature of media distribution. The reaction of the media providers to this phenomenon has been to consider it a significant threat and use legal and technological means to try to stop its expansion. It is clear that the war between the media providers and P2P networks is far from over. Two points, however, are worth considering:

1- The ease of access to media and of media sharing portends a possible scenario where P2P networks become the dominant distribution mechanism [1].
2- It has also been argued that P2P networks actually increase the visibility of media, helping the media providers rather than hurting them by increasing the number of consumers for the output of the industry [2].

A simultaneous consideration of these two points of view led us to believe that a system which would allow a *reasonable compromise* between the user's needs and media providers' needs might allow the media providers to retake control of the market, by authorizing the user to get the fluidity of media she is looking for in today's P2P networks. Furthermore, it could help increase the existing market output and potentially create a large new mass-market for mobile media consumers.

Thus, we wanted to design a system that would meet the following user requirements:

1. User is given flexibility in the way content is moved from one device to another, and this can be done offline (disconnected from the Internet infrastructure).
2. The security implemented for the system should not hinder the ease of usage.
3. A reasonable level of privacy should be provided, guaranteeing that the media bought and played cannot be easily tracked.

At the same time, the system should respect the following legitimate concerns of media providers:

1. Implement adequate security to protect digital contents.
2. Make it difficult and expensive to steal protected digital media and to use the distribution mechanism to propagate unlicensed media.
3. Allow media providers to detect violators quickly, and provide a mechanism to exclude them.
4. Provide a mechanism for license management.

FluidMedia is a digital media transaction system that turns today's media providers' vision upside-down and tries to use financial incentive to encourage media sharing between peers instead of suppressing it. Such a system will potentially be able to create a large mass-market for media distributors in addition to providing a legal, commercial, and convenient way for its users to perform the digital file swapping that, say, KaZaA users practice today.

2 Tenets of FluidMedia

In this section we formally lay down the design requirements for FluidMedia so that it satisfies the needs of both the user and the media providers.

2.1 Increasing the fluidity of media

HP Labs developed the FluidMedia system in order to enable a synergistic collaboration between the user and the media providers. FluidMedia allows media to "flow" from one device to another, while at the same time allowing media providers to preserve their copyrights.

Social interactions have great potential to propagate media by increasing their visibility within a community or strata of society [2]. FluidMedia takes advantage of this aspect of social interactions and enables the transfer of media between two devices belonging to two parties – one a buyer and the other a seller. A significant feature of FluidMedia is that it can function as long as the users have some form of connectivity - local or remote. This transfer is accompanied by monetary payment from the buyer to the copyright owner. We illustrate the paradigm of FluidMedia by means of a few examples:

1. The buyer downloads a song from an MP3 player or stereo of the seller at a social event to her own MP3 player.
2. The buyer downloads a song from the seller who is the co-passenger in a bus, using cell phone. This is done locally, using either Bluetooth or 802.11, without connectivity to the Internet infrastructure.
3. The buyer joins an ongoing networked game in a subway wagon by buying the game from one of the players' portable game player.
4. The buyer downloads a movie from a neighboring car on her car video player in a campground.
5. The buyer buys an e-Book from the handheld of a passenger in an airplane.

It is possible that the payment for the media transfer is deferred till later, as is illustrated by examples 2 and 4 above.

FluidMedia goes one step further – it actually encourages the user to become a point of media sale. To accomplish this, the system rewards a seller with a commission for every digital content transfer from her.

Since typical sales transactions are completed quickly, each user need only sell a new file to a few other users for a distribution tree to evolve, enabling content to propagate rapidly through a community of users. The ability of media to rapidly propagate through a community also means that the opportunities to sell specific media diminish rapidly within a community. As a result, a user who is motivated to sell media must act early or possibly see her community saturated. This provides further incentive to an ambitious seller to engage in aggressive sales.

