Brief Announcement: Theory of BAR Games

Allen Clement
University of Texas at Austin
Austin, Texas
aclement@cs.utexas.edu

Jeff Napper
University of Texas at Austin
Austin, Texas
jmn@cs.utexas.edu

Harry Li
University of Texas at Austin
Austin, Texas
harry@cs.utexas.edu

Jean-Philipe Martin
Microsoft Research
Cambridge, United Kingdom
jpmartin@microsoft.com

Lorenzo Alvisi
University of Texas at Austin
Austin, Texas
lorenzo@cs.utexas.edu

Michael Dahlin
University of Texas at Austin
Austin, Texas
dahlin@cs.utexas.edu

Categories and Subject Descriptors

D.4.5 [**Operating Systems**]: Reliability; C.2.4 [**Computer-Communication Networks**]: Distributed Systems

General Terms

Algorithms, Economics, Reliability, Theory

Keywords

Game Theory, Distributed Systems, Algorithms

1. INTRODUCTION

Distributed systems are increasingly deployed over Multiple Administrative Domains (MADs) in which no single authority has control over all participating nodes. Traditionally, nodes in distributed systems deviate from their specification because they are *broken* (e.g., due to bugs, hardware failures, configuration errors, or even malicious attacks). MAD systems add a new dimension: without a central administrator ensuring that each unbroken node follows the assigned protocol, a node may deviate because it is *selfish* and intent on maximizing its utility.

Byzantine Fault Tolerance (BFT) [7] handles broken nodes well. However, the Byzantine model classifies *all* deviations as faults and requires a bound on the number of faults; this bound is untenable when all nodes may be broken or selfish. Conversely, game-theoretic models [11] handle selfish nodes well. However, these models are often vulnerable to arbitrary disruptions if even one broken node[1] behaves irrationally.

The key challenge in designing and deploying MAD systems is ensuring that the system provides the desired functionality in the presence of both Byzantine and selfish nodes. A convenient way for protocol designers to approach this problem is by first designing protocols that achieve the desired functionality provided that non-faulty nodes follow the protocol and then showing that the specified protocol is incentive compatible, i.e. that selfish nodes will not modify the protocol for personal gain. The first step in this process is conveniently handled by existing approaches in the BFT literature; the second step requires integrating Byzantine behavior into game theory.

Several recent works have addressed this challenge [1, 6] by introducing new solution concepts that are mathematically elegant and powerful. In this paper we argue that these solution concepts are inapplicable to games that capture four important aspects of real distributed systems and propose an alternate approach to integrating Byzantine behavior into game theory that is based on augmenting utility functions to explicitly account for Byzantine behavior.

The key results of this paper are:

1. We define Byzantine fault tolerant communication games that capture important aspects of real distributed systems.
2. We announce that no Byzantine fault tolerant communication game can be $(k-t)$-robust as defined by Abraham et al. [1].
3. We formalize the notion of Byzantine aware utility functions implicitly employed in [3, 8].
4. We announce the existence of an incentive compatible protocol for synchronous terminating reliable broadcast.

2. BFT COMMUNICATION GAMES

In our experience, there are four important characteristics of real distributed systems: (i) the system achieves some functionality despite the Byzantine participants—i.e. ensuring the safety properties of TRB or availability and consistency of a file in a distributed file system, (ii) every node is susceptible to failure—there is no trusted mediator that is unerringly correct, (iii) communication between nodes is necessary—without communication the system is not truly distributed, (iv) communication incurs a non-zero cost—free-riding to reduce communication costs is a significant concern for large-scale applications [2, 4].

We call any game that captures these four properties of a distributed system a *Byzantine fault tolerant communication game* (BFTCG).

[1]We use player and node interchangebly throughout this paper.

PODC'07, August 12–15, 2007, Portland, Oregon, USA.
ACM 978-1-59593-616-5/07/0008.

3. BFTCG AND $(K-T)$-ROBUSTNESS

Abraham et al. [1] introduce the (k,t)-robust equilibrium to incorporate collusion among a group of rational players in addition to the Byzantine behavior of other players. Specifically, for (a) a given strategy profile $\vec{\sigma}$, (b) a coalition of players $\mathcal{C}$ of size at most k following a coalition strategy profile $\vec{\phi}_{\mathcal{C}}$, and (c) a set of Byzantine players of size at most t following a Byzantine strategy profile $\vec{\tau}_{\mathcal{T}}$, no rational player i in the coalition can obtain better utility than when the coalition follows the given strategy profile $\vec{\sigma}_{\mathcal{C}}$. We give the formal definition from [1]:

Definition 1. A strategy profile $\vec{\sigma} \in \mathcal{S}_{\mathcal{N}}$ is a (k,t)-*robust equilibrium* if for all $\mathcal{C}, \mathcal{T} \subseteq \mathcal{N}, \mathcal{C} \cap \mathcal{T} = \emptyset$, $|\mathcal{C}| \leq k$, and $|\mathcal{T}| \leq t$, $\forall \vec{\tau}_{\mathcal{T}} \in \mathcal{S}_{\mathcal{T}}$, $\forall \vec{\phi}_{\mathcal{C}} \in \mathcal{S}_{\mathcal{C}}$, $\forall i \in \mathcal{C}$ we have $u_i(\vec{\sigma}_{\mathcal{N}-\mathcal{T}}, \vec{\tau}_{\mathcal{T}}) \geq u_i(\vec{\sigma}_{\mathcal{N}-(\mathcal{C}\cup\mathcal{T})}, \vec{\phi}_{\mathcal{C}}, \vec{\tau}_{\mathcal{T}})$

While this solution concept is mathematically elegant and implies some very strong properties of a strategy profile, we have observed the following impossibility result in the context of Byzantine fault tolerant communication games.

