L-031

電子透かしを用いたモバイルエージェント改ざん検出システム

Detecting System for Malicious Modification of Data in Mobile Agents

青戸　渉[1]　Wataru Aoto
原　元司[1]　Motoshi Hara

1. はじめに

次世代の分散処理技術として，モバイルエージェントが注目されて久しい．モバイルエージェントは決して新しい技術ではない．しかし，実用的な研究は分散 IDS(侵入検知システム)，アントルーティングなど限られた分野に限られている．この要因としては，モバイルエージェントでなければ実現できない分野が少ないことや，移動先のホストにおいてエージェント保護が困難であることがあげられる．

本研究では，これらの問題を解決するために，モバイルエージェントが保持するデータの改ざん検出システムを提案する．本システムは，悪意のあるホストによってモバイルエージェントのデータが改ざんされた場合に，他のホスト上でその改ざんを検出することを目的とする．

2. モバイルエージェント

モバイルエージェントは，モバイルエージェントサーバ上で実行されるプログラムである．このモバイルエージェントはユーザによって実行されると，自律的にネットワーク上のモバイルエージェントサーバに移動し，そのサーバ上で処理を実行する．処理を終えると，その時の実行状態を保持した上で他のモバイルエージェントサーバに移動する．このようにモバイルエージェントは，異なったモバイルエージェントサーバ間でプログラムを継続的に実行することが可能である．図 1 にモバイルエージェントのイメージを示す．モバイルエージェントの利点としては通信回数の低減，非同期実行，移動先計算資源に対する直接アクセスなどが挙げられる [2]．モバイルエージェントはこれらの特徴から，分散 IDS，アントルーティングなどへの応用が期待されている．

しかし，モバイルエージェントには

- サーバは受け入れたエージェントがどのような動作を行うか予測できない
- エージェントは移動先のサーバにおいてどのような処理が行なわれているか予測できない

といったセキュリティ上の問題が知られている．これらの解決手法についてはこれまでにさまざまな研究が行われているが，移動先のホストがクラックされた場合においては十分にセキュリティを確保できないのが実際である [2]．そこで，本研究では電子透かしとワンタイムパスワードを利用して，モバイルエージェントのデータ改ざん検出システムを考えた．

3. 電子透かしとワンタイムパスワード

電子透かしは，複製が容易にできる画像や動画，音声などのマルチメディアデータに，画質や音質にほとんど

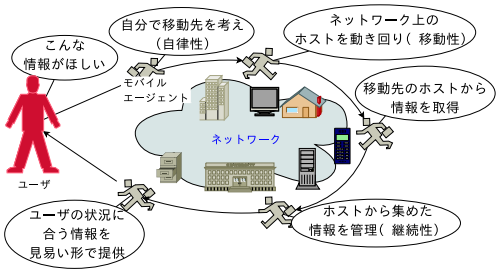

図 1: モバイルエージェントのイメージ

影響を与えずに情報（透かし）を埋め込む技術である．この透かしを取り出すことにより，データが不正に複製されたことや，改ざんされたことを検出できる．

電子透かしは冗長性の高いデータに使われることが一般的である．これは，透かしを埋め込んだとしても，人には元のデータとの違いが容易に認知できないためである．本研究においてモバイルエージェントが扱うデータは数値データである．そのため，電子透かしを実際の動作に影響が少ない数値データの下位ビットに適用することにした．

しかし，電子透かしを数値データの下位ビットに適用する場合，数値データそのものの冗長性が低いため，第三者から電子透かしの存在を見破られる可能性が高い．そのため，電子透かしを埋め込む度に変化させる方式を考えた．これは，ワンタイムパスワード [3] と同じ原理である．本研究では，この方式をワンタイム電子透かしと名付けた．

4. 電子透かしを用いた改ざん検出

提案システムでは，数値データへ埋め込むたびに透かしを計算する．計算には式 (1) を用いる．

$$W_n = \begin{cases} F(S_x) & (n = 1) \\ F(W_{n-1}) & (n \in \mathbb{N}, n \geq 2) \end{cases} \quad (1)$$

ここで，S_x はホスト X に割り振られたユニークな初期値である．W_n は n 回目に埋め込まれる透かしを表す．数学的アルゴリズム F には一方向正関数であるハッシュ関数を用いた．

ワンタイム電子透かしにより，ホストから受け取るデータには毎回異なる電子透かしが埋め込まれる．この方式により，ゲストマシンや第三者は電子透かしの把握が困難になる．

一方，ネットワーク上の全てのホストマシンは，電子透かしを計算する数学的アルゴリズム F と，各ホストマシンへ割り振られたにユニークな初期値 S の情報を知っている．ホストマシン X は，数値データの下位ビットに

