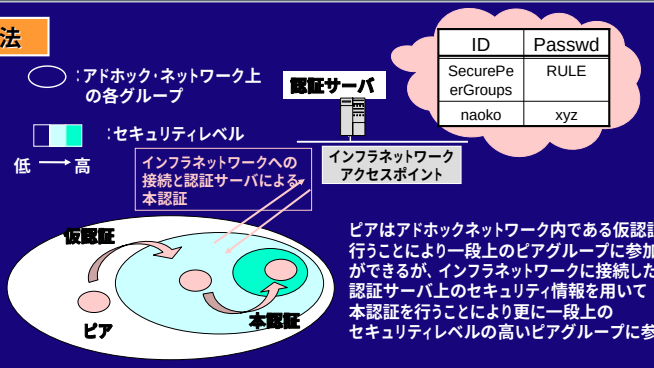
小口研究室　各研究紹介 (2004年度)

クライアントサイド

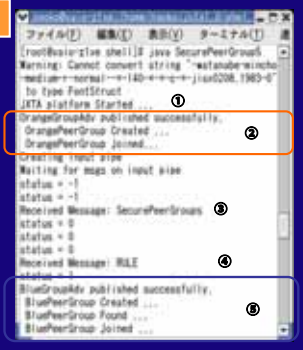
無線アドホックネットワークにおける階層型認証機構の提案と実装 (小原)

提案手法

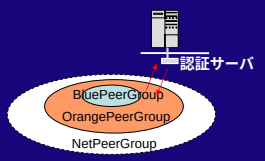


ピアはアドホックネットワーク内である仮認証を行うことにより一段上のピアグループに参加することができるが、インフラネットワークに接続した際に認証サーバ上のセキュリティ情報を用いて本認証を行うことにより更に一段上のセキュリティレベルの高いピアグループに参加できる

実装結果



ピアグループ作成プログラムの実行結果



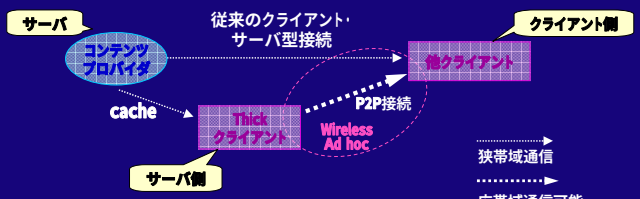
始めにJXTAプラットフォームを初期化しNetPeerGroupを作成 (①)。
次にNetPeerGroupを親ピアグループとしてオープンなピアグループを作成 (②)。
そしてインフラネットワークに接続した時に認証サーバにアクセスし、セキュリティ情報であるID (③) とパスワード (④) を取得。
その情報を基にOrangePeerGroupを親ピアグループとしてセキュアなピアグループを作成。

無線アドホックネットワークにおけるP2P接続ノード間のコンテンツ転送性能評価 (荒牧)

研究背景

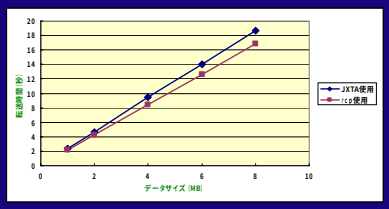
Thickクライアントモデル

- サーバの処理をクライアントに分散して実行
- 従来のクライアント・サーバ型接続とP2P接続を融合



実験内容と実験結果

- データサイズの異なるファイルを用意し、それぞれのファイル転送に要する時間を測定
- ファイル転送性能の理想値を知るためにrcpコマンドを用いて同じファイルのリモートコピーを行い、timeコマンドを用いて転送時間を測定



異種リンク経由の通信における暗号化方式適用手法の定量的評価 (鎌田)

背景と目的

無線通信は通信の傍受がされやすいため暗号化によりデータを守ることが必須

アプリケーション層	S/MIME
プレゼンテーション層	PGP
セッション層	SSH
トランスポート層	SSL/TLS
ネットワーク層	IPsec
データリンク層	WEP
物理層	WPA

各プロトコル階層における様々な暗号化技術

IPsec：IPパケットを暗号化して通信

WEP：無線通信における暗号化

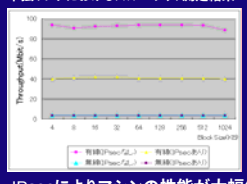
- 一階層の暗号化方式だけでは不十分な場合、複数の暗号化方式を組み合わせた手法が有効
- セキュリティとパフォーマンスはトレードオフの関係
  ⇒性質の異なるリンクごとに適切なセキュリティレベルの設定が望ましい

ホットスポット周辺のようにリンク間をまたがる通信において、セキュリティとパフォーマンスのバランスを考慮した最適な暗号化方式の適用手法を検討

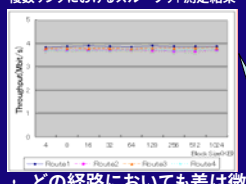
実験結果と考察

- 暗号化技術(IPsec)がパフォーマンスに与える影響を測定
- 最も安全かつ効率の良いセキュリティ環境設定手法を検討

単独リンクにおけるスループット測定結果



複数リンクにおけるスループット測定結果



IPsecを適用するか否かにより4つの経路を設定

- 有線・・・IPsecによりマシンの性能が大幅低下
- 無線・・・変化は微少でIPsecによる影響は少ない

- どの経路においても差は微少でIPsec使用による影響は少ない

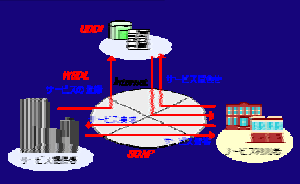
モバイル環境におけるWebサービスのデータ転送性能向上に関する検討 (賀川)

研究背景

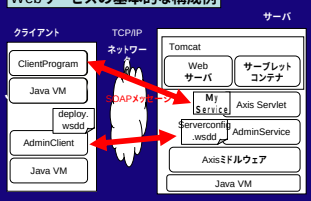
Webサービス

- XMLおよびSOAPを用いて、他のソフトウェアあるいはWebアプリケーションから接続してサービスを利用可能とする枠組み

Webサービスの仕組み



Webサービスの基本的な構成例

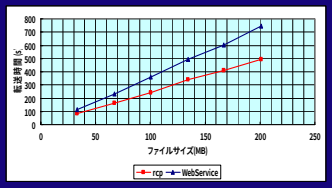


サーバ・クライアント双方を無線LAN接続ノートPCとした環境におけるWebサービスの実現と性能向上

提案手法と実験結果

動画転送サービスのデータ転送時間とリモートコピーした場合のデータ転送時間を比較

動画のファイルサイズに比例して，Webサービスとリモートコピーの転送時間の差が大きくなる



データ転送時の性能向上手法

大きいサイズのファイル転送時のみWebサービスのプログラム中からリモートコピーコマンドを呼び出す

→ 提案手法に基づくプログラムを実装して評価を行った結果，同じWebサービスの枠組みを用いながら理想値に近いスループットが得られた