A Flooding Protocol for MANETs with Self-Pruning and Prioritized Retransmissions

Prioritized Flooding with Self-Pruning (PFS)

Martin Jacobsson, Cheng Guo and Ignas Niemegeers
TU Delft, The Netherlands

LOCAN2005

Washington D.C., USA, November 7, 2005

Disclaimer: The work presented here was funded in part by the Commission of the European Union under the project IST MAGNET and in part by the Dutch Ministry of Economical Affairs under the Freeband PNP2008 project. This work expresses the view of the authors and not necessarily the general view of either the MAGNET nor the PNP2008 projects.

Information Society Technologies

MAGNET My personal Adaptive Global NET

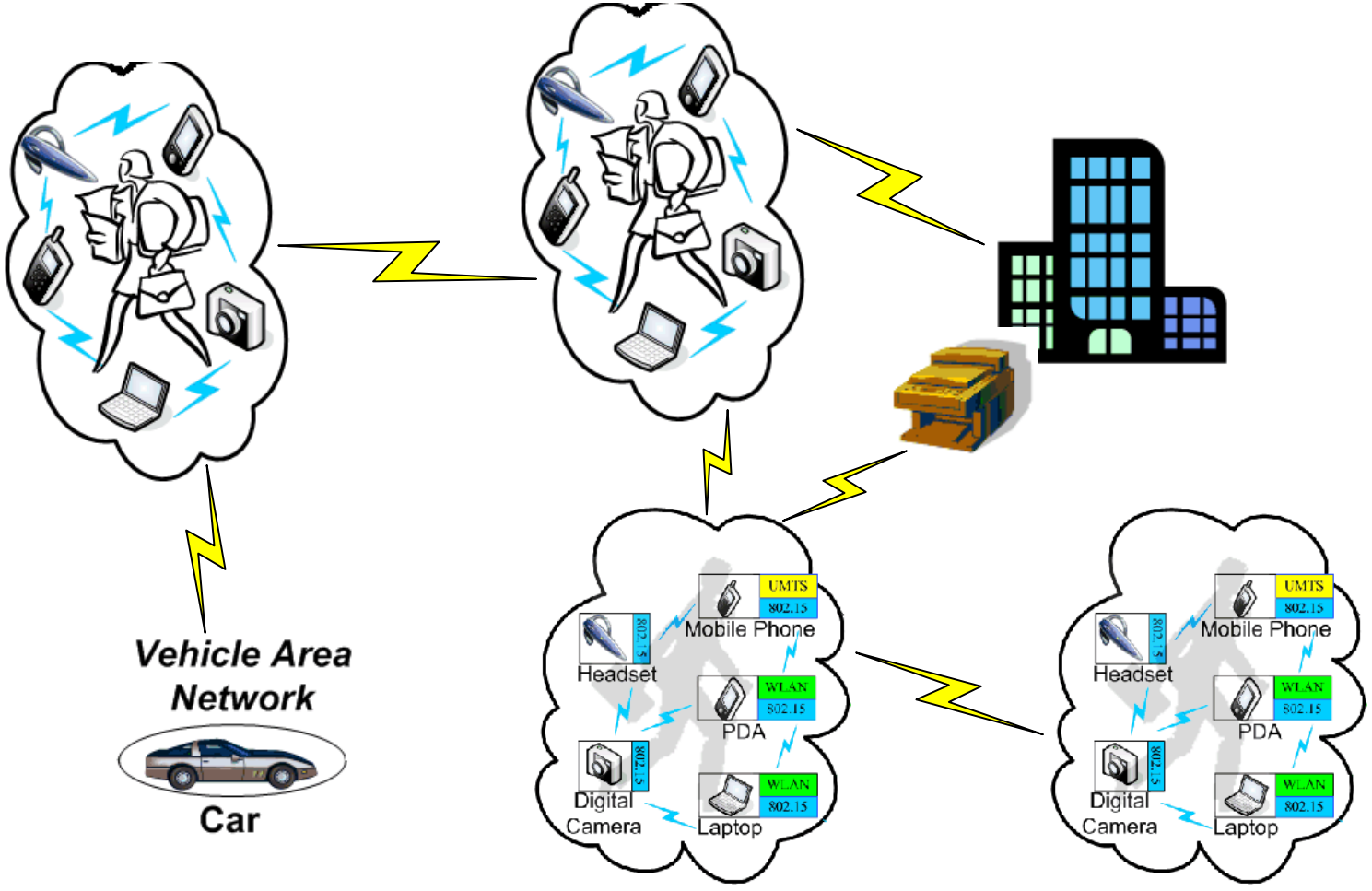
PNP2008 FREEBAND

TU Delft

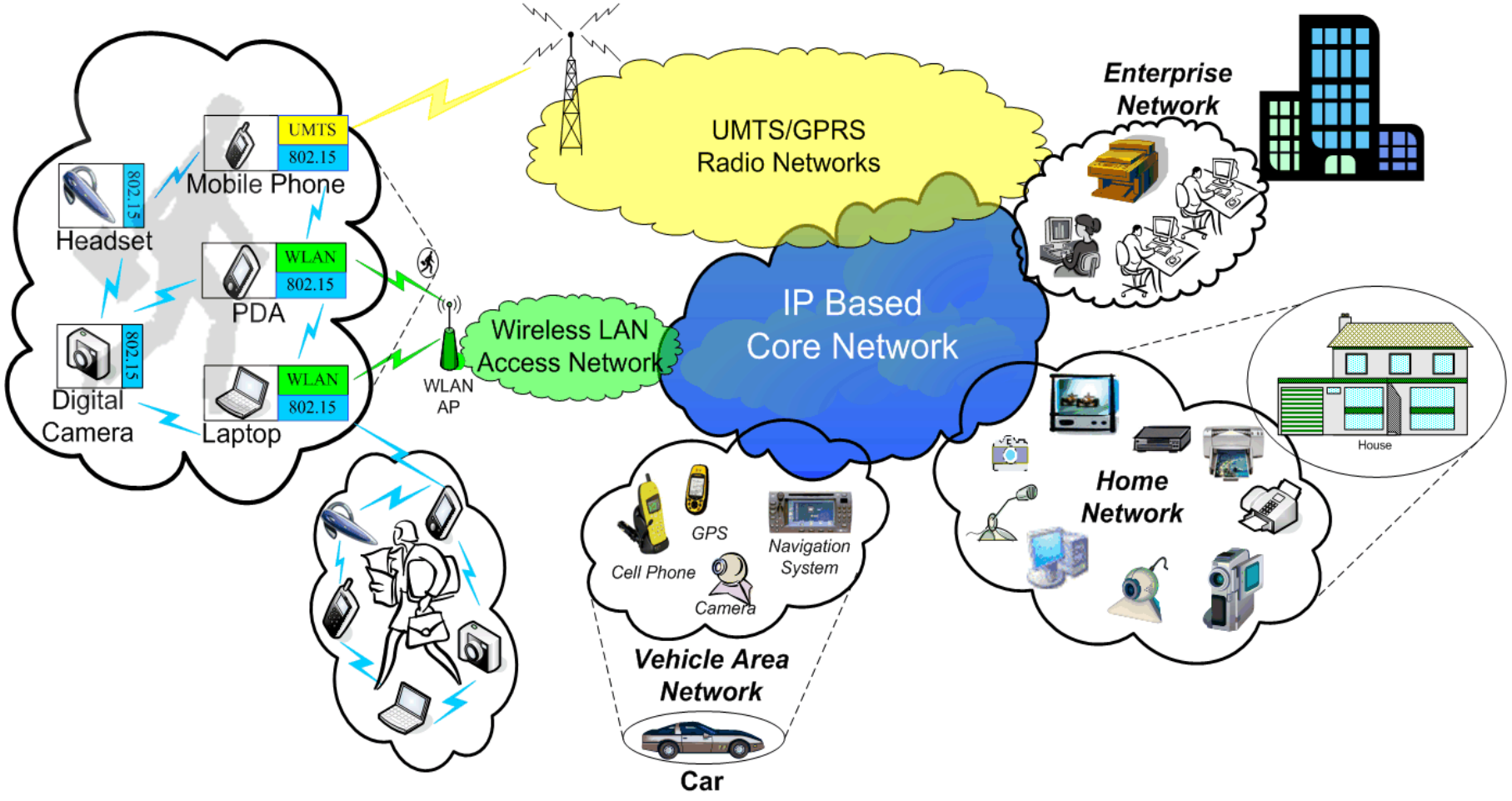
The Outline of this Presentation

- Introduction
- Motivations, objectives and assumptions
- Some existing MANET flooding protocols
- Prioritized Flooding with Self-Pruning: PFS
- Simulation set up and results
- Conclusions and future work

Mobile Ad Hoc Networks: MANETs



Personal Networks



Flooding in Mobile Ad Hoc Networks

- Flooding is a network-wide broadcasting by which a packet is disseminated to all other nodes with some nodes acting as relays.

