104

分散・協調制御生産システムのための高速トラフィック解析装置の開発

道情報大　○中島　潤

分散・協調制御を行う生産システムでは，エージェント群で発生する通信障害の原因追究のために，各エージェント間の通信を捕捉し高速に解析する必要が生じる。特に大規模なシステムでは，高速かつ大容量の通信を完全に捕捉及び記録し，必要な通信を高速検索し解析する機能・性能が要求される。本研究では，分散・協調制御生産システムのための高速トラフィック解析装置を提案し，それを元に試作開発したので結果を報告する。

1. はじめに

分散・協調制御を行う生産システムでは，エージェント間で発生する通信障害の際の原因調査のために，常に行われた通信のトラフィックを捕捉・記録し解析する必要が起きる場合がある。一般的なパソコンやサーバなど,LAN 接続された機器の通信障害の原因調査は，保守用コマンドやツール類，機器から排出されるシステムログ情報，もしくは LAN アナライザ等によって取得される情報を手がかりにして行われる場合が多いが，生産システムでは組込用の特殊 OS を採用した機器が多いことや，システムリソースの面から十分なログ情報の記録・保存が困難な場合が多いという事情から，一般的な情報システムにおけるネットワーク通信障害の原因調査手法を用いることが出来ない場合がある。また分散・協調制御システムでは，多種のタイプやモデルが混在するエージェント間ではプロトコル解釈上の問題が原因となる、高レイヤでの通信障害が発生しやすいという特徴がある。特に大規模なシステムにおいては，長期間にわたり高速かつ大容量の通信を完全に捕捉及び記録し，障害原因となった通信を迅速に特定し解析、プレイバック（再現）できる機能・性能が要求される。そこで本研究では，分散・協調制御生産システムのための Gigabit Ethernet(GbE)クラスの高速 LAN に対応可能なトラフィック解析装置を提案し，それを元に試作開発したので報告する。

2. 高速トラフィック解析装置の開発

前章にあげた要求を満たすトラフィック解析装置を開発しようとする場合，大きく二つの技術的課題が存在する。一つ目の課題は,高速ネットワーク上を流れる LAN フレームを確実に捕捉（キャプチャ）し HDD へ記録保存する課題である。GbE の場合,理論的最大秒間フレーム数は約 300 万フレームにもなり，これを確実に通常の一般的なサーバの LAN インタフェース（NIC）で，ひとつのフレームを落とすことなくキャプチャすることは構造的に困難である。このため、本システムでは LAN フレームキャプチャ用に開発された専用ハードウェア（Endace 社 DAG Card）を採用することで解決することとした。

二つ目の課題は，LAN フレームをキャプチャ・記録保存しながら，後の検索・再現処理に必要なプロトコル解析処理を同時並行的に行う必要があるという課題である。本システムでは，フレームキャプチャとリアルタイム解析を同時実行するためにフレームキャプチャと解析プロセスを並行して実行させた場合に，システムリソースが不足する事態を回避するために、3 Stage Network Flow 解析アーキテクチャを考案し実装した。これは，通信データの解析を，

(1) キャプチャと同時に行うストリーム解析
(2) システムリソースに余裕がある場合に行うアプリケーション解析
(3) 通信内容の再現（可視化）を表示する際に行うプレイバック解析

の 3 ステージに分割し，それぞれを独立して動作させることにより解析負荷を処理の優先度に応じて分散させ，ステージごとに必要最低限の解析処理を行うことにより，リアルタイム解析を実現させたものである。

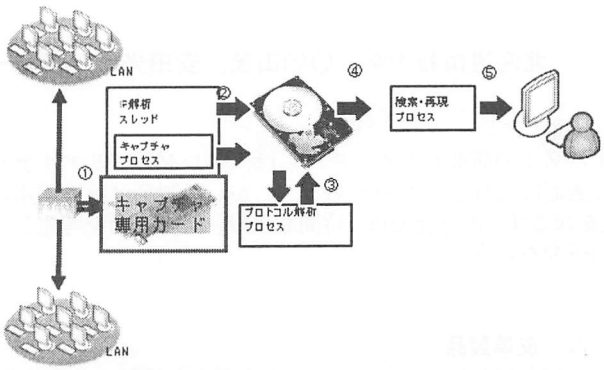

Fig.1　システム構成図

本システムにおける処理フローの概要を以下に示す(Fig.1)。①フレームキャプチャ専用カードによりLANフレームを取得し，取得したLANフレームをHDDに時刻情報等を付加しながら逐次HDDに記録する。②また同時にイーサネットフレームヘッダ及びIP, TCPヘッダを解析し，同時に通信が行われている個々のTCPセッション毎にフレームを識別・並べ替えを行い，この段階でキャプチャしたフレーム相互の関連付けを行うことにより，③のステージで行われるアプリケーション毎の解析処理効率の向上と，④の過程で実行されるオペレータの操作による通信内容の検索・再現処理の高速化，合わせて、セッション毎に再現された状態で記録保存しておくのではなく再現要求時に必要に応じて高速に再現処理を可能としておくことで，システムリソース及び保存容量の節約をも同時に実現した.

4.開発システムの評価

開発したシステムについて，以下の環境・条件で性能評価を行った。

システム用ハードウェアとして，Intel Xeon 3GHzを2個，4GBのメモリを搭載したサーバを用い，HDDへの書込速度がボトルネックとなるのを防ぐためにSATA接続による12台のHDDをRAID5構成した.

実際のLANトラフィックに近いパケットストリームをIP解析エンジンへ渡し，キャプチャ，解析，データ及び解析結果の保存を行った場合のCPU負荷を測定することにより，システム全体としてのパフォーマンス評価を行った。計測用トラフィックはLayer7エミュレータ（Antara Flamethrower)によりHTTPトラフィックを発生させ，そのフレームをキャプチャした。発生させたトラフィック量に応じてリニアにCPU負荷が増加し，1.2Gbpsの時点で100%負荷となり，キャプチャフレームの取りこぼしが見られはじめた。目標するGbE全二重ワイヤレートの理論値である2Gbpsには不足しているが，実運用で十分実用に耐えられる性能を実現できていることを確認した。

5.まとめ

本研究では，分散・協調制御を行う生産システムにおいて発生する通信障害の原因追究支援のために，各エージェント間の通信を捕捉し記録保存しながらリアルタイムに解析するトラフィック解析装置を開発した。

本装置はエージェント間で行われた通信内容をLANフレーム（イーサネットフレーム）の形式そのままでキャプチャし・記録保存を行う構造とした。記録された通信内容は，汎用Webブラウザによって条件指定・検索を行い，目的とする通信セッションの通信内容を忠実に画面上に再現することが出来る。検索は通信時刻,IPアドレスやポート番号、Web等の汎用アプリケーションであればURL等からなる複合条件により可能とした。また，PCAPなどの汎用パケット記録ファイル形式での出力機能を用意してあり，本システムにより捕捉・記録した通信内容を他のプロトコル解析用ソフトウェアで解析することも可能である。現在は一般的なネットワークアプリケーションのみに対応させているが、今後は解析可能なプロトコルの種類を増やしていく予定である。

本システム開発におけるプロトコル解析技術は，あらゆる通信がIP化へ進展している中で，生産システムの障害切り分けのためだけでなく，多方面への応用も可能と考えている。

参考文献

[1]居内寛貴 中島潤，Gigabit Ethernet全二重ワイヤレートに対応したネットワークフォレンジックシステムの開発，情報処理学会第69回全国大会(2007)