2G−6

メンバ間公平性保証方式のセキュリティ向上を目的としたハードウェアによるユーザ操作時間測定手法

谷口幸久† 石原進‡ 西垣正勝‡ 水野忠則‡
†静岡大学情報学研究科 ‡静岡大学情報学部

1 はじめに

マルチホップ型ネットワークの集合であるインターネットにおいて，一般に端末間の遅延は一定ではない。このような環境でクライアントC_1とクライアントC_2がサーバSと早いもの勝ちの論理が働くアプリケーション，例えば早押しゲームを行う場合を考える。C_1–S間の遅延がC_2–S間の遅延より大きいとき，実際にはC_1の方がサーバから到着した問題に対して早くSへ返答を行ったにもかかわらず，遅延差によりC_2の返答が早くSへ到着することが起こりうる。

この問題を解決するための手法として，筆者らはメンバ間公平性保証方式ICEGEM(Impartial Communicatuion Environment for GamE Members)[1]を提案している。ICEGEMでは，クライアントプログラムがサーバのメッセージが到着した時刻から反応を行うまでの時間を測定し，応答メッセージに付加することによって，サーバにおいてクライアントでの反応時間に基づく順序制御を行う。本稿では，ICEGEMにおけるセキュリティ上の問題点を挙げ，その問題に対する解決法としてハードウェアを用いる手法を提案する。

2 ICEGEMの問題点

ICEGEMでは，クライアントプログラム自身が反応時間を測定しサーバに送信するため，図1の右に示すようにクライアントが偽の反応時間を送信した場合（偽証）にサーバがそれを検出できず，正しい制御が行われないという問題が存在する。

2.1 偽証の発生理由

クライアントによる偽証が発生する理由は，以下の2点が考えられる。

1. 経路上における第三者による情報の改竄

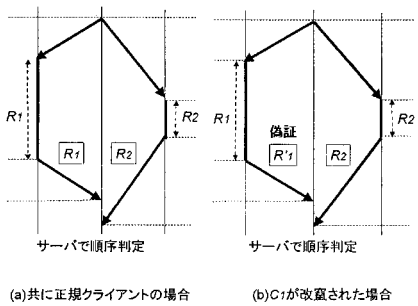

図1: クライアントからのメッセージの改竄

2. クライアントプログラムによる，誤った反応時間の送信

1については既存の暗号化技術，例えば電子署名や，サーバの公開鍵による暗号化によって防止が可能である。本稿においては2における，クライアントによる意図的な反応時間の改竄を防止する方式を提案する。

3 ハードウェアを用いた偽証防止

偽証を防止するためには，クライアントプログラムが正しく動作しているかをソフトウェアによってチェックする方法と，反応時間の測定もしくはそのために必要なデータをハードウェアを用いて収集する方法の2つが考えられる。

しかしながら，ソフトウェアによってチェックを行う場合，チェック用ルーチンがクライアント側で改竄されている可能性がある。チェック用ルーチンで改竄防止のために何らかの秘密情報を用いたとしても，クライアント側ではクライアントの計算機内の全ての秘密情報を知ることが可能である。そのため，ソフトウェアを使用する場合にチェック用ルーチンによって完全な偽証防止を行うことは困難である。[2]

そこで本稿では，クライアントによる偽証を防止するために，クライアントマシンに，耐タンパ性を備えた反応時間測定用のハードウェアSIC (Secure ICEGEM Card)を使用する方式を提案する。クライアントはNICとしてSICを使用する。SICはICEGEMを使用する

Hardware-based method of measuring user's response time for improvement of security on ICEGEM.
Yukihisa Taniguchi† Susumu Ishihara‡
Masakatsu Nishigaki‡ Tadanori Mizuno‡
†Graduate school of Information, Shizuoka University
432-8011, Hamamatsu, Japan
‡Faculty of infomation, Shizuoka University
432-8011, Hamamatsu, Japan

パケット（以下ICEパケット）以外に対しては，通常のNICとして振舞う。ICEパケットはICEパケット識別子とIDをIPのオプションフィールドに持つ。このIDは，SICで測定したT_SとT_Cの組を特定する際と，サーバからのメッセージとクライアントからの返答の組を特定する際に使用する。

SICで行う動作の違いにより，2つのSICの実現方式が考えられる。1つは反応時間をSICが測定する方式（測定型SIC）であり，もう一つはSICはパケットがSICを通過した時刻をサーバへと報告するのみで，サーバが反応時刻を求める方式（時刻報告型SIC）である。