[1]松江工業高等専門学校

電子透かし W_n を埋め込む場合，初期値からの計算回数 (n) を同様に埋め込む．モバイルエージェントが他のモバイルエージェントサーバに移動すると，移動先のホストは，モバイルエージェントが保持する数値データから計算回数の情報を読み取る．続いて，ホストマシンは，自身が持つ S_x と数学的アルゴリズム F を用いて電子透かしを求め，モバイルエージェントが保持するデータの電子透かしと比較することで改ざんを検出する．

5. 提案システム

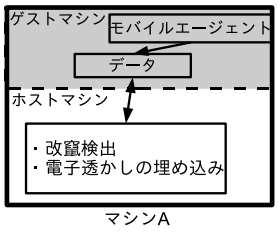

図 2: 提案システムにおけるエージェント環境

本研究では，ワンタイム電子透かしを用いて，悪意のある第三者によって行われるモバイルエージェントのデータ改ざんを検出するシステムを提案する．提案システムでは，仮想環境 (以降仮想環境をゲストマシン，ホスト環境をホストマシンと呼ぶ) を利用する．モバイルエージェントサーバはゲストマシンで動作させることにする．また，ホストマシンでは 4 章で述べた改ざん検出システムを動作させる．仮想環境を用いることにより，ホストマシンで動作する改ざん検出システムのセキュリティレベルを上げることができる．

図 2 に提案システムにおけるエージェント環境を示す．提案システムでは，ゲストマシン上のモバイルエージェントはプログラムの処理に必要なデータをホストマシンから受けとる．ここで，ホストマシンから与えられるデータには電子透かしが埋め込まれている．なお，ゲストマシンあるいは，ネットワーク上の第三者は電子透かしの情報を容易に把握することは困難である．

6. 実験システムの実装と考察

6.1 実験システムの構築

提案システムの実証実験のため，アントルーティング [1] を想定した実験システムを開発した．アントルーティングで扱うデータは遅延時間，リンク利用率，フェロモンの変化量などの数値データが中心となる．そこで，電子透かしを埋め込んだ場合でも影響が最も小さいフェロモンの変化量に電子透かしを埋め込むことにした．ここでは，フェロモンの変化量の値を示す 64 ビット中下位 32 ビットの任意の位置へ電子透かしを埋め込んだ．

表 1 に示した環境のホストを 4 台用意し，フルコネクト型のネットワークを構築して，アントルーティングを模擬したシステムを実装した．

6.2 実験結果と考察

実証実験を行った結果，モバイルエージェントの送信にかかる遅延時間の誤差が大きく，ワンタイム電子透かしが与える影響はアントルーティングではほぼ無視できる範囲であることがわかった．

表 1: 実証実験の環境

ホストマシン	FreeBSD 7.2R
ゲストマシン	FreeBSD 7.2R 上の jail 環境
モバイルエージェントサーバ	Aglets 2.0.2

ホストマシンは数値データへ電子透かしを埋め込む場合，数値データへの影響 (誤差) を考慮した上で電子透かしの桁数を決めることができる．実証実験では，電子透かしを 32 ビットの桁数としたが，改竄されたデータと偶然一致してしまう可能性がある．この問題を防ぐためには，32 ビット中により多くの桁数の電子透かしを埋め込むことが必要である．また，埋め込む電子透かしの最大桁数を増やす方法もある．これらの方法により，モバイルエージェントの改竄検出がより高い確率で行える．しかし，埋め込んだデータと元のデータと比べた場合，データとしての誤差が大きくなり，システムの動作に影響が及ぶ．このように，セキュリティレベルと誤差はトレードオフの関係にある．

一方，電子透かしを計算するハッシュ関数及び，ホストの初期値が知られてしまった場合，本システムではモバイルエージェントのデータを保護できない．このことを防ぐには，ホストマシンが悪意のある第三者にクラッキングされないように保護することが求められる．

7. まとめ

本研究では仮想環境とワンタイム電子透かしを用て，モバイルエージェントのデータ改ざん検出を行うシステムを提案した．課題として，ワンタイム電子透かしのセキュリティ強度の評価方法を検討していく必要がある．今後，P2P や携帯端末を用いて実用的な環境でのモバイルエージェントについて研究を行いたい．

参考文献

[1] 岩田元，確率的ルーティングアルゴリズム ARH の MANET への適用手法，情報処理学会モバイルコンピューティングとユビキタス通信研究会，98 号，pp105-112(2007).

[2] Carrigues Olivella Bellterra, CONTRIBUTION TO MOBILE AGENT PROTECTION FROM MALLICIOUS HOSTS, http://www.tesisenxarxa.net/TESIS_UAB/AVAILABLE/TDX-0323109-164420/cgo1de1.pdf, (2008).

[3] ワンタイム・パスワード，http://itpro.nikkeibp.co.jp/article/COLUMN/20060414/235357/

[4] The Aglets 2.0.2 User's Manual，http://jaist.dl.sourceforge.net/project/aglets/User_s/%20Manual/March%202009/manual031209.pdf