- The most used flooding protocol in MANETs is Blind-Flooding. All nodes always retransmit each received flooding packet to all nodes in its transmission range.

- The only optimization is that each node remembers the flooding messages it received and does not retransmit them again when duplicates are received.

Motivations

- Flooding is a fundamental operation in MANETs and extensively used by routing, multi-cast tree construction, leader election, service discovery, context discovery, automatic addressing, and more...
- "AODV's routing load is dominated by route request packets (often as much as 90%)"

  Charles E. Perkins et al, "Performance Comparison of Two On Demand Routing Protocols for ad hoc networks", *IEEE INFOCOM 2000.*
- However, Blind-Flooding has problems:
  - Causes a lot of unnecessary overhead
  - Causes collisions, which leads to poor reachability
  - Causes contention, which leads to poor performance

Assumptions

- All nodes in a network share a common wireless channel.
- All nodes have the same transmission range. Bi-directional links are assumed.
- All nodes are unaware of their geographic locations, no positioning devices, such as GPS.

Some Existing Flooding Protocols

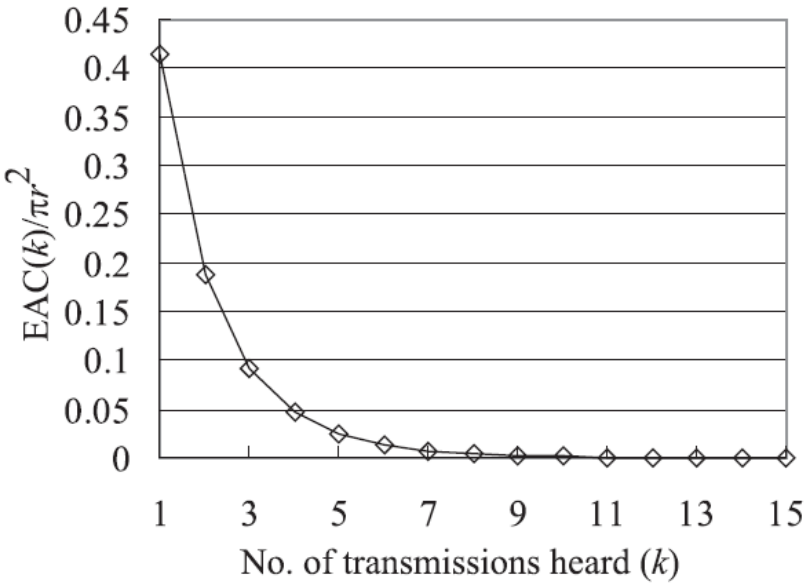
- Blind-Flooding, used in AODV and DSR
- Counter-Based Broadcasting (CBB)

Neighbor knowledge-based protocols:

- Flooding with Self-Pruning (FSP)
- Scalable Broadcasting Algorithm (SBA)
- Multi-Point Relay Flooding (MPR), used in OLSR
- Ad Hoc Broadcasting Protocol (AHBP)

Counter-Based Broadcasting (CBB) - 1

If several nodes randomly distributed around a source node send out the same flooding message, the Expected Additional Coverage, EAC(k) after the node heard the message k times is:



From: Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, Jang-Ping Sheu, The broadcast storm problem in mobile ad hoc networks, Wireless Networks, Volume 8, Issue 2/3, Pages 153-167, Kluwer Academic Publishers, May 2002.

Counter-Based Broadcasting (CBB) - 2

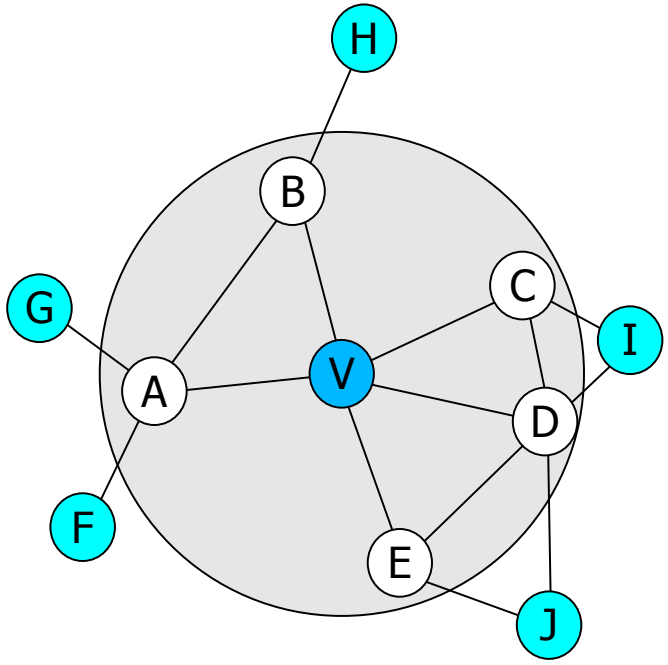
- Upon receiving a flooding message for the first time:
  - Schedules a retransmission after a Random Assessment Delay (RAD) between 0 and T_{MAX}
  - Initialize a counter k to 1
- Upon receiving a duplicate flooding message:
  - Increase k by 1
- When the RAD expires:
  - If the counter k is less than a threshold, then retransmit
  - Otherwise, cancel the retransmission
- The threshold should be around 3

Scalable Broadcasting Algorithm (SBA)

- SBA is a neighbor knowledge-based flooding protocol:
  - It collects information about its neighbors and their neighbors by using two-hop hello messages.
- SBA uses **self-pruning** to avoid unnecessary retransmissions:
  - A node monitors who else is retransmitting the same message.
  - By using the collected two-hop neighbor information it knows if all neighbors have been covered by other's retransmissions. If so, it cancels the retransmission.
- The retransmission delay (RAD) is random but influenced by the number of neighbors.

Ad Hoc Broadcasting Protocol (AHBP)

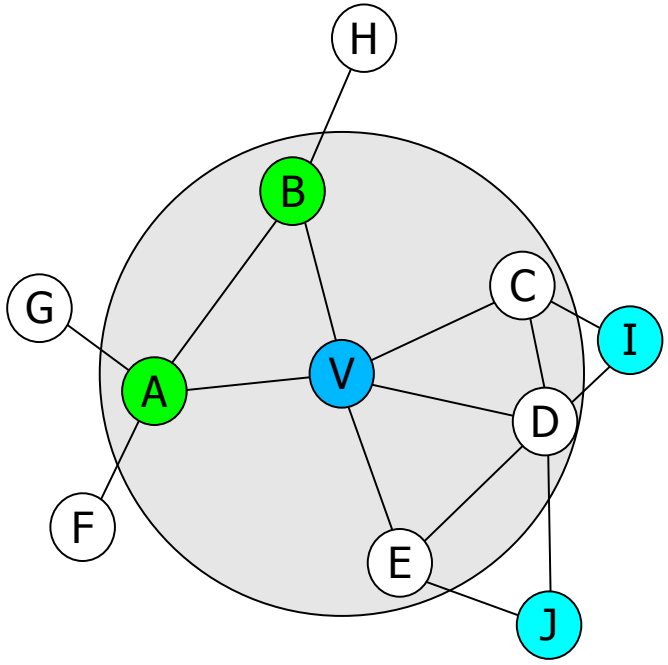
- AHBP also requires two-hop hello messages:
  - one-hop neighbor set: N(v)
  - two-hop neighbor set: $N^2(v)$
- Each node selects a set of its one-hop neighbors as BRG(v) (Broadcasting Relay Gateway) to cover all its two-hop neighbors.
- The BRG list is included in the flooding message header.



