M-42　セキュアP2Pグループコミュニケーション基盤の提案

A Proposal of Secure P2P Group Communication Middleware

野田 潤†　中村 暢達†　田口 大悟†　谷 幹也†
Jun Noda　Nobutatsu Nakamura　Daigo Taguchi　Mikiya Tani

1. はじめに

802.11bやBluetooth等の近距離無線通信インフラの登場により、これらを備えた端末どうしが直接通信し、アドホックに情報交換することが可能になった。このようなアドホックな情報交換は、メールやBBSのように専用のサーバを必須としないため、誰もが自由にいつでもコミュニケーションを行えるという利点がある。一方、オープンな通信路を用いるため、接続可能な通信相手が多く、利用者にとって有益な相手を発見することが難しい。更に、第三者による通信の盗聴も容易であるという欠点がある。

筆者らは、アドホックな情報交換を用いて、目的や興味の一致する利用者でグループを形成し、有益な情報を交換することをアドホックなグループコミュニケーションと定義する。また、これを安全に実現するコミュニケーション基盤として、セキュアP2Pグループコミュニケーション基盤を提案する。

2. アドホックなグループコミュニケーション

2.1 Pure P2P型アーキテクチャ

筆者らが目指すアドホックなグループコミュニケーションとは、時間と空間を共有し、同じ特性（目的意識、興味等）を有する利用者によって展開されるその場限りのコミュニケーションである(図 1)。筆者らはこれを、近距離無線通信機能を備えた端末が直接通信して連携し合うことによって機能する Pure P2P(Peer-to-Peer)型アーキテクチャで実現する。メーリングリストや BBS 等のグループコミュニケーションは、グループの参加者や、交換する情報をサーバで管理するクライアント/サーバ型アーキテクチャで構成・運用されている。しかし、アドホックなグループコミュニケーションではネットワーク構成及びグループ構成が動的に変化するため、サーバ利用の固定的なグループ管理は適さない。Pure P2P 型は特定のサーバに依存しない点で、アドホックなグループコミュニケーションに適している。

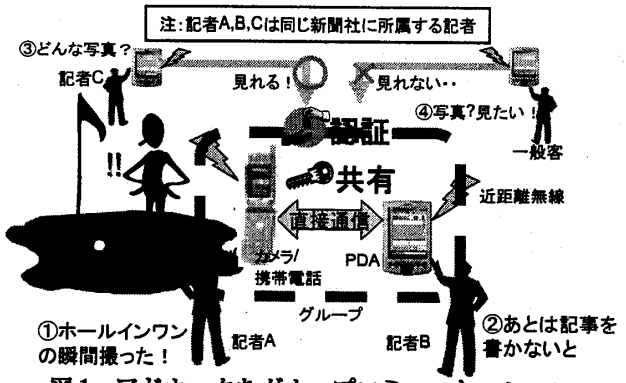

図1　アドホックなグループコミュニケーション

2.2 課題

Pure P2P 型アーキテクチャによる実用的なグループコミュニケーションの実現には二つの課題がある。

第一の課題は、動的に構成が変化するネットワークにおけるピア探索である。Pure P2P 型のピア探索手法には、Gnutella[1]のように、探索メッセージ(Ping)をブロードキャストし、他のピアからの応答(Pong)を待つ手法が知られている。このピア探索は、探索メッセージを発行した時点で存在するピアを検知する手法であり、ピアの出現や消失を継続的に検知することは困難である。しかし、アドホックなグループコミュニケーションでは、ピアの出現や消失を継続的に検知して、コミュニケーションのトリガにすることが重要である。現実世界において出会いや別れがコミュニケーションのトリガとなることと同じである。加えて、特性が共通するピアに限定して出現や消失を検知できれば、更に質の高いコミュニケーションに結びつく。

第二の課題は、通信セキュリティの確保である。オープンな通信路は盗聴が容易なためセキュリティの確保には通信の暗号化が必要である。Pure P2P 型では、公開鍵基盤を用いた認証/暗号化手法などサーバを利用した手法の利用が難しい。そのため、個々のピアが相互に認証する手法と、認証した相手と暗号化通信用の暗号鍵をオープンな通信路で安全に共有する手法の開発が必要である。