THEOREM 1. *There is no (k,t)-robust strategy profile that achieves functionality $\mathcal{F}$ for a Byzantine fault tolerant communication game when $k > 0$ and $t > 0$.*

4. BYZANTINE AWARE UTILITY

We argue that the correct way to incorporate Byzantine behavior into game theory is to explicitly augment utility functions with the expected impact of Byzantine behavior on the utility received by rational player i. We achieve this goal by employing a Byzantine aware utility function.

Definition 2. Let u_i be a traditional utility function and f be the maximum number of Byzantine players tolerated by the system. A *Byzantine aware utility function* is the utility function:

$$\bar{u}_i(\vec{\sigma}) = \underset{\mathcal{T}\subseteq\mathcal{N}:|\mathcal{T}|\leq f}{\text{play}} \circ \underset{\vec{\tau}_{\mathcal{T}}\in\mathcal{S}_{\mathcal{T}}}{\text{strat}} \circ u_i(\vec{\sigma}_{\mathcal{N}-\mathcal{T}}, \vec{\tau}_{\mathcal{T}})$$

consisting of *play* applied to *strat* applied to u_i, where *play* is a function over the expected distribution of which players are Byzantine and *strat* is a function over the expected distribution of their employed strategies.

This definition of a Byzantine aware utility functions defines a template that can be used to model different considerations of Byzantine behavior. A *risk averse* player i would instantiate both strat and play as min on the assumption that all Byzantine players are out to get i, *optimistic* player j could instantiate both functions as max on the assumption that all Byzantine players are going to go out of their way to help j, and a *realistic* player k might instantiate both functions as a probability distribution on the assumption that the Byzantine players are indifferent to k. Risk averse utility functions have been implicitly employed in a variet of recent works [3, 8, 9, 10].

5. INCENTIVE COMPATIBLE TRB

We have considered a system model where players receive benefits correlated to the safety properties of TRB, incur costs based on the size of messages that they send, and are risk averse with respect to the expected impact Byzantine players have on their utilities. In this setting we have shown that the Dolev-Strong TRB protocol [5] is not a Nash Equilibrium[2]; there exists a simple modification to the Dolev-Strong protocol in which a single selfish player acting in isolation can send fewer messages than specified without violating safety. In this same setting we have developed a novel TRB protocol that is a Nash Equilibrium. We believe that these results demonstrate the benefits of incorporating Byzantine behavior into game theory through the use of Byzantine aware utility functions rather than developing novel solution concepts.

6. ACKNOWLEDGEMENTS

This work was supported in part by NSF award CNS 0509338.

7. REFERENCES

[1] I. Abraham, D. Dolev, R. Gonen, and J. Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In *Proc. 25th PODC*, July 2006.

[2] E. Adar and B. A. Huberman. Free riding on Gnutella. *First Monday*, 5(10):2–13, Oct. 2000.

[3] A. S. Aiyer, L. Alvisi, A. Clement, M. Dahlin, J.-P. Martin, and C. Porth. BAR fault tolerance for cooperative services. In *Proc. 20th SOSP*, Oct. 2005.

[4] B. Cohen. The BitTorrent home page. http://bittorrent.com.

[5] D. Dolev and H. R. Strong. Authenticated algorithms for Byzantine agreement. *Siam Journal Computing*, 12(4):656–666, Nov. 1983.

[6] K. Eliaz. Fault tolerant implementation. *Review of Economic Studies*, 69:589–610, Aug 2002.

[7] L. Lamport, R. Shostak, and M. Pease. The Byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 1982.

[8] H. C. Li, A. Clement, E. Wong, J. Napper, I. Roy, L. Alvisi, and M. Dahlin. Bar Gossip. In *Proc. 7th OSDI*, 2006.

[9] J.-P. Martin. *Byzantine Fault-Tolerance and Beyond*. PhD thesis, The University of Texas at Austin, Dec. 2006. TR-06-66.

[10] T. Moscibroda, S. Schmid, and R. Wattenhofer. When selfish meets evil: Byzantine players in a virus inoculation game. In *Proc. 25th PODC*, 2006.

[11] M. Osborne and A. Rubinstein. *A Course in Game Theory*. MIT Press, 1994.

[2]It is interesting to note that if communication is free then the Dolev-Strong TRB protocol is $(k-t)$-robust.