Ad Hoc Broadcasting Protocol (AHBP)

Step 1

- Add one-hop neighbor u to BRG(v), if there is a node in $N^2(v)$ only covered by u.
- Any node in $N^2(v)$ that is not covered by BRG(v) is called an uncovered node.



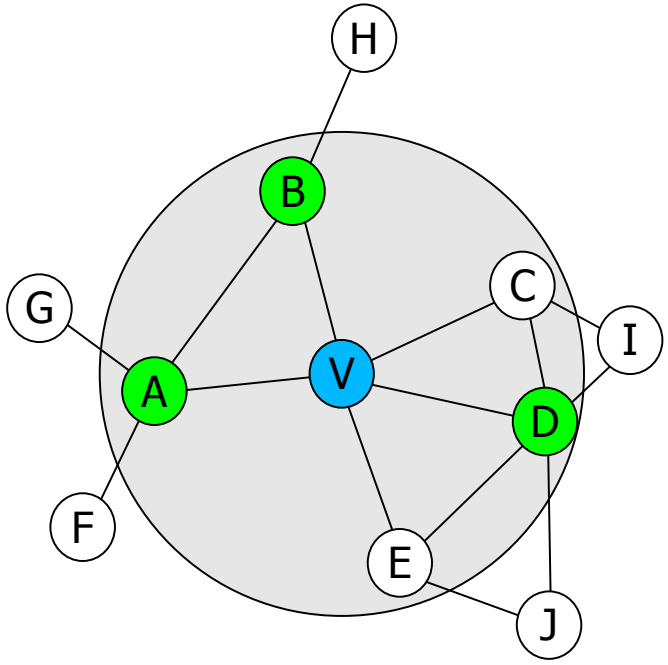
Ad Hoc Broadcasting Protocol (AHBP)

Step 2

- Add one-hop neighbor u to BRG(v), if node u covers the largest number of uncovered nodes in $N^2(v)$.

Step 3

- Repeat step 2 until there is no uncovered node in $N^2(v)$.

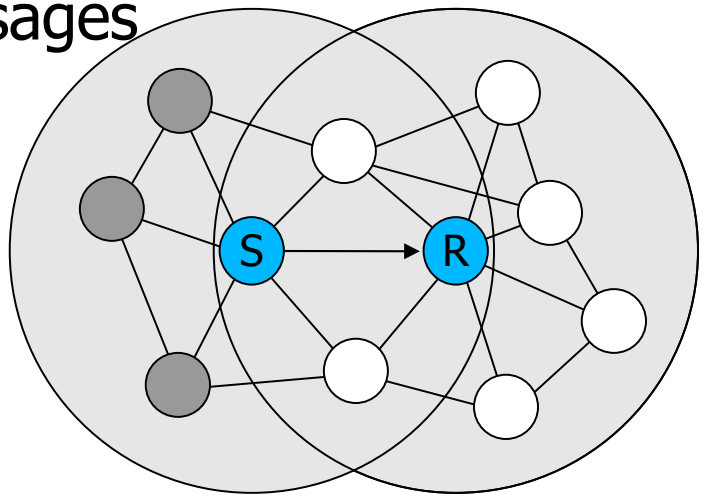


Prioritized Flooding with Self-Pruning

- Prioritized Flooding with Self-pruning (PFS) is similar to SBA.
- PFS has the following characteristics:
  - One-hop hello messages only
  - Self-pruning
  - Strict order of retransmissions based on number of uncovered neighbors
- All this will be explained shortly...

PFS Uses One-Hop Hello Messages

- PFS only requires one-hop hello messages
  - They are small
  - They may already be required by other protocols
  - Many Data Link Layer protocols provide them
- Each node encloses its one-hop neighbor list in the flooding messages

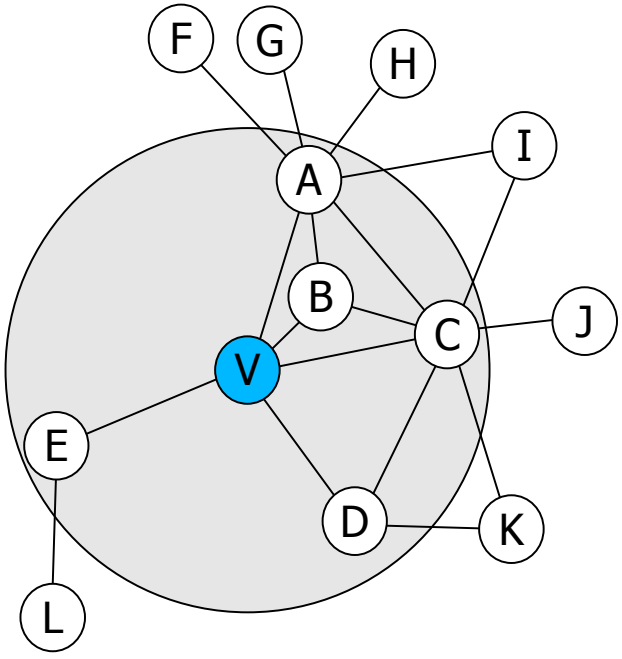


The Basic Idea Behind PFS

- Self-Pruning:
  - Upon receiving a new flooding message, the node schedules to retransmit the message after a RAD and records its neighbors covered by the sender.
  - Upon receiving duplicate flooding messages, the node also records the neighbors covered by the sender.
  - If all its one-hop neighbors are covered, it cancels the retransmission, otherwise it retransmits the message when the RAD expires.
- Priority of retransmissions:
  - Nodes with more uncovered neighbors retransmit earlier.

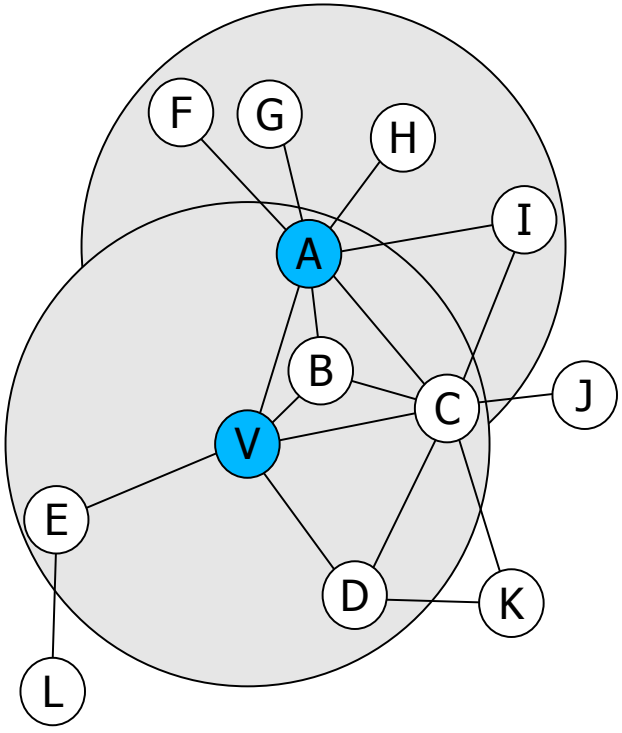
Prioritize the Retransmissions (1)

Node	Neighbours	Uncovered Neighbours	Order
V	A,B,C,D,E	-	0
A	V,B,C,F,G,H,I	F,G,H,I	1
B	V,A,C	Ø	-
C	V,A,B,D,I,J,K	I,J,K	2
D	V,C,K	K	3
E	V,L	L	3