3. セキュアP2Pグループコミュニケーション基盤

3.1 構成

提案する基盤の構成を図 2 に示す。本基盤はアプリケーションへコミュニケーション機能を提供する上位層(1,2,3)と、上位層へ基本機能を提供する下位層(4,5,6,7)からなる。ここではアドホックなグループコミュニケーションの実現に必要な、

1. 継続的かつピア特性に基づいたピア探索
2. 相互通信による認証と通信鍵共有

について詳細に説明する。

本基盤では、各ピアがそのプロファイルを記した会員証を保持していることを前提とする。会員証には、会員の特徴情報（会員メタデータ）、会員で共有する秘密値 s、Diffie-Hellman 法[2]の元 g、法 p が含まれる。セキュア P2P グループコミュニケーション基盤は、この前提のもと、同じ会員証を持つものどうしがお互いを発見し、アドホックにグループを形成して安全にコミュニケーションできる環境を提供する。

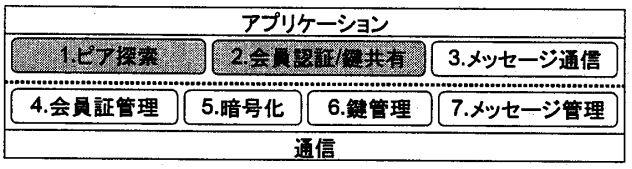

図2　基盤構成

†日本電気（株）インターネットシステム研究所

3.2 継続的かつピア特性に基づいたピア探索

提案手法の特徴は、他のピアから配信されてくる情報によりピアを探索する Push 型探索である。Gnutella のような Ping/Pong による Pull 型ピア探索は、周囲のピアが頻繁に入れ替わる環境では、ピアの出現・消失の継続的な検知のために利用者による頻繁な確認操作を必要とする。Push 型ピア探索は、利用者の確認操作を必要とせずに刻々と変化する周囲のピア状況を検知することができる。Push 型ピア探索手順を以下に示す。

- 各ピアは、有限の通信半径内に存在するピアにプレゼンスメッセージ(Pm)を定期的に同報通信する。

ここで、Pm は、ピアの所持する会員証の会員メタデータのリストである。この Pm を受信したピアは、アドホックに接続可能なエリア内に Pm を送信したピアが存在することを知る。ピアの存在を初めて知ったとき、ピアの出現と認識し、ピアから Pm が一定時間届かなくなったとき、ピアの消失と認識する。次に、

- Pm を受信したピアは、Pm に格納されている会員メタデータと、自身が保持する会員メタデータとのマッチングを行い、目的や興味の一致するピアを発見する。

3.3 相互通信による認証と鍵共有

提案手法では、ピアが持つ会員証に含まれる s、g、p を用いて、ピアがグループへ参加する際の認証と、暗号化通信に用いるグループ鍵の共有を行う。ピア 1 からピア n-1 がグループを形成している所に、ピア n が参加する様子を図 3 に示す。以下図 3 を用いて本手法を説明する。

なお、会員証の不正利用を防止するため、会員証は端末利用者と端末本体に依存する情報から生成した鍵を用いて会員証のハッシュ値と共に暗号化して所持する[3]。

ピアがグループへ参加する際の認証は、グループに属しているピアの一つであるピア i($1 \leqq i \leqq n-1$)と新規に加入するピア n の二者間で次のように行う。以下、k を暗号鍵として d を暗号化した値を k(d)、d を復号した値を $k^{-1}(d)$と表記する。

- Diffie-Hellman 法を用いて、g、p をもとに、二者で値 a を共有する。
- ピア n は a(s)をピア i に送信し、ピア i は $a^{-1}(a(s))$が会員証に保持する s と一致するかを確認する。
- ピア i は s(a)をピア n に送信し、ピア n は $s^{-1}(s(a))$があらかじめ共有した値 a と一致するかを確認する。

