Distributed Consensus

Simulator for Distributed Sleepy Consensus Protocol

SJTU 2017 Cornell Summer Workshop

Instructor

Elaine Shi

Cornell University

Our Group:

- **Framework Team Members**

Junxiang Huang	841450297@qq.com
Yifei Pu	pkq2006@gmail.com

- **Honest Node Team Members**

Tiancheng Xie	wjxtcsgx@hotmail.com
Jiaheng Zhang	ZHANGJIAHENG@sjtu.edu.cn
Xiaotian You	youxiaotian@hotmail.com
Shuyang Tang	tangshuyang25@163.com
Chengyao Li	cyli2014@sjtu.edu.cn

- **Adversary Members**

Qingrong Chen	chenqingrong@sjtu.edu.cn
Ruisheng Cao	211314@sjtu.edu.cn
Shiquan Zhang	zsq007@sjtu.edu.cn
Haochen Huang	hhc98598@189.cn

- **Integrators**

Feiyang Qiu	st.yeah@gmail.com
Lingkun Kong	klk316980786@sjtu.edu.cn
Lanqing Liu	sunnysunny@sjtu.edu.cn
Jialu Li	790359064@qq.com

- **Where to find our project?**

https://github.com/initc3/sleepysim	SleepySim

Table of Contents

1 Introduction

Consensus protocols are at the core of distributed computing and also provide a foundational building protocol for multi-party cryptographic protocols. In the paper about *sleepy consensus* protocol [1], Pass and Shi propose a consensus protocol for realizing a linearly ordered log abstraction – often referred to as state machine replication or linearizability in the distributed systems literature. They name it as sleepy consensus protocol, which respects two important resiliency properties, i.e., consistency and liveness. And in sleepy consensus model, players can be either online (alert) or offline (asleep), and their online status may change at any point during the protocol.

In this paper, we build a simulator for monitoring the real-world performance of sleepy consensus protocol by constructing a framework which implements sleepy consensus protocol, as well as imitating behaviors of honest players and corrupted/adversarial players in the meanwhile. After analyzing the simulating results, **we know ... add text here**

This document is organized as follows. In Section 2, we introduce the framework of simulator. In Section 3, we present how honest players work while simulating. And in Section 4, we imitate the adversarial players' behavior and attack the sleepy consensus protocol by several algorithms. We give the analysis of simulating results in Section 5. Finally, we draw conclusions in Section 6.

2 The Framework of Simulator

In this section, we will illustrate the construction of the framework of our simulator, which includes **add text here**

2.1 Controller

The LLNCS class is an extension of the standard LaTeX "article" document class. Therefore you may use all "article" commands for the body of your contribution to prepare your manuscript. LLNCS class is invoked by replacing "article" by "llncs" in the first line of your document:

```
\documentclass{llncs}
%
\begin{document}
  <Your contribution>
\end{document}
```

2.2 Contributions Already Coded with LaTeX without the LLNCS document class

If your file is already coded with LaTeX you can easily adapt it a posteriori to the LLNCS document class.

Please refrain from using any LaTeX or TeX commands that affect the layout or formatting of your document (i.e. commands like `\textheight`, `\vspace`, `\headsep` etc.). There may nevertheless be exceptional occasions on which to use some of them.

The LLNCS document class has been carefully designed to produce the right layout from your LaTeX input. If there is anything specific you would like to do and for which the style file does not provide a command, *please contact us*. Same holds for any error and bug you discover (there is however no reward for this – sorry).

3 The Imitation of Honest Players

With mathematical formulas you may proceed as described in Sect. 3.3 of the *LaTeX User's Guide & Reference Manual* by Leslie Lamport (2nd ed. 1994), Addison-Wesley Publishing Company, Inc.

Equations are automatically numbered sequentially throughout your contribution using arabic numerals in parentheses on the right-hand side.

When you are working in math mode everything is typeset in italics. Sometimes you need to insert non-mathematical elements (e.g. words or phrases). Such insertions should be coded in roman (with `\mbox`) as illustrated in the following example:

Sample Input

```
\begin{equation}
  \left(\frac{a^{2} + b^{2}}{c^{3}} \right) = 1 \quad
  \mbox{ if } c\neq 0 \mbox{ and if } a,b,c\in \bbbr \enspace .
\end{equation}
```

Sample Output

$$\left(\frac{a^2 + b^2}{c^3}\right) = 1 \quad \text{if } c \neq 0 \text{ and if } a, b, c \in \mathbb{R} \ . \tag{1}$$

If you wish to start a new paragraph immediately after a displayed equation, insert a blank line so as to produce the required indentation. If there is no new paragraph either do not insert a blank line or code `\noindent` immediately before continuing the text.

Please punctuate a displayed equation in the same way as other ordinary text but with an `\enspace` before end punctuation.

Note that the sizes of the parentheses or other delimiter symbols used in equations should ideally match the height of the formulas being enclosed. This is automatically taken care of by the following LaTeX commands:

`\left(` or `\left[` and `\right)` or `\right]`.

3.1 lalala

a) In math mode LaTeX treats all letters as though they were mathematical or physical variables, hence they are typeset as characters of their own in italics. However, for certain components of formulas, like short texts, this would be incorrect and therefore coding in roman is required. Roman should also be used for subscripts and superscripts *in formulas* where these are merely labels and not in themselves variables, e.g. T_{eff} *not* T_{eff}, T_{K} *not* T_K (K = Kelvin), m_{e} *not* m_e (e = electron). However, do not code for roman if the sub/superscripts represent variables, e.g. $\sum_{i=1}^{n} a_i$.
b) Please ensure that *physical units* (e.g. pc, erg s^{-1} K, cm^{-3}, W m^{-2} Hz^{-1}, m kg s^{-2} A^{-2}) and *abbreviations* such as Ord, Var, GL, SL, sgn, const. are always set in roman type. To ensure this use the `\mathrm` command: `\mathrm{Hz}`. On p. 44 of the *LaTeX User's Guide & Reference Manual* by Leslie Lamport you will find the names of common mathematical functions, such as log, sin, exp, max and sup. These should be coded as `\log`, `\sin`, `\exp`, `\max`, `\sup` and will appear in roman automatically.
c) Chemical symbols and formulas should be coded for roman, e.g. Fe not Fe, $\mathrm{H_2O}$ not H_2O.
d) Familiar foreign words and phrases, e.g. et al., a priori, in situ, bremsstrahlung, eigenvalues should not be italicized.

4 The Imitation of Honest Players

ssss

5 The Analysis of Simulating Results

Here is the analysis of Simulating Results.

6 Conclusion

In conclusion....

References

1. Pass, Rafael, and Elaine Shi. *The sleepy model of consensus.* Cryptology ePrint Archive, Report 2016/918, 2016. http://eprint. iacr. org/2016/918, 2016.