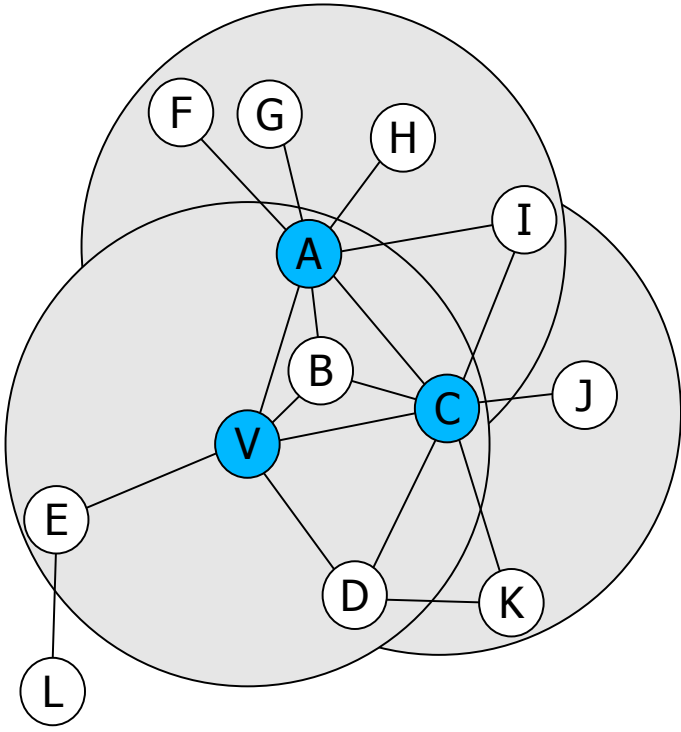
Prioritize the Retransmissions (2)

Node	Neighbours	Uncovered Neighbours	Order
V	A,B,C,D,E	-	0
A	V,B,C,F,G,H,I	Ø	1
B	V,A,C	Ø	-
C	V,A,B,D,I,J,K	J,K	2
D	V,C,K	K	3
E	V,L	L	3



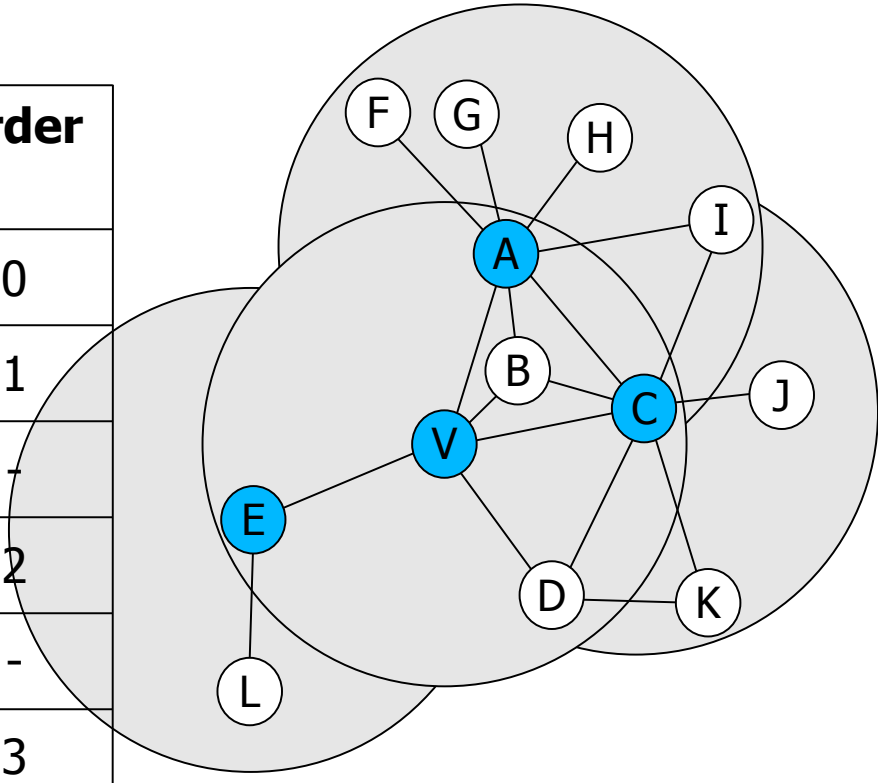
Prioritize the Retransmissions (3)

Node	Neighbours	Uncovered Neighbours	Order
V	A,B,C,D,E	-	0
A	V,B,C,F,G,H,I	Ø	1
B	V,A,C	Ø	-
C	V,A,B,D,I,J,K	Ø	2
D	V,C,K	Ø	-
E	V,L	L	3



Prioritize the Retransmissions (4)

Node	Neighbours	Uncovered Neighbours	Order
V	A,B,C,D,E	-	0
A	V,B,C,F,G,H,I	Ø	1
B	V,A,C	Ø	-
C	V,A,B,D,I,J,K	Ø	2
D	V,C,K	Ø	-
E	V,L	Ø	3



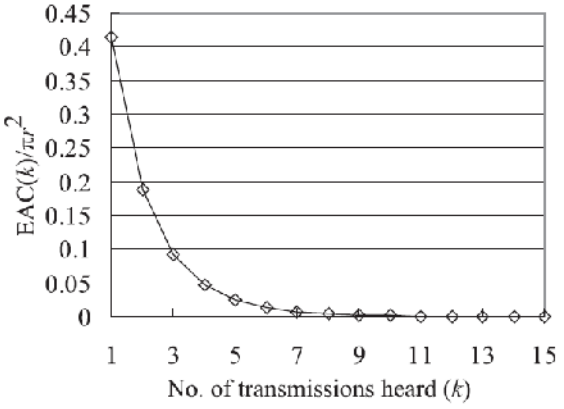
...and his process will be repeated at each receiving node.

Design of the Random Access Delay (1)

- How to determine the order?
  - The sending node does not know the "number of uncovered neighbors" of each receiving node.
  - The receiving nodes do not know the "number of uncovered neighbors" of the other receiving nodes.
- How to determine the delay?
  - The number of receiving nodes with at least one uncovered neighbor is unknown.
  - The maximum "number of uncovered neighbors" a receiving node has is unknown.
- The solution: **Estimation!**

Design of the Random Access Delay (2)

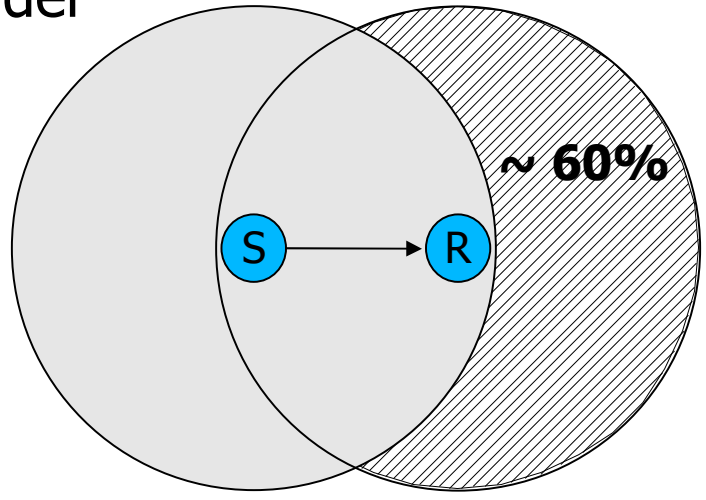
- Estimate the RAD length:
  - No more than four retransmissions are necessary (CBB result)
  - PFS will choose its retransmitting nodes in smart way => even less retransmitting nodes may be required.

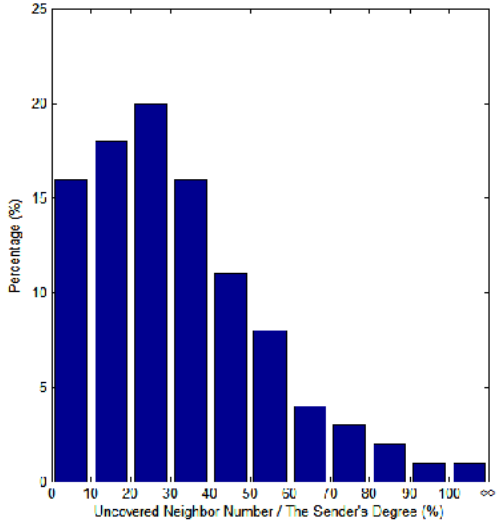


- The maximum RAD length is fixed in PFS:
  - Time needed for **5** retransmissions, including back off etc.
  - Plus some extra space for concurrent traffic
- In sparse networks, the RAD is shorter.