The capability for any FluidMedia user to turn into a point of sale and get remuneration for distributing media can be also applied in the places where media are usually played, for example in nightclubs, coffee shops, at concerts, etc. Those new media retailer can

thus consider media distribution as a source of revenue, and are motivated to extend the concept of impulse purchase to media. Here are some examples of possible scenarios:

1. The buyer purchases the album of the playing artist at a concert.
2. The buyer downloads the song she is dancing on in a nightclub, or listening to in a coffee shop or a supermarket.
3. The buyer purchase the license to play a movie whose preview is playing on a screen in a fast-food or in the street.
4. The buyer use the refill time at a gas-station to download a movie on her car video player.

Finally, FluidMedia provides media providers some means to manage content licenses throughout the distribution chain. They can provide the user the ability to get "trial-versions" which are low quality, 30 seconds of play or automatically erase after a predetermined number of plays. The user can directly purchase it at any moment, without having to reconnect to any Web site. They can as well distribute different quality versions of media at different prices, making it possible for a user to purchase a low-quality version of a song for her cell phone and decide later to upgrade it for playing it full quality on her car sound system.
The architecture of FluidMedia thus tries to reach maximum digital media fluidity. It enables easy and convenient acquisition of digital media by (a) separating the digital content from its license, and (b) allowing offline transactions and deferred fee payment.

2.2 Separation between the digital content and its license

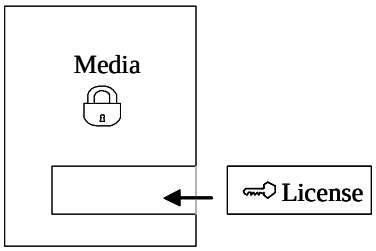

Figure 1: Separation of the content from its license

To enable FluidMedia to attain media optimal fluidity we separates digital media from its license. This paradigm is shown in Figure 1. FluidMedia makes it impossible to read media without having purchased its license first. Thus, within the FluidMedia framework, digital media transactions are actually license transactions, followed by the digital content transfer from one device to another.

This separation of media from its license offers several advantages. Since it is one of the key ideas behind FluidMedia, we expatiate upon these below:

1. It ensures the possibility of doing quick transactions. For example, FluidMedia allows a user to purchase the license of a movie while watching the preview, but

postpone the actual transfer of the movie until later (for example, if she uses a small storage device like a cell phone or a watch to purchase the license).

2. Following this, content becomes ubiquitous. However the copyright is enforced by the fact that the physical presence of its license is required to play a media. Thus two copies of the same media cannot be played *at the same time*. Therefore, in the respect of copyright and by the limits imposed by media providers, FluidMedia makes it possible for a user to copy, at will, any media on any device. Carrying a collection of media becomes equivalent to carrying the collection of licenses.

2.3 Offline transactions

The huge expansion expected in wireless home networks [3, 4] would obviously help the FluidMedia model to thrive online. However, we do not wish to restrict media transactions only to online settings. Such a restriction would undermine our idea of promoting media distribution through social interaction.

Thus, FluidMedia allows the user to perform an offline transfer of license, and to defer the payment for the transferred license. The dues for such transfers can be billed to each user periodically. To ensure compliant behavior, the ability to perform offline transaction could be based on certificates expiring unless these dues are cleared. Additionally, we could also limit the value and quality of offline transactions, or have the quality of the media degrade over time.

3 Architecture and implementation

In this section we look closely at the physical implementation of the FluidMedia system.

3.1 Secure portable co-processor

The FluidMedia system is based on the notion of a highly secure portable co-processor (such as a smartcard), and a trusted host (such as a MP3 player, stereo, or a DVD player). Figure 2 illustrates this asymmetric architecture. The security of the system hinges on the secure co-processing unit. Only a reasonable assumption of security is made for the host. Plugging the secure portable co-processor in a host gives the host access to the licenses and user's personal data stored in the co-processor. Transaction of licenses is done over a secure communication channel between two co-processors. Breaking into the host would give the hacker, at best, some unencrypted media. Protecting the media once the playing device is broken seems however unrealistic. On the other hand, some important data, such as money and licenses, cannot be extracted from the device.

A FluidMedia host is therefore "inert," in the sense that it cannot be used to play any media or perform any transaction, regardless of the quantity of digital content it stores in its memory. Only a FluidMedia co-processor enables the host to play media for which licenses are on the co-processor, and to perform media transactions in the name of the user whose personal transaction data are stored on the co-processor. As an example, various parties can operate a stereo by plugging their individual FluidMedia co-processors into it.

