Multicast and IP Multicast support in Wireless Sensor Networks

Jorge Sá Silva, Tiago Camilo, Pedro Pinto, Ricardo Ruivo, André Rodrigues,
Filipa Gaudêncio, Fernando Boavida
Departamento de Engenharia Informática
Universidade de Coimbra
Polo II - Pinhal de Marrocos, P-3030 Coimbra. Portugal
Tel.: +351 39 790000 Fax.: +351 39 701266 e-mail: sasilva@dei.uc.pt

***Abstract* - Multicast potentially optimises bandwidth consumption and node resources, when several users simultaneously participate in a communication session. Nevertheless, contrary to the expectations, IP multicast has not experienced widespread deployment, with the exception of IPTV. On the other hand, emerging Wireless Sensor Network (WSN) applications could greatly benefit from multicast and constitute another field where multicast can be an effective and efficient technique. The questions are: do multicast advantages hold in WSN scenarios? Can we use IP Multicast functionality in WSNs? This paper discusses and evaluates the use of multicast in WSNs. Specifically, we evaluate the use of Source-Specific Multicast, as it is one of the most promising paradigms for IP networking, considering both IPv4 and IPv6 in WSNs.**

A sensor platform with IP and multicast support that is being developed in our lab is presented. Concurrently, simulation studies were performed in order to assess the usefulness of multicast in WSNs. The results clearly point to the benefits of the use of this technique in processing and energy-restricted environments such as this one.

Index terms – multicast, wireless sensor networks, IP in WSNs

I. INTRODUCTION

Traditional networking involves communications between two end systems. However, important emerging applications like IPTV, remote teaching or videoconference, require simultaneous communication between groups of users.

Multicast protocols can offer several benefits. The use of a set of point-to-point channels to support a virtual multicast environment results in a complex and inefficient process, mainly in wide area networks. When a source needs to transmit a message to *n* receivers using point-to-point communication mechanisms, it is necessary to transmit the same message *n* times. In the case of IPTV, where the number of receivers is extremely large, this is technologically unfeasible due to prohibitively high resource requirements.

The emergence of applications with inherent multicast requirements led to the development of native multicast protocols. In the case of IP networks, multicast support was typically based on the Internet Group Management Protocol (IGMP) [1] to announce hosts interested in receiving multicast information, and on Protocol-Independent Multicast – Sparse Mode (PIM-SM) [2], Multicast Border Gateway Protocol (MBGP) [3] and Multicast Source Discovery Protocol (MSDP) [4] to route multicast messages between core routers.

With the increasing demand for multicast support, new protocols were proposed. One of the most promising protocols is the Source-Specific Multicast (SSM) [5]. According to this protocol, when a host decides to join a multicast group it must specify not only the IP multicast address, as usual, but also the source address or a list of source addresses that the node joining the multicast sessions accepts to receive information from. This source identification significantly reduces the routing complexity. However, as shown in [6], SSM has several limitations when applied to mobile environments.

Recent advances in wireless communications, electronics and miniaturization supported the development of a new generation of multi-functional, low-cost sensor nodes. These new sensor nodes, with control components and communication functionality, are at the basis of the development of Wireless Sensor Networks (WSNs).

Wireless Sensor Networks are composed of a set of several nodes which can cooperate in order to perform certain tasks, such as measurement and monitoring tasks, and can re-organize themselves in an ad-hoc way. Typically, sensors collect ambient measurements, process and transmit them to a sink node.

Sensor Networks may be used in a countless number of applications in many areas. WSNs are applicable to almost every aspect of our daily life, including environment monitoring (temperature, sound, pressure), habitat monitoring, healthcare applications, home automation, traffic control and industrial systems automation. WSNs can be used in environments where traditional networks are not supported.

As the applicability of WSNs is becoming larger, it is crucial to evaluate if:

- multicast can be useful for the next generation Internet, which will integrate WSNs,
- current multicast protocols are well prepared and can be useful for WSN environments.

The objective of this paper is to discuss and evaluate the applicability and usefulness of multicast approaches in WSNs, including the use of traditional multicast paradigms.

