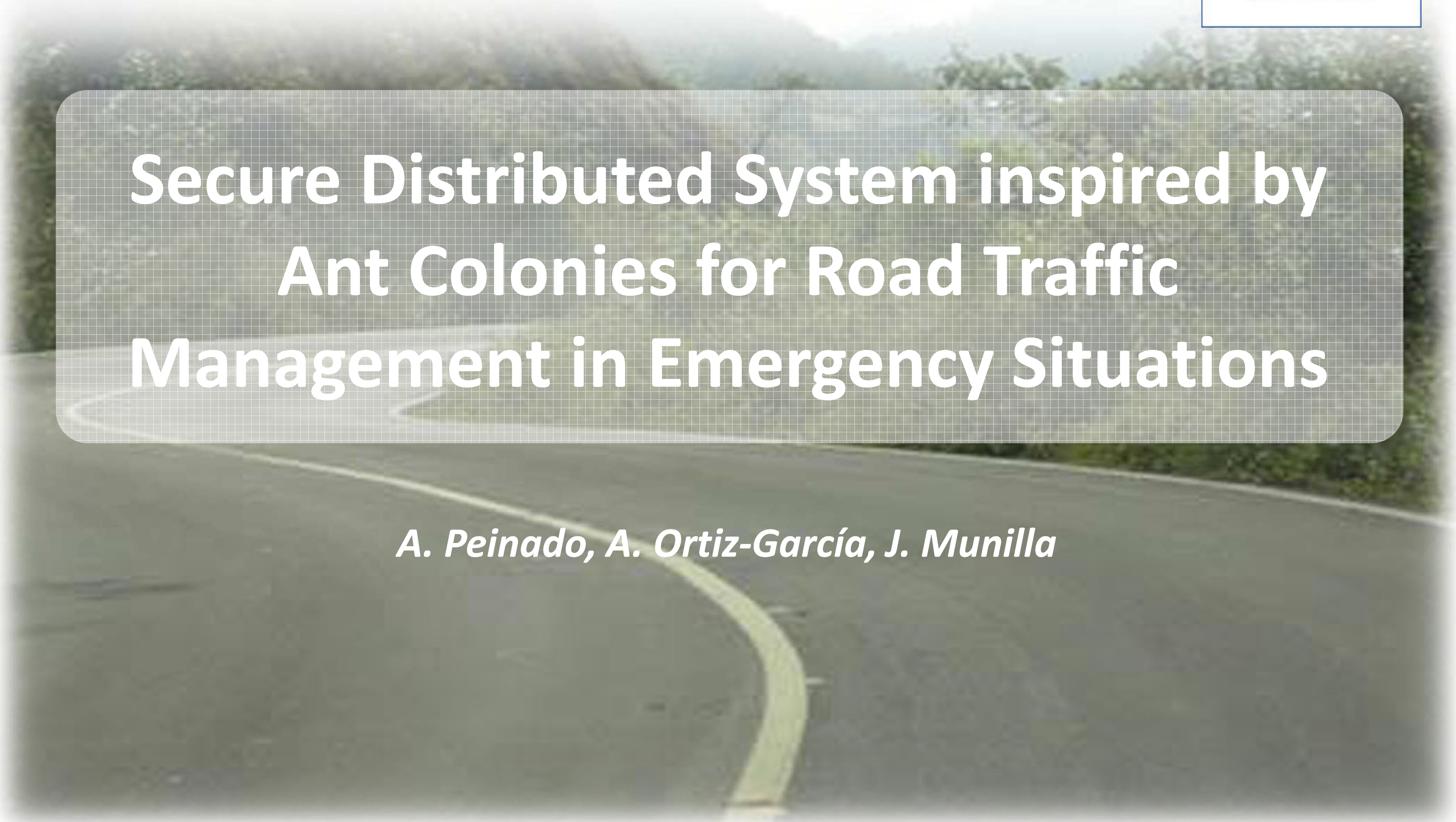
UNIVERSIDAD
DE MÁLAGA

SECURWARE 2013
August 25-31, 2013, Barcelona, Spain

ATIC
Grupo de Aplicación de las
Tecnologías de la Información
y Comunicaciones



Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

A. Peinado, A. Ortiz-García, J. Munilla

E.T.S.Ingeniería de Telecomunicación
Campus de Teatinos, 29071 Málaga

Ingenieria de Comunicaciones

Contents

- VANETs and Road traffic management
- Model inspired by Ant colonies
- System proposed
- Prototype
- Security issues

Road Traffic Management

Supported by TICs

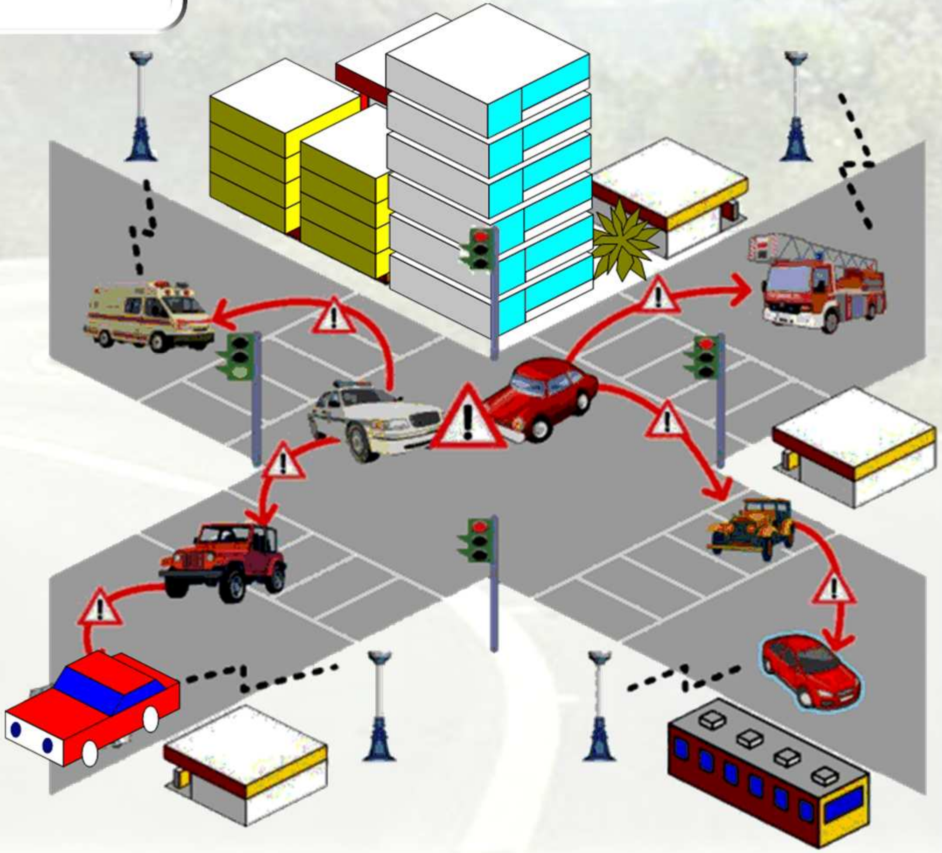
- Cameras
- Sensors
- Screens and displays

VANET

Vehicular Ad hoc NETwork

Elements

- **OBU** (On Board Unit)
- **RSU** (Road Side Unit)



Physical level

IEEE 802.11p:

-WiMax

-GPRS

-WAVE

Communication:

