Formalization of a Generalized Protocol for Clock Synchronization in Isabelle/HOL

Alwen Tiu

September 13, 2023

Abstract

We formalize the generalized Byzantine fault-tolerant clock synchronization protocol of Schneider. This protocol abstracts from particular algorithms or implementations for clock synchronization. This abstraction includes several assumptions on the behaviors of physical clocks and on general properties of concrete algorithms/implementations. Based on these assumptions the correctness of the protocol is proved by Schneider. His proof was later verified by Shankar using the theorem prover EHDM (precursor to PVS). Our formalization in Isabelle/HOL is based on Shankar’s formalization.

Contents

1 Introduction 1
2 Isar proof scripts 2
   2.1 Types and constants definitions ................................. 2
   2.2 Clock conditions .................................................. 3
      2.2.1 Some derived properties of clocks ........................... 5
      2.2.2 Bounded-drift for logical clocks (IC) ....................... 5
   2.3 Agreement property ................................................ 6

1 Introduction

In certain distributed systems, e.g., real-time process-control systems, the existence of a reliable global time source is critical in ensuring the correct functioning of the systems. This reliable global time source can be implemented using several physical clocks distributed on different nodes in the distributed system. Since physical clocks are by nature constantly drifting away from the “real time” and different clocks can have different drift rates, in such a scheme, it is important that these clocks are regularly adjusted so that they are closely synchronized within a certain application-specific safe bound. The design and verification of clock synchronization protocols are often complicated by the additional requirement that the protocols should work correctly under certain types of errors, e.g., failure of some clocks, error in communication network or corrupted messages, etc.

There has been a number of fault-tolerant clock synchronization algorithms studied in the literature, e.g., the Interactive Convergence Algorithm (ICA) by Lamport and Melliar-Smith [1], the Lundelius-Lynch algorithm [2], etc., each with its own degree of fault tolerance. One important property that
must be satisfied by a clock synchronization algorithm is the agreement property, i.e., at any time \( t \),
the difference of the clock readings of any two non-faulty processes must be bounded by a constant
(which is fixed according to the domain of applications). At the core of these algorithms is the
convergence function that calculates the adjustment to a clock of a process, based on the clock
readings of all other processes. Schneider [3] gives an abstract characterization of a wide range
of clock synchronization algorithms (based on the convergence functions used) and proves the
agreement property in this abstract framework. Schneider’s proof was later verified by Shankar [4]
in the theorem prover EHDM (precursor to PVS), where eleven axioms about clocks are explicitly
stated.

We formalize Schneider’s proof in Isabelle/HOL, making use of Shankar’s formulation of the clock
axioms. The particular formulation of axioms on clock conditions and the statements of the main
theorems here are essentially those of Shankar’s [4], with some minor changes in syntax. For the
full description of the protocol, the general structure of the proof and the meaning of the constants
and function symbols used in this formalization, we refer readers to [4].

Acknowledgment I would like to thank Stephan Merz and Pascal Fontaine for useful tips on
using Isabelle and particularly the Isar proof language.

2 Isar proof scripts

theory GenClock imports Complex-Main begin

2.1 Types and constants definitions

Process is represented by natural numbers. The type ’event’ corresponds to synchronization rounds.

type-synonym process = nat

type-synonym event = nat

type-synonym time = real

type-synonym Clocktime = real

axiomatization

\( \delta :: \text{real} \) and
\( \mu :: \text{real} \) and
\( \varrho :: \text{real} \) and
\( \text{rmin} :: \text{real} \) and
\( \text{rmax} :: \text{real} \) and
\( \beta :: \text{real} \) and
\( \Lambda :: \text{real} \) and

\( \text{np :: process} \) and
\( \text{maxfaults :: process} \) and

\( \text{PC :: [process, time] \Rightarrow Clocktime} \) and

\( \text{VC :: [process, time] \Rightarrow Clocktime} \) and

\( \text{te :: [process, event] \Rightarrow time} \) and
\[ \vartheta :: [\text{process, event}] \Rightarrow (\text{process} \Rightarrow \text{Clocktime}) \text{ and} \]

\[ \text{IC} :: [\text{process, event, time}] \Rightarrow \text{Clocktime and} \]

\[ \text{correct} :: [\text{process, time}] \Rightarrow \text{bool and} \]

\[ cfn :: [\text{process, (process} \Rightarrow \text{Clocktime)}] \Rightarrow \text{Clocktime and} \]

\[ \pi :: [\text{Clocktime, Clocktime}] \Rightarrow \text{Clocktime and} \]

\[ \alpha :: \text{Clocktime} \Rightarrow \text{Clocktime} \]

