Traffic classifier for Heterogeneous and Cooperative routing through WSN

Ana Nieto, Javier Lopez
nieto@lcc.uma.es

NICS Lab – University of Malaga
www.nics.uma.es
Wireless Sensor Networks (WSNs) are composed of specific-purpose constrained devices called sensors.

Sensors are autonomous units → they use an independent battery power → battery is a constraint.

Lifetime → time that a sensor/network is useful.

What is useful? For us:

- Sensors still alive → Sensor with battery
- Critical region accessible → sensors with access to the Sink node

Can WSNs deliver QoS-based traffic?

Lifetime is crucial in WSN since it determines network survival.

QoS-based traffic is the future.
Motivation

- Current approaches do not allow the deployment of collaborative sensor networks, where different sensors can work together to provide a common service (e.g. routing).

- Different data to be sent to the Sink require different paths to be efficiently sent through a WSN.

+ Functionality $\rightarrow$ QoS + Lifetime!!
Routing algorithm for WSN using traffic classification and role-assignment to enhance lifetime while improving QoS
- Traffic classification \(\rightarrow\) QoS requirements
- Role-assignment \(\rightarrow\) What a node can provide to the network

The information to be transmitted from \(s\) to \(d\) is sent using the path that best satisfies a criterion \(\rightarrow\) roles
Role assignment

- **Service-based roles** → to provide QoS guarantees
  - *Type of service* that a node can provide
  - *Result* of performing a node classification based on the characteristics allowable in the node to provide services → e.g. trust level

- **Behaviour-based roles** → to protect lifetime
  - Behaviour defined by the node
  - *Result* of a decision process performed by the node based on the resources allowable in the node to prolong the lifetime → e.g. battery
Traffic Classifier

- Similar to **role-assignment** but without considering behaviour-based roles
- The classification task is performed **locally in the node**
  - The data to be sent is tagged with a service-based role in origin
  - Only local information (QoS requirements) is used

This data requires to be **ciphered** and there are no time constraints

I need to exchange security data

I will **select** the best path available

- Based on the **decision process**
Traffic classification

Data type (e.g. security data)

Decision process based on the QoS requirements

Decision process to select the best NEXT (routing)

Role-assignment

What type of traffic can I deliver??

Repeat!!

Cooperative

“egoist”

Preferably none, I’m running out of battery
Decision Process

- **Local Decision**
  - Based on the **local resources** of the node
  - What a node can provide

- **Cooperative decision**
  - Based on information recovered from the **neighbour nodes**
  - We want to detect **clusters of services**

- **Example:**

<table>
<thead>
<tr>
<th>Decision Process</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Decision</td>
<td>Bayesian network</td>
</tr>
<tr>
<td>Cooperative decision</td>
<td>[ P(X)<em>n = \left( \frac{1}{V_n} \sum</em>{i=1}^{N} p(X)<em>i \cdot nb(n,i) \right) + KV</em>{nx} ]</td>
</tr>
</tbody>
</table>
Local Decision: Bayesian network

- **Roles:**
  - *Service-based roles*: security, control-information, real-time
  - *Behaviour-based roles*: charitable, egoist

- **Bayesian Network:**


\[
p(C) > U_c \Rightarrow S \text{ is charitable}
\]
Cooperative Decisions

- The decision process is based on:
  - Lifetime → Behaviour-based role → egoist node?
  - Maximum value of $P(X)$ → requirements
  - Direction to the destination node

- Routing algorithm
  - Ideally, the next node in the path (n), must satisfy:

\[
P(E)_n < U_E
\]

\[
P(X)_n \geq P(X)_i, \forall i \in \{k \mid nb(n,k) = 1\}
\]

We know the location of $d$!!!!

\[
\text{arccos}\left(\frac{a^2 - b^2 - c^2}{-2bc}\right) \leq 90
\]

- Lifetime preserving
- Best suitability
- Direction
Example: sending security data

- SB: Security
- BB: Charitable
- Control Information
- Real-Time
- Egoist
- Node in the path
Example: sending security data

SMPE 2012 – Fukuoka, Japan – March 28th
Example: sending security data

![Diagram of network with nodes and connections]

- Security
- Control Information
- Real-Time
- Charitable
- Egoist

Node in the path

SMPE 2012 – Fukuoka, Japan – March 28th
Conclusions and Future Work

- We have introduced R2WSN, a routing protocol for heterogeneous WSN by using traffic classification and role-assignment.

- R2WSN considers both: lifetime and QoS application preferences for data routing.

  - **Lifetime** is increased due to...
    - Role-assignment allows the node to declare itself “Egoist”
    - Role-assignment enables implicit load balance mechanism

  - **QoS restrictions** are performed due to...
    - Traffic classification enables the node to classify the traffic according its preferences
    - (load balance mechanism)

- We provide an example to perform traffic classification and role-assignment by using Bayesian Networks following our approach.