Verification of Nash Equilibria in Probabilistic BAR Systems

Dileepa Fernando, Naipeng Dong, Cyrille Jegourel, Jin Song Dong

School of Computing
National University of Singapore

8 September 2016

Outline

Introduction

- Multi agent systems
- Each agent should follow a protocol (probabilistic)
- Some components/agents may misbehave (corrupted/misconfigured)
- **Can a multi agent system achieve its goals in the presence of misbehaving agents?**

BAR Framework

Systems with misbehaving agents

Byzantine Player Can deviate from protocol spec. arbitrarily-non-deterministic

Altruistic Player Follows the protocol correctly (probabilistic)

Rational Player Deviates from the protocol only to optimize his utility (non-deterministic)

Consider system protocol as a game

BAR System as a Game

- Concurrent - player moves are independent
- Probabilistic players and non-deterministic players
- Perfect and Imperfect information

Outline

BAR tolerance and Nash-equilibrium

- BAR tolerance - Whether a property holds in a BAR system in the presence of Byzantine and rational players
- Rational players should choose to be altruistic
- BAR tolerance for Nash-equilibrium

Outline

Related Work

Mari et al. Verify Nash-equilibria in infinitely executed, non-probabilistic BAR systems

PRALINE Compute Nash-equilibrium for non-probabilistic, concurrent games

PRISM-games Finding optimal strategies for probabilistic, turn-based games

All these systems had perfect information assumption

Outline

Specification of a Player

Specification $\mathcal{M}_i$ of player i:

- $\mathcal{M}_i^b = (S_i^b, I_i^b, A_i^b, T_i^b)$ [if i is Byzantine]
- $\mathcal{M}_i^a = (S_i^a, I_i^a, A_i^a, G_i^a, T_i^a, P_i^a, H_i^a)$ [if i is Altruistic]
- $\mathcal{M}_i^r = (S_i^r, I_i^r, A_i^r, G_i^r, T_i^r, H_i^r)$ [if i is Rational]

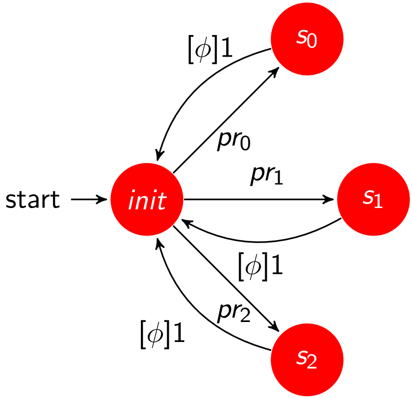
Full Specification

- Full specification of probabilistic game: $\mathcal{M} = (S, I, A, G, T, P, H)$
- Global state set, Initial state set, Action set, Global Proposition set - $S = S_1 \times S_2 \times \cdots \times S_n$, $I = I_1 \times I_2 \times \cdots \times I_n$, $A = A_1 \times A_2 \times \cdots \times A_n$, $G = G_1 \times G_2 \times \cdots \times G_n$
- Transition function $T(\langle s_1, \ldots, s_n \rangle, \langle a_1, \ldots, a_n \rangle) = \langle s_1' \ldots, s_n' \rangle$
- Transition probabilities $P(\langle s_1, \ldots, s_n \rangle, \langle a_1, \ldots, a_n \rangle)) = P_1(s_1, a_1) \times \ldots \times P_n(s_n, a_n)$
- Pay-off $H(\langle a_1, \ldots, a_n \rangle, s) = \langle H_1(a_1, s), \ldots, H_n(a_n, s) \rangle$

Outline

Three player Rock-Paper-Scissors

- rock = 0, paper = 1, scissors = 2
- (i, j, k) corresponds to player p_1, p_2 and p_3 actions
- player p_1's utility : $(i - j) modulo3 + (i - k) modulo3$



Outline

Algorithm

- **Input**: $\langle \mathcal{M}_1, \mathcal{M}_2 \ldots \mathcal{M}_n \rangle$, ϵ, $iter_{max}$, $perfect$
- **Output**: Existence of Nash Equilibrium (NE) $\{PASS, FAIL, NOTDECIDED\}$
- **Approach** :
  1. Find the sufficient number of iterations *iter* to assure the Nash-equilibrium result
  2. Calculate the optimal altruistic utility $(U_i(s,t))$ and optimal rational utility $(V_i(s,t))$
  3. $U_i(init, iter) - V_i(init, iter) \geq 0.$ $\forall$ altruistic $i \iff NE$