**definition**

\[ \text{count} :: [\text{process} \Rightarrow \text{bool, process}] \Rightarrow \text{nat where} \]

\[ \text{count} f n = \text{card}\{p. p < n \land f p\} \]

**definition**

\[ \text{Adj} :: [\text{process, event}] \Rightarrow \text{Clocktime where} \]

\[ \text{Adj} = (\lambda p i. \text{if} \ 0 < i \text{ then } cfn p (\vartheta p i) - PC p (\text{te} p i) \text{ else } 0) \]

**definition**

\[ \text{okRead1} :: [\text{process} \Rightarrow \text{Clocktime, Clocktime, process} \Rightarrow \text{bool}] \Rightarrow \text{bool where} \]

\[ \text{okRead1} f x \text{ ppred} \longleftrightarrow (\forall \ l \ m. \text{ ppred} l \land \text{ ppred} m \longrightarrow |f l - f m| \leq x) \]

**definition**

\[ \text{okRead2} :: [\text{process} \Rightarrow \text{Clocktime, process} \Rightarrow \text{Clocktime}, \text{Clocktime}, \text{process} \Rightarrow \text{bool}] \Rightarrow \text{bool where} \]

\[ \text{okRead2} f g x \text{ ppred} \longleftrightarrow (\forall \ p. \text{ ppred} p \longrightarrow |f p - g p| \leq x) \]

**definition**

\[ \text{rho-bound1} :: [[\text{process, time}] \Rightarrow \text{Clocktime}] \Rightarrow \text{bool where} \]

\[ \text{rho-bound1} C \longleftrightarrow (\forall \ p \ s \ t. \text{ correct } p \ t \land s \leq t \longrightarrow C p t - C p s \leq (t - s) \ast (1 + \vartheta)) \]

**definition**

\[ \text{rho-bound2} :: [[\text{process, time}] \Rightarrow \text{Clocktime}] \Rightarrow \text{bool where} \]

\[ \text{rho-bound2} C \longleftrightarrow (\forall \ p \ s \ t. \text{ correct } p \ t \land s \leq t \longrightarrow (t - s) \ast (1 - \vartheta) \leq C p t - C p s) \]

### 2.2 Clock conditions

Some general assumptions

**axiomatization where**

- **constants-ax**: \( 0 < \beta \land 0 < \mu \land 0 < \text{rmin} \)
- \( \text{rmin} \leq \text{rmax} \land 0 < \vartheta \land 0 < \np \land \text{maxfaults} \leq \np \)

**axiomatization where**

- **PC-monotone**: \( \forall \ p \ s \ t. \text{ correct } p \ t \land s \leq t \longrightarrow \text{PC } p \ s \leq \text{PC } p \ t \)

**axiomatization where**

- **VClock**: \( \forall \ p \ t \ i. \text{ correct } p \ t \land \text{te} p \ i \leq t \land t < \text{te} p (i + 1) \longrightarrow \text{VC } p \ t = \text{IC } p \ i \ t \)
axiomatization where

\[ \text{IClock: } \forall \ p \ t \ i. \ \text{correct} \ p \ t \implies \text{IC} \ p \ i \ t = PC \ p \ t + \text{Adj} \ p \ i \]

Condition 1: initial skew

axiomatization where

\[ \text{init: } \forall \ p. \ \text{correct} \ p \ 0 \implies 0 \leq PC \ p \ 0 \ \land \ PC \ p \ 0 \leq \mu \]

Condition 2: bounded drift

axiomatization where

\[ \text{rate-1: } \forall \ p \ s \ t. \ \text{correct} \ p \ t \land s \leq t \implies PC \ p \ t - PC \ p \ s \leq (t - s)*(1 + \varrho) \text{ and} \]
\[ \text{rate-2: } \forall \ p \ s \ t. \ \text{correct} \ p \ t \land s \leq t \implies (t - s)*((1 - \varrho)) \leq PC \ p \ t - PC \ p \ s \]

Condition 3: bounded interval

axiomatization where

\[ \text{rts0: } \forall \ p \ t \ i. \ \text{correct} \ p \ t \land te \ p \ (i + 1) \implies t - te \ p \ i \leq rmax \text{ and} \]
\[ \text{rts1: } \forall \ p \ t \ i. \ \text{correct} \ p \ t \land te \ p \ (i + 1) \leq t \implies rmin \leq t - te \ p \ i \]