-V2V

- V2I

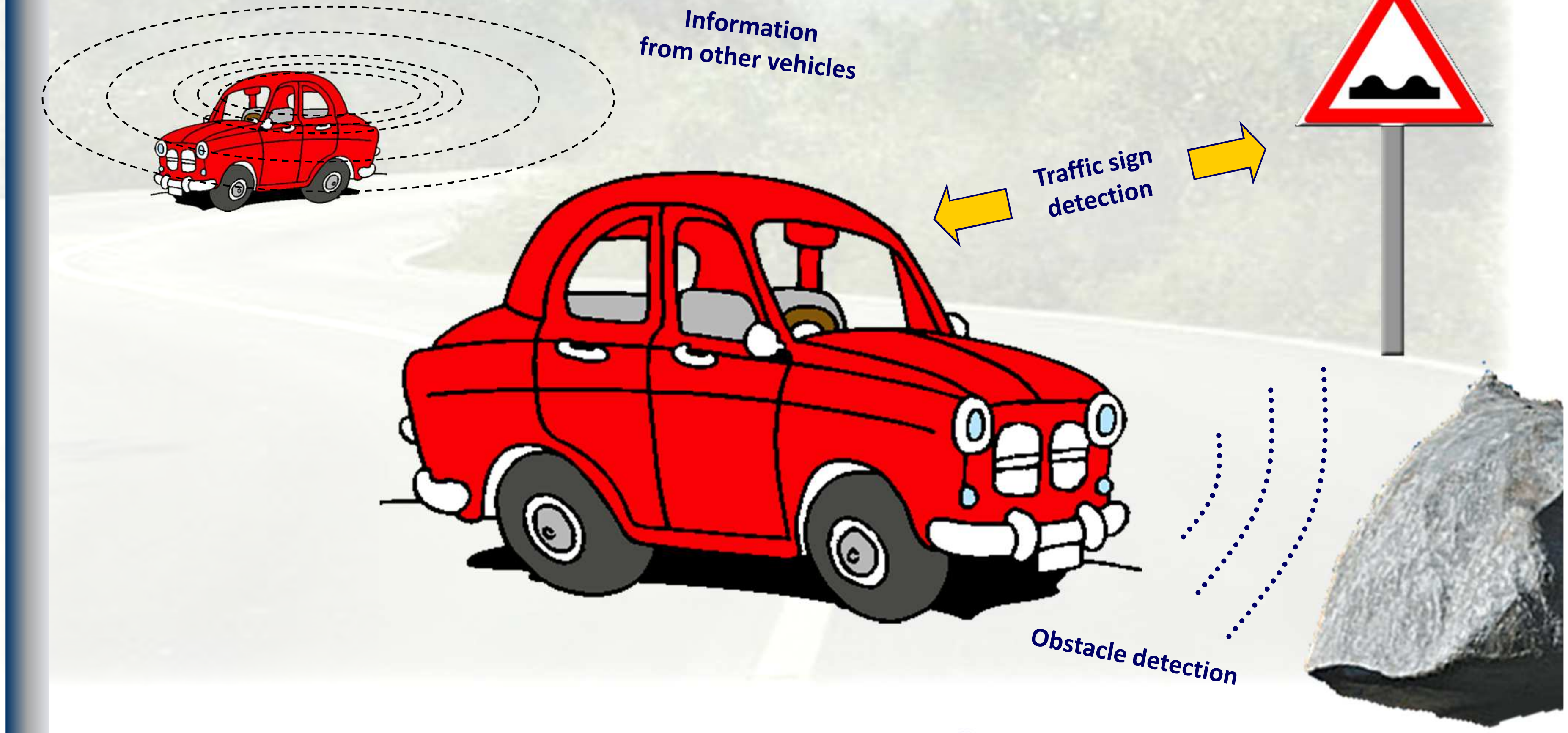
- I2V

VANET

Vehicular Ad hoc NETwork

VANET applications

- Road Traffic Security
- Added-value and Comfort



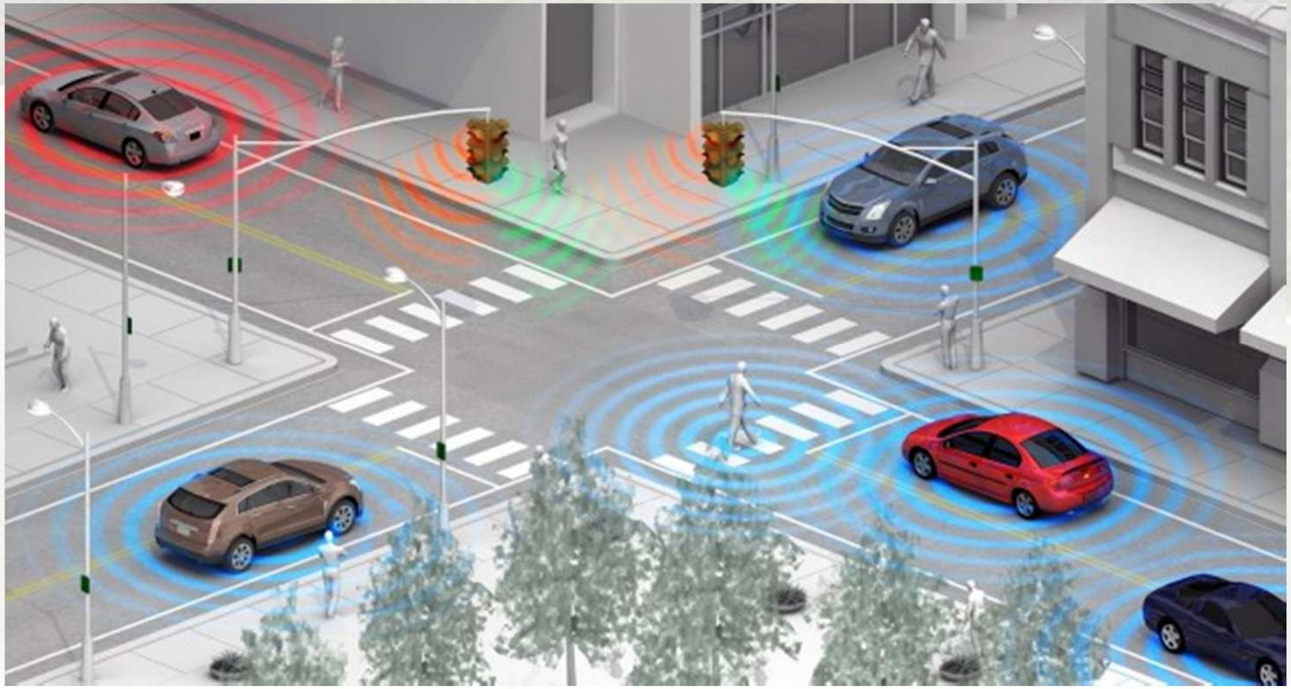
VANET

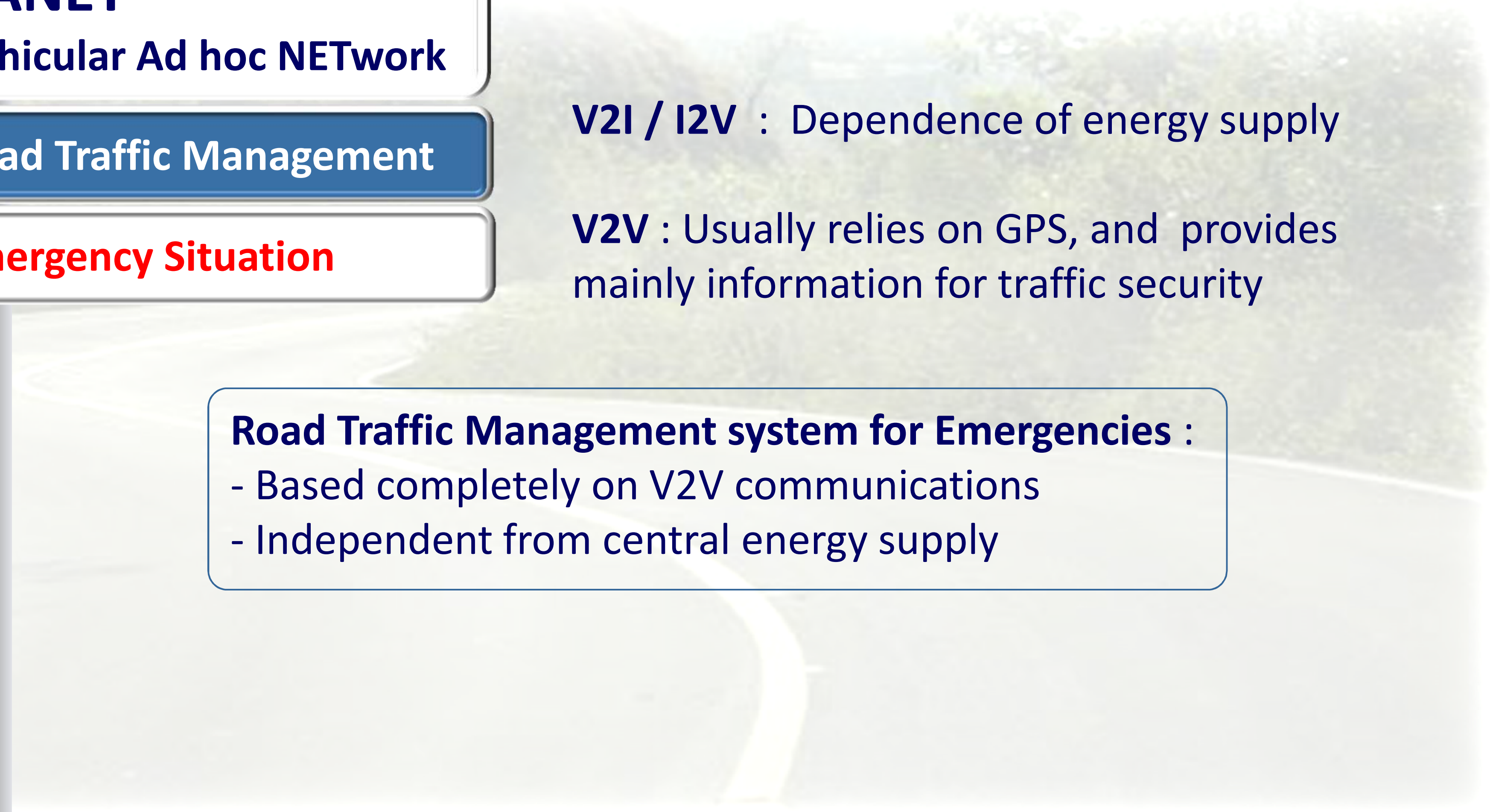
Vehicular Ad hoc NETwork

Road Traffic Management

V2I / I2V : Input to/Output from Central system

V2V : helps to propagate the signals – serves mainly for traffic security





VANET

Vehicular Ad hoc NETwork

Road Traffic Management

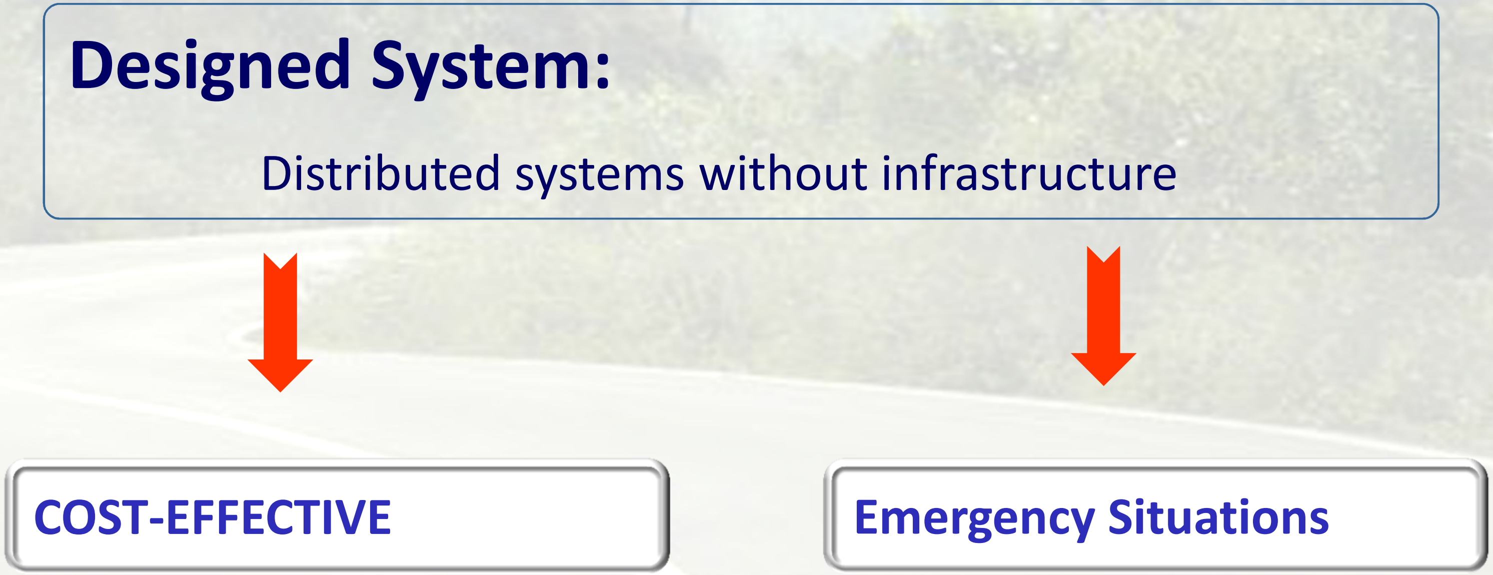
Emergency Situation

V2I / I2V : Dependence of energy supply

V2V : Usually relies on GPS, and provides mainly information for traffic security

