モバイルエージェントセキュリティに関する研究

長谷川 亙 (510080)

北陸先端科学技術大学院大学 情報科学研究科

2007 年 2 月 8 日

キーワード: モバイルエージェント, セキュリティ, 紛失通信, 暗号回路, secure function evaluation.

ネットワーク上のコンピュータを自律的に移動し，ユーザの代理として実行処理をするプログラムをモバイルエージェントという．モバイルエージェントの技術は分散オブジェクトに続く次世代コンピューティング基盤として位置付けられ，注目を集め急速な発展を遂げている．モバイルエージェントの利点として，エージェントの自律的な移動によるコンピュータ間の通信遅延の低減，エージェントを複数生成することによる計算処理の並列化などが挙げられる．

しかしモバイルエージェントの実現にあたり，脅威となる攻撃が２つ存在する．１つは，悪意あるエージェントがウイルスなどによってホストに被害を及ぼす攻撃，もう１つはエージェントが悪意あるホスト上で実行処理をするときにおける秘密情報の盗聴やエージェントの改ざんなどの攻撃である．前者への対策は，ウイルス駆除ソフトや JAVA セキュリティなど確立したものが存在するが，後者への対策は，プログラムを単に暗号化するだけでは実行時に平文に復号しなければならず，暗号化の意味を成さないことから，困難とされてきた．

その解決策として，暗号化されたプログラムを暗号文のまま実行処理できる手法が研究されており，C. Cachin らにより secure function evaluation を用いた手法が提案された．しかし，この手法では悪意ある実行ホスト (malicious behavior) が暗号回路と暗号回路入力，暗号回路出力を不正に操作できるという問題が存在する．そこで，J. Algesheimer らは，エージェントと実行ホスト間に信頼できるホストを導入し，エージェントが保持する暗号回路入力を信頼できるホストの公開鍵で暗号化する手法を提案した．ここで，信頼できるホストから実行ホストへ暗号回路入力を送るために紛失通信と呼ばれる通信を用いる．しかし，このとき 1-out-of-2 紛失通信を単純に用いると，暗号回路入力の 1bit ごとに 1-out-of-2 紛失通信を繰り返し行わなければならず，効率が悪い．そのため，森らは，k-out-of-n 紛失通信をモバイルエージェントに適した形に改良し，1-out-of-2 紛失通信に代わり適用することで，通信量と計算量の削減に成功した．

ここで安全性として，紛失通信に求められる要件に，Correctness，The receiver's privacy，The sender's privacy の 3 つが挙げられる．

- Correctness：両ホストがプロトコルに則った動作を行ったときに，受信者ホスト（実行ホスト）は自身が選択した秘密情報について正しく得られること．
- The receiver's privacy：送信者ホスト（信頼できるホスト）に対して，受信者ホストの選択した（クエリ）秘密情報が秘匿されていること．
- The sender's privacy：受信者ホストに対して，送信者ホストの秘密情報から受信者ホストが選択した秘密情報以外は秘匿されていること．

森らのプロトコルでは，紛失通信において実行ホストが選択するクエリの各 bit を 0 と 1 の 2 つの集合に分割するため，各 bit が全て 0 か 1 である場合や，どちらかの bit に偏りが生じているときなど，特殊な条件下において The receiver's privacy を満たさないことがわかった．

そこで本研究では，特殊な条件下でも安全性を確保するために，実行ホストが選択するクエリを 2 つの集合に分割せず一括して紛失通信を行った．これにより，エージェントと実行ホストの間で，効率が良くかつ安全性を満たす通信手法を提案した．

提案方式 1 は実行ホストがプロトコルに則った動作（honest-but-curious behavior）を行うときに有効であり，実行ホストがプロトコルに従わない動作（malicious behavior）を行った場合は，クエリを特殊な形に変更して信頼できるホストに送ることにより，信頼できるホストが保持する秘密（暗号回路入力）の双方を入手する可能性がある．そこで，提案方式 2 では，実行ホストがプロトコルに従わない動作を行っても，The sender's privacy を満たす（信頼できるホストの秘密が漏洩しない）手法を提案した．ただし，提案方式 1,2 共に信頼できるホストと実行ホスト間で，必ず 3 回の通信が必要となる．

その結果として，森らのプロトコルにおける 2 者間の通信を盗聴する攻撃者に対する安全性の問題を克服した．更に提案したプロトコルの効率性を，通信量と計算量の観点から既存方式と比較した．その結果，Cachin らのプロトコルより効率的であり，森らのプロトコルと同程度の効率性を実現できることを示した．