Security and Game Theory

or

Out of Eden

Jared Saia
A hard fact:

Not everyone follows instructions
Good and Bad

A simple moral code for an aspiring deity (or computer scientist)

Good: follow instructions

Bad: don’t follow instructions
Question: How can we ensure that a group functions, even though some members of the group are bad?
Components Fail, Group Functions
Group Decisions

- Periodically, components unite in a decision

- Idea: components vote. Problem: Who counts the votes?
Our Model

We assume an adversary controls a hidden subset of the components

We control the remaining components

Goal: All the good components unite in a decision
Our Model

We assume an adversary controls a hidden subset of the components.

We control the remaining components.

Goal: All the good components unite in a decision.
Idea: Majority Filtering

Input

0
0
0
1
1

Output

0
0
0
0
0

Thursday, June 16, 2011
Idea: Majority Filtering

Input

Output

0

0

0

0

1

0

1

0

0
Problem

Input

Output
Byzantine Agreement

- Each processor starts with a bit
- Goal: 1) all good procs output the same bit; and 2) this bit equals an input bit of a good proc
- \( t = \# \) bad procs controlled by an adversary
Problem

Input

Output

Thursday, June 16, 2011
All good procs always output same bit

Byzantine Agreement

Input

Output

Thursday, June 16, 2011
If majority bit held by $\geq 3$ good procs, then all procs will output majority bit.
1982: FLP show that 1 fault makes deterministic BA impossible

2007: Nancy Lynch wins Knuth Prize for this result, called “fundamental in all of Computer Science”
Applications

- Peer-to-peer networks
  "These replicas cooperate with one another in a Byzantine agreement protocol to choose the final commit order for updates." [KBCCEGGRWWWZ ’00]

- Rule Enforcement
  "... requiring the manager set to perform a Byzantine agreement protocol" [NWD ’03]

- Game Theory (Mediators)
  "deep connections between implementing mediators and various agreement problems, such as Byzantine agreement" [ADH ’08]
Applications

- Peer-to-peer networks
  “These replicas cooperate with one another in a Byzantine agreement protocol to choose the final commit order for updates.” [KBCCEGGRWWWZ ‘00]

- Rule Enforcement
  “… requiring the manager set to perform a Byzantine agreement protocol” [NWD ‘03]

- Game Theory (Mediators)
  “deep connections between implementing mediators and various agreement problems, such as Byzantine agreement” [ADH ‘08]

- Also: Databases, Sensor Networks, Cloud Computing, Control systems, etc.
Our Model

- Assume Global Coin: source of random bits that everyone can see
- Adversary: takes over 1/3 of the procs
- Private channels: message can be sent privately between any pair of procs
BA with Global Coin, GC

Rabin’s Algorithm

Send your vote to everyone

Let \( \text{fraction} \) be fraction of votes for majority bit

If \( \text{fraction} \geq 2/3 \), set vote to majority bit; else set vote to GC
BA with Global Coin, GC

Rabin’s Algorithm

Set your vote to input bit

Repeat colgn times:

Send your vote to everyone

Let $fraction$ be fraction of votes for majority bit

If $fraction \geq 2/3$, set vote to majority bit; else set vote to GC

Output your vote
fraction >= 2/3. I'm voting for 0.
fraction $< \frac{2}{3}$. I’m checking the coin.
All-to-all

- **fraction >= 2/3**
  - I'm voting for 0.

- **fraction < 2/3**
  - I'm checking the coin.

- **fraction >= 2/3. I’m voting for 0.**

Thursday, June 16, 2011
Note: The procs with \( \text{fraction} \geq 2/3 \) will all change vote to same value. I'm voting for 0.
All-to-all

fraction >= 2/3. I’m voting for 0.

fraction < 2/3. I’m checking the coin.

fraction >= 2/3. I’m voting for 0.
All-to-all fraction >= 2/3. I'm voting for 0.

fraction < 2/3. I'm checking the coin.

fraction >= 2/3. I'm voting for 0.

Probability 1/2 that both groups change vote to the same value
Probability $1/2$ that both groups change vote to the same value

Once this happens, all votes of good procs will be equal evermore

$\text{fraction} \leq 2/3$. I'm checking the coin.

$\text{fraction} \geq 2/3$. I'm voting for 0.
Probability $1/2$ that both groups change vote to the same value

Once this happens, all votes of good procs will be equal evermore

\[
\text{Prob of failure} = \left( \frac{1}{2} \right)^{c \log n} = \frac{1}{n^c}
\]
Probability $1/2$ that both groups change vote to the same value

Once this happens, all votes of good procs will be equal evermore

Prob of failure $= (1/2)^{c \log n}$

$= 1/n^c$

Prob of success $= 1 - 1/n^c$
Probability 1/2 that both groups change vote to the same value

Once this happens, all votes of good procs will be equal evermore

\[
\text{Prob of failure} = \left(\frac{1}{2}\right)^{c \log n} = \frac{1}{n^c} \\
\text{Prob of success} = 1 - \frac{1}{n^c}
\]
Q: Where can we get a global coin?

A1: The procs take turns flipping a coin and sending the results to everyone. The good procs at least will flip a fair coin.

