安全で閉じたP2Pネットワークの構成方法の提案と実装

古志 智也† 飯田 修弘† 齋藤 孝道†
† 東京工科大学 工学部 情報工学科

1 はじめに

近年，様々な場面で，P2P (Peer-to-Peer) ネットワークが注目を浴びている．この P2P ネットワークにおいて，通報を暗号化するためのグループ鍵 (共通鍵) をどのように安全に共有するかという問題がある．また，一般的な P2P ネットワークの研究では CA (Certificate Authority) や DNS (Domain Name System) の利用に関する議論がない．そこで，本論文ではノードのみで構成する安全で閉じたネットワークの実現方法を提案し，その実装を行う．

2 背景

P2P (Peer to Peer) モデル [1] とは，データ通信を行なう際に，ノード同士を直接接続し，情報の共有を行なう通信形態のことである．P2P モデルでは，すべてのノードの立場は等しい関係にあり，特定のノードに処理の負担が掛からず，各ノードに負担を分散することができる．

P2P モデルは，2 つに大別することができる．一方は，Hybrid P2P モデル [2][3][4] と呼ばれるものである．このモデルでは，ルーティングや情報の検索，グループ鍵の管理などの処理はサーバに委託し，情報の共有などのデータ通信を各ノード同士が直接行う．もう一方は，ノードのみでネットワークを構成する Pure P2P モデル [5] と呼ばれるものである．

一般的な Hybrid P2P モデルでは，新規ノードが，P2P ネットワークへ参入する時は，サーバと交渉することでネットワーク内で利用されるグループ鍵を取得することができる．また脱退時には，サーバに脱退の旨を伝えることで，サーバがその他のノードに対して鍵更新を促すことができる．しかし，Pure P2P モデルの場合，通報を暗号化するためのグループ鍵を誰が管理し，どのような方法で安全に共有するかという点が問題となる．

3 提案システム

提案システムでは，ループ型とツリー型の２つのモデルを提案したが，本論文では紙面の都合上，後者は割愛する．

3.1 システムの概略

提案システムでは，最終的に，グループ内の各メンバーは，自身を含めた全てのメンバーの公開鍵や IP アドレスなどを，メンバーリストとして保持する．新規参入者はグループ内にいる知り合い (以降 交渉者) と交渉し，新たにグループに加わる．この際，公開鍵を用いて相互認証をし，2 者間で秘密に共有した共通鍵を用いて，以降，安全な通信路を確保する．以下に，A, B がグループのメンバーで，新規にメンバー N が参入するとき (N は B と知り合いとする) の，メンバーリストを共有するまでの流れを説明する．以下では，1 人のメンバーに対する情報 (公開鍵や IP アドレス) を固有情報と呼ぶ：

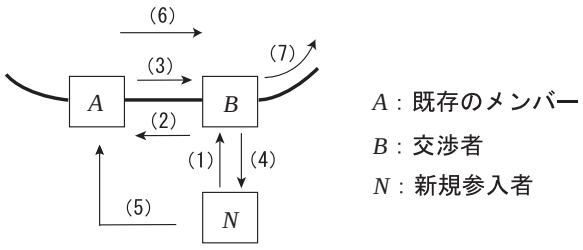

図 1: 提案システムの新規参入の概念

処理の説明 (各数字は図 1 に対応)：

(1) N と B は，予め保持している互いの公開鍵を利用して相互認証し，以降，暗号化通信を行う．その後，N は B にグループへの参入要求を送る．

(2) B は，グループに新規参入者が発生したことを，N と隣接するメンバー (ここでは，N は A と B の間に加わるものとする) に N の固有情報と共に通知する．

(3) A は，N の固有情報を取り出し，N の受け入れの態勢が整ったことを B に通知する．

(4) B は，現在のメンバーリストを N に送信する．

(5) N は，メンバーリストに含まれている A の固有情報を取り出し，A に接続後，A と相互認証を行い，安全に共通鍵を共有する．

(6) A は，N がグループに参入を完了した後に，メンバーリストを更新 (N の固有情報を追加) し，B に N の参入が完了したことを通知する．

A Secure Grouping for Pure P2P Network
† Tomoya Koshi, Nobuhiro Iida, Takamichi Saito
Tokyo University of Technology (†)

