

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

# Safe and Unsafe Disagreement in Vehicular Ad-hoc Networks

***Negin Fathollahnejad, Risat Pathan, Johan Karlsson***

Department of Computer Science and Engineering  
Chalmers University of Technology  
Göteborg, Sweden

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Motivation

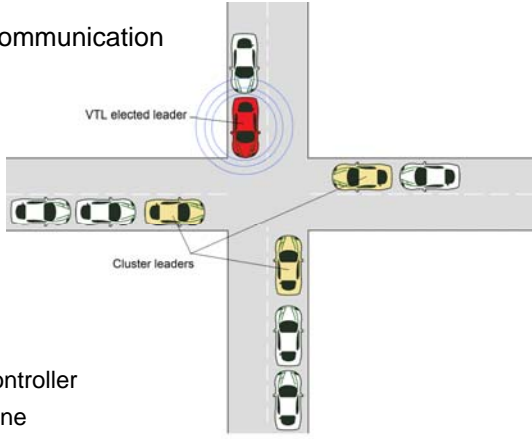
- There is an increasing interest in using **wireless distributed systems** in safety-critical applications.
- Examples include **autonomous and semi-autonomous cooperative systems** for road and air transport such as
  - Virtual traffic lights
  - Vehicle platooning
  - Autonomous maneuvering of cooperating unmanned air vehicles (UAVs).
- These system must ensure a **consistent behavior** among the cooperating vehicles in the presence of communication and node failures.
- We address the problem of designing and analyzing **distributed agreement algorithms** that can cope with **massive communication failures**.
- Our work is motivated by the fact that **the probability of message loss can be high** in distributed systems that rely on wireless communication.

IFIP WG 10.4 Summer meeting 2015 2

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Virtual Traffic Light (VTL)

- Traffic light based on V2V communication
  - No roadside infrastructure
- Key concepts:
  - Vehicle clusters
  - Cluster leader
  - VTL leader
    - Leader election
    - Leader handover
- Role of VTL leader
  - Acts as temporary traffic controller
  - Gives red light to its own lane
  - Initiates transfer of leadership to another vehicle



IFIP WG 10.4 Summer meeting 2015 3

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Agreement in wireless distributed systems

- Leader election and leader handover in a VTL are examples of functions that require distributed agreement.
- **Question:** Can we construct a distributed agreement algorithm that ensures consensus in the presence of an arbitrary number of messages losses?
- **Answer: No!**
- In 1989, N. Santoro and P. Widmayer showed that it is **impossible** to construct a distributed agreement algorithm that guarantees consensus in a **synchronous system with  $n$  nodes** if more than  $n-2$  messages can be lost in one communication round.

IFIP WG 10.4 Summer meeting 2015 4

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Research Questions

Santoro and Widmayer's impossibility result raises many important questions, such as

- How does the **design** of a distributed agreement algorithm influence the **probability of disagreement**?
- How do we **calculate** the **probability of disagreement**?
- What is the **impact of disagreement**?

IFIP WG 10.4 Summer meeting 2015 5

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Agreement problems in VTLs

- Leader election & leader handover
  - Agreement on the identity of the leader (agreement on one value).
- Group formation (network bootstrap)
  - Agreement on the identity of the nodes that make up a ad-hoc network (agreement on a set of node identities).
- This talk focuses on disagreement in a group formation algorithm.

IFIP WG 10.4 Summer meeting 2015 6

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Group formation

- Consider a set of  $n$  cars (nodes) that approach an *empty* intersection from different directions.
- To create a virtual traffic light, the nodes must first establish an ad-hoc wireless network.
- To this end, they must **agree on the set of nodes that constitute the ad-hoc network**.
- We call this the **group formation problem**.
- Note that group formation and group membership are two different problems.

IFIP WG 10.4 Summer meeting 2015 7

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Possible outcomes of a group formation algorithm

- **Agreement** - all nodes have the same view of the system.
- **Agreement on abort** - all nodes decide to abort due to insufficient information (too many messages have been lost).
- **Safe disagreement** - some nodes decide to abort and the other nodes decide on the same set.
- **Unsafe disagreement** - at least two nodes have different views of the system.

