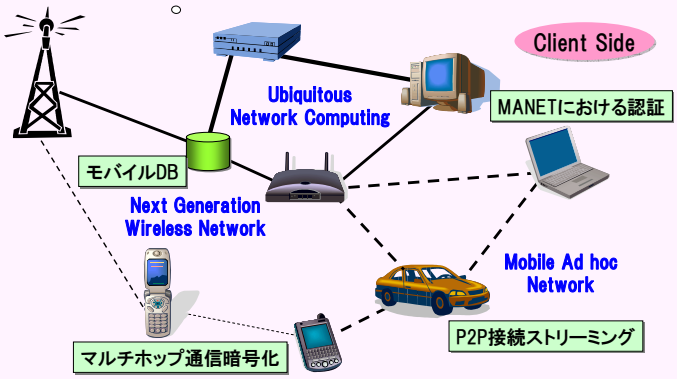
小口研究室　研究紹介 (2006年度)

(お茶の水女子大学理学部情報科学科)

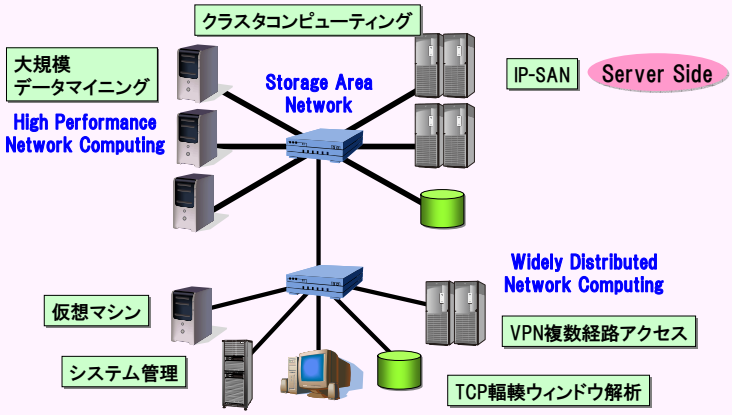
◆ ユビキタスコンピュータ時代

インターネットを中心とする大規模ネットワークにより，種々のコンピュータが互いに連携しながら高度なネットワークコンピューティングが行われるようになってきました．



◆ 研究のターゲット

小口研究室では，ネットワークコンピューティングの資源であるコンピュータや端末，ストレージ等をより効率良く，より便利に，より安全に利用するため，ソフトウェア (ミドルウェア) をどのように構築したらよいかを研究しています．



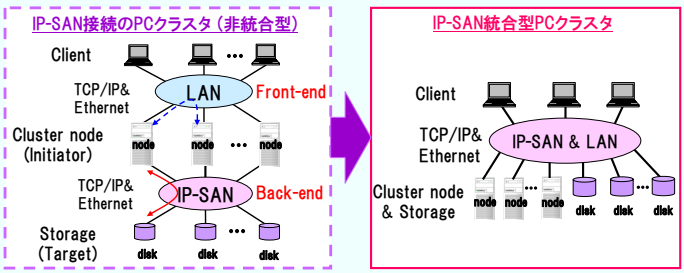
◆ IP-SAN統合型PCクラスタの性能評価 (研究担当：神坂 紀久子)

研究背景と研究目的

- IP-SAN統合型PCクラスタ:
  バックエンドのIP-SANをフロントエンドのLANに統合
  - IP-SANにより，共通のコモディティなネットワークで接続可能
  - 運用管理の効率化，ネットワーク構築・管理コストの削減
- IP-SAN統合型PCクラスタの性能への懸念
  - ノード間通信とストレージアクセスで同じネットワークリソースを共有

