

Formal Verification of Ad Hoc Networks Using Alloy

Yang Yang
Chin-jung Liu
Department of CSE
Michigan State University
Fall 2009

1

Outline

- Background
- Goal
- RTS/CTS Model & Verification
- DHT Model & Verification
- Conclusion & Future Work

2


Background

- Ad hoc network
- RTS/CTS mechanism
- DHT protocol
- Real world testing vs. Formal verification

3

Ad Hoc Network

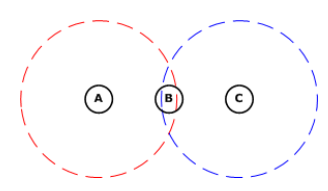
- No infrastructure
- All networking services are provided by nodes themselves
- Cooperation is essential
- Deployed quickly with minimum configuration
- Usually denote wireless ad-hoc network



4

RTS/CTS

- In wireless networks, transmission collision might be introduced by hidden terminal problem.

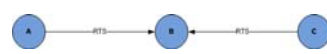


5

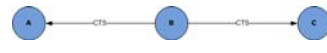
RTS/CTS (cont.)

- RTS: Request-to-Send
- CTS: Clear-to-Send


Step 1



Step 2



Step 3



6

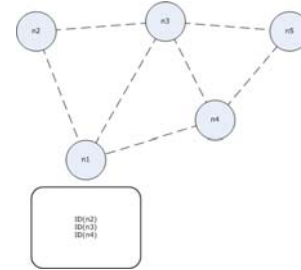
DHT

- **Decentralized** nature of ad hoc network make it suitable for supporting peer-to-peer (P2P) application protocols.
- **Distributed Hash Table (DHT)** is commonly used for resource discovery and load balance in P2P networks.



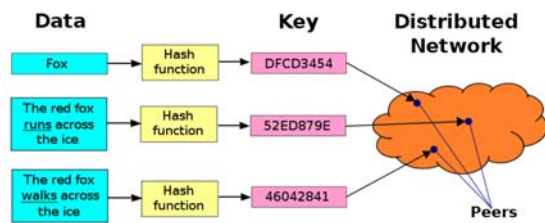
7

DHT (cont.)



8

DHT (cont.)



9

From www.linux-mag.com/id/7399/2/

Real world testing vs. Formal verification

Real world testing

- Require implementation of algorithms and lots of scenario tests.
- Usually difficult to detect boundary cases and potential errors.

VS

Formal verification

- Directly analyze models rather than practical implementation.
- Generate mathematical proof of the correctness of models.

10

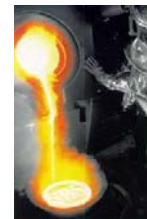
Outline

- Background
- **Goal**
- RTS/CTS Model & Verification
- DHT Model & Verification
- Conclusion & Future Work

11

Goal

- Use Alloy to verify RTS/CTS mechanism and DHT protocol on ad hoc networks.



12

Outline

- Background
- Goal
- **RTS/CTS Model & Verification**
- DHT Model & Verification
- Conclusion & Future Work

13

RTS/CTS Model & Verification

- Scenario
 - A network with multiple senders and one receiver
 - At a time state, one or more senders send RTS message to the receiver
 - The receiver only sends CTS message to the sender which is permitted to transmit
- Visualization

14

RTS/CTS Model & Verification (cont.)

- Result
 - From the instance generated by Alloy, we can see that the mechanism works correctly
 - The assertion shows that there is no more than one CTS at any time state

15

Outline

- Background
- Goal
- RTS/CTS Model & Verification
- **DHT Model & Verification**
- Conclusion & Future Work

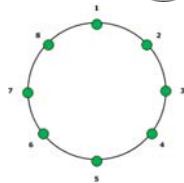
16

DHT Model & Verification

- Goal
 - Verify the correctness of the lookup routine



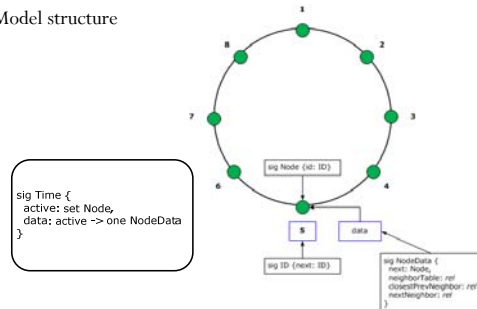
- Overlay topology
 - Simply a ring-like structure



17

DHT Model & Verification (cont.)

- Model structure



18

DHT Model & Verification (cont.)

- Visualization
 - RunNextNeighbor
 - Generate instances with correct neighbor table
 - RunNext
 - Generate instances with correct next entries but incorrect neighbor table
- Result
 - Boundary case (one node) is still correct
 - Assertion `LookupWorks` checks that if the neighbor table entries are correct, then look up routine is correct
 - Assertion `StrongLookupWorks` checks that as long as the next entries are correct, then look up routine is correct even the neighbor table is incorrect

19

Outline

- Background
- Goal
- RTS/CTS Model & Verification
- DHT Model & Verification
- **Conclusion & Future Work**

20

Conclusion & Future Work

- Conclusion
 - Using Alloy, we verified the RTS/CTS mechanism and DHT protocol worked correctly on ad hoc networks
 - Using assertions we proved that DHT is fault-tolerant
- Future Work
 - There are still lots of fields of ad hoc networks where we could apply formal verification to them.
 - Our DHT model for lookup routine could be extended to verify other routines.

21

Thank you!

22