論 文 内 容 の 要 旨

氏 名 （ 中村 純哉 ）	
論文題名	A Study on Asynchronous Randomized Consensus Algorithms for Byzantine Fault Tolerant Replication (耐ビザンチン故障レプリケーションのための非同期乱択合意アルゴリズムに関する研究)

論文内容の要旨

ビザンチン故障は故障時の動作に一切の制限がない故障モデルであり、本来プログラムに規定された動作から離れてどのような動作も行うことができる。この故障はソフトウェアのバグやクラッカーによる攻撃によって引き起こされる。特に侵入やコンピュータウイルスの感染に起因するクラッカーの攻撃はインターネットの普及と発達から深刻な問題となっており、実用的な耐ビザンチン故障手法が強く求められている。

状態機械レプリケーションは、耐ビザンチン故障性のあるサーバシステムを実現する主要なアプローチの一つである。サーバの役割は複数のレプリカに複製され、レプリカがクライアントからのリクエストを処理する。この手法によって、たとえ一部のレプリカがビザンチン故障しても、システム全体ではサービスの提供を続けることができる。レプリケーションが正しく機能するためには、正常なレプリカは全てのリクエストを同じ順序で処理しなければならない。ネットワーク速度は一様ではないから、リクエストがレプリカに届く順序は異なる。そこで、レプリカは合意プロトコルを実行し、リクエストの処理順序について合意を行う。

本論文では、耐ビザンチン故障状態機械レプリケーションにおけるレプリカ間の処理順序合意処理を対象とした二つの効率化手法を提案する。

初めに、耐ビザンチン故障状態機械レプリケーションのための新しい乱択合意プロトコルを提案する。既存の多値合意プロトコルが二値合意問題を繰り返して解くことで多値合意を実現しているのに対し、提案プロトコルでは多値合意問題を直接解くことで必要な通信ステップ数を短縮する。また、状態機械レプリケーションの構造に特化した効率的なコイントス方法を導入する。評価では、レプリカ数が多い環境でも提案プロトコルが平均2ラウンド以内に合意できること、既存プロトコルよりも高いスループットと短いレイテンシを実現できることを示す。

次に、リクエスト処理順序合意処理を並列化する手法を提案する。非同期分散システムでは合意にかかる時間は実行毎に異なる。ある合意に長く時間がかかると、次の合意が始められず全体の処理性能は低下してしまう。この問題は合意処理を並列化することによって解決されるが、単純な並列化ではレプリケーションの要求を満たすことはできない。そこで提案手法では複数並列して実行される合意のレプリカ間の終了順序の違いを調停する処理を導入する。また合意の初期候補を決定する処理を乱択化し合意にかかる時間を短縮することで、並列化の負荷を削減する。評価実験では提案手法と通常用いられる逐次手法を比較し、レプリカの処理やリクエストの配送に遅延がある場合に、並列化手法が大きな効果があることを示す。

様式7

論文審査の結果の要旨及び担当者

氏　名　（　中村　純哉　）		
	（職）	氏　名
論文審査担当者		
主 査	教授	増澤 利光
副 査	教授	萩原 兼一
副 査	教授	楠本 真二
副 査	主任研究員	櫟 粛之（NTT コミュニケーション科学基礎研究所）
副 査	准教授	角川 裕次

論文審査の結果の要旨

本論文では、ビザンチン故障に対する耐性を有する状態機械レプリケーションにおける、レプリカ間の処理順序合意処理を対象とした二つの効率化手法を提案している。

ビザンチン故障は故障時の動作に一切の制限がない故障モデルであり、本来プログラムに規定された動作から離れてどのような動作も行うことができる。この故障はソフトウェアのバグやクラッカーによる攻撃によって引き起こされる。特に侵入やコンピュータウイルスの感染に起因するクラッカーの攻撃はインターネットの普及と発達から深刻な問題となっており、実用的な耐ビザンチン故障手法が強く求められている。

状態機械レプリケーションは、耐ビザンチン故障性のあるサーバシステムを実現する主要なアプローチの一つである。サーバの役割は複数のレプリカに複製され、レプリカがクライアントからのリクエストを処理する。この手法によって、たとえ一部のレプリカがビザンチン故障しても、システム全体ではサービスの提供を続けることができる。レプリケーションが正しく機能するためには、正常なレプリカは全てのリクエストを同じ順序で処理しなければならない。ネットワーク速度は一様ではないから、リクエストがレプリカに届く順序は異なる。そこで、レプリカは合意プロトコルを実行し、リクエストの処理順序について合意を行う。

本論文では、初めに、耐ビザンチン故障状態機械レプリケーションのための新しい乱択合意プロトコルを提案している。既存の多値合意プロトコルが二値合意問題を繰り返して解くことで多値合意を実現しているのに対し、提案プロトコルでは多値合意問題を直接解くことで必要な通信ステップ数を短縮する。また、状態機械レプリケーションの構造に特化した効率的なコイントス方法を導入する。解析的評価および実験的評価により、レプリカ数が多い環境でも提案プロトコルが平均2ラウンド以内に合意できること、および、既存プロトコルよりも高いスループットと短いレイテンシを実現できることを示している。

次に、リクエスト処理順序合意処理を並列化する手法を提案している。非同期分散システムでは合意にかかる時間は実行毎に異なる。ある合意に長く時間がかかると、次の合意が始められず、全体の処理性能は低下してしまう。この問題は合意処理を並列化することによって解決されるが、単純な並列化ではレプリケーションの要求を満たすことはできない。そこで提案手法では、複数並列して実行される合意のレプリカ間の終了順序の違いを調停する処理を導入している。また合意の初期候補を決定する処理を乱択化し、合意にかかる時間を短縮することで並列化の負荷を削減している。評価実験では、提案手法と通常用いられる逐次手法を比較し、レプリカの処理やリクエストの配送に遅延がある場合に、並列化手法が大きな効果があることを示している。

これらの結果は、耐ビザンチン故障状態機械レプリケーションの発展に大いに寄与するものである。よって、博士(情報科学)の学位論文として価値のあるものと認める。