The next section presents the main purpose and characteristics of the WSN platform being developed at the Laboratory of Communications and Telematics of the

University of Coimbra (LCT-UC). In this section we also evaluate and compare the use of IPv4 and IPv6 in WSNs. Section 3 analyzes the main properties of multicast protocols and discusses the requirements of WSNs in terms of multipoint support. In section 4 we evaluate multicast in WSNs' scenarios, comparing it, through simulation, with unicast and broadcast approaches. Special attention is given to SSM, as it is a promising IP Multicast protocol. In the final section we present the conclusions and guidelines for further work.

II. IP IN WIRELESS SENSORS NETWORKS

This section presents a platform currently being built at LCT-UC, which combines IP networks and WSNs. The purpose of this test-bed is to study not only multicast approaches in sensors networks but also the integration of other IP functionality in WSNs. We are particularly interested in exploring the use of IPv6 addressing and auto-configuration for things such as WSN initial deployment, data-centric and location-centric approaches, and energy-efficient routing

WSNs are composed of a potentially high number of nodes, each one equipped with a simple microprocessor, low memory and a basic communication system. Currently existing projects addressing simplified TCP/IP stack integration in sensor networks do not explore key aspects of IPv6 functionality and do not solve a major limitation: the TCP/IP protocol stack is too complex for sensors with reduced processing power and leads to prohibitive power consumption.

Sensor networks typically have power consumption restrictions. Using some key IPv6 capabilities, such as larger address space, anycast routing, Neighbor Discovery and mobile IPv6, this project intends to develop and explore a communications framework that leads to adequate performance in WSN environments.

The integration of the full IP stack is hardly feasible in sensor networks environment, due to the specificity of the latter [7], [8]. [9], [10] describes mechanisms that enable IP addressing in sensor nodes, which allows sensor networks to communicate with any system belonging to 4G-environment, since the core is IP based. However, none of these mechanisms are optimised for mobility, and none of them take advantage of IPv6 functionality.

More recently, an IETF group was created, the LoWPAN WG, which addresses the problem statement, assumptions and goals of IPv6 for Personal Area Networks [11], including limited power and other restricted requirements networks, such as Wireless Sensor Networks. This group represents a big step towards the heterogeneity that will characterise future 4G environments and towards the integration of sensor networks in the Internet. In this line, it is also noteworthy to mention that the SICS research group developed a new microprocessors WSN-oriented operating system – Contiki – which contemplates IP connectivity. More recently, the well known TinyOS platform adopted an extension that allows IP connectivity.

Although the use of IP in WSNs has several potential advantages, its native implementation poses some problems due to the limitations inherent to this type of networks, as can be seen in [12]. For this reason it is necessary to develop a new protocol suited to WSNs. Currently, our group has already started the design of an architecture that fulfills the proposed objectives [13]. Such architecture proposes a new routing protocol based on the Ant Colony Optimization heuristic, which uses a concept similar to the pheromone mechanism used by ants when searching for food.

Although IPv6 addresses are bigger than IPv4 addresses (128 bits long, as opposed to 32 bits in the case of IPv4), the IPv6 header is simpler, as most of the unused or rarely used IPv4 fields were removed. Additionally, IPv6 natively supports some important functionality, such as multicast.

The studies are being performed in the context of the 6MNet project. The purpose of this project is the study of various issues related to multicast in very dynamic and mobile networks. Figure 1 illustrates the test-bed that is being implemented.

We have already concluded some studies regarding multicast in mobile environments, involving other institutions, through the use of IPv6 tunnels. At the moment we are extending our studies to sensor networks. For the test-bed we are using the Contiki package [14]. The Contiki operating system is a highly portable, minimalist operating system, for a variety of restricted systems such as modern 8-bit microcontrollers. This operating system provides an event-driven kernel with optional preemptive multithreading, a dynamic process structure, native TCP/IP support using the uIP TCP/IP stack and a graphical subsystem.

In Figure 1, Quinn is a laptop that supports the inter-working between the IP network and the WSN. So, data gathered by the sensor network can be accessed through the existing IP network infrastructure.

