P2P-Next: Technical and Legal Challenges

Raul Jimenez
Royal Institute of Technology (KTH)
Stockholm, Sweden
Email: rauljc@kth.se

Lars-Erik Eriksson
DACC Systems AB
Täby, Sweden
Email: lars-erik.eriksson@dacc.se

Björn Knutsson
Royal Institute of Technology (KTH)
Stockholm, Sweden
Email: bkn@kth.se

***Abstract*—P2P-Next aims at providing solutions and applications for digital content production and distribution, while keeping a continued analytical focus on the regulatory arena and legal aspects.**

In this paper, we address netorking, access control, and payment in P2P content distribution, three topics which are not only technically challenging, but they also require careful consideration of related legal and commercial issues.

Finally, a design proposal is presented. This design considers technical capabilities, legal requirements and it is flexible enough to support different business models.

I. Introduction

The use of Audiovisual Media is moving from a collective and passive approach to personal active behavior. At the same time use patterns are shifting towards non-linear usages, moving away from the classic model of linear broadcast TV. The TV set no longer has the monopoly of delivery of audiovisual content; the PC, mobile phones, and initiatives from new stakeholders are all becoming increasingly important.

In such heterogeneous environments, efficient content delivery needs optimized unicast, multicast, broadcast, and also support from the recent advances in P2P grids. A phenomenon like P2P that involves over 66% of all Internet traffic is vital to an information society and needs to be investigated to unlock further potential.

This situation has important consequences for the existing business models and institutions, as well as for content production, content distribution, end user experience on various terminals and creators possibility to be remunerated for their works.

II. The P2P-Next Project

P2P-Next [1], an EU FP7 Integrated Project, develops an open source, efficient, trusted, personalized, user-centric and participatory television plus media delivery mechanism with social and collaborative connotation using the emerging (Peer-to-Peer) P2P paradigm taking into account the dynamics in the existing EU legal framework.

P2P-Next will build a next generation P2P content delivery platform, to be designed, developed, and applied jointly by a consortium involves 21 partners in 12 different countries, including large European players, SMEs and Subject Matter Experts to manage highly-focused technology components.

The system architecture is developed according to a user-centric paradigm and shall ensure the networking fabric to be able to drive over 50% of future Internet traffic to enable the field to move from simple file sharing towards content sharing, by seamlessly merging content, communities, communication, and commerce.

The technical approach includes: assessment of the legal situation for all stakeholders of P2P-Next, research and development of sustainable business models for the complete value chain, research and specification of a set of payment models, research and development of a set of advertising and other free view models and related tools suitable for linear as well as non-linear services.

III. Challenges

In this section, three selected challenges are described: networking, payment, and access control.

A. Networking

The current infrastructure of the Internet is not suited to simultaneous transmission of live events to millions of people (i.e. broadcasting). The problem is that a dedicated stream of data must be sent to every single user. With millions of potential users simultaneous streams of data will easily congest the Internet. For several years, we have been told that the answer to this problem is ”multicasting”, whereby the data stream is distributed to many local servers that subsequently ”re-broadcast” the content to local users. However, most IP routers cannot support multicasting and there seems to be no financial incentive for the ISPs to introduce multicasting.

Furthermore, multicasting is synchronous. Receivers can only access the content which is currently being transmitted, a clear departure from what Internet users are accustomed to. While a degree of on-demand service can be provided using a PVR (Personal Video Recorder), similar to traditional broadcast TV, it shares the same limitations.

P2P is based on unicast, the natural way of transmitting information on the Internet. Peers transfer data to one another in a end-to-end fashion. What makes P2P so powerful is its “exploding” capability. It uses peers as exploders, making each peer simultaneously receive and send data to several peers. This scheme provides scalability and decreases the amount of resources needed for a producer to distribute its contents.

One of the main challenges in P2P distribution is the lack of topological-awareness. Unlike multicast, flows of data are not topology aware in P2P networks. Currently, peers connect to randomly selected peers therefore, the flow (the P2P overlay) is completely independent from the network topology.

This means that a single piece of data is likely to be transmitted through the same network link several times, unlike multicast, where it would be transmitted just once.

Several approaches are being developed to provide P2P topology awareness. P4P [2], for instance, uses an oracle service provided by the ISPs which hints peers with information about network topology.

In P2P-Next, a combination of topology-awareness and caching is proposed. In this paper, we focus on caching because it does not only poses a technical challenge but also other challenges such as commercial and legal.

ISPs are in an excellent position to host a P2P cache. By doing that, inter-ISP traffic is reduced and costumers enjoy a better service. In order to be efficient, however, the caching process has to be totally automatic. ISPs must be able to cache any piece of content without needing prior agreements with the distributors and/or the copyright holders.