IFIP WG 10.4 Summer meeting 2015 8

## Why is group formation a difficult problem?

- The difficulty lies in the problem itself:  
***Neither the identity of the nodes in the system, nor the size of the system, are initially known to any node.***
- If each node would know the identify of all other nodes in the system, group formation would not be necessary.
- Note: we can construct agreement algorithms that avoids ***unsafe disagreement*** (for an unbounded number of message losses), if each node knows the identity of all other nodes in the system.

## Outline

- System model
- Failure assumptions and failure model
- A simple group formation algorithm
- Some results
- Conclusion and future work

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## System model

- There are  $n$  processes in the system.
  - A process is an instance of the algorithm running in one vehicle.
- Processes are indexed as  $\{p_1, p_2, \dots, p_n\}$
- Processes communicate via broadcasts messages over an unreliable wireless network.
- The agreement algorithm runs in  $R$  rounds of message exchange.
- $R$  is fixed at design time

IFIP WG 10.4 Summer meeting 2015 11

**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## Failure assumptions

- Communication failures
  - Any number of messages can be lost.
  - No value failures. (The content of a message is either lost or correct)
- Fault-free processes (nodes, cars).

IFIP WG 10.4 Summer meeting 2015 12

## Failure model

- We consider two types of communication failures:
  - Send omissions (symmetrical failures)
  - Receive omissions (asymmetrical failures)
- In this talk, I will only consider only receive omissions since they are more difficult to cope with.
- We assume that the probability of a receive omission failure is constant over all rounds of protocol execution.
- We let  $Q$  denote the probability of a receive omission.

## Group formation algorithm

---

**Algorithm 1** Generic group formation algorithm for  $p_i$

---

```

 $msg_i \leftarrow \{p_i, \Pi_i\};$ 
for  $r = 1$  to  $R$  do
  begin_round
  send ( $msg_i$ );
  receive ();
  compute ( $msg_i$ );
  end_round;
end for
execute_decision_algorithm();

```

---

- The aim of the algorithm is to form a group of processes (nodes, cars) that will implement a cooperative safety function, e.g., a virtual traffic light.
- $\Pi_i$  is process  $p_i$ 's current view of the set of nodes in the system.

## The compute message algorithm

---

**Algorithm 2** Compute ( $msg_i$ ):  $\Pi_i$

---

```

1: for all  $p_j$  such that  $p_i$  has received  $msg_j = \{p_j, \Pi_j\}$  do
2:    $\Pi_i = \Pi_i \cup \Pi_j$ ;
3: end for
4:  $msg_i \leftarrow \{p_i, \Pi_i\}$ ;

```

---

- The compute message algorithm updates  $\Pi_i$  after each communication round using info received from other nodes.

## The decision algorithm

---

**Algorithm 3** Decision Algorithm for  $p_i$

---

```

 $o_i \leftarrow p_i$  query its oracle
 $m_i \leftarrow$  size of  $\Pi_i$ 
 $c \leftarrow$  confidence
if  $m_i < c * o_i$  then
  abort;
else
   $p_i$  selects  $\Pi_i$ ;
end if

```

---



**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## The oracle

- We assume that each process  $p_i$  has access to an oracle that provides an unreliable estimate of the number nodes that wants to join the group.
- We let  $o_i$  denote the estimate provided by the oracle to
- We assign a confidence number  $c$  to  $o_i$ , where
  - $c = 1$  means that we trust the oracle to produce estimates without bias.
  - $c < 1$  means that we assume that the oracle overestimates the number of nodes the wants to join the group.
  - $c > 1$  means that we assume the oracle underestimates the number of nodes the wants to join the group.
- The oracle's estimate is obtained by independent sensors, such as cameras or wireless messages sent by road side infrastructure.

