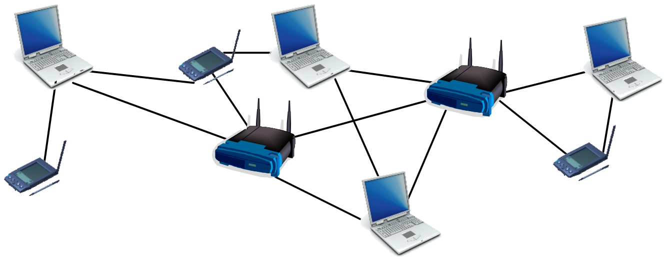
EURECOM
Sophia Antipolis

Methodology for Formal Verification of Routing Protocols for Ad Hoc Wireless Networks

D. Câmara, A. A. F. Loureiro, F. Filali

Introduction

- **Routing is a crucial task for wireless networks**
  - Having robust and correct algorithms is essential
  - Given their distributed behavior, designing such algorithms is a complex and error prone task



- **Formal Verification**
  - Is a technique to guarantee that a formal specified system has/has not an specific property

Formal Verification Approaches

- **Still not very commonly applied to routing**
  - Although, some researchers have been working on it
  - Considered hard and not worthy by many
- **Existing methods**
  - Hard to implement
  - Not general enough
    - Focus one specific case or algorithm
    - Specific topologies, number of nodes
  - Not able to handle the *dynamic* behavior of the network
    - Topology changes and mobility

Methodology

- **Intend to be a simple and general**
- **Step by step guide**
  - List of procedures that should be followed to formal verify a given algorithm
  - Most of the steps are well known and used in the field
- **Based on model checking**
  - Almost all the procedures exist to avoid the combinatorial state explosion problem

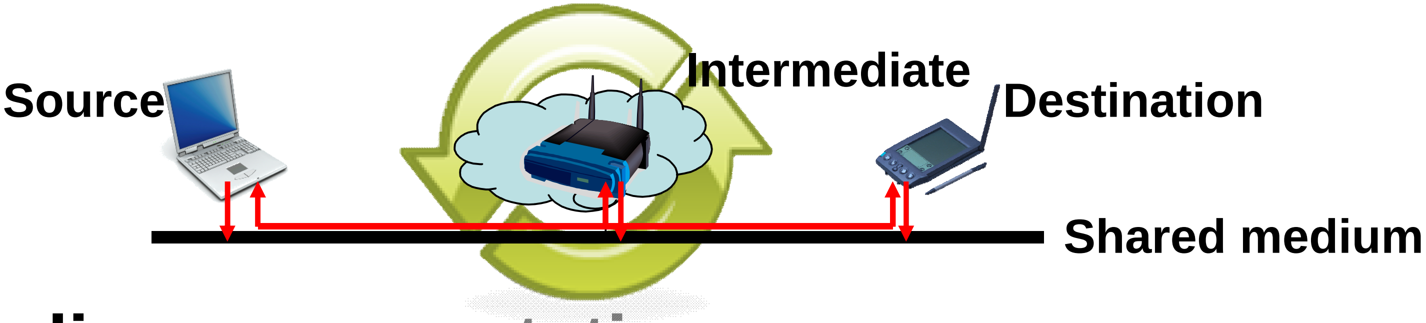
Ground Principles

- **The methodology is grounded on some basic principles**
  - ➢ Topology abstraction
  - ➢ Node position independence
  - ➢ Lower layers services trustability

Applications
Operating System
Standard SCSI Command Set
iSCSI
TCP
IP

Modeling

- Represent all possible relations
- Communicating channel
  - Common to every node in the network
- Three *kinds* of nodes to represent the network



- Flooding representation
  - Two messages can represent all existing relations in a flooding

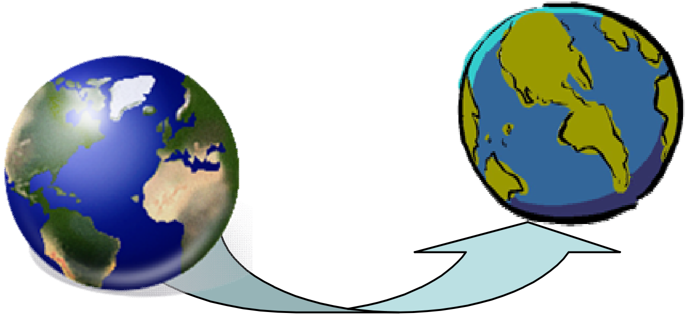
Modeling

- **Mobility**
  - The main consequence of the mobility is the occurrence of broken links, If we model all possible relations we also model mobility

- **Information modeling**
  - Model as variable, boolean if possible
  - Initialization should be random whenever possible

Modeling

- **Simplifications and abstractions**
  - As far does not compromise the protocol representation