Iterative Utility Value Update

- Consider a set of *iter* global action sequences
  - For probabilistic action sequences we calculate the expected pay-off
    - $V_i(s, t)$ is optimal expected pay-off value for **rational** i
    - $U_i(s, t)$ is optimal expected pay-off value for **altruistic** i
  - For non-deterministic action sequences, choice is made based on the player type
- Choose different optimal actions for different player types
  - Minimum pay-off over Byzantine actions
  - Expected pay-off over altruistic actions
  - Maximum pay-off over rational actions

Example: Continued

$\langle \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \rangle$ Strategy: rock-0, paper-1, scissors-2

Pay-offs of altruistic player p_2 when p_1 plays rock

p_1	0	0	0	0	0	0	0	0	0
$\boldsymbol{p_2}$	0	0	0	1	1	1	2	2	2
p_3	0	1	2	0	1	2	0	1	2
pay-off(p_2)	0	-1	1	2	1	0	-2	0	-1

Pay-offs of rational player p_2 when playing rock

p_1	1	1	1
$\boldsymbol{p_2}$	0	0	0
p_3	0	1	2
pay-off(p_2)	-1	-2	0

Example : Continued

Expected pay-off calculation for player p_2

	t=0	t=1	t=2	...
$V_2(S_0, t)$	0	-1	-1.66	...
$U_2(S_0, t)$	0	0	0	...

- $\langle b, r, a \rangle,\ V_2(\langle s_0, s_0, s_0 \rangle) = -3$
- $\langle b, a, a \rangle,\ U_2(\langle s_0, s_0, s_0 \rangle) = 0$
- $U_2(\langle s_0, s_0, s_0 \rangle) \geq V_2(\langle s_0, s_0, s_0 \rangle) \implies NE$

Correctness of the Algorithm

We proved two following assertions.
Let $i \notin Z$, $init \in I$

- $V_i(init, t)$ and $U_i(init, t)$ converge in our setting
- $(V_i(init) - U_i(init)) \neq 0 \implies (V_i(init, iter) - U_i(init, iter))(V_i(init) - U_i(init)) > 0$

Outline

Case Study 1 : Three player Rock-Paper-Scissors Game

Description Defined in the example

Evaluation
- Verified NE for four configurations
  - $\langle \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \rangle$
    - 1^{st} player Byzantine
    - No Byzantines
  - $\langle \frac{1}{5}, \frac{1}{5}, \frac{3}{5} \rangle$
    - 1^{st} player Byzantine
    - No Byzantines

Should a rational player follow the protocol?

Strategy \ Byzantines	Zero	One
$\langle \frac{1}{3}, \frac{1}{3}, \frac{1}{3} \rangle$	Yes	Yes
$\langle \frac{1}{5}, \frac{1}{5}, \frac{3}{5} \rangle$	No	Yes

Case Study 2: Randomized Secret Sharing Protocol

Description

- Randomized Secret Sharing protocol[1]
- Verify no player can gain more utility by deviating from the protocol
- Sends the secret share based on a random value generated
- Message passing to communicate global state
- Reconstruct the secret if all the secret shares received

Evaluation

- 3 players, no Byzantine Vs one Byzantine
- Possible deviations - Not sending messages
- Verified NE.

Outline

Conclusion

- Defined a framework to model probabilistic BAR systems
  - Byzantine players are non-deterministic
  - Altruistic players are probabilistic
  - Rational players are non-deterministic
- Developed an algorithm to verify Nash-equilibrium
- Applied the model and algorithm in a game and a real application (Randomized Secret Sharing)
- **Can Byzantine players enforce altruism in rational players?**

Thank You!!!

Questions?

J. Halpern and V. Teague.
Rational secret sharing and multiparty computation: Extended abstract.
In *Proc. 36th Annual ACM Symposium on Theory of Computing*, pages 623–632. ACM, 2004.