Modelling And Analysis Of IEEE 1588 Precision Time Protocol

TerraSwarm

http://terraswarm.org/

Ankush Desai, David Broman, John Eidson and Sanjit Seshia, UC Berkeley

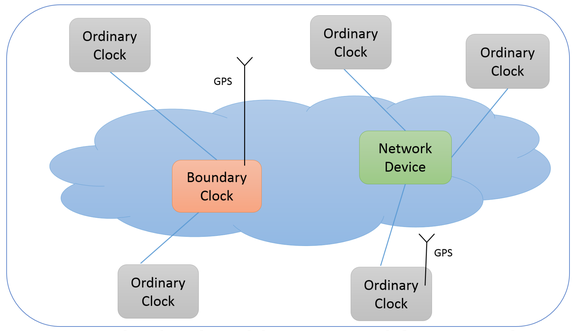
November 5, 2013

Motivation

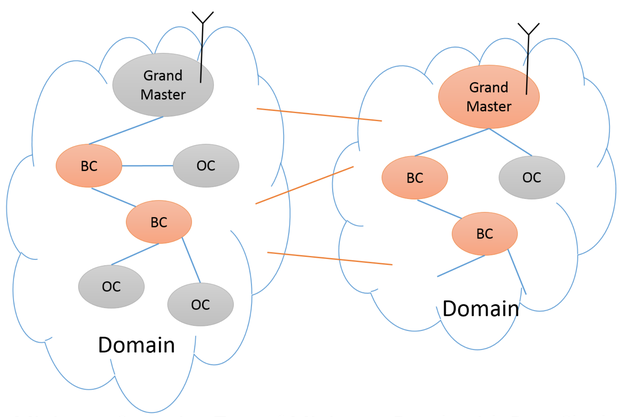
- Extending the state-of-the-art in verification of *distributed protocols*, with a special focus on protocols *for time synchronization* which is fundamental to TerraSwarm systems.
- IEEE 1588 is now adopted across domains, like industrial automation, telecommunication, etc.

IEEE 1588

- Distributed, autonomous and fault tolerant protocol.



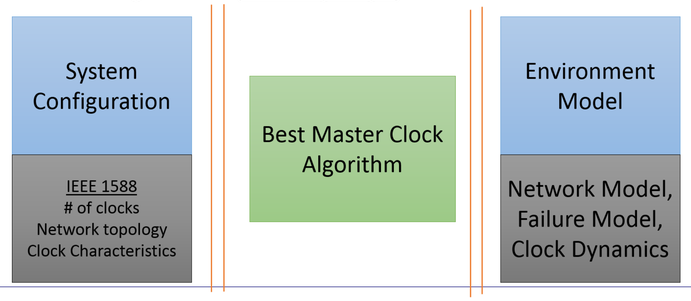
- Best Master Clock Algorithm : Used for Creating Master-Slave Synchronization Hierarchy



Minimum Spanning Tree of Minimum Depth with Best Clock as Root

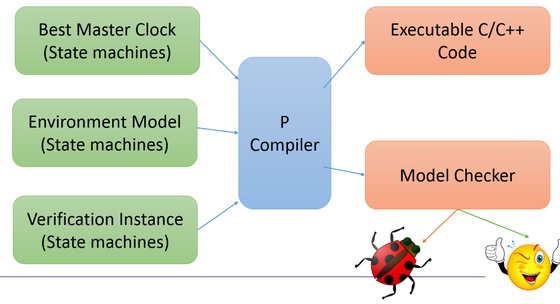
Modelling

- Use Interacting state machine based language for modeling the BMC algorithm (P Language).



Model Based Design

- Model Based Design with Correct by Construction Code.



Verification

- Verification Instance = $< C, Rank, GM, NT, Cut >$
  $C : Set\ of\ Clocks, Rank : C \to \mathbb{N}, GM : C \to C, NT : C \to 2^C, Cut \subseteq 2^{c\ x\ c}$
- Convergence property

  Eventually a unique minimum spanning tree is selected

  $FG(\forall_i\ ParentGM_i = GM(c_i)) \wedge FG(resultingCut = Cut)$
- Weak Safety Property (For finding bugs faster)

  Always there is a unique master in a domain

  $MetaStable\ State \equiv (|Domains| = |range\ of\ GM|)$

  $G(MetaStableState \to \forall_i ParentGM_i \in range\ of(GM))$

Bounded Model Checking with External Scheduler

- Distributed Protocol Models have Large State Space
- Used Bounded Asynchrony with correct mapping from Real-Time to Logical Time.
- Used Zing – Explicit State Model Checker for systematic exploration

Results

- Modelled various topologies (linear, star, ring) with 5 clocks.

Topology	No. Of States	With Bounded Asynchrony	Safety Property
	1.65 E 11	7.8 E 6	
	2.45 E 12	2.3 E 7	
	2.33 E 14	6.2 E 8	

- The test cases for various configurations can be generated automatically

Future Work

- Check the convergence property.
- Use other verification techniques like symbolic model checker (Inductive Invariant) to check BMC.
- Fully Verify or Find crucial bugs in IEEE 1588 !!!

Sponsored by the TerraSwarm Research Center, one of six centers administered by the STARnet phase of the Focus Center Research Program (FCRP) a Semiconductor Research Corporation program sponsored by MARCO and DARPA.