Condition 4: bounded delay

axiomatization where

\[ \text{rts2a: } \forall \ p \ q \ t \ i. \ \text{correct} \ p \ t \land \text{correct} \ q \ t \land te \ q \ i + \beta \leq t \implies te \ p \ i \leq t \text{ and} \]
\[ \text{rts2b: } \forall \ p \ q \ i. \ \text{correct} \ p \ (te \ p \ i) \land \text{correct} \ q \ (te \ q \ i) \implies \text{abs}(te \ p \ i - te \ q \ i) \leq \beta \]

Condition 5: initial synchronization

axiomatization where

\[ \text{synch0: } \forall \ p. \ te \ p \ 0 = 0 \]

Condition 6: nonoverlap

axiomatization where

\[ \text{nonoverlap: } \beta \leq rmin \]

Condition 7: reading errors

axiomatization where

\[ \text{readerror: } \forall \ p \ q \ i. \ \text{correct} \ p \ (te \ p \ (i + 1)) \land \text{correct} \ q \ (te \ p \ (i + 1)) \implies \text{abs}(\vartheta \ p \ (i + 1) - IC \ q \ i \ (te \ p \ (i + 1))) \leq \Lambda \]

Condition 8: bounded faults

axiomatization where

\[ \text{correct-closed: } \forall \ p \ s \ t. \ s \leq t \land \text{correct} \ p \ t \implies \text{correct} \ p \ s \text{ and} \]
\[ \text{correct-count: } \forall \ t. \ np - maxfaults \leq \text{count} \ (\lambda \ p. \ \text{correct} \ p \ t) \ np \]

Condition 9: Translation invariance

axiomatization where

\[ \text{trans-inv: } \forall \ f. \ 0 \leq x \implies cfn \ p \ (\lambda \ y. \ f \ y + x) = cfn \ p \ f + x \]

Condition 10: precision enhancement

axiomatization where

\[ \forall \ ppred \ p \ q \ g \ x \ y. \ np - maxfaults \leq \text{count} \ ppred \ np \land \]
\[ \text{okRead1} f \ y \ ppred \land \text{okRead1} g \ y \ ppred \land \]
\[ \text{okRead2 } f \ g \ x \ \text{ppred} \land \text{ppred} \ p \land \text{ppred} \ q \rightarrow \text{abs}(cfn \ p \ f - cfn \ q \ g) \leq \pi \ x \ y \]

Condition 11: accuracy preservation

**axiomatization where**

\[ \forall \text{ ppred} \ p \ q \ f \ x. \ \text{okRead1 } f \ x \ \text{ppred} \land \text{np} - \text{maxfaults} \leq \text{count} \ p \ q \ p \land \text{ppred} \ p \land \text{ppred} \ q \rightarrow \text{abs}(cfn \ p \ f - f \ q) \leq \alpha \ x \]

### 2.2.1 Some derived properties of clocks

**lemma** rts0d:

**assumes** cp: correct p (te p (i+1))

**shows** te p (i+1) - te p i \leq \text{rmax}

(proof)

**lemma** rts1d:

**assumes** cp: correct p (te p (i+1))

**shows** \( \text{rmin} \leq \text{te} \ p \ (i+1) - \text{te} \ p \ i \)

(proof)

**lemma** rte:

**assumes** cp: correct p (te p (i+1))

**shows** te p i \leq \text{te} \ p \ (i+1)

(proof)

**lemma** beta-bound1:

**assumes** corr-p: correct p (te p (i+1))

and corr-q: correct q (te p (i+1))

**shows** \( \theta \leq \text{te} \ p \ (i+1) - \text{te} \ q \ i \)

(proof)

**lemma** beta-bound2:

**assumes** corr-p: correct p (te p (i+1))

and corr-q: correct q (te q i)

**shows** \( \text{te} \ p \ (i+1) - \text{te} \ q \ i \leq \text{rmax} + \beta \)

(proof)

### 2.2.2 Bounded-drift for logical clocks (IC)

**lemma** bd:

**assumes** ic: \( s \leq t \)

and rb1: \( \rho\text{-bound1 } C \)

and rb2: \( \rho\text{-bound2 } D \)

and PC-ie: \( D \ q \ t - D \ q \ s \leq C \ p \ t - C \ p \ s \)

and corr-p: correct p t

and corr-q: correct q t

**shows** \( |C \ p \ t - D \ q \ t| \leq |C \ p \ s - D \ q \ s | + 2 * g * (t - s) \)

(proof)

