SOME NOTES AND PROPOSALS ON THE USE OF IP-BASED APPROACHES IN WIRELESS SENSOR NETWORKS

Tiago Camilo, Jorge Sá Silva and Fernando Boavida
Department of Informatics Engineering,
University of Coimbra, Coimbra, Portugal
tandre@dei.uc.pt

ABSTRACT

Wireless Sensor Networks (WSNs) are gaining visibility and importance in a variety of fields and they will certainly be part of our day-to-day lives in the near future. This trend is, in effect, putting WSNs under the research community spotlight. The feverish activity around WSNs has led to some myths and misconceptions over the last years that, in some way, have blocked the way forward. This paper addresses some of these myths and discusses a model for Wireless Mesh Sensor Networks that go beyond them, showing that it is time to look at WSNs under a different light. The paradigms that support the proposed model have a direct impact on the addressing scheme, mobility support and route optimisation. These have been put to the test both by simulation and prototyping, showing that they constitute solid ground on which future Wireless Mesh Sensor Networks can be built.

Keywords: wireless sensor networks, IP, ant colony optimization, anycast.

1 INTRODUCTION

Composed of a potentially high number of very small devices, Wireless Sensor Networks (WSNs) are one of the most promising technologies for the 21st century. Emerging WSNs make use of recent advances in electronic sensors, communication technologies and computation algorithms.

WSNs have unique characteristics, mainly due to their component devices, called sensor nodes. These nodes are typically small size devices with communication and monitoring capabilities, as well as limited resources, namely in terms of memory, energy and processing power. A node in a WSN consists of a sensor or an actuator that is connected to a bidirectional radio transceiver. In contrast to sensor nodes, sink nodes (special WSN nodes that act as central nodes which gather/distribute information) have fewer restrictions, allowing them to store relatively large amounts of information and perform highly demanding processing and routing tasks. These devices are responsible for managing the communication between a sensor network and its respective base station (wireless or wired).

Wireless Mesh Sensor Networks (WMSNs) aggregate several types of sensor nodes under a single working network, thus giving access to the data, information and/or services of each component in the WSN platform. In a typical mesh network each sensor node can communicate with more than one node, enabling better overall connectivity than in traditional star topologies. WMSNs are characterized by: offering a combination (mesh) of several types of nodes; being self-healing, since sensor nodes cooperate in order to automatically re-route their signals to the out-of-network node, thus ensuring a more reliable communication path; supporting multi-hop routing, since data can be forwarded through multiple nodes before it reaches a sink-node.

The overall performance of a sensor node is affected by the features of its components: battery, memory, processor, sensors and the receiver/transmitter. Hill et al. [7] grouped sensor nodes into four classes, depending on their physical size, radio bandwidth and memory size (Table 1).

Table 1: Sensor nodes classes [7]

Sensor Type	Size	Radio Bandwidth	Memory	
			Flash	RAM
Specialized sensing platform	mm3	<50 Kbps	0,1 Mb	<4 Kb
Generic sensing platform	1-10 cm3	<100 Kbps	0,5 Mb	<10 Kb
High-bandwidth sensing	1-10 cm3	~500 Kbps	10 Mb	<128 Kb
Gateway	>10 cm3	>500 Kbps	32 Mb	<512 Kb

Sensors like Spec

(http://www.jlhlabs.com/jhill_cs/), which are characterized by being extremely small, belong to the first class, the specialized sensing platform. This class covers sensor nodes that only perform monitoring and send their sensor data directly to the sink-node. Mote [9] devices are bigger and they can perform forwarding tasks. Such devices belong to the generic sensing platform class. High-bandwidth sensing nodes have more resources than the nodes belonging to the previous classes. However, the size of the device also increases, mainly due to the power supply. An example of an instance of such sensor class is the iMote [9] sensor node. iMote nodes have video, audio and air-monitoring capabilities. Lastly, the gateway class aggregates nodes that can execute all the above mentioned tasks and, additionally, support the interaction between the sensor network and the infrastructured network, being strategically placed between them. The devices from this class (e.g., Stargate, http://platformx.sourceforge.net) typically have several interfaces and make use of a more powerful energy source.

Security, traffic control, military strategy, industrial control, healthcare and habitat monitoring are examples of possible applications of WSNs and WMSNs. This wide range of applications requires that WMSN protocols are adaptable to their deployment environment.

This paper proposes a WMSN architectural model, named IPSense, which supports such adaptation requirements, namely by using flexible addressing, enhanced mobility and energy-efficient routing. IPSense also demonstrates that some of the myths associated with wireless sensor networks – namely: the use of multiple addressing schemes, the use of IP and the use of complex routing protocols have high cost – do not hold.

The following section identifies and discusses some of the WSN myths, their implications and possible ways to circumvent them. Section 3 presents the IPSense model, describing its key paradigms, features and approaches. These were put to the test by simulation and prototyping, and the results of that evaluation are presented in Section 4. Section 5 presents some conclusions and guidelines for further work.

2 MYTHS IN WIRELESS SENSOR NETWORKS

This section discusses some of the myths normally associated with WSNs. These are common misconceptions that, in general, limit the current use of this type of networks. This section analyses each issue from several angles, identifying real problems and possible ways forward.

2.1 WSNs Should Be Data-Centric

Three main communication paradigms can be used in sensor networks: data-centric, location-centric and node-centric [12]. WSNs are application-specific and, in general, use a data-centric communication paradigm, contrary to the node-centric approach followed by most networks, including ad hoc networks and the Internet. The node-centric approach is regarded as unsuitable to WSNs, as it generally relies in complex signalling/routing protocols. In the following, each communication paradigm is explained.

The data-centric communication paradigm is built on the data gathered by the sensor. In this case the observer is not interested in knowing which particular sensor replies to a specific query. Instead, the most important thing is to get the answer to the query. Therefore in protocols such as Directed-Diffusion [8], the user only needs to specify a certain condition when querying the network. The returned data can be provided by one or more sensor nodes, or even be an aggregation of sensor data gathered by a group of sensors. Data-centric communication provides the ability to specify various parameters, such as rate of publication, rate of subscription, validity of the data and many others. In short, this communication paradigm routing is based on the data provided by a sensor, not on the identity or on location of the sensor.