In order to maintain current business models, producers need to restrict access to their content and ISPs need to be able to cache content. Here is the dilemma; if ISPs are able to download any content without prior agreement, so is any other peer in the network. Therefore, the producers have an incentive to make caching impossible, and we all lose.

In the long term we can expect that producers adapt their business models to the new environment. The process, however, can take a long time. P2P-Next is willing to face the challenge now and offer a system which supports existing business models as well as more innovative ones.

B. Payment System

One of the main problems facing the Information Society is a lack of transparency in IT services and products. This causes end users to lack trust in IT solutions. Technical developments are today so rapid and the possibilities of electronic surveillance and accumulation of personal data are huge. Today successful products and services ought to be fast, customised secure and trustworthy. Trustworthiness is becoming a key factor.

Business start to discover that good privacy is of great interest to users. Examples are new payment solutions where users do not have to give away such personal data like credit card information. It has become more and more evident that privacy protection cannot be based exclusively on directives, regulations and law enforcements (e.g. EU directives 2006/24/EC (on the retention of data generated or processed in connection with the provision of publicly available electronic communications), and the previous related directive, 2002/58/EC concerning the protection of privacy in the electronic communications sector.)

P2P-Next intends to implement a service for payment of content since there are several reasons to go beyond state of the art in relation to present payment systems. Some examples are:

- Micro-payments. Many existing services claim they implement micro-payments but are not micro-payments in the original sense (1/1000 Euro) but rather in the order of 1 - 5 Euro.
- Metadata. Existing payment services cannot interact with content metadata and make use of price information to enable flexible billing services.
- Business models. Existing payment services cannot easily implement specific business models.

There are several privacy issues to be considered beyond what directives, regulations and national implementations of these require:

- A payment system shall not know what users buy. Only the buyer, the seller and their associated accounts and the price shall be known and possibly time.
- A seller on the other hand shall know only the price paid, the content and other relevant data for statistical use.
- Users shall not be able to figure out what other users are buying and be able to collect such material.
- It shall be possible for documentation purposes in special cases to re-create the full sale and buy process. Who, content, seller, price paid, time, etc.

C. Access Control

Although part of P2P-Next's tasks is to research and develop innovative business models, we would like to build a flexible platform where different business models can compete.

Traditional business models rely on access control mechanisms. For instance, a producer selling its content will have in place a mechanism which determines whether a given user paid for the content, and if so, deliver the content to him.

Another example is a national broadcaster. Usually, national broadcasters buy the rights to show a piece of content within the national territory. Therefore when offering on-line services, the broadcaster must check where the user is located. This is usually done by checking the user's IP address against a geolocation database.

Currently, file sharing networks such as BitTorrent are unaware of these restrictions, therefore the content is indiscriminately distributed. The scenario can be further illustrated with the attempt to distribute the movie "Slacker Uprising" via BitTorrent while restricting the distribution to just USA and Canada.[1]

The challenge lays on reconciling the dramatically opposed goals of the underlying distribution system (BitTorrent) and the existing commercial distribution model.

IV. Discussion

The main characteristic of P2P file sharing systems such as BitTorrent [3] is that they are scalable. This means that any single producer with limited resources would be able to distribute a piece of content to a very large number of consumers. The reason why this is possible is because consumers not only receive data but also redistribute to others, not only consuming but also adding resources to the system.

This fact dramatically changes the rules of the game. Now, the consumers are active components in the distribution

[1]Michael Moore on Slacker Uprising's Piracy 'Problem' http://torrentfreak.com/michael-moore-on-slacker-uprisings-piracy-problem-081006/

process. Therefore, restricting distribution in order to deploy an access control mechanism necessitates the consumer's cooperation.

The first step would be to place trust at the consumer's side. This can be done by simply trusting the consumer to voluntarily follow the policies specified by the producer. Or, if the consumer cannot be trusted, then by requiring the consumer to use tamper-resistent hardware that will execute only software signed by the producer, it is possible to create obstacles for circumventing the policies. (Since P2P-Next produces open-source software, it is not possible to just rely on security by obscurity.)

Some would argue that such access control mechanisms already exist in BitTorrent in the form of private trackers. Private trackers' goal, however, is to force users to share their bandwidth and not actually to protect the content being distributed. [4]

This model works because the users which follow the rules are protecting their bandwidth from free-riders[2]. If the item to be protected were the content, users would lose the main incentive and be tempted to break the rules leaking the content to other users.