Design of the Random Access Delay (3)

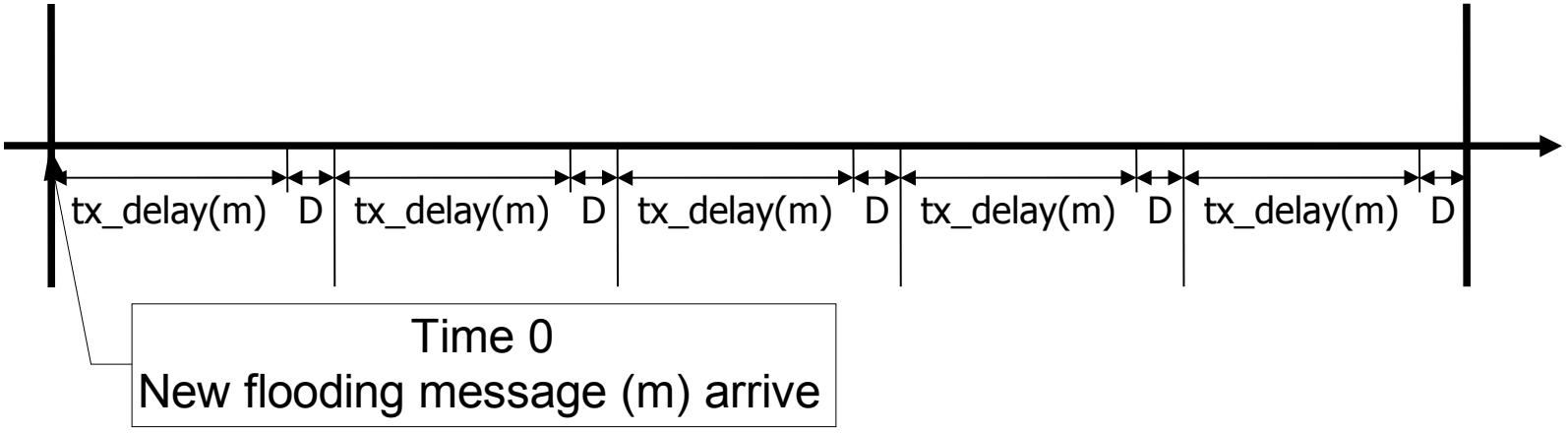
- Estimate the maximum number of uncovered neighbors
  - Assume evenly distributed nodes.
  - The (number of) neighbors of the sender is known from the flooding message.
  - The estimation is: 60% of the number of neighbors of the sender





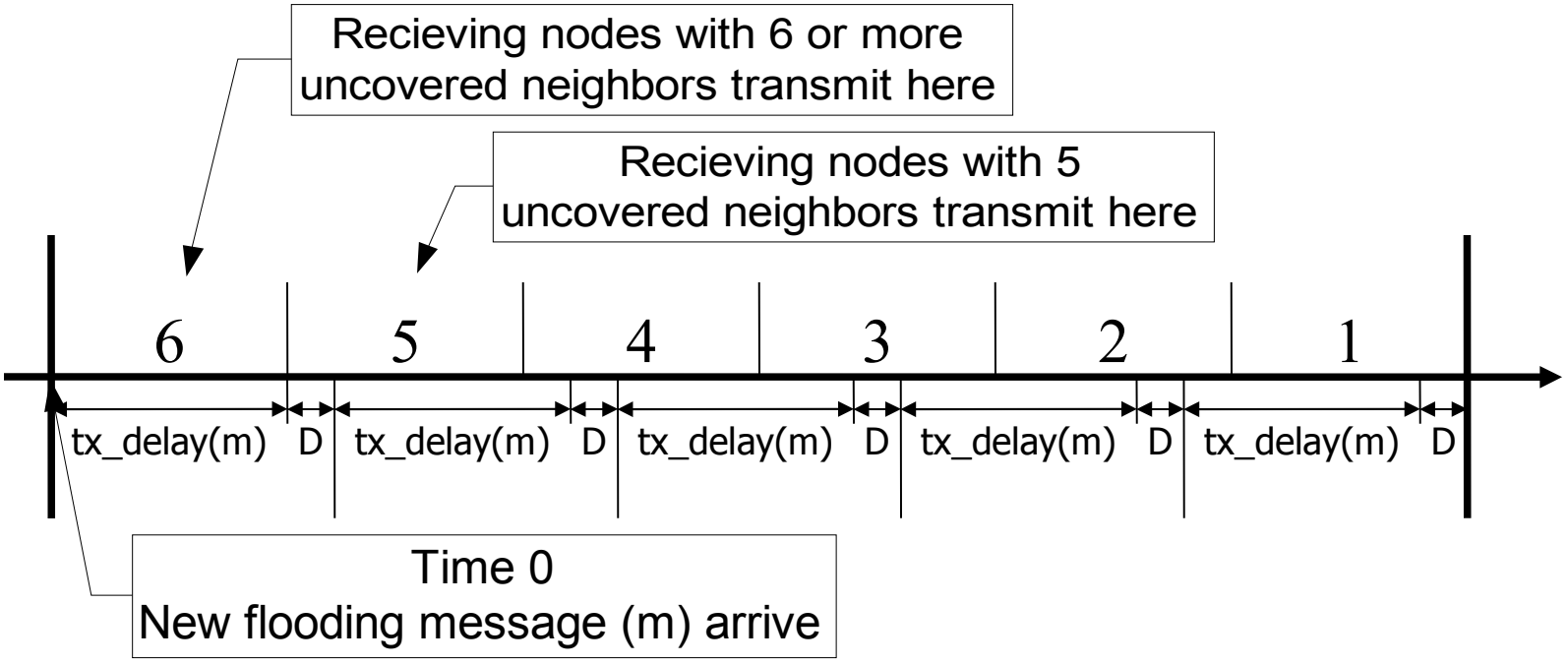
Design of the Random Access Delay (4)

- The RAD length is 5 * (tx_delay(m) + D)
  - tx_delay(m) is calculated based on message length, transmission speed, back off times, etc.
  - D is a fixed constant



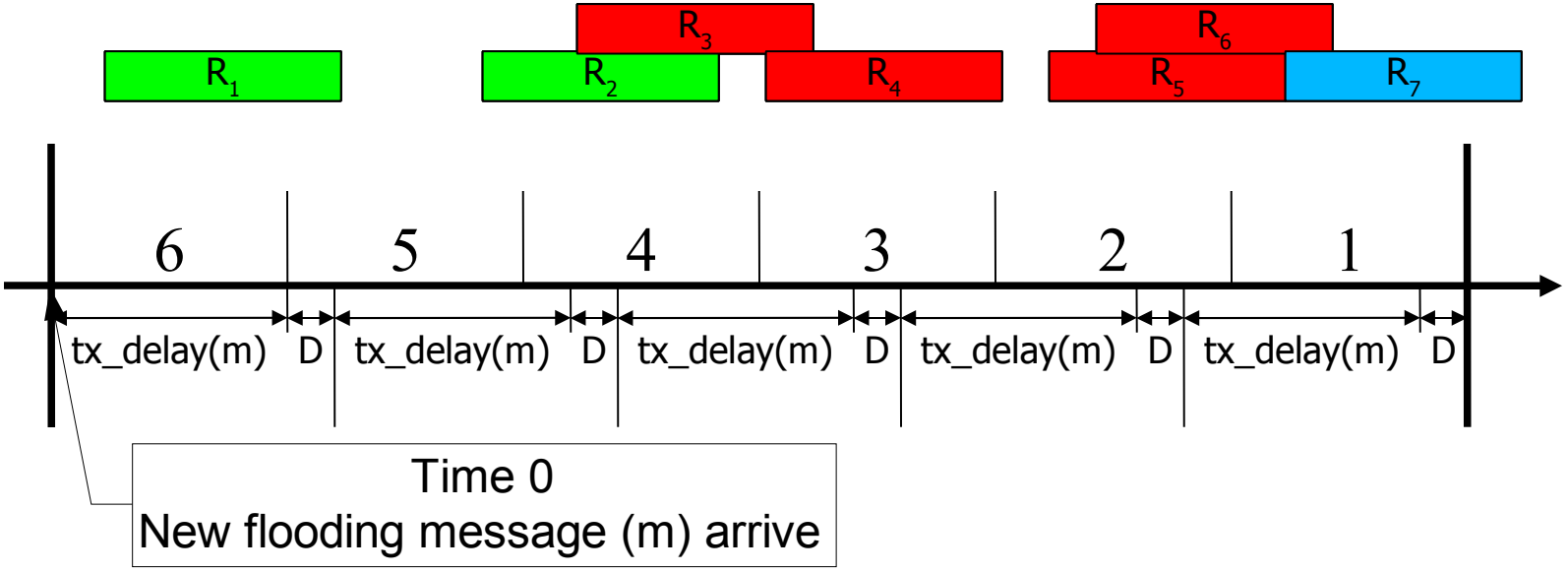
Design of the Random Access Delay (4)

- The sender has 10 neighbors
- The estimated maximum number of uncovered neighbors is therefore 6



Design of the Random Access Delay (4)

- When a node transmits, some other nodes will self-prune and cancel their retransmissions



Interface Queue Delay Problem

- A packet sent to the MAC layer may be delayed in the interface queue or waiting in MAC layer for a long time before finally being retransmitted.
- In the due time, the node may receive redundant flooding messages and self-prune. However, it is already too late!
- Solutions:
  - Increase the RAD length to minimize this effect. This introduces extra delay and the effect does not go away completely…
  - Delete the flooding messages from the interface queue and/or MAC layer with a special cross-layer function.