The location-centric communication approach uses the location of sensor nodes as a primary means for addressing and routing (e.g. CODE [13]). The co-operation between devices in a given area, performing local aggregation, takes a special role in this kind of communication. This paradigm is extremely dependent on positioning systems, such as the Global Positioning System (GPS), which may not always be feasible since it requires high amounts of energy. In addition, this type of communication approach may lead to increased cost and may be restricted to outdoor use. The most important advantage of this approach is related to the absence of routing tables in the network. Each node forwards packets based on the destination location. Such characteristic is very helpful in mobile scenarios, since mechanisms such as route discovery and routing updates are not required, decreasing the energy spent on control messages. However each sensor node has to know the correct location of intermediate and destination nodes.

Lastly, in node-centric communication sensor nodes are labelled with unique identifications, such as IP addresses, which are used to populate the routing tables and to perform packet forwarding. This communication paradigm is the "traditional" communication method nowadays used in the Internet, throughout wired and wireless networks. Due to its characteristics, it is possible to perform hierarchical addressing, creating simpler routing schemes. However this approach is the less used in WSNs/WMSNs environments since it can lead to considerable amount of control traffic, which will dramatically reduce the network lifetime. Nevertheless, it has the advantage of enabling global connectivity and the support of well know IP-based protocols.

Each of the presented communication paradigms has advantages and drawbacks and, contrary to common belief, they all can be applied to WMSNs. It is up to the WMSN developer to choose the best approach that fulfils the application requirements. It is important to note that hybrid solutions can also be applied, where the conjunction of two or more communication models can lead to specific benefits.

2.2 IP is to Complex to WSNs

The main motivation for using IP in WMSNs is global connectivity. Such use would greatly increase the potential for interaction between sensors and observers, allowing the latter to access the gathered data from virtually anywhere, in what is normally known as a 4G scenario. Nevertheless, IP was not designed for energy-restricted, low-memory and low-processing-power devices, which has led to the belief that IP is too complex for WSNs/WMSNs. In spite of this, an increasing number of researchers are looking into the use of IP in sensor networks due to the potential that it represents.

There exist several differences between IP-based networks and the current WSN/WMSN models. On one hand, the broad applicability of WMSNs has led to architectural models that are application-specific. On the other hand, WMSNs are, by nature, data-centric systems, where sensor data is the key for the routing mechanism. This is not the case in an IP-based network, where devices/applications are reached through the use of IP addresses, which are application-independent.

In IP-based networks the communication is typically performed on a one-to-one basis, with the possibility to support one-to-many interactions in the case of multicast. On the other hand, in WSN/WMSN communication is usually of the many-to-one or one-to-many types, since sensor nodes usually transmit to a single point, the sink-node which, in turn, queries sensor nodes. Such behaviour considerably reduces the amount of data transmitted over the network.

In IP-based networks, bandwidth is the most important obstacle/restriction, due to the amounts of data transferred between elements (video, sound, etc). In WMSNs the amount of data transferred between devices is typically small. Moreover, there can be relatively long periods of time with no data exchanges.

WMSNs are very peculiar regarding the development phase. Contrasting with most networks, the nodes location is very important, and in some cases it has a direct impact on the network lifetime. Typically, WMSNs need to be self-configured and unattended due to the fact that access to sensor nodes is not always possible, contrary to IP-based networks where administrators know the nodes physical location and frequently access them.

The most common approach to integrate WMSNs with IP-based networks is to incorporate a proxy between the two networks (e.g. [15]). This element acts as a protocol translator, allowing inter-network communication. The proxy needs to understand the protocols of the networks that it interconnects: the IP stack and the protocol stack used within the WMSN (Fig. 1). Strategically placed, the WMSN/IP proxy acts as a database (normally through software), collecting and storing the monitored data provided by the sensors nodes.

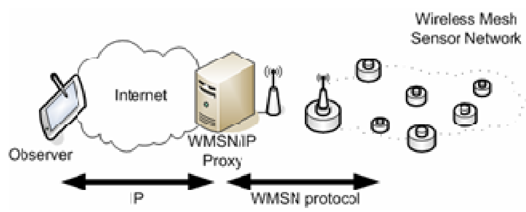


Figure 1: Proxy WMSN/IP architecture

This architecture provides access to the collected data through the use of standard TCP/IP protocols, without losing the capability to create application-specific protocols for the WMSN. However, the proxy architecture is based on a single, centralized access point, leading to problems in terms of reliability, scalability and mobility support.

The main problems that are commonly pointed out when direct support of IP in WMSNs is concerned are: lack of available addresses, lack of configuration management, and energy efficiency due to heavy processing required by the IP stack [3]. Nowadays, solutions for each of these problems exist, namely the use of NAT mechanisms, the use of the Dynamic Host Configuration Protocol, and the use of efficient and thin IP stacks. Computational limitations and low memory resources are commonly pointed as limitations to a full support of the IP stack in WSNs [2]. However the work performed in [5] with the μIP TCP/IP, proves the feasibility of such integration. Developed to be executed in 8-bit micro-controllers, this stack allows nodes to directly communicate with full-IP devices, as illustrated in Fig. 2.

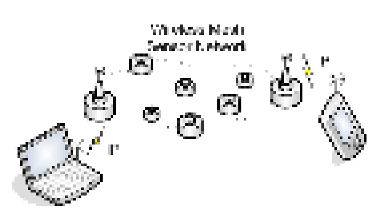


Figure 2: IP-based WMSN

By endowing sensor nodes with IP addresses, they will be able to benefit from the main capabilities of this protocol. In this model de communication between mobile devices and mobile nodes is completely transparent. Neither tunnel mechanisms nor intermediate devices are required to perform the protocol translation. Sensor nodes are accessible from any other IP-capable device, such as a PDA.

Although IP seems to be a viable protocol for micro-controllers, the IP header is too large when compared with the typical size of data packets exchanged between sensor nodes. The overhead can reach up to 90% [6]. However, it is possible to use compression mechanisms to reduce the total message size [10].

2.3 IPv6 Is Even More Complex And Can Hardly Be Used In WSNs

When developing a WMSN, it is important to have scalability in mind. WSN/WMSN networks with up to 1000 sensor devices will be quite common in the future. With these numbers, it is unfeasible to use public IPv4 addresses on each device, which is why NAT mechanisms may be a solution. However, such solution also has drawbacks in terms of end-to-end transparency, security, performance and processing time.