Road Traffic Management system for Emergencies :
- Based completely on V2V communications
- Independent from central energy supply

Road Traffic Management



Designed System:

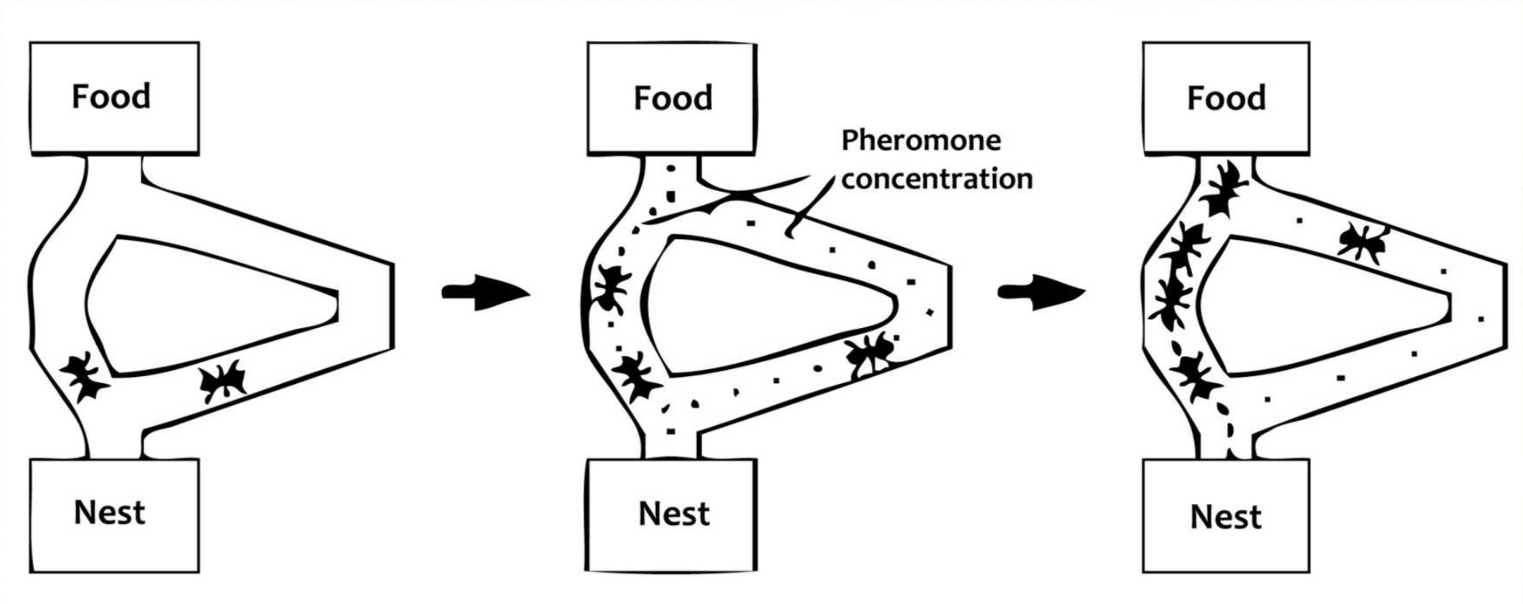
Distributed systems without infrastructure

COST-EFFECTIVE

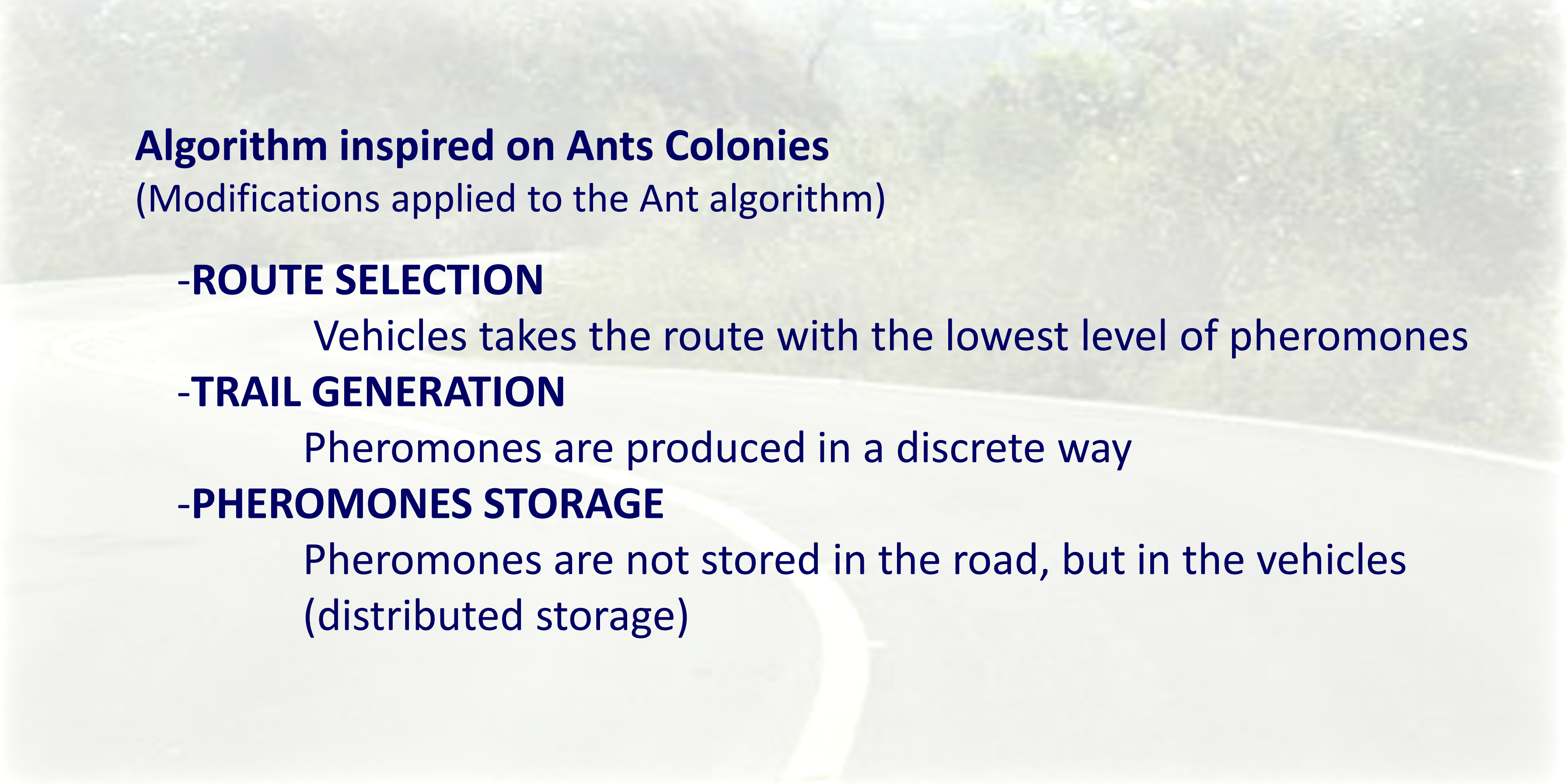
Emergency Situations

Model inspired by Ant colonies

Ant Colonies



Model inspired by Ant colonies



Algorithm inspired on Ants Colonies
(Modifications applied to the Ant algorithm)

-**ROUTE SELECTION**

Vehicles takes the route with the lowest level of pheromones

-**TRAIL GENERATION**

Pheromones are produced in a discrete way

-**PHEROMONES STORAGE**

Pheromones are not stored in the road, but in the vehicles (distributed storage)

System proposed

-**LOCATION SYSTEM**

RFID

-**CONTROL PLACES**

The most significant nodes of the road.

ID_{loc}: Identification of the control place

-**PHEROMONES GENERATION**

Broadcast message: ID_{SVeh} and ID_{loc}

-**DISAPPEARING EFFECT**

The vehicles are not synchronized between them.