P2P-Next aims for a trackerless/distributed tracker model, which complicates the implementation of this model of protection, since it shifts the responsibility to correctly implement the restrictions to all participants, instead of only the single tracker.

Whether centralized or distributed, there are some disadvantages implementing this kind of access control mechanism. It adds complexity to the core of the P2P system. It is difficult to replace should a flaw be discovered. Finally, it makes caching more difficult, if not impossible.

As described in Section III-A —caches being part of the P2P network— there is no way to tell the different between a normal peer and a cache. Unless there is a prior agreement between the producer and the ISP, the caching peer is a non-authorized peer. Therefore, protected content cannot be cached.

There exists access management models where distribution and access are totally separated, e.g., satellite- and cable TV [5]. While a satellite's beam covers a large area, not every person with a satellite disc is able to access the content. The disc receives encrypted data which can only be decrypted with the right key. Satellite TV vendors do not attempt to control the distribution data channel, but rather access to the actual content by controlling the distribution of the keys.

Satellite TV has another similarity with P2P, the fact that every user receives exactly the same encrypted content. That is, encrypted with a single key which is valid everywhere. If we were to individually encrypt the content, the satellite's capacity requirements would be linear with the number of users instead of constant. The same is valid for P2P networks, if the content is individually encrypted, the content provider alone would have to provide the bandwidth capacity because the users could not help in the distribution.

When we consider the payment requirements regarding privacy, it is very clear that the access control mechanism and the payment system must be separated.

In a pay-per-view scenario, a consumer would need to show a proof of payment in order to get access to the content. A payment entity can create a certificate which do not include any identifying information.

This would open the possibility of anonymous payment from the producer's point of view. A reconstruction of the process could be done with the collaboration of both entities in special cases such as police investigations.

We can expect that a system which allows producers to conveniently and cheaply distribute their content would drive content prices down, pushing payment entities to implement micro-payments in the order of cents instead of Euros. This also opens the market for innovative business models which could dramatically change the content distribution business as a whole.

V. Proposed Design

In this section, we propose a design which addresses the challenges previously described in Section III and discussed in Section IV.

As seen in Figure 1, there are five major components in this system: producer, consumer, p2p core, ACS, and payment.

Producer refers to the software application used by the producer to interact with the system. *Consumer* in turn, is the user's software application.

P2P Network is the transportation mechanism which transfers data from producers to consumer. Removing restrictions on the transportation mechanism simplifies its design, letting developers focus on efficient data distribution. It also enables easy caching, meeting the requirements described in Section III-A.

P2P-Next's system is currently based on Tribler [6] which is an implementation of the widely deployed BitTorrent protocol [3]. Our design, however, is generic enough to be used with any transportation mechanism.

The *Access Control Service (ACS)* is the mechanism which applies the policies given by the producer, i.e., providing access only to authorized users. A consumer must provide a token in order to get access the content.

Finally, the *Payment* subsystem transfers money from the consumer to the producer. The consumer, in return for the payment, receives a token (i.e., a proof of payment).

Notice that the content transiting the P2P network can be encrypted[3] if the business model requires access restrictions. This fact moves the restrictions from the P2P network to the ACS. The Access Control Service restricts access to the decryption key to only authorized users while the data is freely distributed and cached.

There is also a clear separation between the payment and the access control systems. They can communicate through

[2]Leechers in BitTorrent jargon.

[3]{content} symbolizes encrypted content.

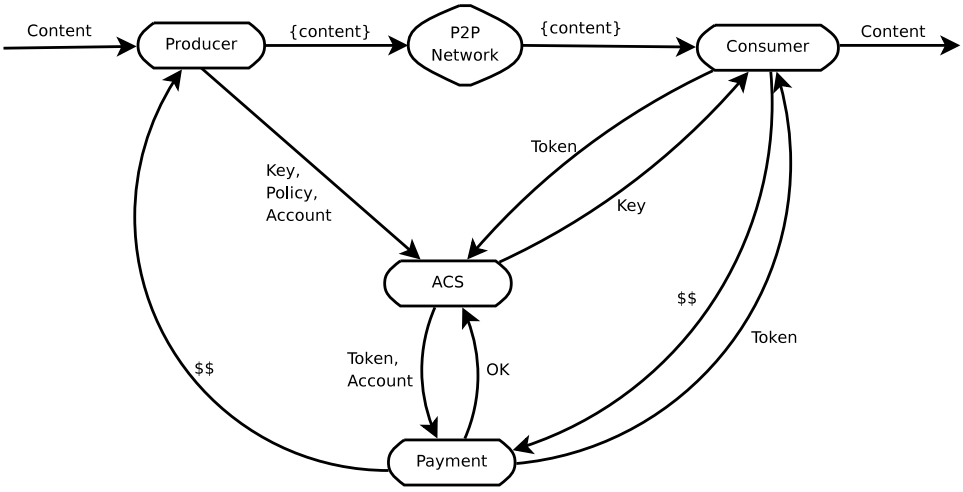

Fig. 1. Proposed design

a simple interface which limits private information leakage. Therefore, complying with the privacy requirements described in Section III-B

VI. Use Cases

In this section, three use cases are described to demonstrate the flexibility of the design.