**lemma** bounded-drift:

**assumes** ic: \( s \leq t \)

and rb1: \( \rho\text{-bound1 } C \)
and \( rb2 \): \( \rho\text{-bound2} C \)
and \( rb3 \): \( \rho\text{-bound1} D \)
and \( rb4 \): \( \rho\text{-bound2} D \)
and \( corr-p\): correct \( pt \)
and \( corr-q\): correct \( qt \)
shows \( |C pt - D qt| \leq |C ps - D qs| + 2*\varrho*(t-s) \)

\( \langle \text{proof} \rangle \)

Drift rate of logical clocks

\textbf{lemma} \textbf{IC-rate1}:
\( \rho\text{-bound1} (\lambda pt. IC pi t) \)
\( \langle \text{proof} \rangle \)

\textbf{lemma} \textbf{IC-rate2}:
\( \rho\text{-bound2} (\lambda pt. IC pi t) \)
\( \langle \text{proof} \rangle \)

Auxiliary function \( ICf\): we introduce this to avoid some unification problem in some tactic of isabelle.

\textbf{definition} \( ICf \):: \( \text{nat} \Rightarrow (\text{process} \Rightarrow \text{time} \Rightarrow \text{Clocktime}) \) where
\[
ICf i = (\lambda pt. IC pi t)
\]

\textbf{lemma} \textbf{IC-bd}:
\textbf{assumes} \( ie\): \( s \leq t \)
and \( corr-p\): correct \( pt \)
and \( corr-q\): correct \( qt \)
shows \( |IC pi t - IC qj t| \leq |IC pi s - IC qj s| + 2*\varrho*(t-s) \)
\( \langle \text{proof} \rangle \)

\textbf{lemma} \textbf{event-bound}:
\textbf{assumes} \( ie1\): \( 0 \leq t::\text{real} \)
and \( corr-p\): correct \( pt \)
and \( corr-q\): correct \( qt \)
shows \( \exists i. t < \max (te p i) (te q i) \)
\( \langle \text{proof} \rangle \)

\textbf{2.3 Agreement property}

\textbf{definition} \( \gamma_1 x = \pi (2*\varrho*\beta + 2*\Lambda) (2*\Lambda + x + 2*\varrho*(rmax + \beta)) \)
\textbf{definition} \( \gamma_2 x = x + 2*\varrho*rmax \)
\textbf{definition} \( \gamma_3 x = \alpha (2*\Lambda + x + 2*\varrho*(rmax + \beta)) + \Lambda + 2*\varrho*\beta \)

\textbf{definition} \( okmaxsync :: [nat, \text{Clocktime}] \Rightarrow \text{bool} \) where
\[
okmaxsync i x \iff (\forall p q. \text{correct } p \ (\max (te p i) \ (te q i)))
\land \text{correct } q \ (\max (te p i) \ (te q i)) \quad\longrightarrow\quad
|IC p i \ (\max (te p i) \ (te q i)) - IC q i \ (\max (te p i) \ (te q i))| \leq x
\]

\textbf{definition} \( okClocks :: [\text{process}, \text{process}, \text{nat}] \Rightarrow \text{bool} \) where
\[
okClocks p q i \iff (\forall t. 0 \leq t \land t < \max (te p i) \ (te q i))
\land \text{correct } p t \land \text{correct } q t
\quad\longrightarrow\quad |VC p t - VC q t| \leq \delta
\]

6
lemma okClocks-sym:
assumes ok-pq: okClocks p q i
shows okClocks q p i
⟨proof⟩

lemma ICp-Suc:
assumes corr-p: correct p (te p (i+1))
shows IC p (i+1) (te p (i+1)) = cfn p (ϑ p (i+1))
⟨proof⟩

lemma IC-trans-inv:
assumes ie1: te q (i+1) ≤ te p (i+1)
and corr-p: correct p (te p (i+1))
and corr-q: correct q (te p (i+1))
shows IC q (i+1) (te p (i+1)) =
cfn q (λ n. ϑ q (i+1) n + (PC q (te p (i+1)) − PC q (te q (i+1))))
is ?T1 = ?T2
⟨proof⟩

lemma beta-rho:
assumes ie: te q (i+1) ≤ te p (i+1)
and corr-p: correct p (te p (i+1))
and corr-q: correct q (te p (i+1))
and corr-l: correct l (te p (i+1))
shows |ϑ q (i+1) l + (PC q (te p (i+1)) − PC q (te q (i+1))) −
ϑ p (i+1) | ≤ 2*ϱ*β + 2*Λ
⟨proof⟩

This lemma (and the next one pe-cond2) proves an assumption used in the precision enhancement.