共通の会員証を持ち、かつ本処理に携わった当事者だけが値 a を共有でき、交換した値 $a^{-1}(a(s))$、$s^{-1}(s(a))$と保持する値 s、a がお互いに同値であると確認できれば、両者が同じ会員証を持つことが保証される(図 3-①)。値 a は認証毎に異なる値であるので、通信路に流れるデータを盗聴・記録して、会員になりすますことは十分困難である。

グループ内での暗号化通信に用いるグループ鍵は、次のように共有する。ここでピア n が参加する前に、ピア 1 からピア n-1 で形成するグループで共有しているグループ鍵を Kn-1 とする。

- ピア i は、Kn-1(a)を、ピア j($1 \leqq j \leqq n-1$, $i \neq j$)のすべてに同報通信する(図 3-②)。

この時、ピア i は現在のグループ鍵 Kn-1 を用いて値 a に署名を付加する。同報通信を受けたピア j は署名を検証することで、確かに同じグループに属しているピアによって値 a が送られてきたことを確認できる。確認できた場合、

- $Kn\text{-}1^{-1}(Kn\text{-}1(a))$を新しいグループ鍵 Kn に設定する(図 3-③)。

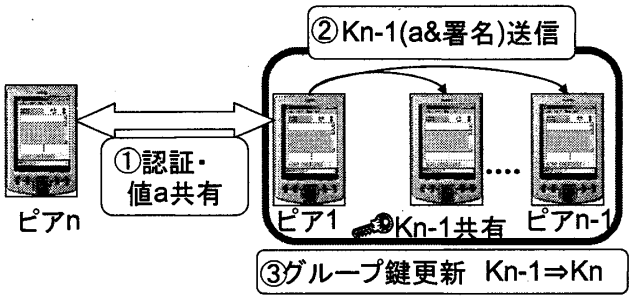

図3 会員認証と鍵共有

このようにしてグループに属するすべてのピアは、同じグループ鍵 Kn(=a)を共有できる。以降のグループ通信はこの Kn を用いて暗号化される。また本手法はグループに新しいピアが参加するたびに鍵を更新するため、暗号鍵のライフサイクルが短くなり、セキュリティ強度が高い。

4. 実装

セキュア P2P グループコミュニケーション基盤の検証のため本基盤と基盤上で動作するメッセージングツール(図 4)を試作した。本試作では、モバイル端末における汎用的な実行環境である Personal JAVA を用い、相互運用性を高めている。メッセージングツールは、Pocket PC と無線 LAN 環境で動作し、1)無線 LAN の無線到達範囲に現れたピアを発見、2)共通の会員証を持つピアとグループを形成、3)安全にテキスト/バイナリデータを交換/共有する。

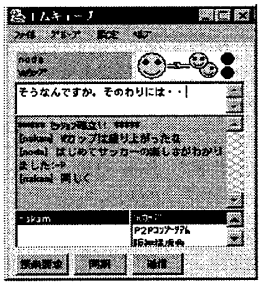

図4 メッセージングツールプロトタイプ

5. おわりに

アドホックなグループコミュニケーションを安全に行えるコミュニケーション基盤を提案した。近距離無線通信インフラに対応したモバイル端末の普及が予測され、セキュリティを必要とするアドホックな情報交換型のアプリケーションが期待されている。

今後は本基盤のビジネス利用について検討を進め、本基盤上で、オフィス環境において利用するツールの開発・運用実験を通じて、本基盤の有用性を検証する。また既存 P2Pインフラ[4]との連携による機能強化も図りたい。

参考文献

[1] Gnutella：http://www.gnutella.com/

[2] W.Diffe and M.E.Hellman: New direction in cryptography Trans, IEEE on Information Theory, IT-22, No.6, pp.644-654, Nov. 1976

[3] コンテンツ利用管理システム：モバイル RightsShell-コンテンツ配信方式-、中村,仁野,谷,市山、情報処理学会 63 回全国大会 5V-01、2001.09

[4]JXTA：http://www.jxta.org/