Using IPv6 in WMSNs would allow us to overcome some of the IPv4 limitations and would open a whole new range of possibilities. The large address space available with IPv6 would allow us to assign public addresses to all sensor nodes, eliminating the need for NAT. Communication between sensor nodes and external devices would be done without intermediate nodes, protocol translation or proxies. In contrast with IPv4, the IPv6 header is designed to keep the overhead to a minimum, by shipping unused fields to extension headers.

One important property in WMSNs is the lack of network management. After the deployment of sensor nodes, it becomes unfeasible (in most scenarios) to perform administrative operations, such as to choose the best configuration (e.g. routing) for each node. Therefore it is important to use auto-configuration mechanisms such as the Neighbour Discovery Protocol and other auto-configuration facilities natively found in IPv6.

Finally, IPv6 provides a new type of address, the anycast address. The use of anycast addressing is normally associated with fault tolerance mechanisms, where the same service is provided by more than one device, all using the same IP address. A packet destined to an anycast address is delivered to the "best" interface, from all those using the same anycast address.

In spite of the general belief that IPv6 is too complex for WMSNs, part of the IPv6 features can be easily ported to this type of networks at reduced cost, boosting the usefulness of IP in WMSNs. Mobility support and auto-configuration are just two examples of IPv6 features that can be extremely useful in WMSNs.

3 THE IPSENSE MODEL

This section presents a model – which, for ease of reference we will call IPSense – for WMSNs that uses and explores paradigms that are contrary to the myths and misconceptions presented in the previous sections. Specifically, IPSense has the following features:

- Global connectivity, through the use of IP-enabled nodes;
- Support for all the addressing paradigms mentioned in the previous section;
- Mobility and Auto-configuration support;
- Optimised routing;
- Reduced protocol overhead;
- Energy-efficiency.

The following sections detail the IPSense model.

3.1 Sensor Router And Mobility Support

IPSense explores sensor node aggregation in clusters, through the use of Sensor Routers (SRs), in order to manage the communication between the cluster members and the access point, located in the wired/wireless network (Fig. 3). Sensor Routers are gateways between wireless sensor networks and the outside world comprising a whole range of heterogeneous networks (Fig. 4). SRs are special devices that have more powerful hardware capabilities when compared to sensor nodes, in what concerns energy, memory and processing power.

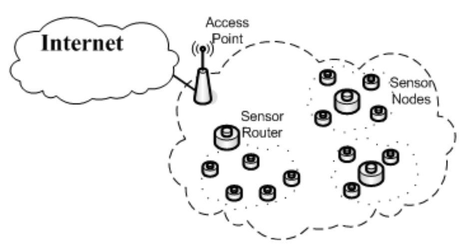


Figure 3: Sensor Router concept

Sensor routers are responsible for configuring the sensor nodes in their own sub-network. Each node will be provided with one IPv6 unicast address and a set of IPv6 anycast addresses. Unicast addresses allow the unique identification of each sensor node. Anycast addresses are assigned according to the device sensor properties, thus providing an efficient way to address sensor nodes with similar capabilities. The Sensor Router concept is fundamental to guarantee energy efficiency in WMSN networks. By concentrating energyexpensive communication between WMSN and wired/wireless networks in a dedicated element, it is possible to considerably relax the energy management and communication requirements of sensor nodes, allowing them to efficiently deal with sensor operations and local communication.

The proposed mechanism provides to the mobile sensor router the possibility to be contactable anywhere by its home IP with the minimum control updates procedures. All the heavy tasks maintaining the routing tables updated are performed by more capable sensor nodes.

In addition, SRs can easily provide mobility support inside the sub-networks, according to the network mobility model developed by IETF's NEMO working group [17]. In this context, SRs play the role of Mobile Routers, managing several tasks: route IPv6 unicast addresses, forward IPv6 anycast addresses, map unicast/anycast addresses, and act as gateway between the Internet and WMSNs. WSN mobility support opens the possibility to monitor different types of mobile phenomena such as migrations or vehicle movement. In a typical mobile sensor environment, possible issues are the location of each individual node or the location of the whole sensor network. Such features are normally supported by complex protocols that require considerable power. To overcome this problem, IPSense explores the use of some of the Mobile IPv6 characteristics in Sensor Routers.

The role of the home agent is made by one or more entities - the Mobile Responsible Sensor Router (MRSR), in order to provide redundancy, which will be responsible to concentrate the mobility information. This entity should be elected among sensor routers, that choose the sensor router that provides more resources. In fact the network gateway is the best node to provide such operations, but should not be chosen alone due to the wired restriction. The primary MRSR is responsible to respond (only if necessary) to the CN request with the new CoA of the moving sensor router. Moreover it is also responsible to maintain updated the mobile information among the secondary MRSRs.

Whenever a sensor router is informed that a moving router entered in its network, it configures the new sensor node with a local address and it informs the nearest MRSR, regarding the new mobile element in its network (Fig. 4, step 3). This information carries the home IP address (the unique identification) and the new CoA. The MRSR that receives this information will inform the primary MRSR (Fig. 4, step 4) that floods this information among the remaining MRSR (Fig. 4, step 5).

3.2 Addressing Scheme

IPSense combines the three WSN communication paradigms mentioned before. It supports the ability to communicate and to interact with a specific sensor, using IPv6 addresses, according to the node-centric routing approach. The use of anycast addresses supports the two remaining routing paradigms in WSNs: data-centric and location-centric.

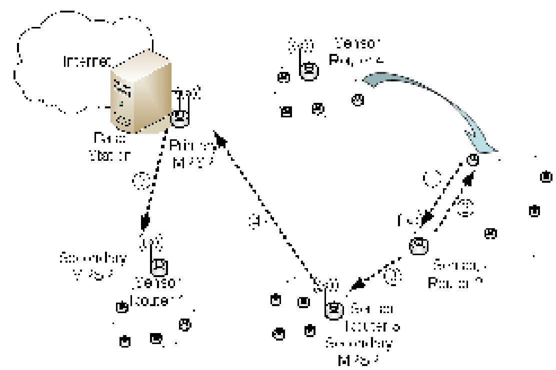


Figure 4: Connectivity model between IPSense and 4G networks

3.2.1 Anycast addressing

IPSense enables the association of IPv6 anycast addresses to specific services or locations. Therefore it is possible to associate an address to devices with the same sensing capabilities, such as video, sound and temperature. Such addressing scheme can also be useful to determinate which functionality a specific sensor node can offer, just by inspection of the list of its anycast addresses.