A Heavy Flooding Traffic Extension

- When the frequency of flooding messages increases, some neighbor lists enclosed in the flooding packet headers are frequently repeated.

- Possible solution:
  - Each node caches the neighbor lists of their neighbors from the flooding messages.
  - This cache is used to self-prune instead
  - The neighbor lists in the flooding messages is only included if there is a change in the sender's neighbor list

Simulation Parameters

Number of nodes	120 or 100 ~ 190
Simulation area	1000 m x 200 m
Transmission range	100 m
Transmission data rate	2 Mbit/s
Simulation time	100 s
Flooding message payload	64 bytes
Flooding rate	2 or 1 ~ 40 packet/s
Hello message frequency	1 packet/s
Random waypoint pause time	0 s
Maximum node speed	0 or 1 ~ 10 m/s
PFS delay parameter (D)	1.2 ms
CBB threshold	3

Measurements

1. **Reachability:**

   The percentage of how many nodes received the flooding message

2. **Number of Retransmissions:**

   The number of retransmissions required to flood a message

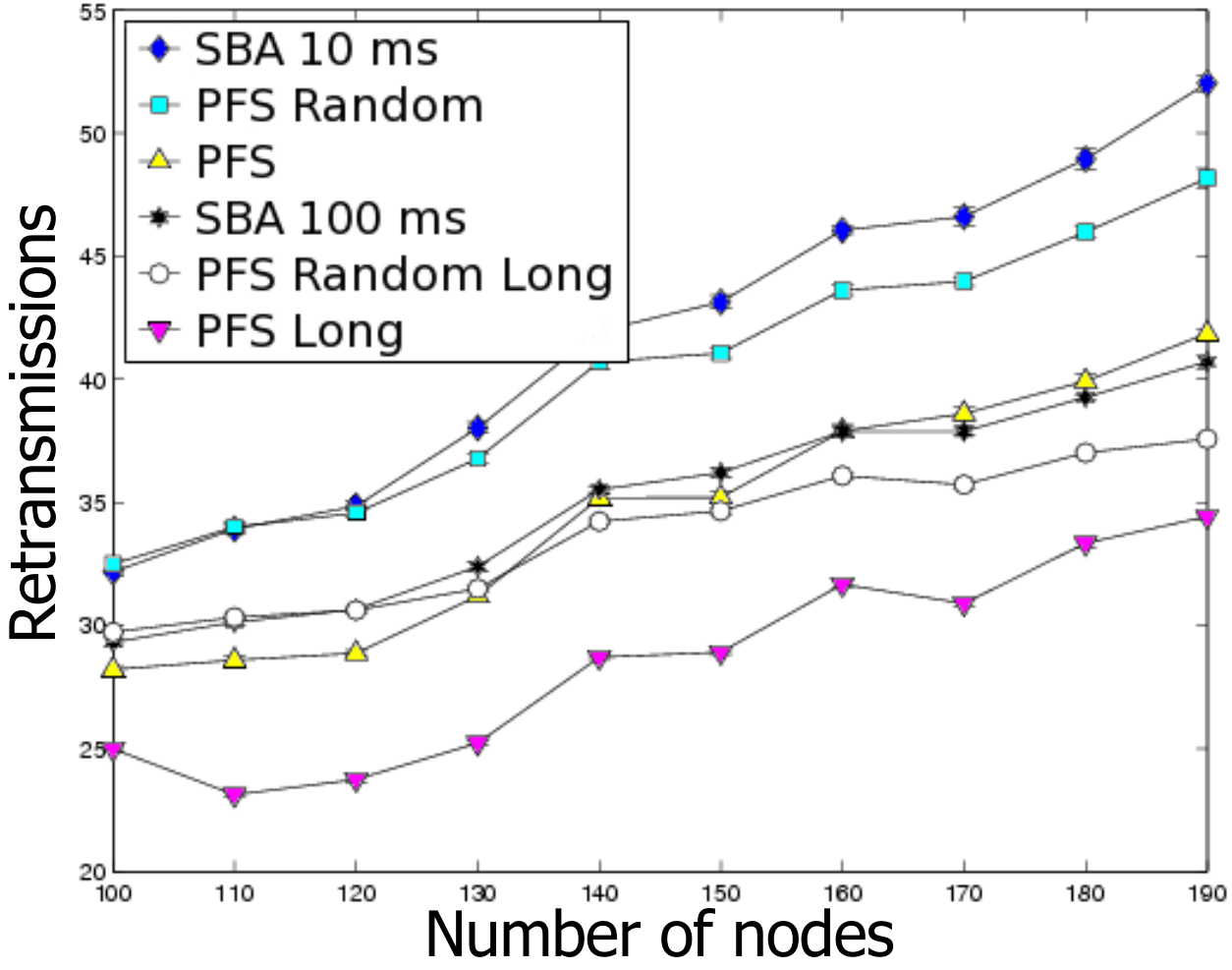
3. **Overhead:**

   How many bytes were transmitted in total to flood a message, including hello messages

