Randomized Asynchronous Byzantine Consensus Algorithms: A Survey

A Distributed Systems Course Report
by Yanju CHEN
29th Jun 2015
Byzantine Generals Problem

- Agreement on A Common Decision: Consensus
Byzantine Generals Problem

• A Fault Tolerance Problem
• Introduced by Leslie Lamport
• An Intuitive Solution
My Work

• A Survey into randomized asynchronous Byzantine Consensus Algorithms
  • Comparisons between Classical Study and Recent Advances
  • Implementations of the Recent Algorithms
  • Tentative Experiments on Recent Algorithms
  • Analysis of Future Trends
Several Definitions

• Correct/Faulty Process

• 3 Properties of Byzantine Consensus:
  • Validity
  • Agreement
  • Termination

• FLP Impossibility Result
  • No Determined Consensus in Asynchronous Env.
  • Circumventions
    • Probabilistic/Randomized

• This Paper:
  • *Randomized Byzantine Consensus Algorithms*
Additional Problems...

- Optimal Resilience
  - \( n > 3t \)
- Authentications
  - Signatures
- Performance
  - Scalability
  - Resilience
Randomized Techniques

- Modified Property
  - P-Termination
- Started by Rabin and Ben-Or
  - Uncertainty
  - Tossing A Coin
  - Proved P-Termination Satisfied
Classical Study

- All Based on *Rabin’s* and *Ben-Or’s* Work
- Imperfections
  - Resilience NOT Optimal
  - Signatures Required
  - Too Many Steps and Broadcasts
  - Not Practical (Too Theoretical)

**TABLE I: Classical Randomized Asynchronous Byzantine Algorithms, Complexity and Resilience**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>$n &gt;$</th>
<th>signatures</th>
<th>msg/round</th>
<th>bits/msg</th>
<th>steps/round</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rabin 1983</td>
<td>$10t$</td>
<td>yes</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>2</td>
</tr>
<tr>
<td>Ben-Or 1983</td>
<td>$5t$</td>
<td>no</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>2</td>
</tr>
<tr>
<td>Toueg 1984</td>
<td>$3t$</td>
<td>yes</td>
<td>$O(n^3)$</td>
<td>$O(n)$</td>
<td>3</td>
</tr>
<tr>
<td>Bracha 1987</td>
<td>$3t$</td>
<td>no</td>
<td>$O(n^3)$</td>
<td>$O(log(n))$</td>
<td>9</td>
</tr>
<tr>
<td>Srikanth Toueg 1987</td>
<td>$3t$</td>
<td>no</td>
<td>$O(n^3)$</td>
<td>$O(log(n))$</td>
<td>9</td>
</tr>
<tr>
<td>Canetti Robin 1993</td>
<td>$3t$</td>
<td>yes</td>
<td>$O(n^2)$</td>
<td>$poly(n)$</td>
<td>9</td>
</tr>
</tbody>
</table>
Recent Advances

- Still Based on *Rabin’s* and *Ben-Or’s* Work
- Improvements
  - Better Resilience
  - Simpler Communication Steps
  - More Specialized Optimizations
  - More Practical

### TABLE II: Recent Randomized Asynchronous Byzantine Algorithms, Complexity and Resilience

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>$n &gt;$</th>
<th>signatures</th>
<th>msg/round</th>
<th>bits/msg</th>
<th>steps/round</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cachin Kursawe Shoup 2000</td>
<td>$3t$</td>
<td>yes</td>
<td>$O(n^2)$</td>
<td>$O(l)$</td>
<td>$2$</td>
</tr>
<tr>
<td>Friedman Mostefaoui Raynal 2005</td>
<td>$5t$</td>
<td>no</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>Song Renesse 2008</td>
<td>$7t$</td>
<td>no</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>$1$</td>
</tr>
<tr>
<td>Mostefaoui Hamouna Raynal 2014</td>
<td>$3t$</td>
<td>no</td>
<td>$O(n^2)$</td>
<td>$O(1)$</td>
<td>$2$ or $3$</td>
</tr>
</tbody>
</table>
Tentative Experiments

- Objective
  - Characteristics Exploring
- Simulations
  - Python Threading
- Experiment Settings

<table>
<thead>
<tr>
<th>Exp.No.t</th>
<th>n &gt;</th>
<th>t</th>
<th>Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10t</td>
<td>99</td>
<td>Ben-Or’s, OracleBased, OracleBasedFast, RS-BOSCO, BV-Broadcast</td>
</tr>
<tr>
<td>2</td>
<td>7t</td>
<td>140</td>
<td>OracleBased, OracleBasedFast, RS-BOSCO, BV-Broadcast</td>
</tr>
<tr>
<td>3</td>
<td>5t</td>
<td>199</td>
<td>OracleBased, OracleBasedFast, BV-Broadcast</td>
</tr>
<tr>
<td>4</td>
<td>3t</td>
<td>330</td>
<td>BV-Broadcast</td>
</tr>
</tbody>
</table>
Experiment Results & Analysis

- Exp.No.1: Resilience $n > 10t$, $n=1000$, $t=99$
Experiment Results & Analysis

- Exp.No.2: Resilience $n > 7t$, $n=1000$, $t=140$
Experiment Results & Analysis

- Exp.No.3: Resilience $n>5t$, $n=1000$, $t=199$
Experiment Results & Analysis

- Exp.No.3: Resilience $n>3t$, $n=1000$, $t=330$
Experiment Results & Analysis

• Convergence

<table>
<thead>
<tr>
<th>P.Stage</th>
<th>Ben-Or’s</th>
<th>OB</th>
<th>OBF</th>
<th>RS-B</th>
<th>BV-B</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 0</td>
<td>81s</td>
<td>54s</td>
<td>51s</td>
<td>32s</td>
<td>12s</td>
</tr>
<tr>
<td>10%</td>
<td>82s</td>
<td>56s</td>
<td>52s</td>
<td>34s</td>
<td>28s</td>
</tr>
<tr>
<td>20%</td>
<td>83s</td>
<td>57s</td>
<td>52s</td>
<td>34s</td>
<td>50s</td>
</tr>
<tr>
<td>30%</td>
<td>83s</td>
<td>65s</td>
<td>53s</td>
<td>34s</td>
<td>75s</td>
</tr>
<tr>
<td>40%</td>
<td>84s</td>
<td>74s</td>
<td>54s</td>
<td>35s</td>
<td>92s</td>
</tr>
<tr>
<td>50%</td>
<td>86s</td>
<td>83s</td>
<td>57s</td>
<td>38s</td>
<td>107s</td>
</tr>
<tr>
<td>60%</td>
<td>92s</td>
<td>110s</td>
<td>62s</td>
<td>43s</td>
<td>122s</td>
</tr>
<tr>
<td>70%</td>
<td>98s</td>
<td>121s</td>
<td>68s</td>
<td>48s</td>
<td>164s</td>
</tr>
<tr>
<td>80%</td>
<td>103s</td>
<td>169s</td>
<td>72s</td>
<td>54s</td>
<td>201s</td>
</tr>
<tr>
<td>90%</td>
<td>108s</td>
<td>189s</td>
<td>76s</td>
<td>57s</td>
<td>271s</td>
</tr>
<tr>
<td>100%</td>
<td>113s</td>
<td>311s</td>
<td>82s</td>
<td>60s</td>
<td>381s</td>
</tr>
</tbody>
</table>
Future Trends

• Condition-Based Optimizations
• Ensemble Techniques
• Natural Adaptations