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

A. Peinado, A. Ortiz-García, J. Munilla
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Contents

• VANETs and Road traffic management
• Model inspired by Ant colonies
• System proposed
• Prototype
• Security issues
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Supported by TICs
- Cameras
- Sensors
- Screens and displays

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

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

**VANET**
Vehicular Ad hoc NETwork

**VANET applications**
- Road Traffic Security
- Added-value and Comfort

Information from other vehicles
Traffic sign detection
Obstacle detection
**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
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

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

**Designed System:**
Distributed systems without infrastructure

- **COST-EFFECTIVE**
- **Emergency Situations**
Model inspired by Ant colonies

Ant Colonies

Food
Nest

Food
Nest

Food
Nest

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

**Location system**

**RFID**
Radio Frequency ID

**System proposed**

- **UHF Passive tags**
- **HF Passive tags**
- **LF Passive tags**

**General Features**

- Low cost
- Low storage capacity
- Low computational capacity
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

**Architecture**
Tag onboard
Reader on the road

**V2I**

**RFID**
Radio Frequency ID

**VANET**
Vehicular Ad hoc NETwork

**Location system**

Support system
RFID reader

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

**Architecture**

Reader onboard
Tag on the road

**I2V**

**Location system**

**RFID**
Radio Frequency ID

**VANET**
Vehicular Ad hoc NETwork
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Control places

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

**Information points**, $I_{\text{loc}}$: is assigned to points after the node.

**Decission points**: before the node.
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Pheromones generation

Broadcasted Message

ID_{SVeh}  ID_{loc1}

VANET communication

RFID communication

RFID tag (ID_{loc1})

RFID tag (ID_{loc2})
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Route Selection

Vehicle reads its internal variables

| ID_{loc1} | 80 |
| ID_{loc2} | 65 |

Vehicle reads its internal variables.
Disappearing Effect

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

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

<table>
<thead>
<tr>
<th>Location</th>
<th>Pherom.</th>
<th>Message arrival time</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>ID_{loc1}</td>
<td>80</td>
<td>12:31:45</td>
</tr>
<tr>
<td>ID_{loc2}</td>
<td>65</td>
<td>13:23:07</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

\( \Delta t \): Current time – Arrival time
\( \gamma \): Decreasing coefficient

New Pher. Level = Pher. Level - \( \Delta t \cdot \gamma \)
Real scenario:
Routes between two main hospitals in Málaga
- “Carlos Haya” University Regional Hospital
- “Virgen de la Victoria” University Clinical Hospital
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Prototype

Control places

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

- RFID tag – Decision places
- RFID tag – Pheromones Generation places
- RFID tag – Internal uses
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Security Issues

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

Weaknesses
- Fake messages (message injection)
- Fake content in authenticated messages
Security Issues

General Considerations

- Authentication is the main security mechanism
- Confidentiality is not necessary
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

Main threat

Fraudulent messages:
Authenticated messages with false content

Proposed Solution
Reputation lists and Data Aggregation

Vehicle receives Msg

$ID_{\text{Sveh}}$ in IRL?

YES

Msg is discarded

NO

$ID_{\text{loc}}$ consistent?

YES

Signature aggregation
Msg is retransmitted

NO

Agg. Sign.? 

YES

Msg is retransmitted

NO

Msg is included in IRL
Msg is discarded
Secure Distributed System inspired by Ant Colonies for Road Traffic Management in Emergency Situations

**Security Issues**

- **Vehicle generates pheromones**
  - **Any vehicle near?**
    - **YES**
      - **Broadcast Msg**
    - **NO**
      - **Msg is discarded**
        - **Delayed Msg are not allowed**
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.
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