以下，両方式の動作の詳細の説明と比較を行う。

3.1 測定型SIC

測定型SICは，SICのみでクライアントの反応時間を測定する。反応時間の計算には，パケットがクライアントに到着した時刻T_Sと，パケットがクライアントから送信された時刻がT_Cが必要となる。そこで，SICはT_Sを記憶するために到着時刻を保持するテーブルを持つものとする。この到着時刻保持テーブルに保存されたT_SとT_Cを対応付けるため，サーバは各パケットにIDを割り振る。あるIDのパケットに対してサーバへの返信を行う際に，クライアントは同じIDを用いる。SICはパケットがクライアントから返信された際にテーブル内からT_Sを取り出し，反応時間を計算し，その結果をサーバへ送信する。テーブル内のデータは参照されるか，もしくは一定時間が経過すると消去される。

3.2 時刻報告型SIC

時刻報告型SICにおけるSICの動作は，ICEパケットが通過した際にT_SまたはT_Cを，パケットのIDと共にサーバへ送信するのみである。反応時間は，SICから受信したT_SとT_Cの差からサーバが求める。サーバはT_SとT_Cを対応付けるため，パケットに一意となるIDを割り振る。あるIDのパケットに対してサーバへの返信を行う際に，クライアントは同じIDを用いる。SICはICEパケットがSICを通過した時刻とIDを，共にサーバへ送信する。サーバはクライアントへのICEパケット送信後，T_SとT_Cが共にSICから到着するまで，先に到着したT_SもしくはT_Cと，IDを保持するテーブルを持つ。ただし，一定時間が経過した場合，SICからのパケットがロスしたとみなしてテーブル内のT_SまたはT_Cは消去される。

3.3 両方式の比較

測定型は，SIC自身がT_Sの保存と反応時間の計算を行うため，SICにある程度高い処理能力とメモリを必要し，コストが高くなる。時刻報告型は，SICは単純な動作を行うだけなので，コストは低くなる。しかし，サーバが反応時間を計算するため，特にクライアント数が増加した際にサーバに高い負荷がかかる。また，経路上のトラフィックが高い場合，SICからの通過時刻パケットが失われる可能性があるが，この場合サーバは反応時間を計算できない。そのため，時刻報告型は信頼性が低い。以上の性質から，経路上におけるパケットロスがおきにくい環境においてはコストが安い時刻報告型SIC，パケット到着の信頼性が重要とされるアプリケーションにおいては測定型SICの使用が適している。

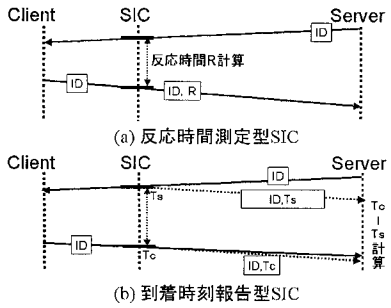

図 2: SIC2方式動作比較

3.4 攻撃に対する耐性の検討

SICは耐タンパハードウェアであり，SICの改造により偽証を行おうとした際にSICのNICとしての機能に支障をきたすように設計される。これにより，SICの改造による偽証は防止可能である。しかしながら，クライアントがSICを使用せず，SICのエミュレータをクライアントの計算機内で動作させた場合には偽証が可能である。これを防止するために，SICはサーバと通信を行う際に，正規のSICのみが可能な電子署名を付加する。

4 まとめ

ICEGEMにおけるクライアントの偽証を防止するため，クライアントに取り付けることによりサーバが必要とする情報を取得するハードウェア，SICを提案した。SICの実装方式として，反応時間測定型と，通過時刻報告型の2つを提案し，そのコストと信頼性について比較を行った。今後の課題は，提案方式のソフトウェアによる実装と評価，プライバシを考慮した電子署名用の鍵管理方式の検討である。

参考文献

[1] 石川貴士, 石原進, 井手口哲夫, 水野忠則: 遅延差のあるネットワークにおけるメンバ間公平性保証方式の特性評価, IPSJ 論文誌, Vol.42, No.7, pp.1819-1827, (2001.7).]

[2] 谷口幸久, 石原進, 水野忠則: メンバ間公平性保証方式におけるハードウェアを用いた偽証防止，マルチメディア，分散，協調とモバイル（DICOMO 2001）シンポジウム論文集, pp.771–776(2001. 6)