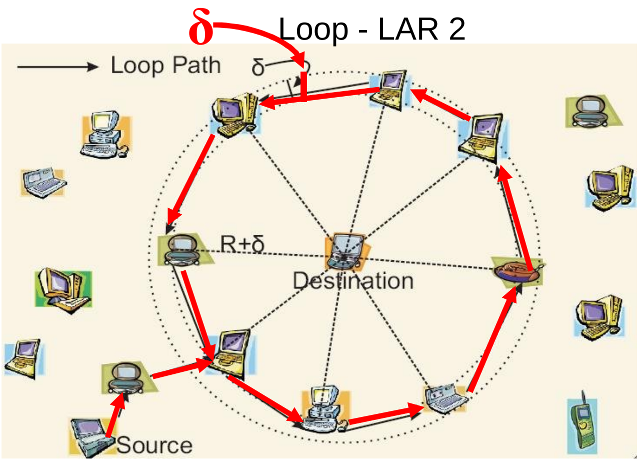
- **Analysis**
  - Every response MUST to be analyzed to guarantee it is an error in the protocol and not in the model

Methodology Applied

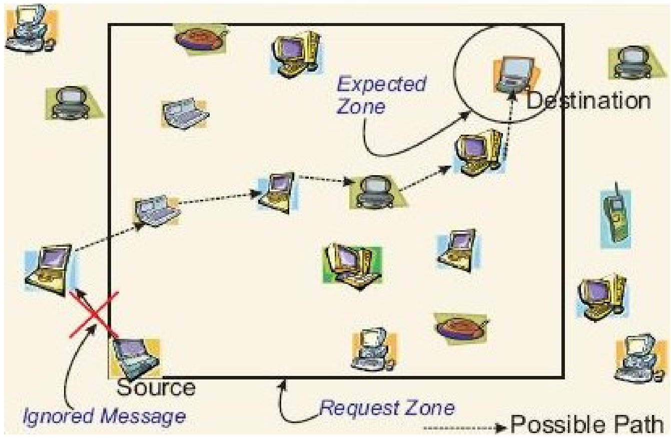
- **To validate the method three different algorithms where chosen**
  - LAR, DREAM, OLSR
  - Two geographic algorithms
  - One newer and standardized
  - We used SPIN model checker but, in principle, any tool that enables the channel implementation could be used
- **All of them present designing errors, some of these not reported before**

Methodology Applied

- **LAR 1 and 2**
  - Geographical
  - Controlled flooding
- **Failures**
  - Loop
  - Delivering message failure



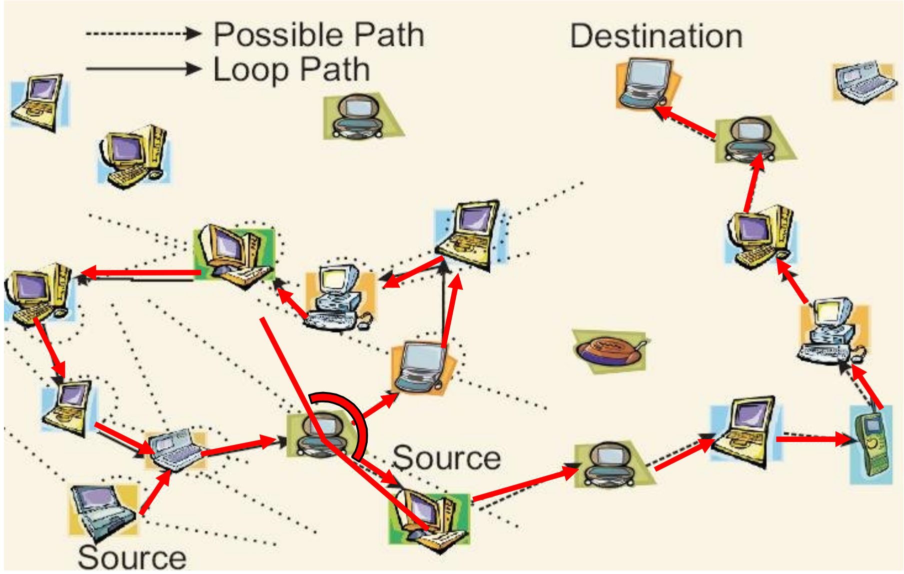
Loop - LAR 2



Delivering message failure - LAR 1

Methodology Applied

- **DREAM**
  - Geographical
  - Controlled flooding
- **Failures**
  - Loop
  - Delivering message failure



Methodology Applied

- **OLSR**
  - May fail delivering messages during routing table recalculation
  - Does not control counter overflow
  - Older information may be kept on the routing tables instead of newer ones
  - The two previous errors can also lead to routing loop, at least for a period of time
  - Control messages may be discarded and not all two hop neighbors may receive it

Conclusion

- **The method presented is simple, but effective**
  - Formal verification does not NEED to be hard to give useful results
- **Independent approach**
  - Handles mobility
  - Handles flooding
  - Independent of number of nodes
- **General verified procedures can be aggregate into a library to make the verification of newer protocols even easier**

EURECOM

Sophia Antipolis

Methodology for Formal Verification of Routing Protocols for Ad Hoc Wireless Networks

D. Câmara, A. A. F. Loureiro, F. Filali