Local clock is used to reduce the level

-**ROUTE SELECTION**

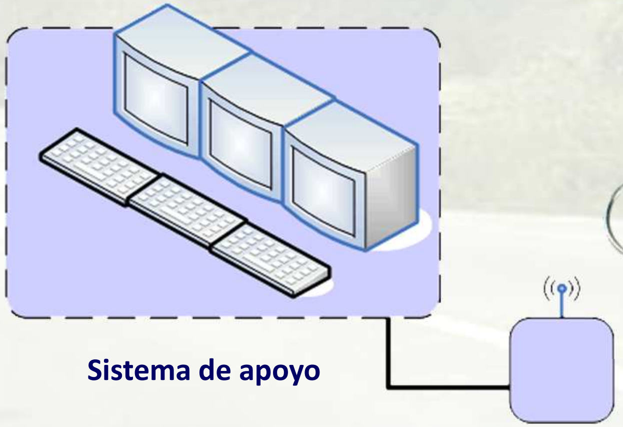
Route is selected based on internal variables

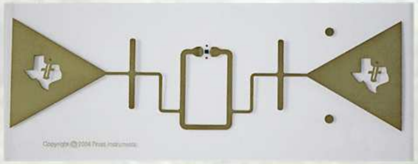
Location system

System proposed

RFID

Radio Frequency ID





UHF Pasive tags

HF Pasive tags

LF Pasive tags

General Features

- Low cost
- Low storage capacity
- Low computational capacity

Location system

RFID
Radio Frequency ID

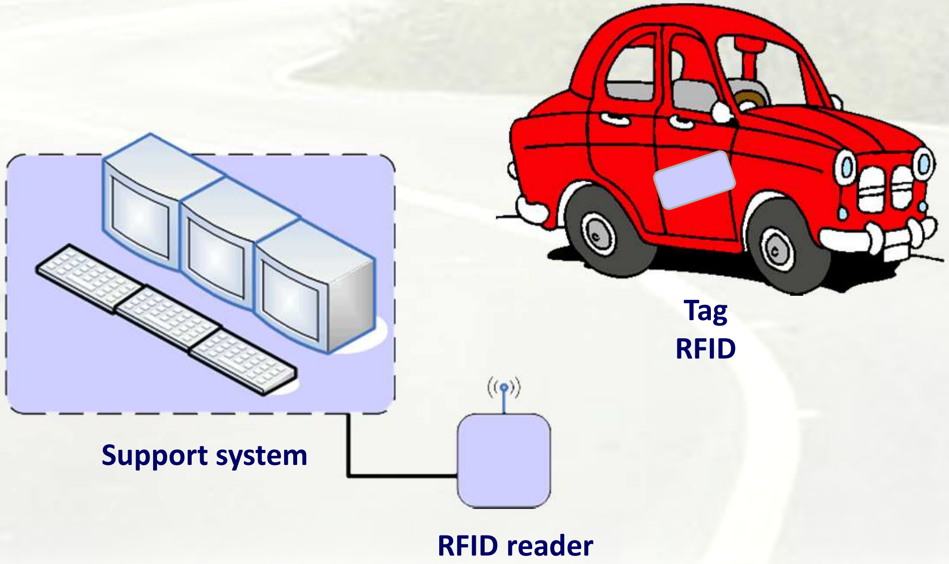
VANET
Vehicular Ad hoc NETwork

Architecture

Tag onboard

Reader on the road

V2I



Location system

RFID
Radio Frequency ID

VANET
Vehicular Ad hoc NETwork

Architecture

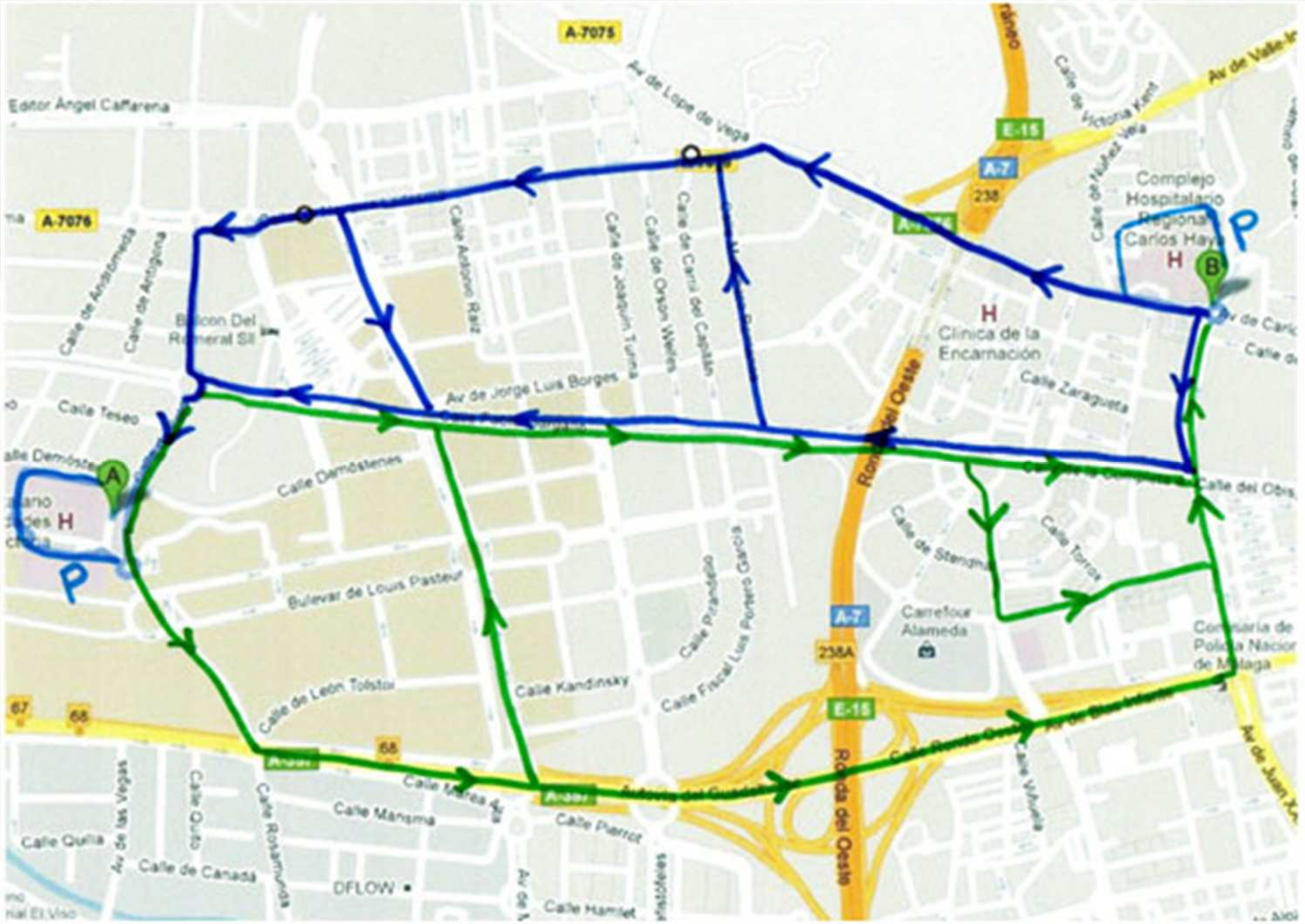
Reader onboard

Tag on the road

I2V

Control places

Main crossroads are identified

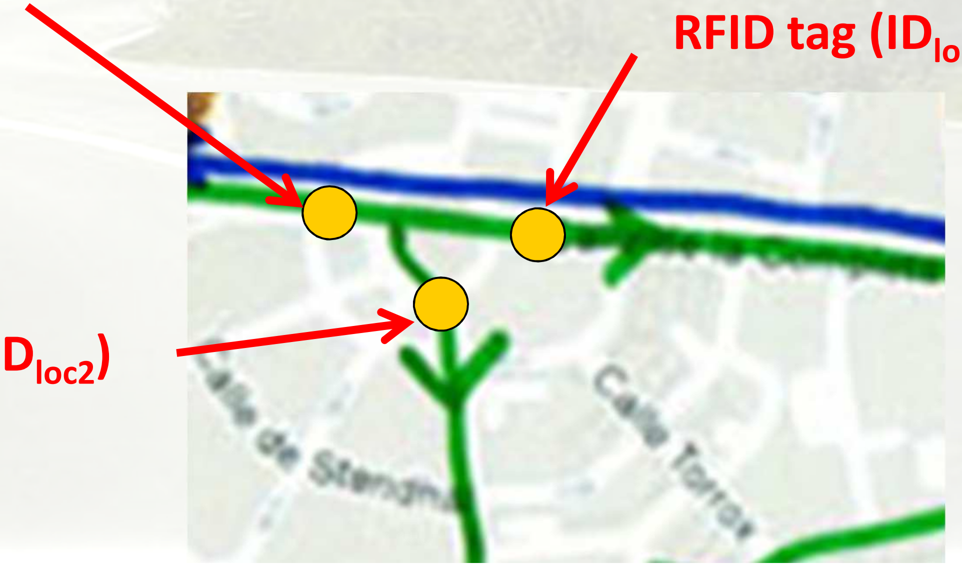


Control places

Significant crossroads (nodes) are selected and pointed out by a RFID tag:

Information points, ID_{loc}: is assigned to points after the node.

Decission points: before the node.