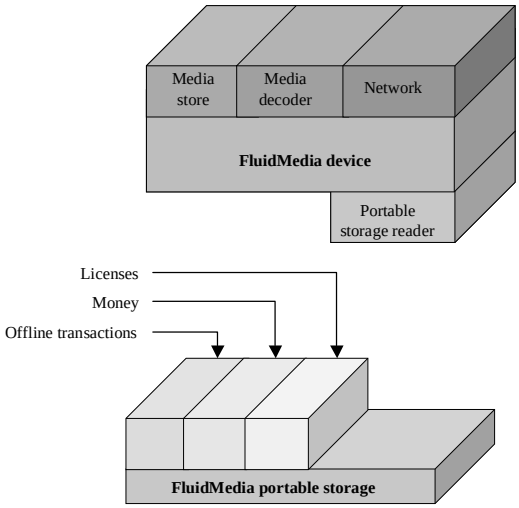

Figure 2 : FluidMedia architecture

The money used on the secure co-processor can follow the prepaid model, where a user buys some tokens in advance that allow him to purchase media. Alternatively, these tokens can represent the amount of money owed by a user to a media provider. This use of virtual money is likely to decrease the incentive for hacking the co-processor. Tokens are used as real money to set the price of digital content, can be transferred using hosts from one secure co-processor to another, or redeemed later by media providers.

3.2 Ad-Hoc Connectivity

A transfer of media between two FluidMedia hosts involves a wireless connection. This connection can use IrDA, 802.11, Bluetooth or any other wireless technology. Connection diversity [5] is used to make the details of the technology used and the wireless configuration transparent to the user. From the user point of view, connecting a remote device is as simple as pointing at it and pressing the connect button or browsing the surrounding devices when looking for a particular media. In this last case, all the FluidMedia devices assemble in a bounded space, like a shopping center or a subway wagon into a local network where all users have an incentive to share music and video with each other or purchase on-going multi-player games.

The following table shows the bandwidth offered by the today's wireless technologies. It shows how a device using 802.11a can download a full quality movie in a reasonable time. However power considerations restrict its use to "big" devices such as stereos or car video players. The low power consumption of 802.11b and Bluetooth make them perfect for small appliances such as PDAs, MP3 players and cell-phones. Those can quickly download medium to full quality music, as well as games, e-Books and other "compact" media.

	Power consumption (*) (mA)	Actual Speed (*) (Mbps)	MP3 file (4MB) download time	Serie episode (80MB) download time	Movie file (600MB) download time
BlueTooth	60	0.7	45 s	15 min	2 h
802.11b	300	2-3	16 s	5 min	40 min
802.11a	500	27	1.2 s	23 s	3 min

Figure 3 : Wireless performances
(*) average data from products on the market

3.3 Selling station

A user will regularly connect to a selling station to clear her offline transaction log by:

1- paying her dues,
2- getting a reward for the sale of media, and
3- backing up the media log in case of loss of the co-processor.

Additionally, she can purchase new tokens and media. As we have mentioned, several techniques ensure that the user regularly connects to a selling station. In the case where FluidMedia would include several media providers, the same selling station could interface all the media providers. Alternatively, there could be a selling station for every single media provider.

Two types of selling stations can be envisioned: remote and local. A user would connect a remote selling point through the Internet, or through a connection to a FluidMedia device connected to the Internet and acting as a proxy. An example of the latter scenario is a user buying a song in a nightclub and taking advantage of this transaction to clear her offline transaction log. On the other hand, more security could be guaranteed to the media provider with local selling station which would operate on a model similar to that of Automatic Teller Machines.

3.4 Back-end

While FluidMedia allows offline transactions to leverage opportunities to acquire and share media, it takes advantage of connectivity whenever possible. From the point of view of the media providers, online transactions are more secure. They thus provide additional services that act as an incentive for the user to perform media transactions while connected to the Internet infrastructure. Online transactions allow the user to connect several remote devices, creating a wide network like KaZaA. As an incentive, each user is rewarded proportionally to her contribution in media sharing. Performing an online transaction presents the added safeguard to the user of allowing a backup of the purchased media by the media provider.