↓

- 研究目的:IP-SAN統合型PCクラスタの実用性を実証
  - 統合した環境が性能に与える影響を評価
  - バックエンドにIP-SANを持つ非統合型と比較

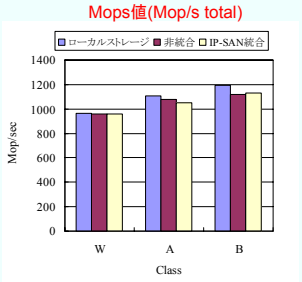


性能評価:マクロベンチマーク

NAS Parallel Benchmark 2.4 I/O による性能測定

評価:I/O処理を伴う並列計算ベンチマークを使用し
3つのPCクラスタ環境を比較
- 対象問題:BT (Block Tri-diagonal)
- ノード数:4

結果:IP-SAN統合クラスタと非統合クラスタでは
並列演算処理性能に性能差がみられない．

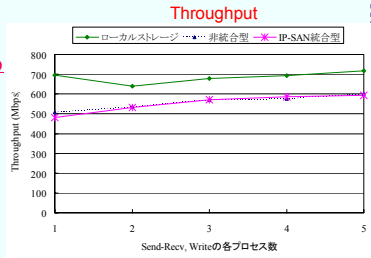


性能評価:マイクロベンチマーク

複数プロセスを使用した同時アクセスによる性能測定

評価:同一ノード上において，ストレージアクセス
(Write)とノード間通信(MPI_Send-MPI_Recv)
を並行して複数のプロセスとして実行
- ノード数:2

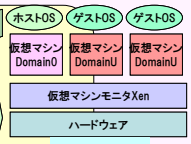
結果:ネットワークに高負荷をかけた場合でも
統合の影響は小さい．
IP-SAN統合型PCクラスタは有効．



◆ 仮想マシンを用いた階層型認証機構に基づくMANET利用環境の提案と実装 (研究担当：小原 奈緒子)

研究背景

仮想マシンモニタ:Xen
- コンピュータ上に異なる複数の実行環境を仮想的に構築
- 高いセキュリティ
  個々の仮想マシンは独立 → たとえ攻撃されても障害や攻撃を隔離
- Xenのネットワーク
  Xen内の仮想的なインタフェースを利用して様々なネットワーク形態を構築可能
  →セキュリティ性の高いネットワーク構成を生成することが可能



Xenの構成図

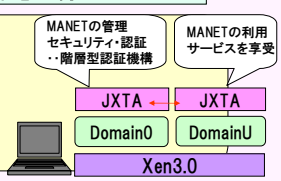
研究目的

固定基盤ネットワーク接続時同等の完全な認証は不可能であるが
全てのノードを等し「未認証」とするより、多くの場合MANET内で有効である仮認証等を
行い信頼度に差をつけた方が望ましい
**→認証に段階を付け、信頼度のレベルに応じた安全なコンテンツのやり取りを
行うための枠組みを検討:階層型認証機構**

仮想マシンの高いセキュリティ性を利用して安全性をより向上

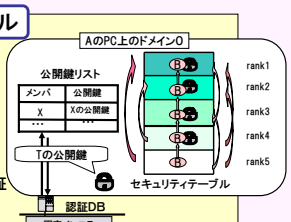
仮想マシンを用いたMANETの実現モデル

Xenのネットワークではドメイン0でセキュリティを確保すれば
ドメインUは他の処理に専念することが可能
→Xen上に複数のOSをインストール
- ドメイン0はセキュリティ・認証を含むMANET管理
- ドメインUは他の処理(MANETの利用など)に専念



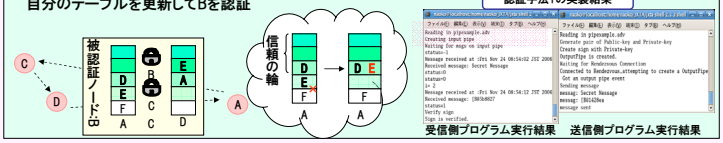
MANETにおける階層型認証機構の提案モデル

個々のノードがセキュリティテーブルと公開鍵リストをドメイン0に持ち
MANET内の他のメンバを認証してレベル付け
- セキュリティレベル:rank4からrank1に近づくに従って高くなる
  - 認証手法1 (レベル:rank1)
    MANETを形成する前から知っていたノード(友人)の
    公開鍵を用いて認証
  - 認証手法2 (レベル:rank2)
    友人が信頼するノード(友人の友人)の公開鍵を使って認証
  - 認証手法3 (レベル:rank3)
    自分の**信頼の輪**(友人の友人の‥友人)に属するメンバの
    公開鍵を用いて認証
  - 認証手法4 (レベル:rank4)
    自分の信頼の輪に属さないメンバから教えてもらった公開鍵を用いて認証



階層型認証機構の概要

AがBを認証する時(A:認証ノード B:被認証ノード)
1. 認証要求してきたBの公開鍵をAはMANET内で探索
2. Aのパケットを受信したノードはBの認証に必要な情報(セキュリティテーブル等)を付加し，他のノードへ転送
3. パケットがAに返信されたらパケット内の情報をもとにAは
   自分のテーブルを更新してBを認証



http://ogl.is.ocha.ac.jp/　　oguchi@computer.org