(7) Bは，メンバーリストにNの固有情報を追加し，右に隣接するメンバーにNの固有情報を配布する．これによって，全てのメンバーのメンバーリストが更新される．

グループからの脱退，グループ情報の同期については，紙面の都合上割愛する．

3.2 システムの安全性

提案システムにおける安全性は，新規参入者Nと交渉者Bとが，予め互いに信頼していることに依存する．Nを受け入れるメンバーAの観点からすると，Aは既にBを信頼している．そのため，信頼しているBから受け取るNの情報を信頼できる．また，Nの観点からすると，Nは予めBを信頼している．そのため，信頼しているBから受け取るメンバーリスト(Aの情報)を信頼できる．よって，グループのすべてのメンバーは正しい情報を取得できる．したがって，提案システムは，安全で閉じたネットワークを利用者に提供する．

3.3 実装

提案システムでは，グループへの参入時の認証に，SSL (Secure Socket Layer) の 相互認証モードを利用した．認証が成功した後，全ての通報はこのSSL の暗号化通信路を利用する．今回は Java 言語で実装を行った．

4 比較検討

ここでは，提案システムと一般的なHybrid P2P モデルとの比較を，鍵管理，ストレージと通信のコスト，ネットワーク構成の3つの観点から行う．

4.1 鍵管理による比較

Hybrid P2P モデルでは，グループ鍵やノードのIP アドレスなどをサーバが全て管理する．このモデルには，グループへの新規参入や脱退で生じる鍵更新や鍵配布などの管理が容易に行なえるといった利点がある．また，鍵更新の通報を受け取れなかったノードは，サーバに問い合わせることによって，容易に鍵の同期化を行なえる．ただし，これはサーバが機能し，サーバとの通信が行えることを前提としている．

提案システムでは，通報の暗号化に2者間で秘密に共有している共通鍵を使用しているため，鍵の同期をする必要はない．また，メンバーの参入や脱退時に，特定のメンバーに処理の負担が偏ることがない．したがって，提案システムはフォールトトレラントである．

4.2 ストレージと通信のコストによる比較

Hybrid P2P モデルでは，サーバが鍵やIP アドレスを保持していたため，その他のノードには，ストレージコストは比較的要求されなかった．

提案システムでは，最終的に，各ノードがグループ内にいる全ノードの公開鍵とIP アドレスを保持しなくてはならないため，Hybrid P2P モデルに比べ，各ノードにストレージコストが要求される．例えば，公開鍵が1024bit，IP アドレス，ホスト名をそれぞれ32bit，メンバー数を10000名と仮定した場合，提案システムでは各メンバーに約1.36Mbyte のストレージコストを強いるが，現在のハードディスク事情であれば，扱えないことはないであろう．また，グループメンバーの更新によるリストの分配についても，グループ内の全てのメンバーの情報を送信するのではなく，新規参入者もしくは脱退者のみの情報を送信するだけでよい．

4.3 ネットワーク構成による比較

図2に示すように，提案システムでは，CA やDNS などを利用しなくても安全で閉じたネットワークを形成することができる．

	従来のシステム	提案システム
公開鍵	PKIにおけるCAが必要，もしくは，議論されていない	グルーピングの際に獲得するため，CAを利用する必要はない
IP アドレス	DNSを利用している	グルーピングの際に獲得するため，DNSを利用する必要はない

図2: ネットワーク構成の比較

5 まとめ

一般的なHybrid P2P モデルでは，通報を暗号化するためのグループ鍵は，サーバが一元管理していた．一方，Pure P2P モデルの場合，通報を暗号化するための共通鍵を誰が管理し，どのような方法で共有するかという点が問題であった．本論文では，Pure P2P モデルにおいて，CA を利用しない公開鍵分配方式を提案し，ノードのみで構成する安全で閉じたネットワークのこれまでにない構成方法の提案と実装を行った．

参考文献

[1] 第2特集・P2P ネットワークがやってきた，Software Design，2001年8月号

[2] Bruno Dutertre, Valentin Crettaz, Victoria Stavridou：Intrusion-Tolerant Enclaves, System Design Labortory, May 2002

[3] A. Perrig, Dawn Song, J.D.Tygar：ELK a New Protocol for Efficient Large-Group Key Distribution, Proceedings of 2001 IEEE Symposium on Security and Privacy

[4] PROJECT JXTA：http://wwws.sun.com/software/jxta/

[5] Gnutella.com： http://www.gnutella.com/