When an observer needs to know the values of some monitored parameter (e.g., humidity), a query is made with the IPv6 anycast address associated to such service. The message is routed to the node that is best positioned to respond to such query (Fig. 5), e.g., the sensor node belonging to that specific anycast group with highest remaining power or the sensor node closest to the SR.

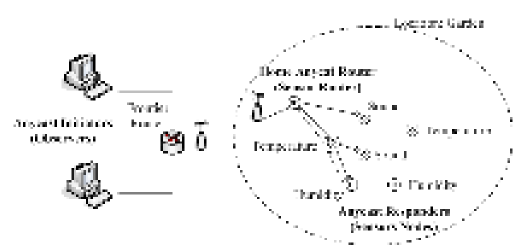


Figure 5: Anycast addressing scheme

This procedure is based on the concept presented by Ata et al. [1], where new network architecture is proposed to solve known inter-domain anycast problems. The authors propose the addition of a new element, the Home Anycast Router (HAR), which is responsible for forwarding packets to its network prefix (Fig. 6). This device has to be placed in the incoming/outgoing network link of the group of devices configured with anycast addresses, the

Anycast Receivers (ARs). The HAR is configured with one unicast address, the unique identification, and with a set of anycast addresses that are equal to the anycast addresses configured in the ARs. The Anycast Initiator (AI) is the node who wishes to communicate with one AR. It can be located inside or outside the network managed be the HAR.

In IPSense we propose to delegate the HAR competences in the SR, which is the device responsible for a group of sensor nodes, the ARs. The AI will be the mobile/wired device used by the observer to collect monitoring data from the WMSN.

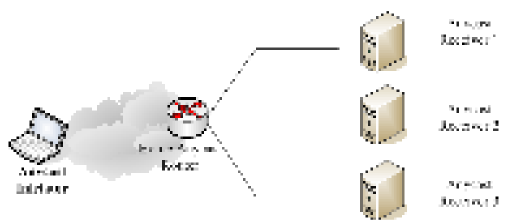


Figure 6: IPv6-based global anycasting architecture

IPv6 was initially designed to support geographic addresses [1]. By assigning IPv6 to well known geographic places, it is possible to create a networking map representing the specific place of each access point. This can be explored in the SR scenario by assigning a specific geographic network prefix to each SR (Fig. 7). This association is valid for fixed and mobile networks, since the network management is located in the network border, being the SR the only responsible for the forwarding of the outgoing traffic.

The SR carries out a set of tasks: build and manage routing tables, assign anycast addresses, perform the correspondence between sensor types and anycast addresses, forward unicast and anycast packets in both directions and, finally, manage its sub-network in terms of energy levels.

By combining sensor type and sensor location, the IPSense model allows the observer to query a specific type of sensor (e.g. humidity) from a specific location (e.g. the garden) just by specifying one anycast address. This approach has the potential to deal with several disperse sub-networks at global scale, without loosing contact with the sensor nodes, adopting a uniform, universal, IP-based paradigm.

3.2.2 Unicast Addresses

Another important aspect is the ability to communicate with one specific node directly. This is only possible due to the unicast address configuration. Each node will be assigned, as already described above, not only anycast addresses, but also one unique identifier, one unicast address that will be used to identify the sensor node outside/inside the network.

From an energy-efficiency perspective, it is not feasible to use the native IPv6 128-bit addresses for communications between sensor nodes. Therefore intra-WSN communications should use MAC addresses (64 bits) or the reduced address identification (16 bits) proposed by the IETF 6LoWPAN working group [11]. Whenever an observer intends to communicate directly with one specific sensor node, the SR translates the destination address from the 128-bit address to the corresponding internal address (64 or 16 bits). Header compression techniques are also necessary to reduce the impact of IPv6 headers on WMSN packets. In [5] the authors suggest the use of an additional field that codes the unnecessary fields in the communication between two link-local nodes.

3.2.3 Auto-configuration

Sensor node configuration is one of the critical factors in WMSNs. It is fundamental to find configuration mechanisms that do not require human intervention. IPv6 natively supports address and network prefix configuration. This is based on IPv6 link-local addresses [16], which are plug-and-play addresses formed by the combination of a network prefix and a 64-bit MAC address.

In the IPSense model, a typical address is divided into three parts, as illustrated in Fig. 9: network prefix (which should be less than 64 bits), MAC address, and an intermediate space that will be used to identify the type of address (anycast or unicast). This intermediate address space should also be used to identify the anycast service: location or type of service. Unicast addresses (unique identification) are formed as illustrated in the figure: the intermediate space should be field with zeros.

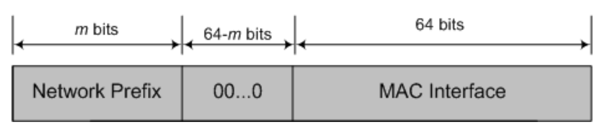


Figure 7: Formation of the unicast/anycast address

The anycast address configuration is more complex than the unicast address configuration. To each node is assigned a group of anycast addresses according to its own capabilities. For example, if a sensor node supports the monitoring of three distinct parameters, it will be assigned at least three anycast addresses, each one representing one type of parameter. The anycast assignment occurs only after the sensor node has acquired the unicast global address. It is the responsibility of each node to inform the SR of all its capabilities.

A sensor node requires a new unicast/anycast address in any of the following situations:

- The interface is initialized at system start-up
- The interface is restarted after a temporary system fault

- The system administrator activates the interface after an inactivity period.

3.2.4 Ant colony route optimization

IPSense proposes a route optimisation algorithm tailored to the needs of WMSNs, called Ant Colony Route Optimisation (ACRO). This protocol is based on the Ant Colony Optimization heuristic [4] that uses a model based on the behaviour of ant colonies. Ants are insects with simple individual behaviours and efficient processes for individual survival but, as a colony, they can create complex organizational systems, where each ant plays a specific part that is essential to the survival of its anthill.

Ant Colony Optimization (ACO) is based on the observation of real anthill behaviours, more specifically in the way ants find the shortest path between the food and the anthill. To bring food to the anthill, the ant colony solves an interesting optimization problem. Initially, ants randomly course the region near the anthill searching for food. Each ant, while travelling its path, places a chemical substance in the soil named pheromone, creating a pheromone trail. The following ants detect the present of this substance and tend to choose the path marked with the bigger concentration of pheromones. These substances enable the formation of the return path to the ant and inform other ants about the best paths to the food. After a period of time, the more efficient paths (paths with the shortest distance to the food) will have a bigger pheromone concentration. Conversely, the less efficient paths will have a lower pheromone concentration, due to the smaller number of ants travelling those paths and also because of the natural pheromone evaporation. In the optimization problem that the anthill has to face, each ant is capable of building a complete solution for the problem. However, the best solution is achieved with the information gathered by the colony as a whole.