Quinn runs Microsoft's Windows XP ™ operating system. This laptop has an interface to the wireless sensor network through SLIP, an e-Gate (small USB device for communication with the sensor network) and an Ethernet interface connected to the lab network. Quinn is used for the development and testing of new and modified functions on the software side. The external network card enables interoperability testing between the uIP stack and other IP networks. Using this process we can access services provided by the wireless sensor network from the lab network without any restriction.

A second PC was also used for software development and testing. The connectivity of this second PC was limited to the WSN.

The sensors used in the test-bed were the Embedded Sensor Boards (ESB) developed by Freie Universität of Berlin, which are one of the most widely used sensors for the research of new solutions throughout the world. The main features of this platform are the 8-bit micro-controller from Texas Instruments MSP430, a JTAG interface to program the sensor boards, an

RS232 interface for communication and monitoring, a low consumption transceiver (TR1001) for wireless communication using 866 Mhz free frequency, support for three AA batteries or other power supplies such as solar cells, infrared port for sending and receiving data and a wide range of sensors like tilt, humidity and temperature.

The eGate [15] model used in our test-bed was connected to a USB port and it has all the capabilities of an embedded sensor board except the sensorial part. The e-Gate makes use of the same TR1001 transceiver for wireless communication with the wireless sensor network, and it has also a JTAG interface for programming purposes.

The communication between the e-Gate and the PC is made through a SLIP connection. The e-Gate has to be flashed with the Contiki operating system [14] in the same way as a normal Embedded Sensor Board, but with packet forwarding enabled to route packets between the WSN and the PC or other external networks.

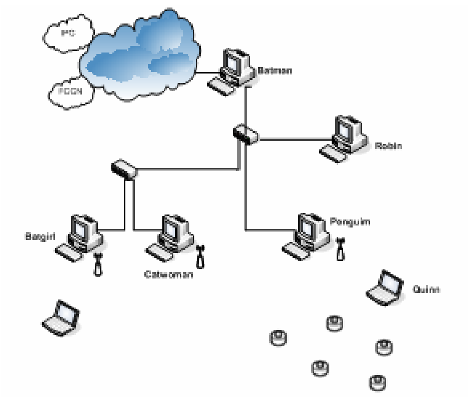

Figure 1 – LCT-UC testbed

One of the future challenges in the field of Computer Networks is to provide IPV6 support for sensor networks. Although there are some studies that discuss advantages and disadvantages of this integration, these studies are scarce, especially if we consider real test-beds.

In order to evaluate the energetic impact and performance of a future IPv6 stack in a sensor network using the Contiki operating system, we ran several tests. The objective was to study the behaviour of the platform with the load increase that results from the larger IPv6 packet header size.

With the objective of testing some IPv6 properties, we started by modifying the uIP stack. We were particularly interested in getting several types of packets circulating in our sensor network. We started to change the structure of IPv4 packets to that of IPv6 packets in order to test the impact of size on various aspects of the sensor network, especially energy consumption and performance.

For this purpose we developed a small and simple JAVA application that redirects packets captured by a predefined network interface to the sensor network, with a pre-selected set of modifications in the packet structure: IHL field, version or address sizes. In this way, our application sent packets through the RS232 interface of the PC which is connected to the sensor network by a SLIP connection. This SLIP connection sends the data byte-by-byte without any error control or validation procedures.

The following figure compares battery duration with the number of sent packets using SLIP technology.

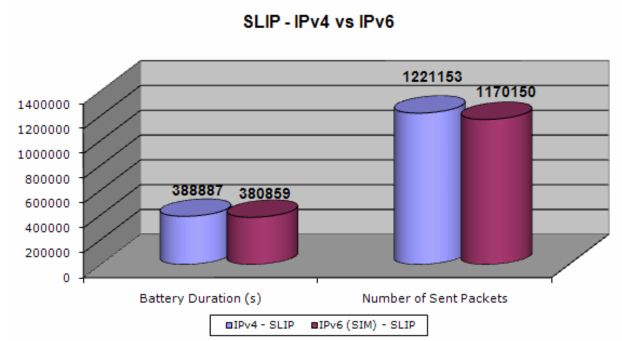

Figure 2 – IPv4 vs IPv6 using a SLIP connection

The impact of IPv6 on energy consumption was very low, leading to a 2,07% decrease in battery duration. The number of sent packets decrease 6,93% only.