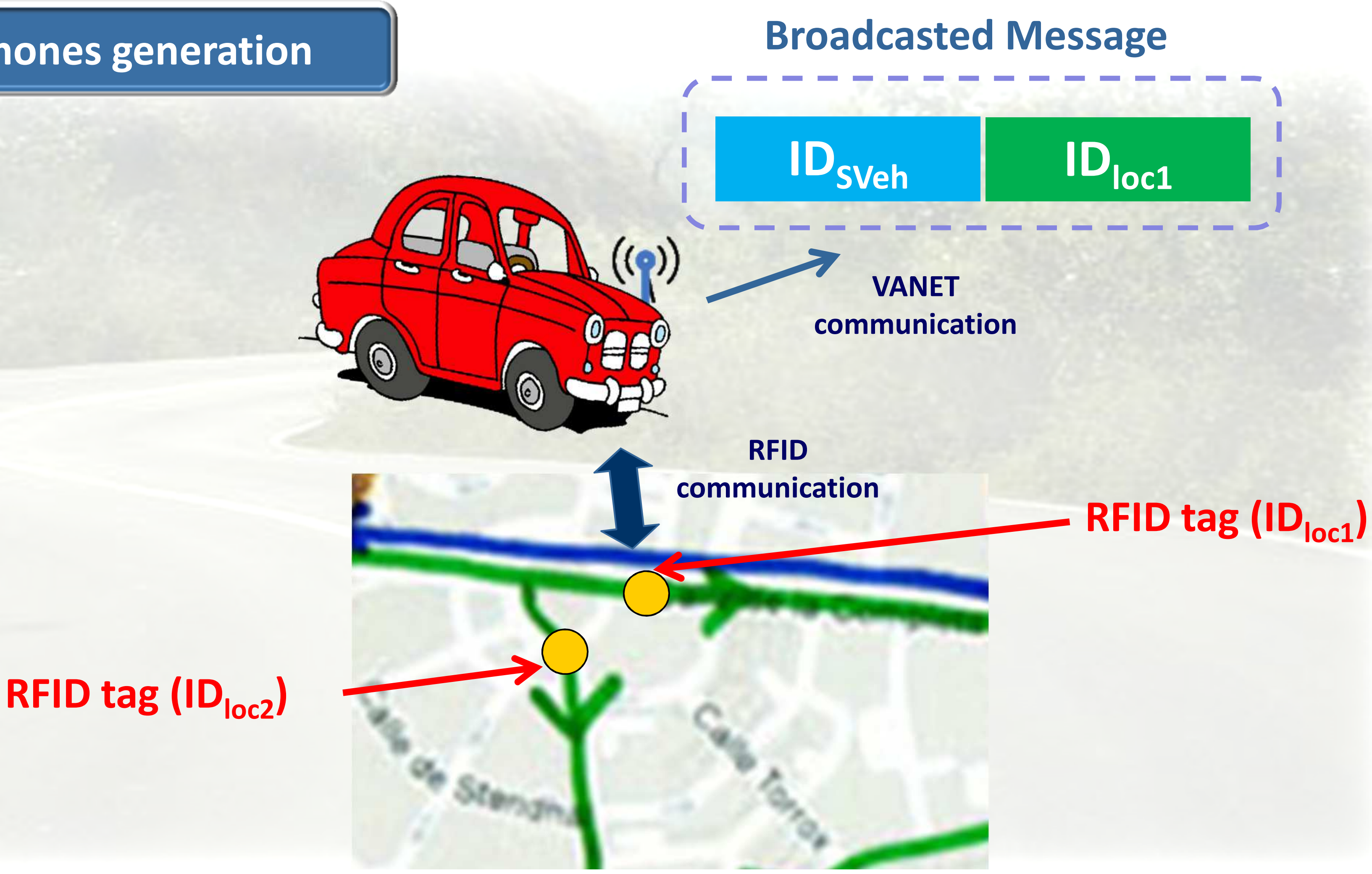


RFID tag (decission point)

RFID tag (ID_{loc1})

RFID tag (ID_{loc2})

Pheromones generation



Broadcasted Message

ID_{SVeh} ID_{loc1}

VANET communication

RFID communication

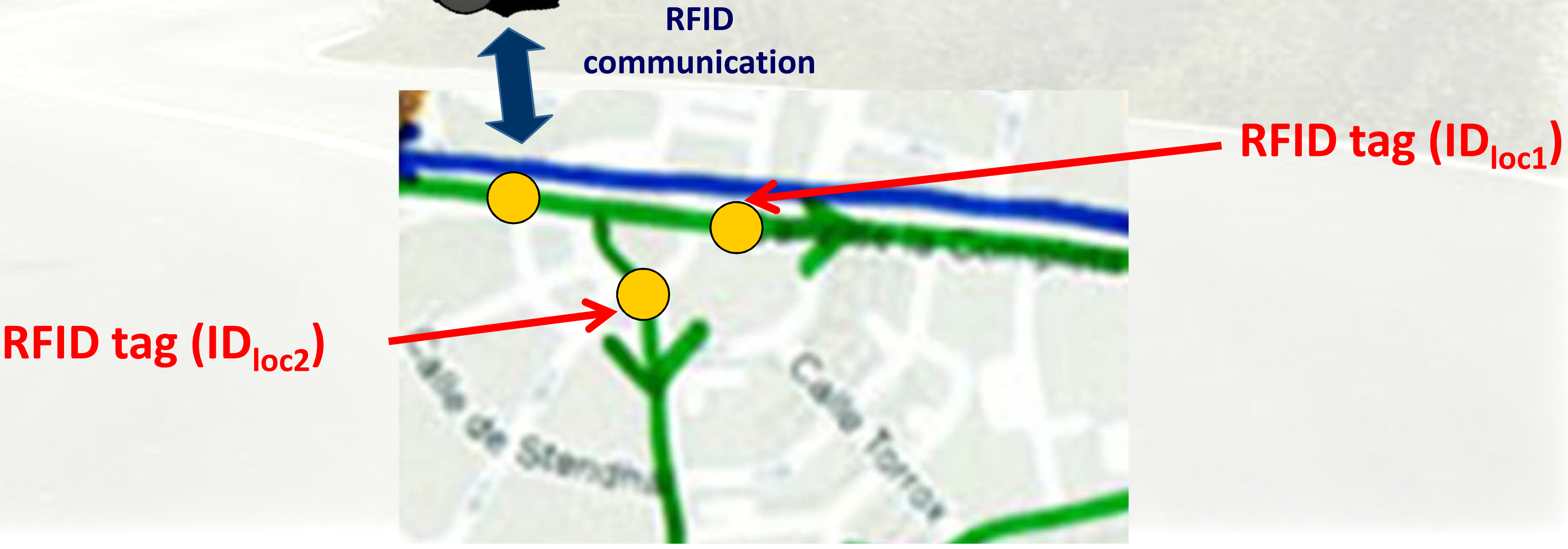
RFID tag (ID_{loc1})

RFID tag (ID_{loc2})

Route Selection

Vehicle reads its internal variables

…	…
ID_{loc1}	80
ID_{loc2}	65
…	…



Disappearing Effect

Vehicles decrease the content of the internal variables proportionally to the time elapsed

Vechicle are not synchronized between them.
They do not use global clock, but internal time reference

Location	Pherom.	Message arrival time
…	…	…
ID_{loc1}	80	12:31:45
ID_{loc2}	65	13:23:07
…	…	…

Current internal time

13:35:02

Δt : Current time – Arrival time
γ : Decreasing coefficient

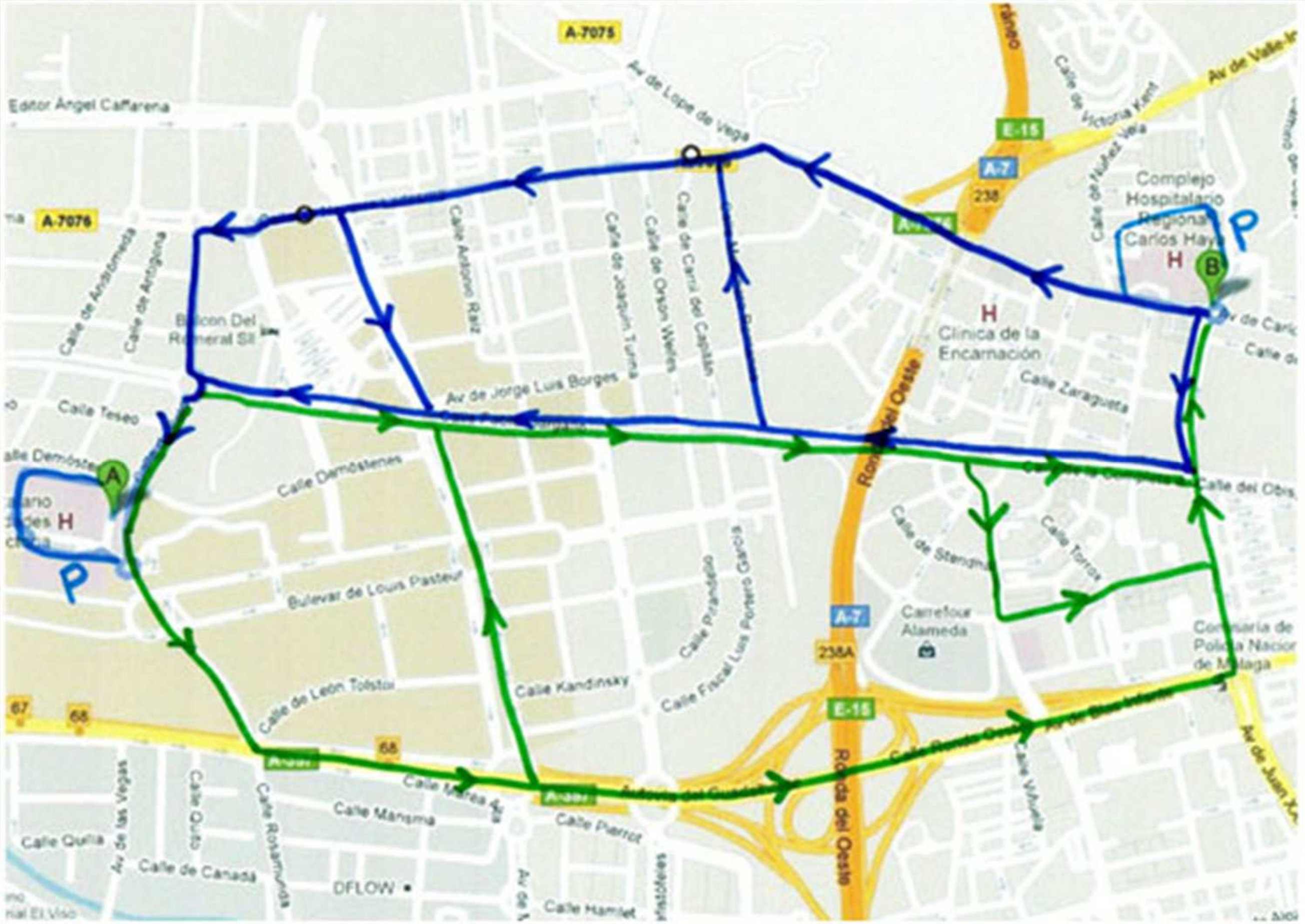
New Pher. Level = Pher. Level - $\Delta t \cdot \gamma$