In the IPSense model, each node belonging to an SR sub-network generates an ant *k* (control packet) at regular intervals, which travels through the network, jumping from sensor to sensor until it reaches the SR. At each sensor router *i*, the ant chooses the next sensor node *j*. At each node *r*, a forward ant selects the next hop using the probabilistic rule presented in (1). The identifier of every visited node is stored in M_k and carried by the ant.

$$p_k(r,s) = \begin{cases} \dfrac{[T(r,s)]^{\alpha}[E(s)]^{\beta}}{\sum_{u \notin M_k}[T(r,u)]^{\alpha}[E(u)]^{\beta}} & \text{if } s \notin M_k \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where $p_k(r,s)$ is the probability that ant *k* chooses to move from node *r* to node *s*, *T* is the routing table at each node that stores the amount of pheromone trail on the (*r,s*) path, *E* is the visibility function given by $(C - e_s)^{-1}$ (C is the initial energy level of the nodes and e_s is the actual energy level of node *s*), and α and β are parameters that control the relative importance of trail versus visibility.

The selection probability is a trade-off between visibility (which means that nodes with more energy should be chosen with high probability) and actual trail intensity (that means that if on the *(r,s)* path there has been a lot of traffic then it is highly desirable to use this path).

Each sensor node records the travel data of each forward ant: the previous node, the forward node, the ant identification and a timeout value. Whenever a forward ant is received, the node searches its memory for a record of that specific ant, to detect possible loops. If no record is found, the node saves the required information, restarts a timer, and forwards the ant to the next node. If a record containing the ant identification is found, the ant is eliminated. When a node receives a backward ant, it searches its memory to find the next node to where the ant must be sent. The timer is used to delete the record that identifies the backward ant if, for some reason, the ant does not reach that node within the time period defined by the timer. Each ant k carries information on the average energy available on the path that ends in the current node (*EAvgk*), and the minimum energy level registered in that path (*EMink*). These values are updated at each node that receives forward ants, and they will be used to calculate the pheromone parameters. When a forward ant reaches the SR, it carries information regarding the travelled path. The SR uses this information to determinate the quality of the path, following an optimization function, which considers the main WMSN limitations (i.e. energy). Before a backward ant *k* starts its return journey, the destination node computes the amount of pheromone trail that the ant will drop during its journey, using (2):

$$\Delta T_k = \frac{1}{C - \left[{EMin_k - Fd_k} \big/ {EAvg_k - Fd_k} \right]} \quad (2)$$

where *C* is the maximum energy level of nodes and *Fdk* is the distance travelled by the forward ant *k* (the number of nodes stored in its memory). Whenever a node *r* receives a backward ant coming from a neighbouring node *s*, it updates its routing table by using (3).

$$T_k(r,s) = (1-\rho)\cdot T_k(r,s) + \left[{\Delta T_k} \big/ {\varphi \cdot Bd_k} \right] \quad (3)$$

where ρ is a coefficient such that *(1 - ρ)* represents the evaporation of trail since the last time

Tk(s,r) was updated. *φ* is a coefficient and *Bdk* is the travelled distance (the number of visited nodes), by backward ant *k* until node *r*. These two parameters will force the ant to loose part of the pheromone strength during its way to the source node. The idea behind this behaviour is to build a better pheromone distribution (nodes near the sink-node will have more pheromone levels) and will force remote nodes to find better paths. Such behaviour is extremely important when the sink-node is able to move, since the pheromone level adaptation will be much quicker.

The Ant Colony Route Optimisation approach combines mobile agents (ants) with the Ant Colony Optimization heuristic, and finds the best routing path between two nodes based on a specific optimization function. This routing algorithm is extremely adaptable, since it uses an optimization function that the administrator/observer can change according to the goals. It is possible to build paths based on energy-efficiency, as the example presented above, but by changing (2) the algorithm can focus on QoS, for example, choosing paths according to the available bandwidth or other parameters.

4 BREAKING THE MYTHS

In a way, IPSense intends to 'break the myths' presented in section 2. In order to do so, it is necessary to subject this model to a series of tests that prove the feasibility of the underlying ideas and shows that they do not lead to performance problems. These testing procedures were, in fact, carried out, and the results are presented in this section. These were obtained by simulation and prototyping.

4.1 Mobile IP Based Protocols In WSNs

In a first phase it is important to understand the implications of using well-known mobile ad hoc protocols in WSN environments. Therefore, realistic scenarios were simulated in order to study the behaviour of such protocols in static and dynamic environments.

In a first set of simulations, the sensor nodes were randomly distributed over a square area (1000mx1000m), they remained static during the entire simulation runs (300 sec) and the only moving entity was the phenomenon, here simulating a moving bird that stimulated the sensors by its chip. In the second scenario all the sensors were moving entities, simulating the movement of a group of birds (each sensor representing a moving bird).

To simulate the movement of birds, the authors adapted the boids model, produced by Reynolds (http://www.red3d.com/cwr/), to NS-2. This model simulates the coordinated movement observed in groups of animals, e.g. birds and fish. The model is based on a decentralized management, where each individual provides instructions to its neighbours, and the behaviour of the group results from the combined action of each individual. Reynolds identified three simple rules that, when followed by each individual member of a group, result in a behaviour that closely follows the one observed in groups of wild animals. In each scenario, well known ad hoc protocols were used: the Destination Sequence Distance Vector (DSDV) protocol, representing the group of Table Driven Routing protocols, and the Ad hoc On-Demand Distance Vector Routing (AODV) protocol, from the group of On-Demand Routing Protocols. In each scenario one of the sensor nodes was randomly elected as the sink-node. This device was responsible for collecting all the monitored data provided by the entire WMSN. In each simulation run, eight network sizes were used, from 25 nodes up to 200 nodes per network. The following parameters were used on each node.

- sensing power = 0.00000175 mW;
- transmitting power = 0.175 mW;
- receiving power = 0.145 mW;
- idle power = 0.0 mW;
- initial energy = 0.5 J;

As previously mentioned, the main goal of this study was to evaluate existing ad hoc protocols, in a realistic WMSN deployment scenario, including highly dynamic environments. Therefore, energy consumption, being one of the most restrictive parameters in WMSNs, was part of the study. The results are illustrated in Fig. 8, where static and mobile scenarios are compared. The remaining energy is calculated by adding the energy levels from all the sensor nodes at the end of the simulation.