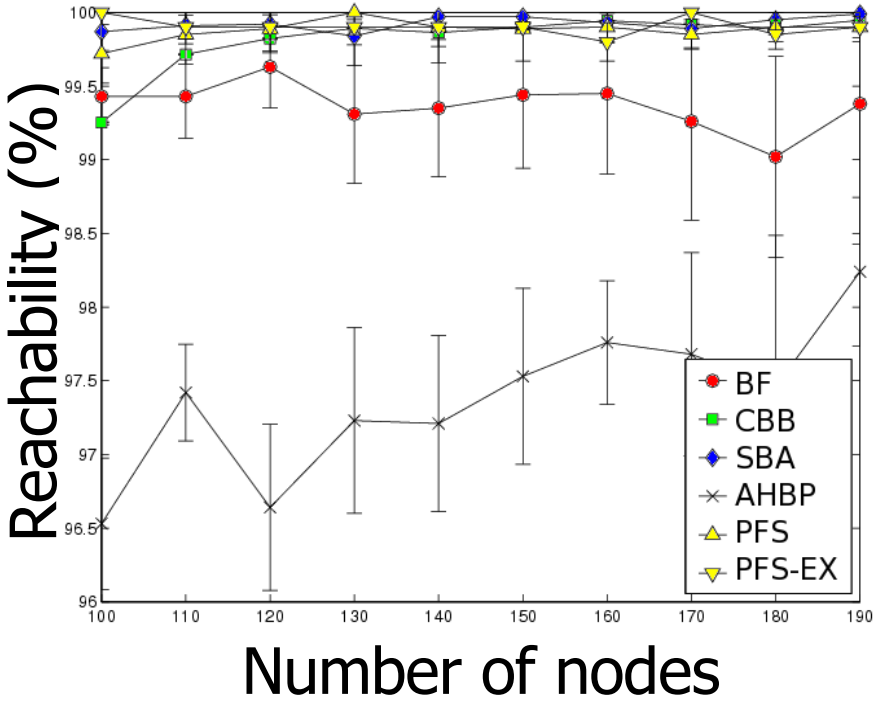
4. **End to end delay:**

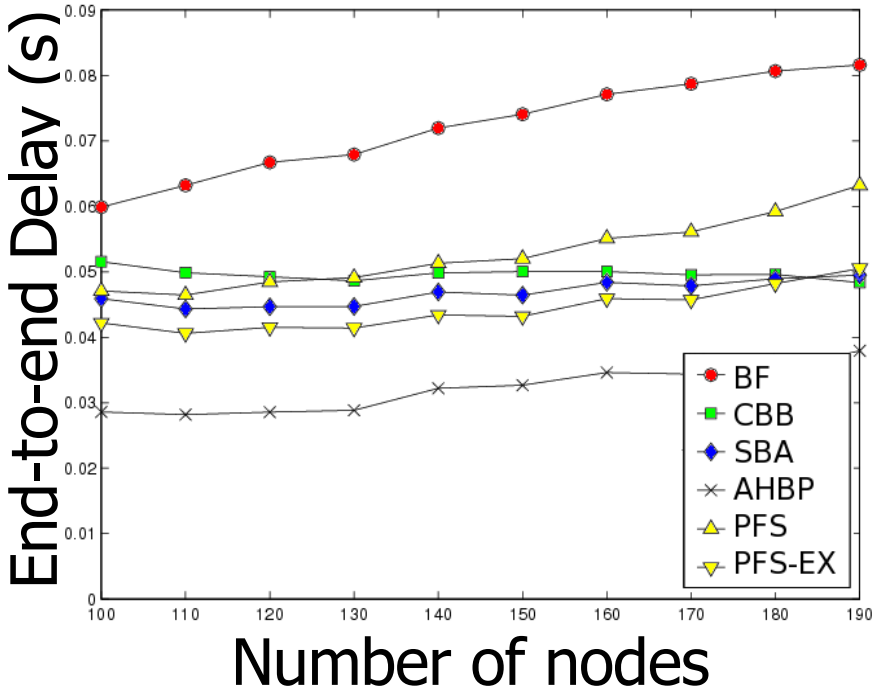
   The time interval from the moment that a flooding message is first transmitted until the moment that the last node receives the message

The Delay Factor (D)

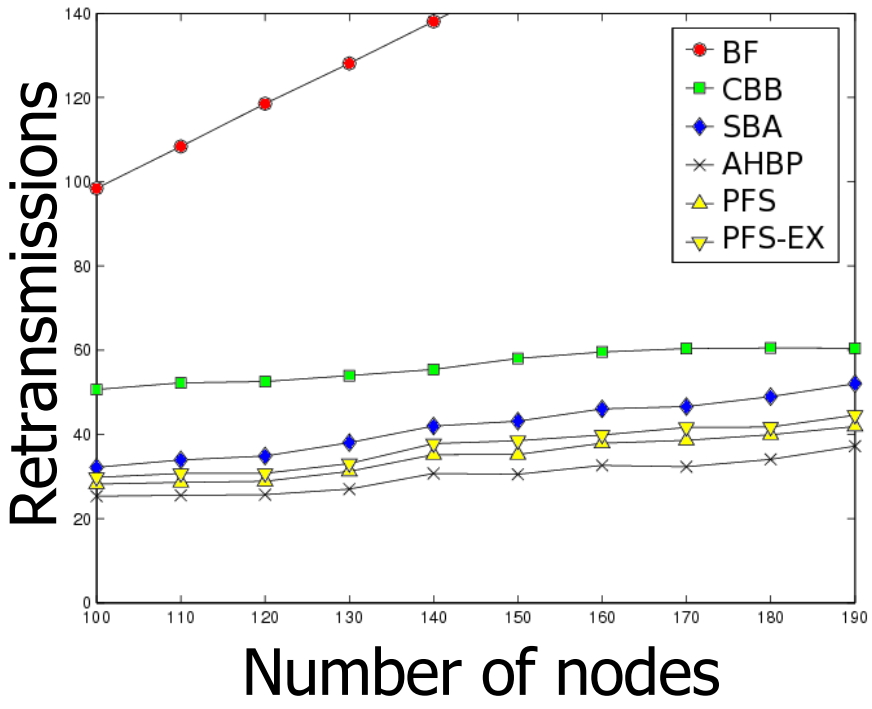


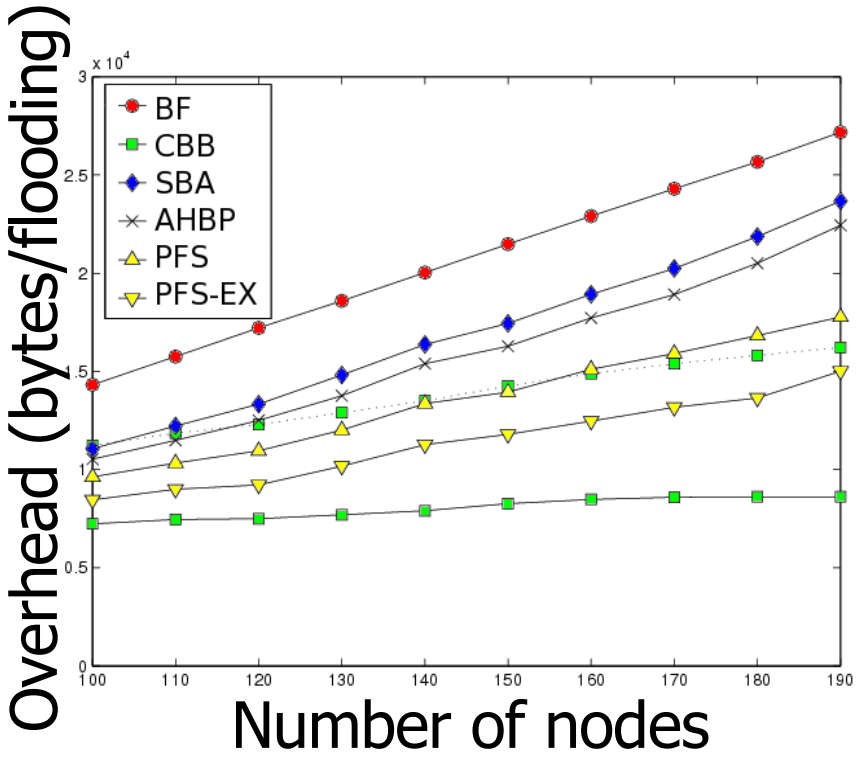
Scalability (1)





Scalability (2)