17

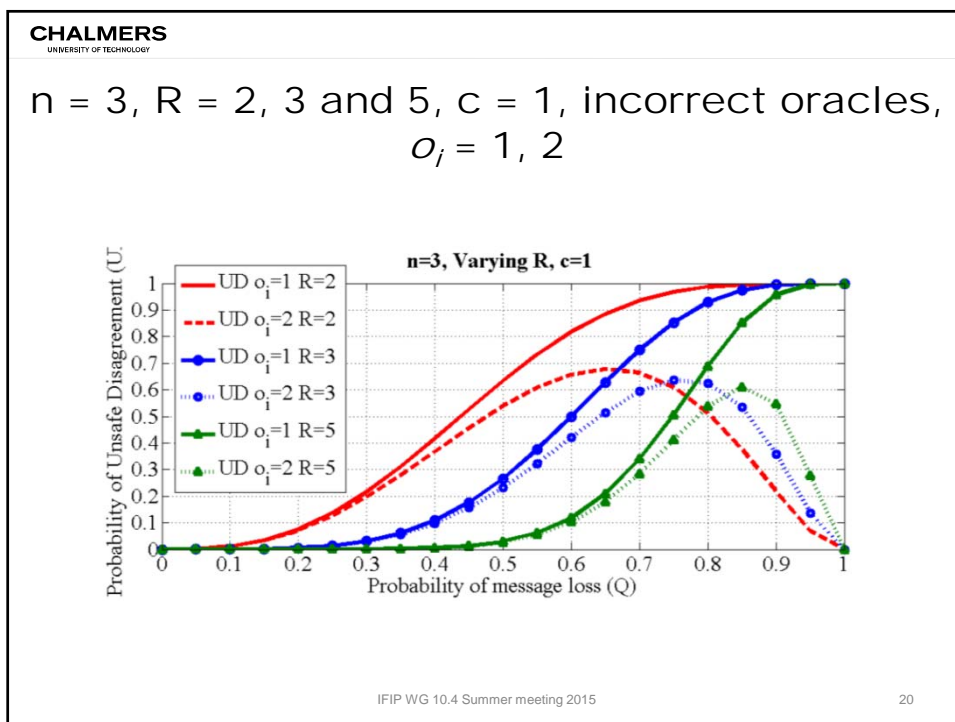
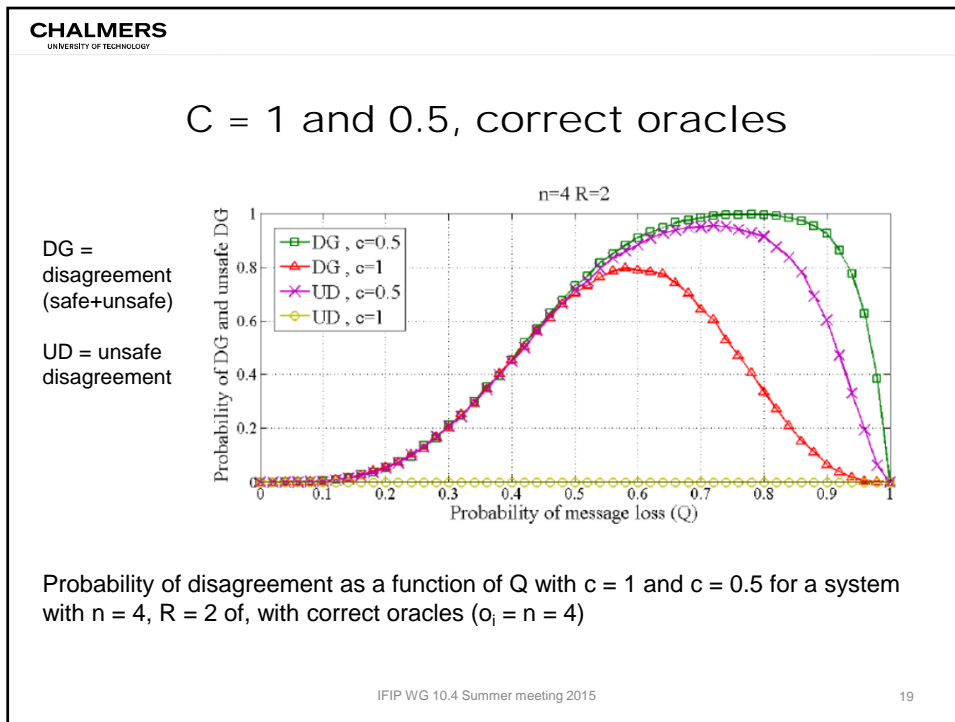
**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

## 4 nodes, 2 rounds, correct oracles, receive omissions

$n=4$   $R=2$

Probability of outcomes for four processes as a function of  $Q$ , correct oracles ( $o_i = n = 4$ )

18



## Conclusions

- Group formation is an important and difficult problem in ad-hoc vehicle networks.
- We introduced the concepts of safe and unsafe disagreement.
- Unsafe disagreement cannot be avoided under realistic communication failure assumptions
- Open question: How do we design group formation algorithms that have a low probability of unsafe disagreement?

## Questions?