In mobile environments using the AODV protocol, the network became very unstable as we reached 100 nodes, dropping until only 14% of total energy in the end of simulation. With more sensor nodes the network became inactive during the simulation, due to the high number of nodes that drained their energy. With 200 nodes the DSDV protocol still kept the energy level at 56% of the initial energy in mobile scenarios, contrasting with the very good performance in static scenarios (the remaining energy was 83% of the initial energy).

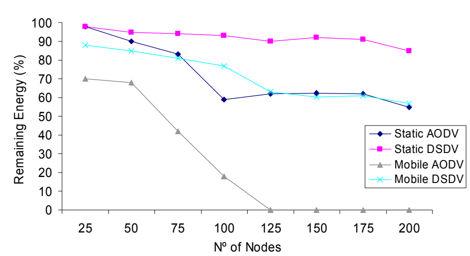


Figure 8: Remaining energy vs. network size

In terms of packet delivery ratio, the DSDV protocol, once again compared to the AODV protocol, led to better results. Fig. 9 presents the number of packet drops per protocol for each scenario. In the mobile scenario packet drops grow exponentially. AODV with 125 nodes already presents 60.000 packet drops, and it stays at this level up to 200 nodes due to the energy behaviour registered in the previous study. On the other hand, DSDV presented better results in both scenarios. In static environments the increase of sensor nodes resulted in a relatively small increase in the number of dropped packets. However in the mobile scenario, an exponential growth was observed

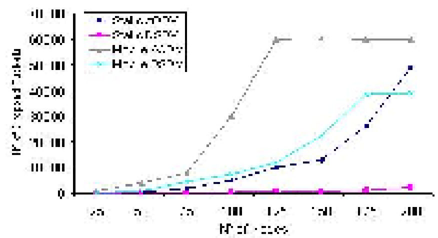


Figure 9: Dropped packets vs. network size

All the results suggest the need to create a new protocol, capable of minimizing the number of lost packets and of reducing energy consumption in scenarios where the sensor nodes have mobility and IP support. By analyzing the well known WSN mobile protocols (SENMA and MULE [14]) it is possible to conclude that they present limited capabilities and are not the most adequate to dynamic WMSNs. In the SENMA architecture, the integration of mobile agents, such as little airplanes, reduces the WMSN applicability. On the other hand, the MULE model presents a new element in the WMSN architecture, with specific characteristics, which may be difficult to find in the phenomenon environment. Therefore, there exists the need to study new protocols that natively support mobility, and from all the WMSN elements perspectives: phenomenon, sensor, network and observer movement. Only by supporting such characteristics will it be possible to make a true integration of the WMSNs in heterogeneous systems.

4.2 IPv6 In WMSNs

The second study addressed the use of IPv6 in WMSNs, when compared to the use of IPv4. IPv6 packets have a 40-bytes header (without extension fields), 20 bytes more than the IPv4 header. The study was carried out both by simulation and by prototyping.

In order to use a network topology that minimized the number of lost packets, the sensor nodes were strategically distributed in a grid layout (1000m x 1000m). This deployment strategy is not realistic. However, the main goal of this simulation was to study the advantages and drawbacks of IPv6 in WMSNs, in a controlled environment. The grid spacing was 100 units (*d*) and 100 sensor nodes were deployed, each with a radio range of 141.4 units (derived by $\sqrt{2d^2}$), and with up to 8 neighbours. The phenomenon was simulated by using a moving device that stimulated the sensor nodes every 2 seconds, which could be representative of a moving animal. After being stimulated by the phenomenon, each sensor node forwarded the data to the sink-node using the well know ad hoc protocol AODV. The sink-node was placed in one of the edges of the grid, and it had no energy restrictions. The simulated time was 100 seconds and the energy-related parameters were the same as in the previous study. Different levels of packet lengths were considered: from 32 bytes to 256 bytes (802.15.4-based devices use 127-byte packets). The first set of results (Fig. 10) compares the network remaining energy percentage as a function of packet length. This was achieved by summing the remaining energy in all nodes. In the scenario with 32-byte packets the remaining energy was 5.6% of the initial energy, contrasting with 3% when using 256-byte packets.

Fig. 11 illustrates the percentage of nodes that, at the end of the simulation, still had energy levels capable of monitoring the phenomenon. Due to the nodes and sink-node geographic distribution and the phenomenon movement, the first sensors achieving null available energy were the devices placed in the middle of the grid. As the packet length grew, the number of sensor nodes unable to transmit also increased. The last graph presents packet losses in the simulated network (Fig. 12). Losses are mainly due to the protocol characteristics, but they also reflect the increasing number of dead nodes in the communication path between the excited node and the sink-node.

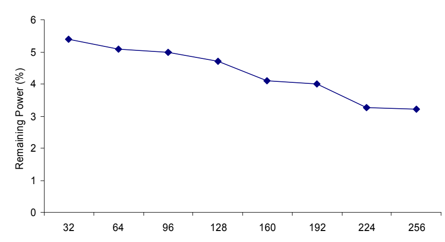


Figure 10: Remaining energy vs. packet length

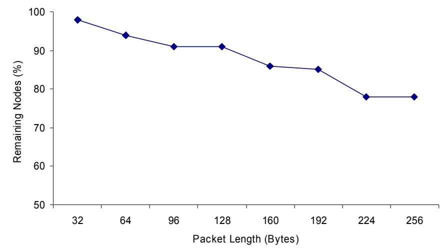


Figure 11: Remaining nodes vs. packet length

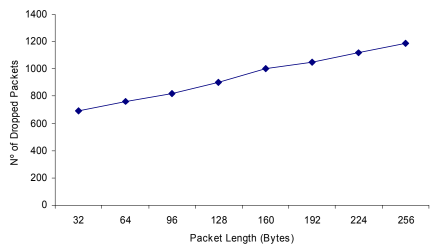


Figure 12: Dropped packets vs. packet length

The use of an additional 32 bytes (i.e. the 32-64 bytes interval) represents an increase of 9.4% in the packet losses, at the end of the simulation. Such difference in packet length leads to a decrease in the remaining energy of only 4% of the initial energy.