Problem: If n procs, this method may take \( \sim n \) rounds

A2: Parity of closing price of stock market
Leader Election

- n processors
- Less than a 1/3 fraction of them are bad
- Goal: Elect a leader such that 1) all good procs agree on the leader; and 2) the leader has constant probability of being good
Committee Election

- n processors
- Less than a 1/3 fraction of them are bad
- Goal: Elect a committee such that 1) all good procs agree on the committee; and 2) the fraction of bad procs in the committee isn’t too large
Idea: Lightest Bin Algorithm

1. Each proc. picks a bin uniformly at random
2. Winners are candidates in lightest bin
a,b,c,d,e,f,g,h,i
you guys go first
With $O(n/\log n)$ bins, whp, each bin has about same # of good procs
With $O(n / \log n)$ bins, whp, each bin has about same # of good procs.

So fraction of bad in lightest bin will be not increase by much.
e, i

curses, foiled again!
Problem: Bad procs can be inconsistent in telling good procs which bin they choose.
Problem: Bad procs can be inconsistent in telling good procs which bin they choose

Solution: Use Byzantine agreement to enforce a single bin choice for each proc!
A hard(er) fact:

Nobody follows instructions that aren’t in their own best interest
A hard(er) fact:

Nobody follows instructions that aren’t in their own best interest
Game Theory

- We assume all agents are selfish and rational.
- **Nash equilibrium**: Situation where no player has any incentive to change its action.
- **Note**: There may be more than one.
Price of Anarchy (POA)
(Papadimitriou and Koutsoupias ’99)

- Social Welfare (SW) = Sum of costs of all players
- In most games, SW in Nash equil. is worse than SW with benevolent dictator
- POA measures that difference
POA (KP '99)

\[ POA = \frac{SW \text{ in Worst Equilibria}}{SW \text{ with Benevolent Dictator}} \]

- Measures “tragedy of the commons” effect
POA

- POA can vary widely from one game to the other
- But there are many, many games with high POA
POA

- POA can vary widely from one game to the other
- But there are many, many games with high POA
- Problem: Can we reduce POA, without changing a game or injecting money or other resources?
Pollution Game

- Each player decides to pollute or not pollute
- Cost to a player is number of other players that pollute plus 2 if they do not pollute
Pollution Game

- Each player decides to pollute or not pollute
- Cost to a player is number of other players that pollute plus 2 if they do not pollute
- Nash Equilibrium: Everybody pollutes
- Benevolent Dictator (Optimal): Nobody pollutes
Pollution Game

- SW in Nash: \( n^2 \)
- SW in Optimal: \( 2n \)
- Price of Anarchy: \( n/2 \)
Infinite Round

- Mediator: Advises each player not to pollute, until some player disregards advice. If this happens, from then on advise everyone to pollute.

- Result: Nobody pollutes!

- Significantly improves the SW
Mediator privately suggests an action to each player

Players can ignore suggestions of mediator; they retain free-will and remain selfish

Goal: Use mediator to improve SW
Mediator

- The mediator is an algorithm!

- The mediator might conceivably be a *randomized* algorithm

- A mediator may work even for a single round game!
El Farol Var.

\[ f_1(x) = \frac{1}{2} \]

\[ f_2(x) \]

\[ f_2(x): \]

\[ \text{cost} \]

\[ \begin{array}{c}
0 \\
1/2 \\
1 \\
\end{array} \]

\[ \begin{array}{c}
\text{flow} \\
\end{array} \]
El Farol Var.

\[ f_1(x) = \frac{1}{2} \]

\[ f_2(x) \]

Mediator:
- With probability 1/3, tell all players to go up
- With probability 2/3, tell half the players to go up and half to go down

Thursday, June 16, 2011
El Farol Var.

\[ f_1(x) = \frac{1}{2} \]

\[ f_2(x) : \]

Mediator:
- With probability 1/3, tell all players to go up
- With probability 2/3, tell half the players to go up and half to go down

Achieves S.W. of 1/3 vs 1/2 for the Nash
Q: Where does the mediator come from?
Mediator?

Q: Where does the mediator come from?

“It is the final proof of God’s omnipotence that he need not exist in order to save us.” - Peter De Vries
Mediator
No Mediator
No Mediator
Distributed Mediation

- A mediator can be implemented in a fully distributed manner by the players themselves ("cheap talk")

- Similar to cryptographic results on e.g. global coin toss and secure multiparty computation

- These algorithms make critical use of Byzantine agreement!
Auctions

- Similar techniques have been used to design completely distributed auctions
- No auctioneer!
- Nobody learns your bid unless you win!
Conclusion

We can still accomplish some goals even if not all agents blindly follow our instructions
Conclusion

We can still accomplish some goals even if not all agents blindly follow our instructions

We can accomplish some goals (just by offering advice) even when all agents have free-will
Conclusion

We can still accomplish some goals even if not all agents blindly follow our instructions.

We can accomplish some goals (just by offering advice) even when all agents have free-will.

However, the whole field is in its infancy and there still is a lot we don’t understand about what is and what is not possible.
Open Questions

- How efficiently can we perform Byzantine agreement?
- How efficiently can we implement a mediator?
- What properties must a game have in order for a mediator to be able to improve the social welfare?
Interested?

“When I talk about computer science as a possible basis for insights about God, of course I’m not thinking about God as a super-smart intellect surrounded by large clusters of ultrafast Linux workstations and great search engines. That’s the user’s point of view.” - Donald Knuth
Interested?

Join Us!!!

Thursday, June 16, 2011
Contact Info

- Questions, Ideas or thoughts?
- Google: Jared Saia to get my contact info
- I’m always interested in working with smart students