A. Pay-Per-View

The pay-per-view business model is rather straightforward. In order to access a given content, the consumer must pay a price determined by the producer.

The setup is made by the producer which must: (1) generate a key and a policy which are sent to the ACS along with its account information, (2) encrypt the content with the key, (3) inject the encrypted content into the P2P network.

The consumer, in turn: (1) selects a content and pays for it through the payment system which returns a token, (2) provides the token to the ACS which returns the decryption key and, finally (3) uses the key to access the encrypted content.

Notice that the ACS validates the token against the payment service to check that it is valid and has not been re-used. The ACS also indicates the producer's account information, where the money will be transferred.

B. Tip Jar

The tip jar model is a variant of the pay-per-view model. In the tip jar case, the payment is usually done after the access (if any payment) and the amount is not fixed by the producer.

The main characteristic of this model is that the access is not restricted in any way. Therefore, the content can be transmitted without any encryption and the role of the ACS is simply to link the payment made by the consumer with the producer's account.

C. Geo Restrictions

As described in Section III-C, geo restrictions are a major concern for broadcasters which distribute content whose rights are only cleared for a given region or country. In this case, a payment service is not needed. The token does not represent a proof of payment but, instead, proof of being at one given location.

In many cases, the IP address used to send the query can be mapped to a location by a geolocation service, i.e., the consumer is using an implicit token. The ACS can then check the consumer's location against the policy provided by the producer to determine whether to return the key or not.

VII. Conclusion

As we have shown, the design of a P2P-based system for distribution of digital media must take many parameters and challenges, both technical and non-technical, into consideration.

The design presented in this paper, while still a work in progress, meet the most important challenges we have identified. In its current incarnation, it offers a way to support most of the current business models and technologies for selling and protecting digital content, while at the same time avoiding creating technical obstacles to efficient distribution, such as preventing the use of caches, or requiring unwieldy trust management schemes.

It also creates a way to allow viewers near-anonymous access to content, thus resolving many of the privacy pitfalls that on-demand TV otherwise create.

The ability of this design to support many novel business models is also a strong point, including those models that rely on the cooperative P2P approach to reduce distribution costs for content creators to near zero.

Last, but not least, the design presented offers flexibility in the choice of content access management techniques, as well as the ability to rapidly deploy new or updated access

management, i.e., in the case that a scheme is found to be flawed.

ACKNOWLEDGMENT

The research leading to these results has received funding from the Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 21617 (P2P-Next).

We would like to thank our colleagues in P2P-Next for their comments and constructive discussions on the topic.

We specially thank Jorge Sainz, University of Zaragoza, Spain, for providing us with feedback while developing a prototype based on the design described in this paper.

REFERENCES

[1] "P2P-Next. http://www.p2p-next.org/ (last accessed April 2009)."

[2] H. Xie, R. Yang, A. Krishnamurthy, Y. Liu, and A. Silberschatz, "P4P: Provider portal for (P2P) applications," in *Proc. of ACM SIGCOMM*, 2008.

[3] B. Cohen, "Incentives Build Robustness in BitTorrent," in *Workshop on Economics of Peer-to-Peer Systems*, vol. 6. Berkeley, CA, USA, 2003.

[4] J. Mol, J. Pouwelse, D. Epema, and H. Sips, "Free-Riding, Fairness, and Firewalls in P2P File-Sharing," in *Proceedings of the 2008 Eighth International Conference on Peer-to-Peer Computing-Volume 00*. IEEE Computer Society Washington, DC, USA, 2008, pp. 301–310.

[5] W. S. Rudolf F. Graf, *Video scrambling & descrambling for satellite & cable TV*. Newnes, 1998.

[6] J. A. Pouwelse, P. Garbacki, J. Wang, A. Bakker, J. Yang, A. Iosup, D. H. J. Epema, M. Reinders, M. R. van Steen, and H. J. Sips, "Tribler: a social-based peer-to-peer system: Research articles," *Concurr. Comput. : Pract. Exper.*, vol. 20, no. 2, pp. 127–138, 2008.