

著作権管理のための匿名通信

木下研究室

遠山 真一郎 (200402898)

1 はじめに

近年、デジタルコンテンツを無断で P2P ネットワークなどを介しコンテンツの不正流通が社会問題となっており、DRM や使用目的の変更や二次利用の著作権調停を自立的に行うためにコンテンツのカプセル化とモバイルエージェントが利用されている。本稿ではプライバシーを保護しつつ流通後のコンテンツのエージェントと権利者のエージェントが通信可能な匿名経路制御を提案する。

2 匿名通信

2.1 個人情報と著作権管理

個人情報を制御して保護するために以下の機能が必要

- ・個人情報に関連する人は情報用法の目的を制限可能
- ・この目的の正当性をチェック可能
- ・分配された情報が正しいかをチェック可能
- ・分配された情報の使用目的を変更可能
- ・分配された情報をアップデートするか削除可能

2.2 分配された情報のコントロール

情報カプセルは DRM システムのためにあり複雑な著作権を決議して個人情報を扱うために開発された。情報はカプセル化されたメタデータとモバイルエージェント。メタデータはルーティングとアクセス制御情報を含む。エージェントの機能は情報の権利を決議して権利に基づくアクセス管理を操作することです。エージェントはユーザと接続して権利を交渉します。最初にエージェントはメタデータで交渉し、もしエージェントが独自に交渉できないのならルーティング情報に基づく配布者と接続する。たとえば内容が複数のソースの二次使用ならソースの各著作権は決議される。

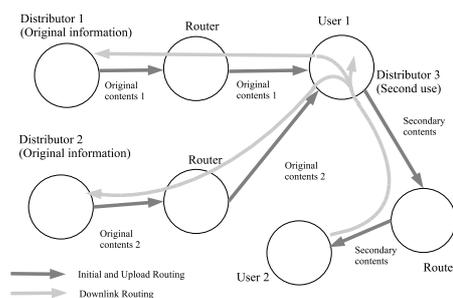


図 1: 提案のネットワーク

2.3 経路制御の基本概念

トレースマトリクスとはルータ I の各ポートにある n 次元マトリクス M_I で各次元 A_i は 2 の m 乗の要素が存在する。(トレースとは痕跡) コンテンツはマトリクスのいくつかの点 (1 点) を使用する。コンテンツに $1 \times m \times n$ ビットで構成された独自の識別番号が存在。配布者とユーザの接続が確立されたときこれらのトレースはチェックされる。もしルータがコンテンツのトレースを発見したならば次の移動はそのトレースを持つポートから選ばれる。

2.4 提案するネットワーク

ネットワークが図 1 に示すノードで構成されるよう仮定。カプセルはコンテンツ、アクセス制御とルーティング確認を管理するエージェントを持つ。これらのノードの機能はカプセルを作成、使用、転送。

ネットワークの構造は以下の通り

- distributor (配布者) は著作権を所有しているか配布されたコンテンツの所有者。所有者はコンテンツのアクセス権と目的を変更可能
- ユーザはコンテンツを使用し二次コンテンツを作成。したがってユーザは配布者ともなりえる
- エージェントはコンテンツに同伴してユーザのノードでのコンテンツの使用を管理
- ルータはコンテンツをメタ情報と共に転送。この情報はエージェントとルーティングに使用されたトレースセットからなる
- カプセルはコンテンツ、エージェント、トレースセットでできている。
- アップリンクメッセージは配布者からエージェントまで転送されたデータもしくはメッセージ。このメッセージはコンテンツを更新するかアクセス権を制御するのに使用。
- ダウンリンクメッセージはエージェントから配布者まで転送されたデータもしくはメッセージ。このメッセージはエージェントがコンテンツの証明を確認できないときそれをチェックするのに使用。