Prototype

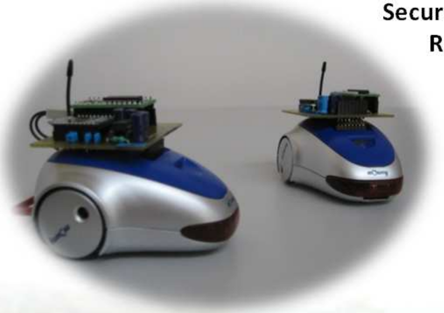
Real scenario:

Routes between two main hospitals in Málaga

- "Carlos Haya" University Regional Hospital
- "Virgen de la Victoria" University Clinical Hospital

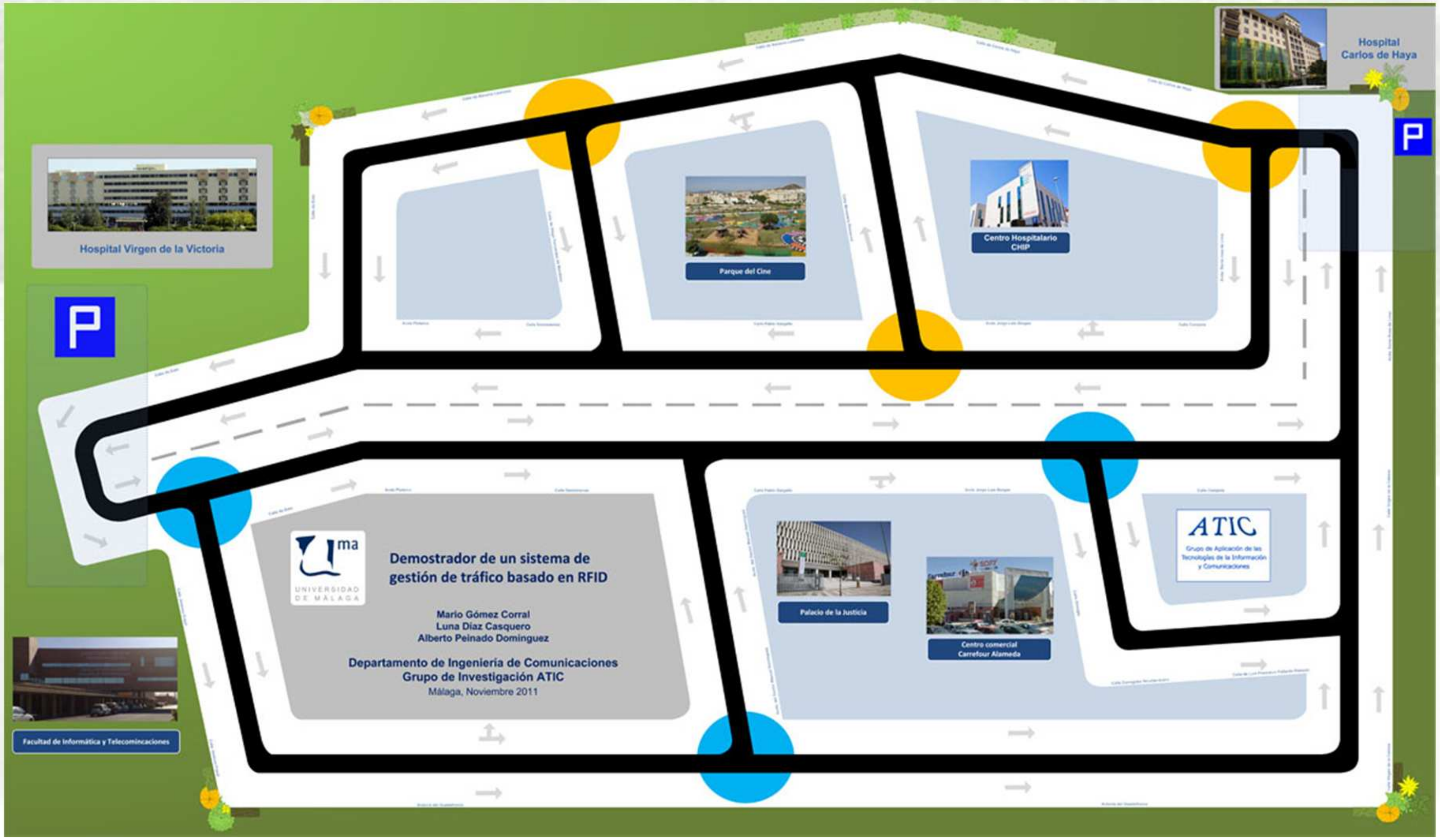


Prototype



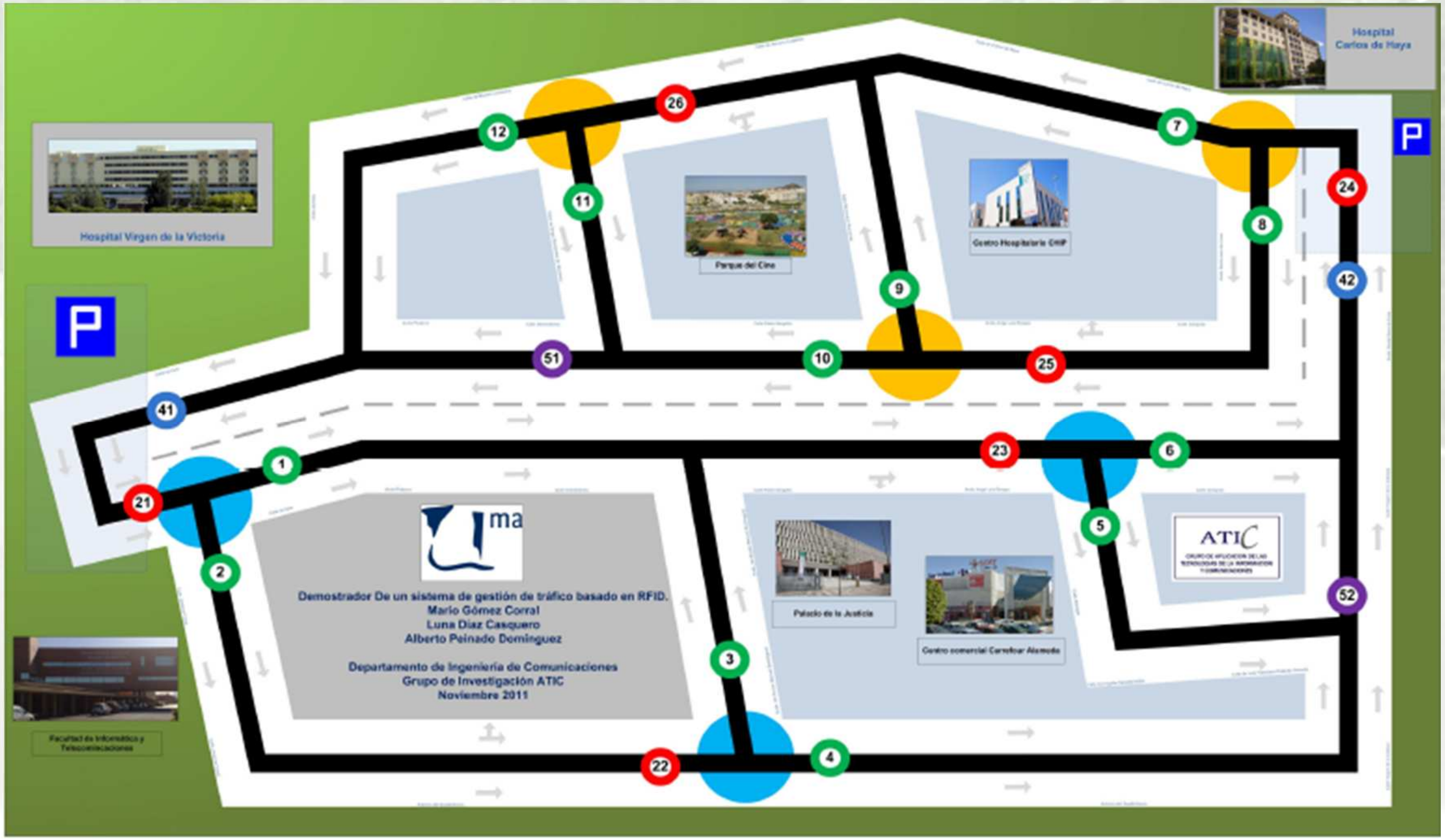
● ● Control places

Simplified scenario

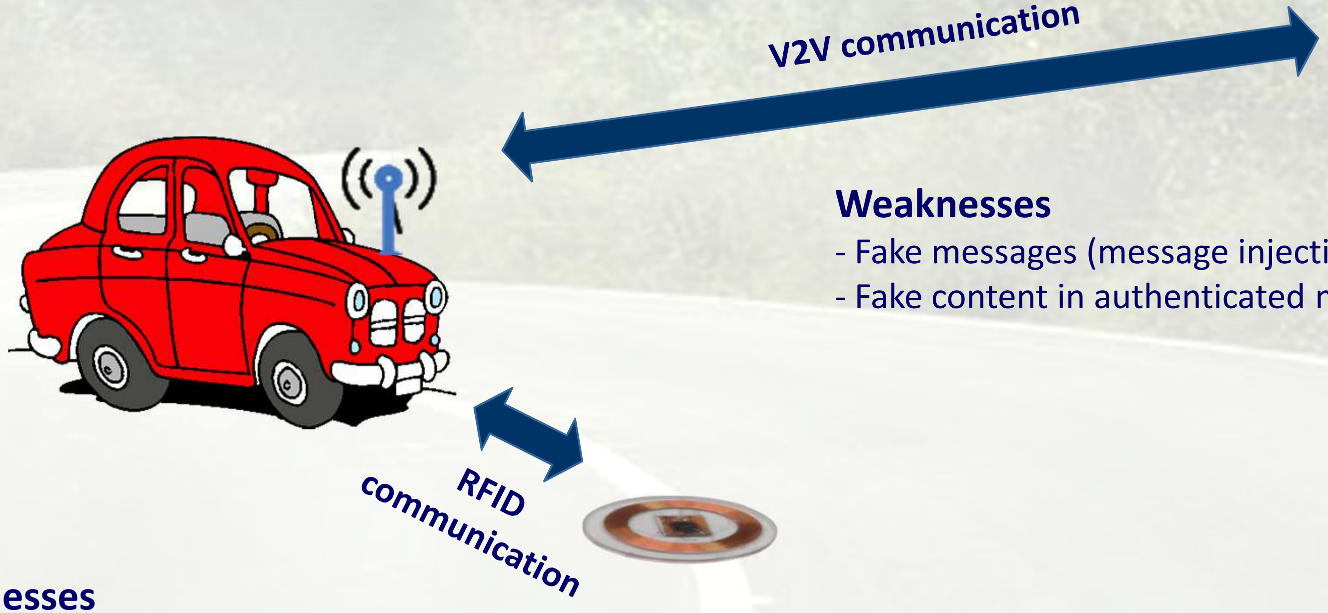

Hospital
Carlos de Haya
P
Hospital Virgen de la Victoria
P
Parque del Cine
Centro Hospitalario
CHIP
Demostrador de un sistema de
gestión de tráfico basado en RFID
Mario Gómez Corral
Luna Díaz Casquero
Alberto Peinado Domínguez
Departamento de Ingeniería de Comunicaciones
Grupo de Investigación ATIC
Málaga, Noviembre 2011
Palacio de la Justicia
Centro comercial
Carrefour Alameda
ATIC
Facultad de Informática y Telecomunicaciones

