A Game-Theoretic Framework for Analyzing Trust-Inference Protocols

Ruggero Morselli_ Jonathan Katz_ Bobby Bhattacharjee
岡田行央

ゲーム理論による信用推定解析プロトコル

■はじめに

P2P ではメンバーに協力が求められる。リソースシェアリングではコンピュータの処理能力を提供し、協力する事が欠かせない。ここにただ乗りする free riders が増えると、寄与してくれるユーザが減少する。Free riders へ罰を与える方法が様々なシステムで取り上げられている。

■Free riders 防止既存の方法

事前に作業にストレスが掛かる予備行為が必要であり、同じ方向を目指すものたちの間で成り立つ。特定の(理性がある) 敵対者に柔軟ではなく、チートも発生する。EigenTrust などでは名士(notable exceptions) が必要な場合もある。サーバを用いた方法では事前行為として、公開掲示板などで掲載されるようにする。

■提案手法で改善できる点

明確なプロトコルの上で動く厳密な証明を可能にするセキュリティプロトコルである。信頼推論プロトコルは様々なシステムに柔軟に対応可能なモデルと言え、中央集権サーバの Global knowledge コントロールや中央認証を必要としなくなる。

様々な Sybil attack や非同期取引に有効

■敵対者のフレームワーク

敵対モデル(adversarial model) で調整があっても丈夫であり、信用推論プロトコルは、ゲーム理論による均衡を形成する。ただし敵が多すぎないことを前提としている。

■Basic framework

(前提)

・ペンネームを使う
・ユーザが簡単にペンネームを作成可能
・他のパーティがまねることが不可能
・ペンネームを公開鍵と同一視することによって満たされる。
・サーバで公認する必要が無い
・ユーザは 同じペンネームをずっと使い続ける

(取引)

A(敵) 新しい正直なユーザはペンネーム i を登録し A はペンネームを学習する。正しい処理では 2 ユーザのゲームを行う。プロトコルΠ で振舞う。 i は Π にしたがってゲームをする。敵は i にプレーヤ id を送る。Id は正直なパーティに保持されていることを必要とする。正直なユーザ同士では A からの干渉無しにメッセージを送信でき (A が匿名を代表して送る場合を除いて)、A はΠ の元で送信されるメッセージを眺められる環境

協力 C(cooperate), 欠陥 D(defect) で示す。

	C	D
C	(1, 1)	(-1,2)
D	(2, -1)	(0, 0)

利得行列
時間や異なったゲームが動く

解決法
■ 時間の概念を(割引係数の様に) 追加する。
□t(t ≥ 0 の整数)
□ 短い時間でそれほどたいしたことができない事を元にする
□ 同時に余りたいした量の人と取引できない。
□ 時間の経過とともにΠ が走る
■N であるなら安全というのはウィルス等で破綻するので、この手法を用いる場所は気をつけましょう

■何回、δ 訪問するかで敵のユーティリティは増大する。
□ D を play する A に C は計算時間をδ 分支払う

■A がΠ に従うことでユーティリティを増大するのであれば、Π は有効
□Π がだめになったら、subgame 完全均衡を形成する必要がある。

■Π が理想的に振動に柔軟であるべき
■ 振動する確立ε による
■Eigentrust などは新参者に厳しいので、ユーザが加わるのをおもいとどまる
■ 送らなければならないメッセージの数

■ 有効な strategy
□Grim trigger 確立ε が高いとき信頼できない
□Veteran
を使う。
(利点)
■ 会員資格をネットワークで繋ぐ。
□ コンスタントに新規ユーザがはいってくるかも
□Tit for tat で解決する
■ 複数を相手にできないから強固(?)

Grim trigger の説明
■ 最初の亡命が起こるまですべてのプレーヤーは協力し、亡命が起こったと聞くとどんどん亡命する

Grim trigger をつかった説明
■ それぞれのラウンド終わりにパートナーが逸脱したか・従ったかにかかわらず broadcast する

■ 言いなりになった場合も、いいなりになったという事と、メッセージを送信する
■ 例外として、ベテランと新人 2 人の取引で、ベテランが亡命した場合
■ j　が i にたいして、前のラウンドにおいてのことを broadcast すると i は亡命する
■ ただ、j が嘘をついた場合これを増大させないために、例外を導入した。