For the prototype, Embedded Sensor Boards (ESB) (http://www.scatterweb.net) nodes were used, running the Contiki operating system (http://www.sics.se/~adam/contiki/). In this study, sensor nodes were excited by a phenomenon that moved in a uniform way. Each time a sensor detected movement an UDP packet was sent to the sink-node, in a point-to-point communication. Two types of connections were used: wired connection using SLIP, and wireless connection.

Fig. 13 and 14 present the results of the experience in terms of number of sent packets and battery time, respectively. As can be seen, the wireless communication case leads to better results, mainly due to the low energy consumption of the TR1001 transceiver used in this case, and also the relatively high number of SLIP control packets.

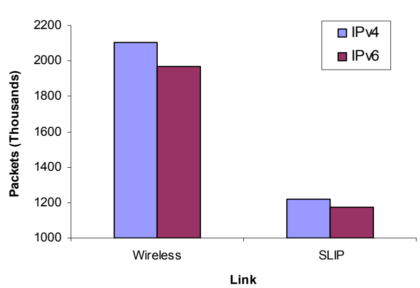


Figure 13: Number of packets sent by IPv4 vs. IPv6

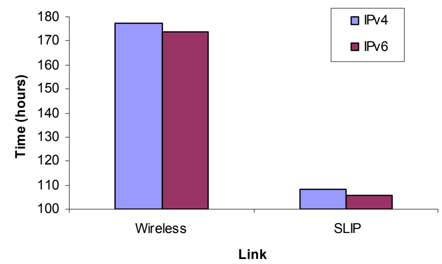


Figure 14: Battery time

In what concerns energy consumption, it is possible to observe that the results obtained in the prototype implementation do not differ from the ones obtained by simulation. In wireless environments, IPv6 leads to an excess energy consumption of only 1% when compared to IPv4. In the wired scenario the difference is even lower.

Packet reception is also different for both technologies. When connected via SLIP, packets are sent without any validation or control, which causes them to arrive with errors at the receiver in the final portion of the test. When connected via wireless, packets either arrive correctly or are lost.

From the results presented above we can conclude that the use of IPv6 does not have a decisive effect on the ESB platform. All values obtained have marginal differences, perfectly acceptable when compared to the advantages IPv6 can bring to wireless sensor networks.

4.3 Ant Colony Route Optimization Testing

This section presents the experimental results obtained in the tests made to the Ant Colony Route Optimisation (ACRO) protocol presented in section 3.3. In a WMSN, energy is a vital resource. This is why it is necessary to use a protocol that, in addition to being compatible with IP, is energy-efficient. In this study we compared the ACRO protocol with the IP-aware well-known ad hoc protocols AODV and DSDV.

In order to better understand the efficiency of ACRO, two test cases were used. Both simulations used the same node configuration, already presented in earlier tests. However, in order to have a more realistic scenario, the nodes were charged with different initial energy levels, namely 100, 75, and 50 J (one third of the nodes were charged with each of the three energy levels). In each simulation run different network sizes were used, from small networks with 10 nodes up to 100 nodes per network. In all cases nodes were deployed in a random fashion (in a 600mx600m field), since in most real WSN deployments sensor locations cannot be controlled by an operator. The location of the phenomenon and the sink-node were not known. Nodes were responsible for monitoring the phenomenon and sending the relevant sensor data to the sink-node.

Four metrics were used to compare the energy performance of the protocols under study: average final energy (the average of the nodes' energy at the end of simulation); minimum final energy (the energy of the node with the lowest energy at the end of simulation); final energy standard deviation (the standard deviation of the various energy levels of the nodes); and energy efficiency (the ratio between the total final energy and the number of data packets received by the sink-node).

The first scenario simulates a randomly deployed WMSN monitoring a static phenomenon, which excites one of the sensor nodes at 30000 bits/sec for 100 seconds. At the end of the simulation, different numbers of packets were delivered to the sink-node by each of the three routing protocols. ACRO presented always the best ratio between the total final energy and the number of delivered packets, as illustrated in Fig. 15 d). This is in agreement with the values obtained for the average energy parameter: once again ACRO presents the best results (Fig. 15 a)), and the gain is more visible in bigger networks (e.g. 50 to 100 nodes). In networks where the energy level varies it is important that the used protocol has some form of balancing these levels, by using nodes with more energy more often than nodes with less energy. The better performance of ACRO is also apparent in Fig. 15 c) (standard deviation), and Fig. 15 b) (minimum energy).

The second study introduces mobility to the phenomenon. Therefore, the nodes were excited by a mobile device. Once again, node and sink locations were unknown. The phenomenon moved randomly in the field. In this scenario, the difference in the final results, presented in Fig. 16, became smaller. However, the ACRO protocol still led to the best results in all categories. Moreover, similarly to what happened in the previous study, in this simulation the difference between the protocols' performance increased with the network size.

These results show that ACRO has clear advantages over the well-known AODV and DSDV routing protocols, in what concerns energy efficiency and packets delivery ratio.

5 CONCLUSIONS

In this paper we addressed several issues currently influencing the effective deployment of WMSNs. Some of these issues result from misconceptions or clichés that are or will shortly become outdated.

We argued that WMSNs should have global connectivity, through IPv6 deployment in Sensor Routers, mobility support (also through Sensor Routers), multiple addressing schemes (data-centric, node-centric, and location-centric), auto-configuration and energy-efficient routing. These features were combined in a proposed model, called IPSense. We have proved that these features are worth exploring and are feasible, by simulating and implementing them. The tests addressed the use of IP-based approaches in WSNs, the impact of IPv6 when compared to IPv4, and the energy and transmission performance of the Ant Colony Route Optimisation protocol relative to other well-known WSN routing protocols. The results have shown that the proposed model has clear benefits with low cost.

Our future work will address new methods to adjust WMSNs characteristics/capabilities with the environment (deployment scenario) variables. By adopting a flexible algorithm, such as ACRO, it is possible to create routing paths based several criteria, including the network characteristics and ambient conditions. Therefore, by creating a system capable to be adaptable to several conditions, we intend to increase the lifetime of the WMSN, without the need of human interaction.

ACKNOWLEDGEMENT

The work presented in this paper is partially financed by the Portuguese Foundation for Science and Technology, FCT, under the 6MNet POSI/REDES/44089/2002 project, and by the IST FP6 CONTENT Network of Excellence (IST-FP6-0384239).

6 REFERENCES

[1] S. Ata, M. Hashimoto, H. Kitamura, M. Murata, 'Mobile IPv6-based Global Anycasting', draft-ata-anycast-mip6-00 (2006).