Prototype

- 🔴 RFID tag – Decission places
- 🟢 RFID tag – Pheromones Generation places
- 🟣 RFID tag – Internal uses


Hospital Virgen de la Victoria
Hospital Carlos de Haya
Parque del Cine
Centro Hospitalario CHIP
P
P
Palacio de la Justicia
Centro comercial Carrefour Alameda
ATIC
Facultad de Informática y Telecomunicaciones
ma
Demostrador De un sistema de gestión de tráfico basado en RFID.
Mario Gómez Corral
Luna Díaz Casquero
Alberto Peinado Domínguez
Departamento de Ingeniería de Comunicaciones
Grupo de Investigación ATIC
Noviembre 2011
12
26
7
11
24
8
42
9
51
10
25
41
23
6
1
21
5
2
52
3
22
4

Security Issues



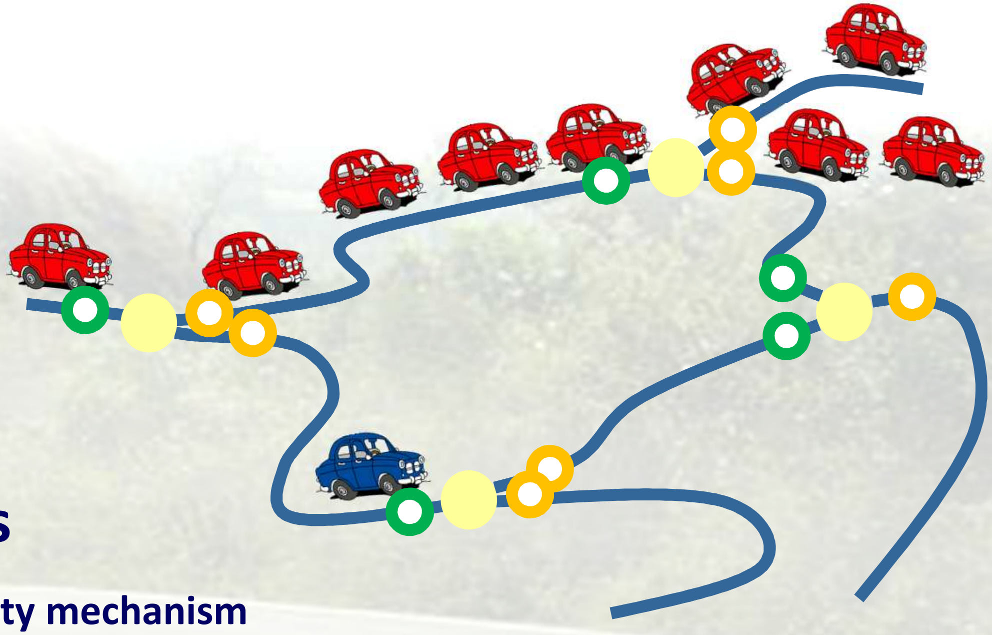
Weaknesses

- Fake messages (message injection)
- Fake content in authenticated messages

Weaknesses

- Tag clonning (or legal tag moved)
- Fake tags

Security Issues



General Considerations

- Authentication is the main security mechanism
- Confidentiality is not necessary
-

Security Issues

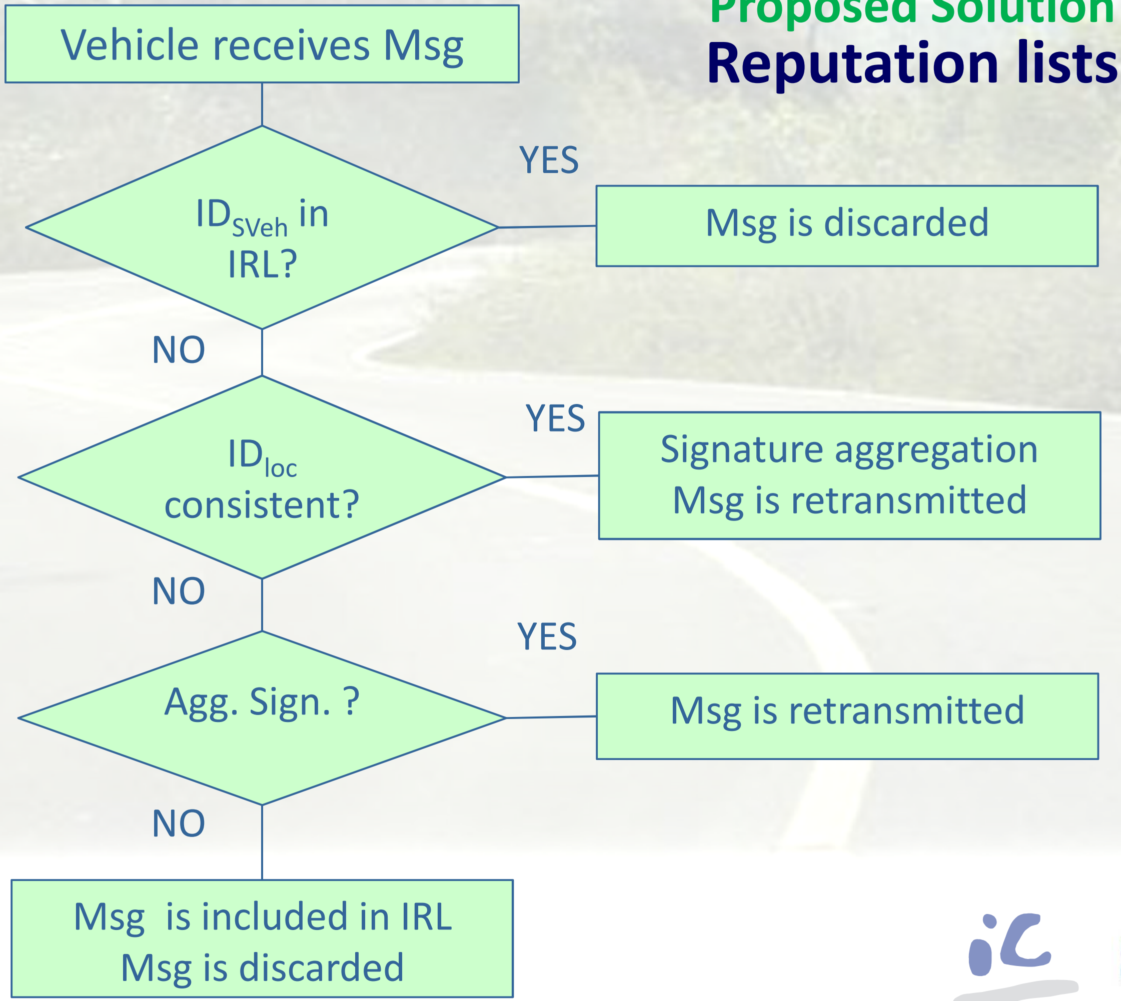
Main threat

Fraudulent messages:

Authenticated messages with false content

Proposed Solution

Reputation lists and Data Aggregation



Vehicle receives Msg

ID_{SVeh} in IRL?

YES

Msg is discarded

NO

ID_{loc} consistent?

YES

Signature aggregation
Msg is retransmitted

NO

Agg. Sign. ?

