

大域ディペンダブル情報基盤プロジェクト

ディペンダブルシステムグループ

喜連川 優

情報理工学系研究科電子情報学専攻

1 はじめに

大域ディペンダブル情報基盤プロジェクトの、ディペンダブルシステムグループは、ディペンダブルシステムを達成するためのネットワーク技術、基盤ソフトウェア技術を中心に研究を行う。研究テーマにはユビキタスネットワーク、セキュリティ・セキュアな計算システム、高性能ストレージ・通信・計算システムなどが含まれる。

2 ユビキタス・アドホックネットワーク

2.1 ユビキタス環境実現に向けたネットワークキング技術(青山友紀)

本年度は、環境の多様性に適応するオーバーレイネットワーク技術(CORTH)、汎用的なセンサネットワーク^{U³}、およびセンサデータからのユーザコンテキストの推定などに関する成果を得た。

2.2 Location Based Serviceのための基盤技術(瀬崎 薫)

位置情報に依存したサービス(LBS)のための基盤技術として、位置情報を利用したネットワーク制御、省電力を考慮したルーティング、サービス利用者の動きの現実的なモデル化と予測、などの研究を行って成果を得た。

3 セキュリティ

3.1 ヒューマンクリプトに基づく超ディペンダブル暗号系に関する研究(今井秀樹・松浦幹太)

人に対する安心感を飛躍的に高めることをテーマとした暗号系に関する研究を行っている。本年度は、Password-Authenticated Key Exchangeの拡張、バイオメトリクス情報を利用した鍵の生成と更新方式、セキュアシステムの構築技術、Web of trust モデルに基づいた公開鍵インフラにおける協力者のプライバシー保護技術などに関する成果を得た。

3.2 安全な基盤ソフトウェアの構築(米澤明憲)

信頼性の高いセキュアなシステムの構築を系統的に支援するプログラミング言語に関する研究を行う。昨年度はから行っている既存の C プログラムを安全

に実行できる C 言語の研究を継続し、外部インタフェース記述(IDL)、その処理系による実用的なネットワークプログラム(sendmail)の実行ならびに既知攻撃の検出、などの成果を得た。また、ユーザプログラムをカーネルモードで実行可能な Linux、移動コードによって DDoS 攻撃を防御するシステム、移動コード記述言語、などの様々な成果を得た。

4 高性能ストレージ・通信・計算

4.1 デペンダブルストレージシステム(喜連川優)

iSCSI を用いた IP-SAN のアクセス性能の解析を行った。iSCSI の既存の 3 実装を解析し、TCP の Nagle アルゴリズムによる性能低下などを確認し、その対処の方式を複数検討し、評価した。

4.2 大域分散並列コンピューティング(田浦健次朗)

大域環境における並列処理の記述システムである Phoenix の研究開発を行っている。本年度は、それを用いた、広域環境用 LU 分解の研究を行った。無負荷時の性能が、高速 LU 分解実装として有名な HPL と同等であり、一部のノードに負荷が加わったときや、ネットワーク遅延が大きい(数百 ms 程度)ときにはそれを大きく凌駕することがわかった。また数百ノードから成るノードで高速に資源発見とルーティング表の構築を行うアルゴリズムを構築した。

4.3 科学技術研究向け超高速大域ネットワーク基盤(平木・稲葉)

大域環境で超高速にデータを共有するためのネットワーク基盤システム「データレゾボワール」の研究を行っている。TCP のレート制御や、複数の並列ストリーム間の協調的なウィンドウサイズ調整などによって、長距離における高速転送を実現した。日米間を折り返し往復する総距離 24,000km、RTT 約 350ms、理論上の最大大域幅 8.2Gbps (3 経路を用いた合計)のネットワークで 7.01Gbps の転送速度を記録した。これはバンド幅距離積の世界記録で、SC2003 バンド幅チャレンジにおいて「最高バンド幅・距離積・ネットワークテクノロジー賞」を受賞した。