lemma pe-cond1:
assumes ic: te q (i+1) ≤ te p (i+1)
and corr-p: correct p (te p (i+1))
and corr-q: correct q (te p (i+1))
and corr-l: correct l (te p (i+1))
shows |ϑ q (i+1) l + (PC q (te p (i+1)) − PC q (te q (i+1))) −
ϑ p (i+1) l| ≤ 2*ϱ*β + 2*Λ
⟨proof⟩

lemma pe-cond2:
assumes ic: te m i ≤ te l i
and corr-k: correct k (te k (i+1))
and corr-l-ik: correct l (te k (i+1))
and corr-m-ik: correct m (te k (i+1))
and ind-hyp: |IC l i (te l i) − IC m i (te l i)| ≤ δS
shows |ϑ k (i+1) l − ϑ k (i+1) m| ≤ 2*Λ + δS + 2*ϱ*(rmax + β)
⟨proof⟩

lemma theta-bound:
assumes corr-l: correct l (te p (i+1))
and corr-m: correct m (te p (i+1))
and corr-p: correct p (te p (i+1))
and IC-bound:
\[
|IC\ l\ i\ (\max\ (te\ l\ i)\ (te\ m\ i)) - IC\ m\ i\ (\max\ (te\ l\ i)\ (te\ m\ i))| \leq \delta S
\]
shows \(|\vartheta\ p\ (i+1)\ l - \vartheta\ p\ (i+1)\ m| \leq 2*\Lambda + \delta S + 2*\varrho*(r_{\text{max}} + \beta)\)
(proof)

lemma four-one-ind-half:
assumes ie1: \(\beta \leq r_{\text{min}}\)
and ie2: \(\mu \leq \delta S\)
and ie3: \(\gamma_1 \delta S \leq \delta S\)
and ind-hyp: okmaxsync i \(\delta S\)
and corr-p: correct p (te p (i+1))
and corr-q: correct q (te p (i+1))
shows \(|IC\ p\ (i+1)\ (te\ p\ (i+1)) - IC\ q\ (i+1)\ (te\ p\ (i+1))| \leq \delta S\)
(proof)

Theorem 4.1 in Shankar’s paper.

theorem four-one:
assumes ie1: \(\beta \leq r_{\text{min}}\)
and ie2: \(\mu \leq \delta S\)
and ie3: \(\gamma_1 \delta S \leq \delta S\)
shows okmaxsync i \(\delta S\)
(proof)

lemma VC-cfn:
assumes corr-p: correct p (te p (i+1))
and ie: te p (i+1) < te p (i+2)
shows VC p (te p (i+1)) = cfn p (\vartheta p (i+1))
(proof)

Lemma for the inductive case in Theorem 4.2

lemma four-two-ind:
assumes ie1: \(\beta \leq r_{\text{min}}\)
and ie2: \(\mu \leq \delta S\)
and ie3: \(\gamma_1 \delta S \leq \delta S\)
and ie4: \(\gamma_2 \delta S \leq \delta\)
and ie5: \(\gamma_3 \delta S \leq \delta\)
and ie6: te q (i+1) \leq te p (i+1)
and ind-hyp: okClocks p q i
and t-bound1: 0 \leq t
and t-bound2: t < \max\ (te\ p\ (i+1))\ (te\ q\ (i+1))
and t-bound3: \max\ (te\ p\ i)\ (te\ q\ i) \leq t
and t-bound4: \max\ (te\ p\ i)\ (te\ q\ i) < \max\ (te\ p\ (i+1))\ (te\ q\ (i+1))
and corr-p: correct p t
and corr-q: correct q t
shows |VC p t - VC q t| \leq \delta
(proof)

Theorem 4.2 in Shankar’s paper.

theorem four-two:
assumes ie1: \(\beta \leq r_{\text{min}}\)
and $ie2: \mu \leq \delta S$
and $ie3: \gamma_1 \delta S \leq \delta S$
and $ie4: \gamma_2 \delta S \leq \delta$
and $ie5: \gamma_3 \delta S \leq \delta$
shows $\text{okClocks } p \ q \ i$

(\textit{proof})

The main theorem: all correct clocks are synchronized within the bound $\delta$.

\textbf{theorem} \textit{agreement}:
\textbf{assumes $ie1: \beta \leq r_{min}$}
and $ie2: \mu \leq \delta S$
and $ie3: \gamma_1 \delta S \leq \delta S$
and $ie4: \gamma_2 \delta S \leq \delta$
and $ie5: \gamma_3 \delta S \leq \delta$
and $ie6: 0 \leq t$
and $cpq: \text{correct } p \ t \land \text{correct } q \ t$
shows $|\text{VC } p \ t - \text{VC } q \ t| \leq \delta$

(\textit{proof})

end

References