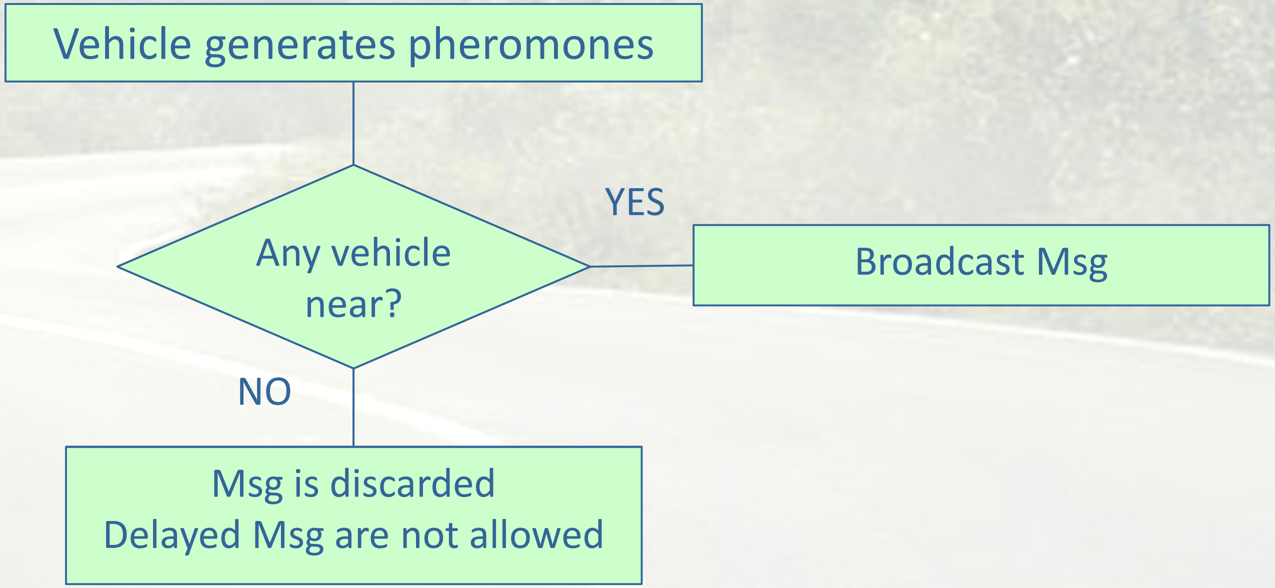
YES

Msg is retransmitted

NO

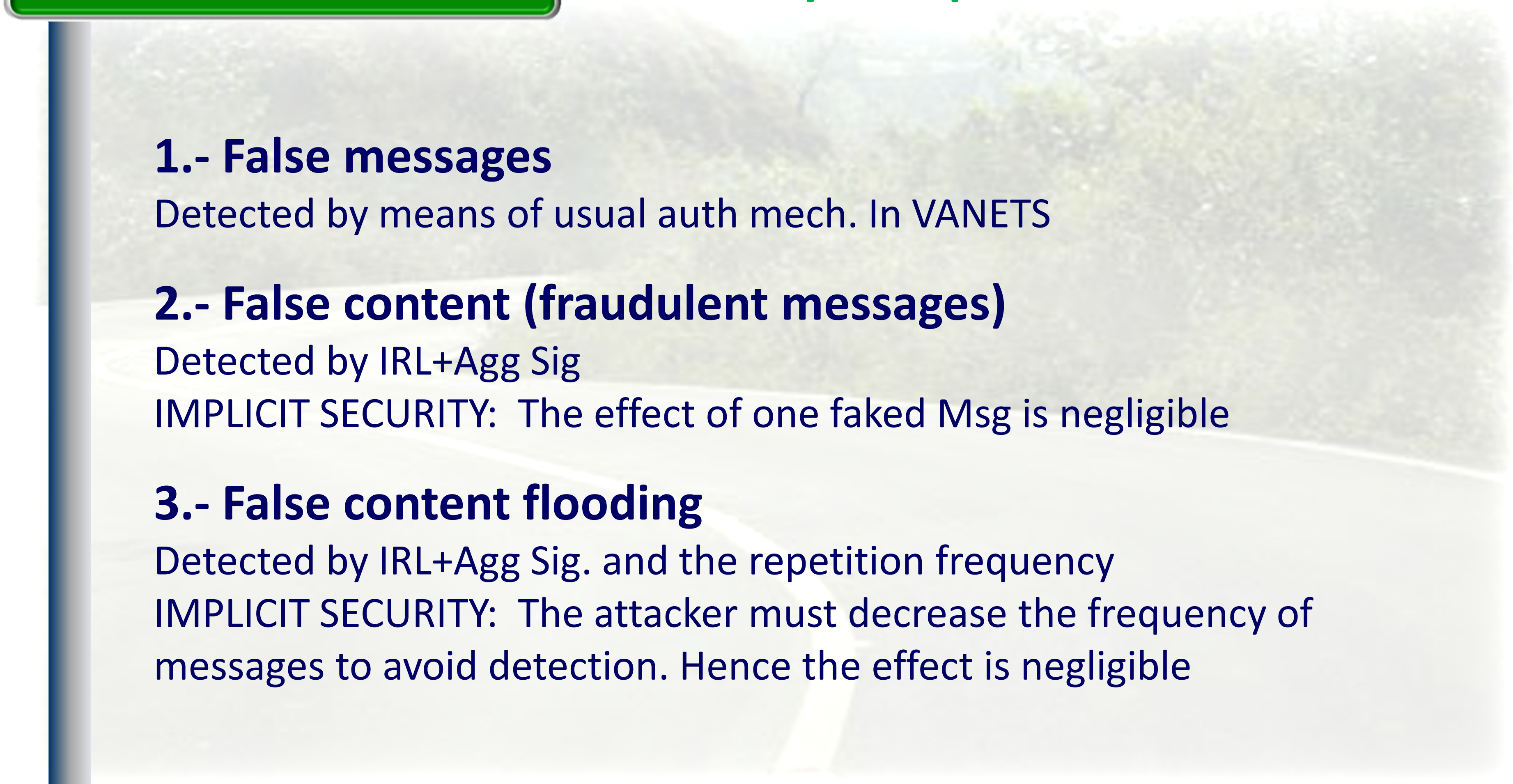
Msg is included in IRL
Msg is discarded

Security Issues



Security Issues

Analysis of potential attacks



1.- False messages

Detected by means of usual auth mech. In VANETS

2.- False content (fraudulent messages)

Detected by IRL+Agg Sig

IMPLICIT SECURITY: The effect of one faked Msg is negligible

3.- False content flooding

Detected by IRL+Agg Sig. and the repetition frequency

IMPLICIT SECURITY: The attacker must decrease the frequency of messages to avoid detection. Hence the effect is negligible

Security Issues

Analysis of potential attacks

4.- Conspiracy

Detected by IRL+Agg Sig.

IMPLICIT SECURITY: Many attackers are necessary. Hence the attack is not effective

5.- Discarding aggregated messages

IMPLICIT SECURITY:

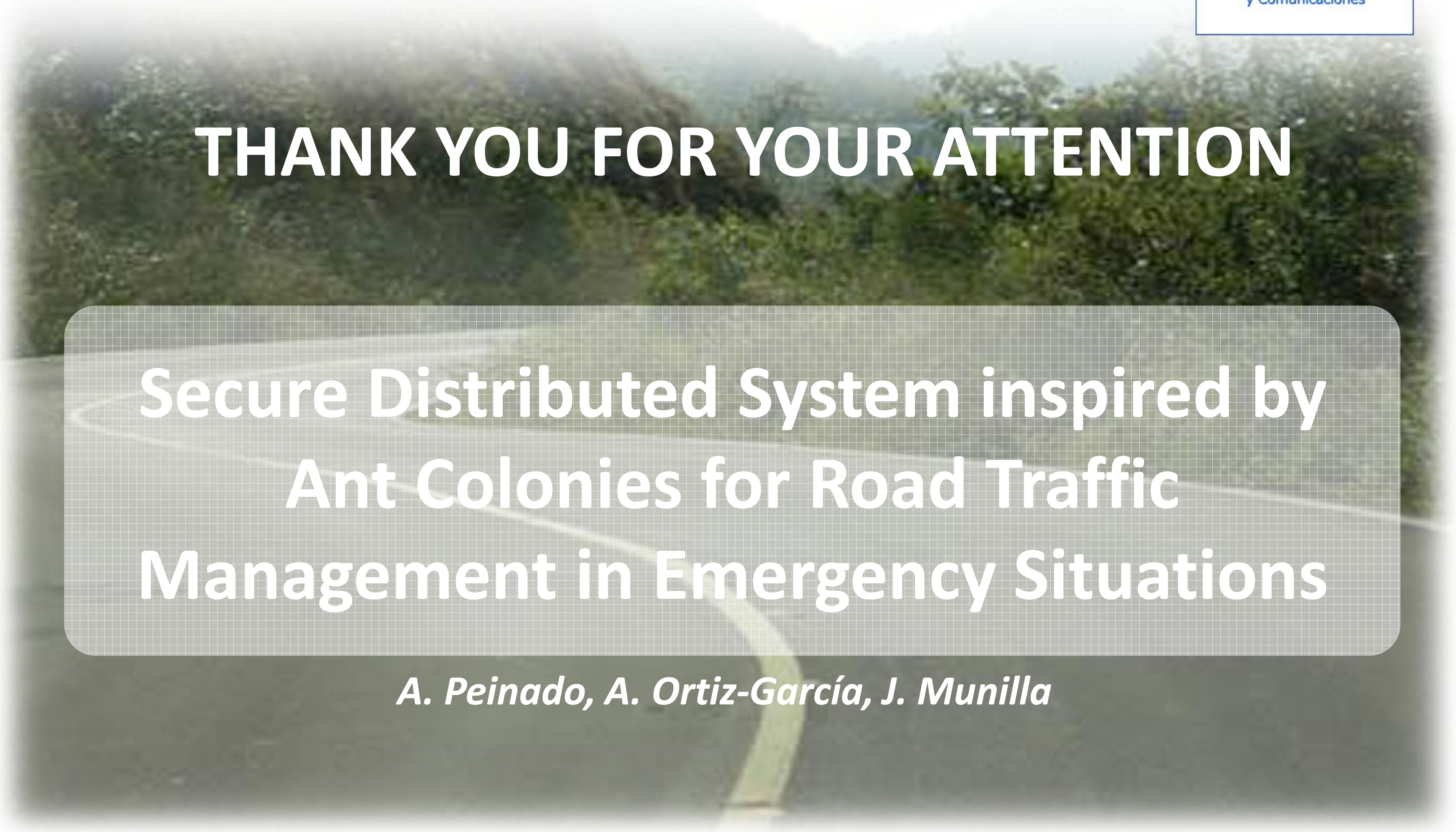
If traffic density is low, the attack is not effective since the nodes are not saturated.

If traffic density is high, the attack is not effective since others vehicles will retransmit the same Msg.

UNIVERSIDAD
DE MÁLAGA

SECURWARE 2013
August 25-31, 2013, Barcelona, Spain

ATIC
Grupo de Aplicación de las
Tecnologías de la Información
y Comunicaciones



THANK YOU FOR YOUR ATTENTION

Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

A. Peinado, A. Ortiz-García, J. Munilla

E.T.S.Ingeniería de Telecomunicación
Campus de Teatinos, 29071 Málaga

iC Ingenieria de Comunicaciones