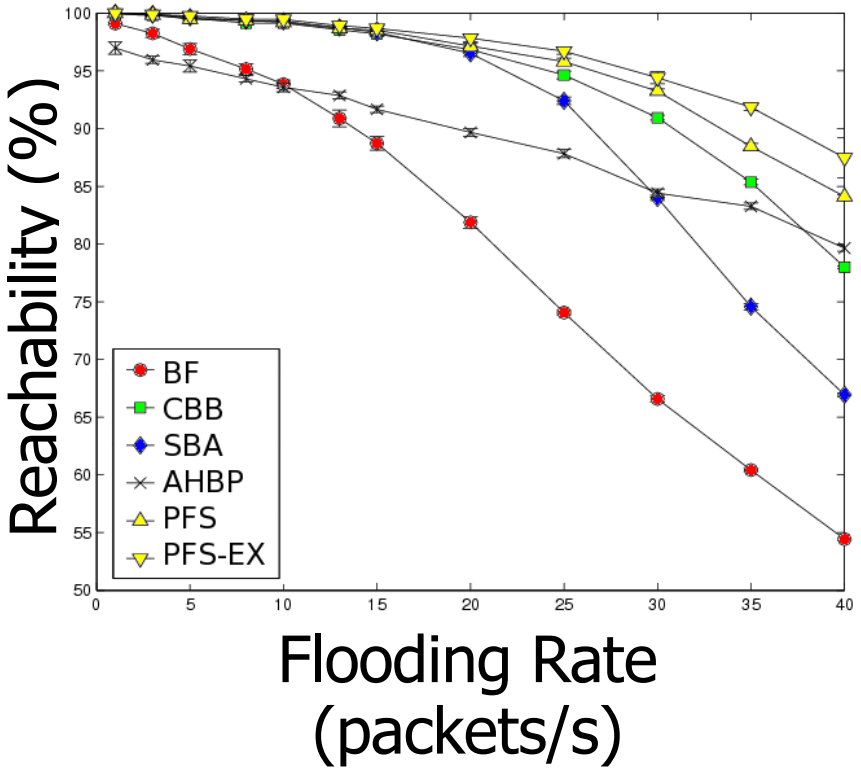
Information Society Technologies

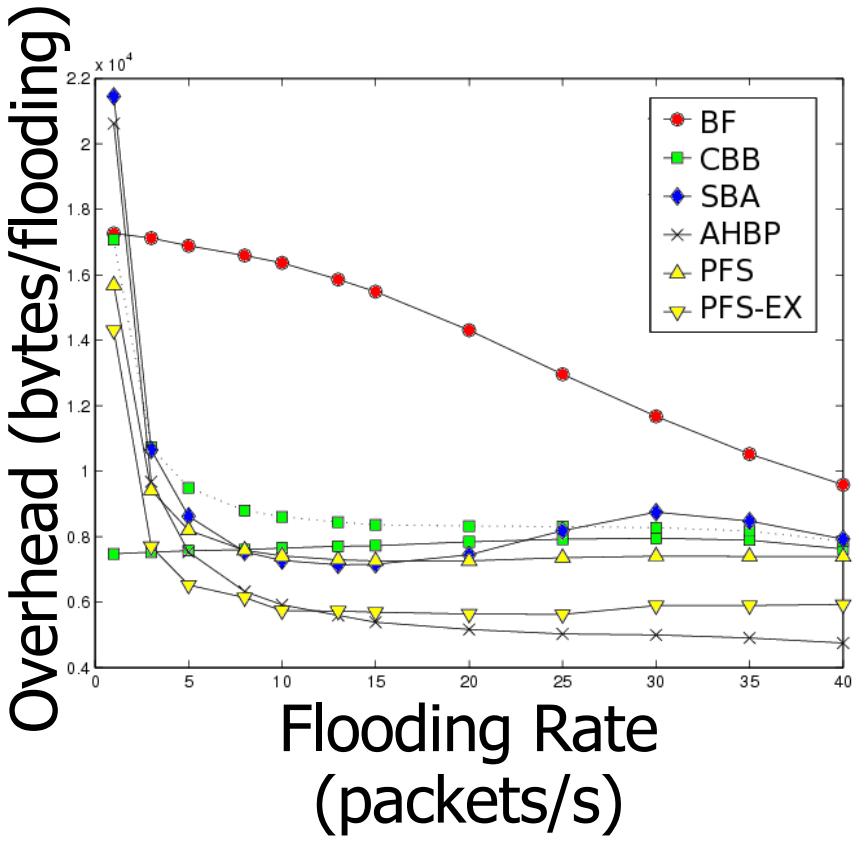
MAGNET
My personal Adaptive Global NET

PNP 2008
FREEBAND

TU Delft

Congestion





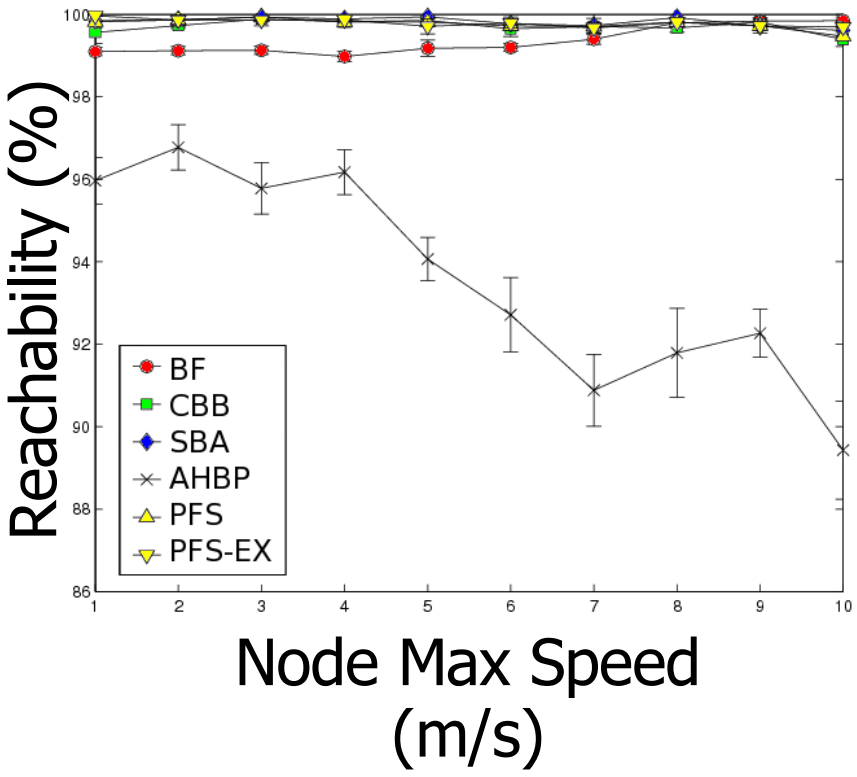
Information Society Technologies

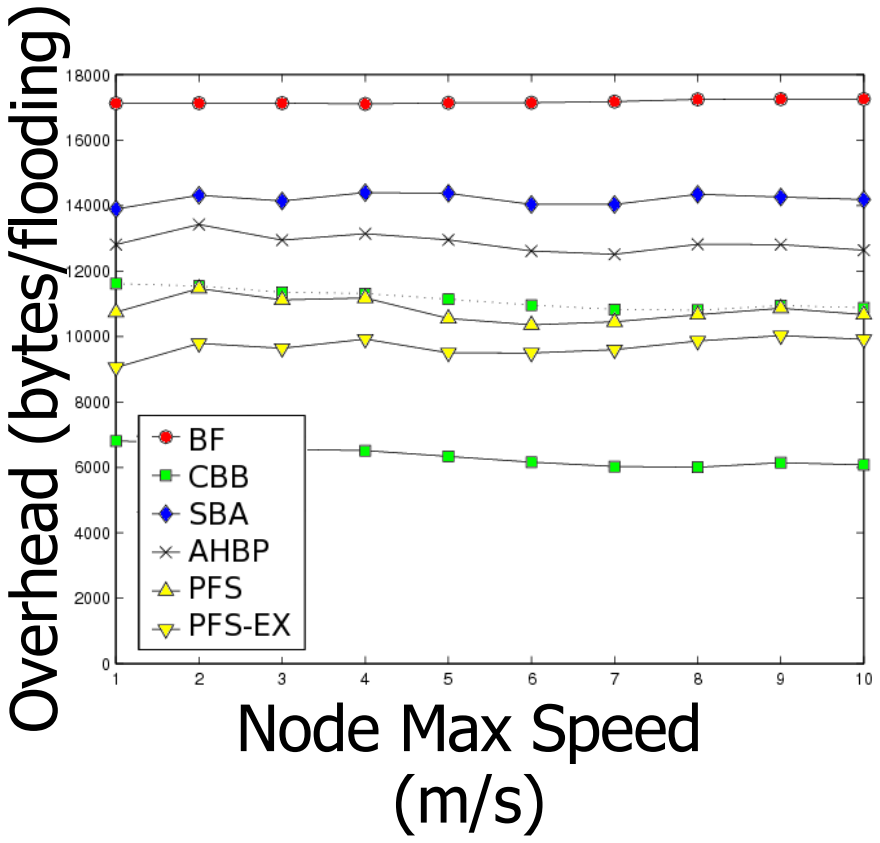
MAGNET
My personal Adaptive Global NET

PNP 2008
FREEBAND

TU Delft

Mobility





Conclusions

- We proposed a new flooding protocol for multi-hop ad hoc networks — PFS
- In comparison with existing flooding protocols, PFS:
  - copes very well with collisions
  - has a high reachability even when mobility is high
  - efficient in overhead, especially when one-hop hello messages are already provided
  - is able to finish a flooding within a relatively small end to end delay

Future Work

- Further investigate the trade-off between Overhead and end-to-end delay in PFS
- Try PFS in routing protocols, service discovery, etc
- Implement and test PFS in a real ad hoc network