In case of loss or theft of the co-processor carrying the media licenses, FluidMedia provides a mechanism for retrieving the lost licenses even if they have not been directly backed up during a connection to the media provider. Analyzing the transaction logs of the users she did transactions with can reconstruct the list of licenses owned by a particular user with reasonable accuracy.

4 Prototype

HP Labs implemented FluidMedia using a tamper-proof smartcard as the secure portable co-processor used to carry licenses and deferred offline transactions. We explain our choice below.

Smartcards offer several characteristics very desirable for FluidMedia:

1. Their small size makes them easily portable,
2. They embed memory and an integrated circuit chip which can be optimized for cryptographic calculations, and
3. They are tamper proof.

However, there are two important limitations to the use of smartcard for implementing FluidMedia:

1. First they have very low resources in terms of memory and computation capabilities, which could become a problem when dealing with digital media. The best off-the-shelf smartcards provide 64Kbytes of EEPROM, while the latest prototypes go up to 256K. This is far from the average size of an MP3 file, several megabytes.
2. They are not absolutely tamper-proof, as shown by Anderson and Kuhn [6]. These attacks, though expensive, must be taken into account while designing the security model.

The separation of licenses and content provides an elegant way to deal with memory limitations. Only the licenses are stored on the smartcard, while media stays on host devices. A license is basically a key that allows a user to decrypt the associated media. A key of 128 bits provides a satisfactory encryption level, and allows the storage of 250 licenses in a 32 Kbytes memory. Figure 3 shows how we deal with a 64 Kbytes smartcard. A 128Kbytes smartcard would thus contain nearly as many FluidMedia licenses as most of today's MP3 players. The eXtensible rights Markup Language XrML is also used to implement different license policies in FluidMedia. As for digital content, the rights XML headers are not stored in the smartcard itself, but are added to the digital content. A single media file can thus have different types of licenses (basic license, "trial-version" license, etc.), represented by different XrML headers at the beginning of the file. A specific license is stored in the smartcard and contains a pointer to the corresponding XrML header.

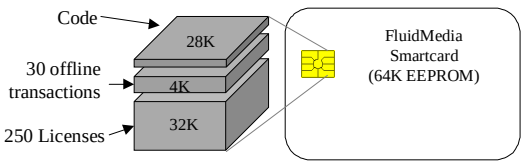

Figure 4 : Memory management of a smartcard

Finally, our implementation gives a unique decryption key for each piece of media, regardless of the device on which the media is downloaded. This enables the user to read a purchase media on any device. As we will see however, a same piece of media is encrypted differently on different devices.

4.1 Transactions in the FluidMedia model

Figure 5 : FluidMedia MP3 player and FluidMedia video player

We developed two prototypes of FluidMedia devices presented on figure 4. Both of them present the novelty, compared to usual media players, of having a smartcard reader and wireless connectivity, allowing them to connect to other FluidMedia devices. Completing a purchase transaction is a three-step process. First, the smartcards authenticate each other and establish an encrypted connection. Next, the smartcards verify that the user initiating the purchase has sufficient tokens to purchase the selected media. Assuming sufficient tokens, the purchasing smartcard deducts the purchase price and the selling smartcard delivers a media key to allow the purchasing device to decode the purchased file. During the transaction, the smartcard logs some details of the transaction, such as the IDs of the peers doing the transaction and the fee to be paid to the distributor of the media.

The purchaser then has the option to download the actual media file. Before the transfer, the media file is decrypted and re-encrypted using a key suitable for the buying device, ensuring that it can only be decoded when a smartcard with the right media key is present in the buying device. Once download is complete, the user can play the newly purchased file on the device.

Alternatively, a user can use a device to connect to a PC running a FluidMedia server. While the PC resident service can perform the same media sale function as any other FluidMedia device, it is additionally capable of selling tokens to a user's smartcard. Prior to updating the tokens on a smartcard, the service deducts tokens representing fees due the media distributor and checks transaction logs from the smartcard to detect possible fraudulent use of the system.