From this we can conclude that the transmission of IPv6 packets does not have a decisive effect on the ESB platform. All values obtained on these tests have minimal differences, which are perfectly acceptable when compared with the advantages that IPv6 can bring to WSNs.

We are also implementing a new mechanism using the anycast functionality of IPv6 to combine the geographic routing paradigm used in WSNs with the node-centric routing paradigm used by the TCP/IP approach.

III. MULTICAST IN WIRELESS SENSOR NETWORKS

Multicast in IP networks is based on the concept of group. An arbitrary set of receivers express their interest in receiving a particular data stream. This group does not have any specific physical or geographical boundaries. Hosts that are interested in receiving packets sent to a particular multicast group must join the group using Internet Group Management Protocol (IGMPv3) [16] or Multicast Listener Discover (MLDv2) [17], for IPv4 and IPv6, respectively. These protocols manage the communication between hosts and routers. Each router maintains a list of active members per multicast group in its sub-network.

Forwarding of multicast packets is subject to certain risks. If there are several routers on the same physical network and if special care is not taken, they may all relay the packets again and again. In this way, there is the risk of creating not only a multicast loop but also a multicast avalanche (network flood), bringing the whole network to a stop as it is quickly filled to capacity. The whole purpose of multicast routing is, precisely, to achieve delivery of multicast packets without loops and without excess transmissions.

There are different routing protocols, some using rudimentary techniques such as flooding, and others using more elaborate techniques that rely on source-based trees or shared-based trees algorithms. Work in the multicast area started by developing and refining intra-domain routing protocols. Later, particular emphasis was placed on developing inter-domain multicast routing protocols.

Nowadays, with the advent of wireless systems and with the use of 4th Generation Protocols, it is also important to apply and to study each new protocol in mobile environments. There are several projects addressing the problems of multicast and mobility. The main approaches are based on home subscription, remote subscription and hybrid solutions.

Adding the TCP/IP stack to sensors can be too much for sensors with reduced processing power and can lead to prohibitive power consumption, as was discussed in the previous section. However, if it is possible to deploy a thin IP protocol, it will be possible to integrate future WSNs with the Internet, and a significant number of new applications will appear.

Mobility is another important requirement in WSNs. Only recently a few projects are considering mobile scenarios [18], and usually at MAC-layer [19] only. But, if we integrate some IP functionality in WSNs, it is also possible to use some features of the Mobile IP framework.

In the case of multicast there are several situations where it is important to transmit the same information to a group of sensor nodes as, for example, during the configuration procedure of a group of sensors. Middleware is another topic for which multicast can offer an efficient solution, since whenever it is necessary to update a group of nodes with the latest version of a component (e.g. light module) it is not advisable to send the module to every sensor in a point-to-point fashion. In this situation, multicast can provide WSNs with the necessary routing tools to perform an efficient software component distribution.

These tasks are necessary for correction of software bugs or for application reconfiguration of nodes. Since code distribution protocols are, in general, quite traffic-intensive and should be performed without disturbing other critical traffic, using multicast procedures is of crucial importance. Our aim is to evaluate the use of some standard multicast protocols and to propose new extensions.

However, multicast protocols used in WSNs must be simple. Current multicast protocols are quite complex even for traditional IP networks. This is more critical in WSNs due to the well-known limitations of sensor nodes. In the following section we will evaluate the use of multicast in WSNs, having in mind their processing and energy limitations.

IV. EVALUATING MULTICAST IN WSNs

Various research projects address the development of middleware for wireless sensor networks. Middleware offers flexibility and can be a potential solution for the creation of software abstractions that ease the development process. The next logical step in WSNs will be the development of a middleware that adapts to network changes (e.g. addition of new nodes with distinct functionalities) and that dynamically chooses the best solutions for the services required by the applications running on the network. In fact, we anticipate that future WSNs will support more than one application at the same time.