[2] M. Zuniga, B. Krishnamachari, 'Integrating Future Large-scale Wireless Sensor Networks with the Internet' Department of Electrical Engineering, University of Southern California. http://ceng.usc.edu/~bkrishna/research/papers/ZunigaKrishnamachari_sensorIP.pdf, (2005)

[3] C. Chong, S. Kumar, 'Sensor Networks Evolution, Opportunities,and Challenges', Proceedings of The IEEE (2003).

[4] M. Dorigo, M. Caro, 'Ant Colony System: A Cooperative Learning Approach to the Travelling Salesman Problem', IEEE Transactions on Evolutionary Computation (1996).

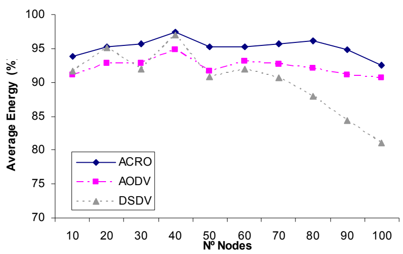
[5] A. Dunkels, 'Full TCP/IP for 8-bit architectures', in Proceedings of The First Internacional Conference on Mobile Systems, Applications, and Services (MOBISYS03) (2003).

[6] A. Dunkels, J. Alonso, T. Voigt, H. Ritter, J. Schiller, 'Connecting Wireless Sensornets with TCP/IP Networks', wwic2004 (2004).

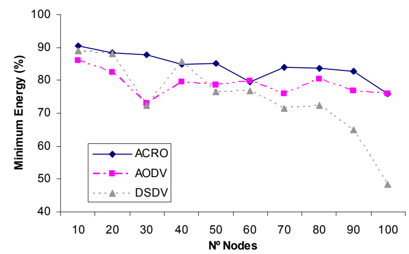
[7] J. Hill, M. Hoton, R. Kling L. Krishnamurthy, 'The Platforms enabling Wireless Sensor Networks', Communications of the ACM, vol. 47, no. 6, pp. 41-46 (2004).

[8] C. Intanagonwiwat, R. Govindan, D. Estrin,

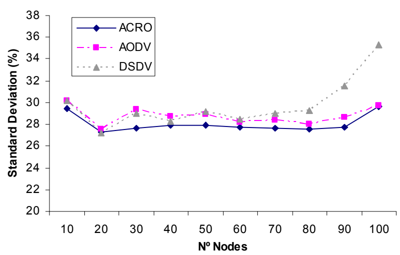
‘Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks’, Proc. ACM MobiCom’00, Boston, MA, pp. 56-67 (2000).
[9] L. Krishnamurthy, R. Adler, P. Buonadonna, M. Yarvis, ‘Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the north sea’. In SenSys ’05: Proceedings of the 3rd international conference on Embedded networked sensor systems, pages 64–75 (2005).
[10] S. Mishra, R. Sridharan, R. Sridhar, ‘A Robust Header Compression Technique for Wireless ad hoc Networks’, in MobiHoc2003 (2003).
[11] G. Montenegro, N. Kushalnagar, ‘Transmission of IPv6 Packets over IEEE 802.15.4 Networks’, draft-montenegro-lowpan-ipv6-over-802.15.4-12, (2007).
[12] D. Niculescu, ‘Communication Paradigms for Sensor Networks’, IEEE Communications Magazine (2005).
[13] P. Ramanathan, ‘Location-centric Approach for Collaborative Target Detection, Classification, and Tracking’, IEEE CAS Workshop on Wireless Communication and Networking (2002).
[14] R. Shah, S. Roy, S. Jain, W. Brunette ‘Data MULEs: Modeling and analysis of a three-tier architecture for sparse sensor networks", Elsevier Ad Hoc Networks Journal, vol. 1, issues 2-3 (2003);
[15] R. Szewczyk, E. Osterweil, J. Polastre, D. Estrin, ‘Habitat Monitoring with Sensor Neworks’, Communication of the ACM (2004).
[16] S. Thomson, T. Narten, T. Jinmei ‘“IPv6 Stateless Address Autoconfiguration’, draft-ietf-ipv6-rfc2462bis-08 (2005).
[17] R. Wakikawa, A. Petrescu, P. Thubert, ‘Network Mobility (NEMO) Basic Support Protocol RFC3963 (2005).



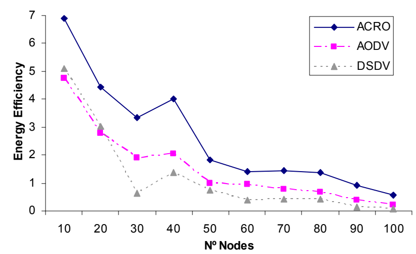
a) Average Energy



b) Minimum Energy

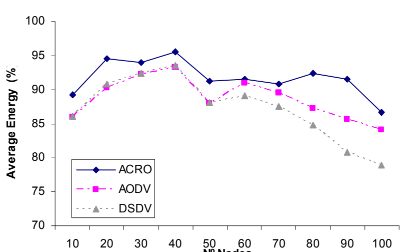


c) Standard Deviation

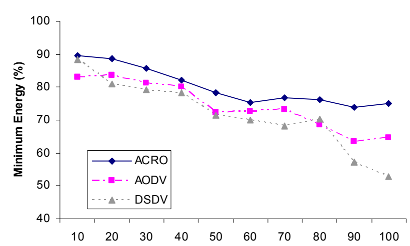


d) Energy Efficiency

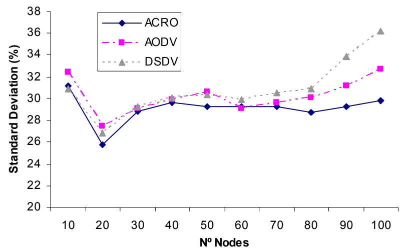
Figure 15: Energy performance comparison – static phenomenon



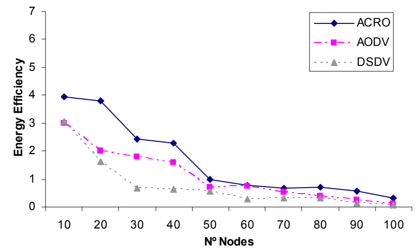
a) Average Energy



b) Minimum Energy



c) Standard Deviation



d) Energy Efficiency

Figure 16: Energy performance comparison – moving phenomenon