4.2 Security issues

Security is a key to ensuring the success of the FluidMedia system. We want to design our security model so that it discourages most users from cheating, mainly because it is too expensive (requires breaking an MP3 player). But most of all we focus on the fact that the hacker can neither make other FluidMedia users benefit from her hacking nor generate money by distributing fake media. All she can get is unencrypted media.

Having a single decryption key for each piece of media means that each user of the media would have this key. Therefore, if one of them breaks her device and extracts the key, she could publish it and allow everyone to decrypt this media. We solve this issue by keeping this key inside the tamper-proof smartcard, and using it as a master key to generate a device-dependent decryption key. It is, of course, worthless to publish this device-dependent key.

Before each license-key transaction, the smartcards authenticate each other and derive a one-time-use session key from this mutual authentication. This session is used to create an encrypted communication channel between the smartcards. The transfer of tokens and licenses is then performed over this encrypted channel. The mutual authentication protocol is based on certificates expiring periodically. It means that the user must connect periodically to the media distributor to get his/her certificate renewed. The media distributor takes advantage of this connection to upload the transaction log and get the user to pay for his/her offline transactions.

If we suppose smartcards are absolutely tamper-proof, our model is secure in the sense that cracking the FluidMedia device would not give the cracker access to media decryption keys or money. In reality smartcards are not unbreakable. We are thus exploring the possibility of using other secure devices such as TCPA hardware running Palladium [7]. Such secure FluidMedia devices would authenticate FluidMedia smartcards to be valid and contain valid licenses before playing media. We address the issue of tampering with money by performing statistical analysis of uploaded transaction logs. In this model, a user generating fake money gets caught when the users she has done transactions with report their transactions log.

See [8] for details about the security design.

5 Conclusion and future work

In this paper we present a paradigm that encourages the movement (or “fluidity”) of media through financial incentives given to the user to share and propagate her media. This represents a paradigm shift from the existing setup where such sharing and propagation is deemed undesirable and illegitimate.

While we were working on this paper and prototypes for FluidMedia, Apple unveiled their iTunes technology which enables media to be fluid, but within the constraint of a single user. In other words, using iTunes, it is possible to port media from one device to another, provided they are operated by the same user.

The paradigm we propose for FluidMedia takes this one step further and allows media propagation both within a single user environment, and between several users. Thus it is a more “interuser” framework than iTunes, which is in some sense “intrauser.” We thus view iTunes as the first step in a paradigm shift towards total fluidity of media. What we propose therefore, is “media sans frontier” but within a legal framework that makes it profitable for all parties to engage in such transactions.

Future work is proceeding along two distinct lines. Firstly, we are exploring whether the notion of sharing can be extended to other domains besides media. Secondly, we are trying to strengthen the security framework which will provide the backbone of such paradigms in future.

6 Acknowledgement

We thank Vinay Deolalikar for his comments, suggestions and for reviewing the paper.

7 References

[1] S. Ghosemajumder, P. Bangayan, and G. Bonet. Digital Music Distribution. *Digital Business Strategy Professional Seminar*. 2002.

[2] T. O'Reilly. Piracy is Progressive Taxation, and Other Thoughts on the Evolution of Online Distribution. www.openp2p.com/pub/a/p2p/2002/12/11/piracy.html

[3] K. Scherf. Trends and Outlook for Wireless Home Networks. *Parks Associates' White Paper*. 2002.

[4] K. Scherf. The Emergence and Growth Of Entertainment-Centric Home Networks. *Parks Associates' White Paper*. 2002.

[5] J. Tourrilhes, V. Krishnan. Using wireless diversity for more than just connectivity. *HP External Report HPL-2002-258*. 2002.

[6] Ross Anderson, Markus Kuhn. Tamper Resistance - a Cautionary Note. *Proceedings of the Second Usenix Workshop on Electronic Commerce, pp. 1--11*. 1996.

[7] Ross Anderson. TCPA / Palladium Frequently Asked Questions. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html. 2003.

[8] K. Zhang, C. Brignone, C. Gouguenheim, F. Kitson, S. Pradhan, J. Recker, and B. Serra. FluidMedia: an offline peer-to-peer media transaction system. *HP Technical Report HPL-2002-342*. 2002.