When it is necessary to upgrade specific nodes or modules, there is a significant volume of data to transmit to the involved sensor nodes. The use of broadcast techniques can be prohibitive, mainly in multi-hop scenarios. We used the scenario presented in section II – a typical WSN with a sink node (represented by the laptop) and a set of sensor nodes – to compare the Multicast Ad hoc On-Demand Distance Vector (MAODV), PIM-SSM and the AODV protocol, when they are used to distribute middleware packages to different groups of nodes.

It was also important to study the use of an SSM approach in WSNs, as SSM is one of the most promising multicast protocols for IP-based networks. SSM was an incremental response to the issues associated with the Internet Standard Multicast (ISM) model and addressed several of its weakness with utmost simplicity. In PIM-SSM, delivery of datagrams is based on (S,G) channels. Traffic directed to one (S,G) channel consists of datagrams with a unicast source address S and the multicast group address G. Nodes that wish to receive specific information have to become members of the (S,G) channel, identifying not only the multicast group address G, but also the source of the multicast traffic S. Contrasting to SSM, the support of dynamic environments, whenever a new source intends to inform the receivers of its activity, requires the use of additional signalling protocols.

In future middleware scenarios, each node will have installed only the components that it requires, from a group of components. For instance, it may be necessary to support some security mechanisms in some nodes while other nodes, from the same group, may need mobility support. For these scenarios it will be necessary to group the nodes with the same requirements in the same multicast group.

As described above, multicast can constitute an optimal solution to this. Such functionality can truly help next generation networks, including wireless sensors, to dynamically perform in real time required modifications, in order become more adaptable to external (e.g. radio interference) and internal (e.g. energy parameters) constraints.

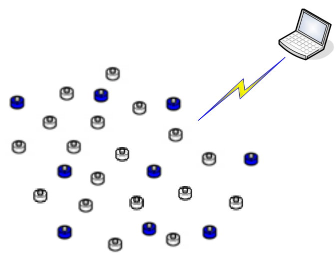

Figure 3 – Typical WSN scenario

MAODV [20] is one of the most popular protocols for multicast in mobile ad hoc networks. According to its specification, the MAODV protocol discovers multicast routes on-demand, through the use of broadcast mechanisms. When a node wants to join a multicast group or to send a multicast message and does not have the route in its own table, it sends a route discovery message. For the evaluation of MAODV we used the NS-2 [21] with the MAODV 2.26 [22] and the NRLSensorSim 2.27 [23] packages.

As NS-2 does not offer support for the study of SSM, our group needed to develop this support.

The NS-2 simulator is a program developed using the object oriented languages C++ and OTcl. Functions, procedures, or classes that are processor-intensive must be written in the C++ language. To develop topologies that use pre-built modules and are not processor-intensive, it is convenient to use OTcl in the specification phase. However, this rule was not followed in the development of multicast modules, since they are practically all written using OTcl language. This fact is responsible for a set of problems affecting NS-2 multicast modules.

The PIM-SSM protocol has several similarities with PIM-SM. The development of the SSM module for NS-2 was, for this reason, based on the Centralized Multicast code, with some modifications, so that the new protocol fully supports all the SSM functionalities.

The main differences between these two protocols are:

- In SSM, the Join and Prune messages have to specify the Group and the Source of the multicast channel. Routers cannot accept (*,G) messages, like in normal PIM-SM protocol behaviour.
- In SSM environments the Rendezvous Point is no longer necessary. The routing tree becomes decentralized, which is the opposite of SM behaviour where all packets have, necessarily, to pass, at least in a first stage, through the RP node.

For the simulated scenario we selected a network with 50 sensors. It was assumed that four different middleware components were to be injected into four multicast groups. These four components had different memory requirements; consequently, it was necessary to use a different number of packets to transmit each component.

In these simulation studies, packets of 127 bytes were used, since this length reflects the maximum packet length for the future IEEE 801.15.4 networks. Each simulation spanned 300 seconds. Combining the multicast groups presented in Table 1, four distinct scenarios were created during the simulation:

- in Scenario 1 (S1) only a multicast group was used, namely group A, composed of 10 elements;
- in the Scenario 2 (S2) the middleware components were injected in two multicast groups, A and B, representing 30 nodes;
- for the third scenario (S3) we selected 3 different multicast groups (A, B and C), resulting in 45 nodes receiving the new updated modules;
- In the last scenario (S4) all the multicast groups were configured, summing up a total of 75 (virtual) nodes receiving the middleware components. It is important to realize that some nodes were listening to more than one multicast group, meaning these nodes had more than one updatable component.

Figure 4 illustrates the sensor network topology used to simulate our scenarios. Each node is identified by one ID number, and belongs to the groups identified in Table 1. The sensor with ID zero is the sink-node, the device that transmits the middleware packets (components update) to the remaining sensor nodes.

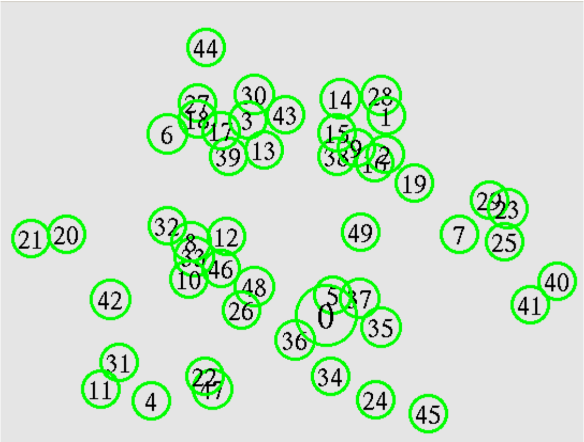

Figure 4. Topology of the simulated scenarios

The following simulation parameters were used:

- Transmitting power: 0.175 mW
- Receiving power: 0.145 mW
- Sensing power: 0.00000175 mW
- Idle power: 0.0 mW
- Initial energy: 5.0 Joule

On each scenario, four different communication protocols were used: a broadcast, a unicast and two multicast protocols. The broadcast protocol used in the simulation redirects all the messages to all nodes in the network. Each node will receive one or more data packets even if they did not request them. The unicast protocol used in the simulation was AODV. The sink-node was responsible for demanding the routing path towards the destination nodes, and the communication was performed on a point-to-point basis.

In terms of the multicast protocols, the same behaviour was implemented in the sink-node/source (to create and maintain the routing paths), but the communication was based on point-to-multipoint paths.

Figure 5 presents the number of packets needed to inject each middleware component into the nodes by the protocol (control and data packets). It is possible to observe that the number of packets was similar in the cases of broadcast and multicast approaches. In a broadcast/multicast communication, the source only needs to send a packet once, contrary to the unicast solution where a unique packet is sent to each node, forcing the source device to send more packets, as is apparent in Figure 5. The only difference between multicast and broadcast is due to the multicast control packets which are necessary to maintain the multicast session, contrary to the broadcast case where no control packets are necessary. However, if we analyze the total number of forwarded packets the differences are significant.

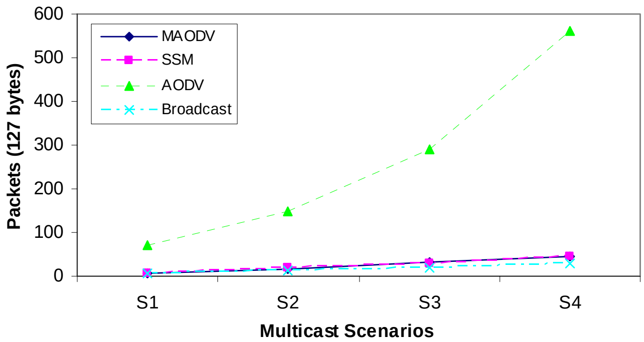

Figure 5. Number of data packets transmitted by the source

Since communication is the function that requires more energy from a node, it is important to reduce the number of communication events between sensor nodes. Therefore, the selected protocol must route the packets directly and only to the nodes that really need to receive those packets. Such behaviour is achieved by using multicast protocols. The gains of using multicast are illustrated in Figure 5, leading to a reduction of 73% and 48% in the number of data packets forwarded by intermediate nodes when compared to the unicast and broadcast approaches, respectively (in scenario 4).

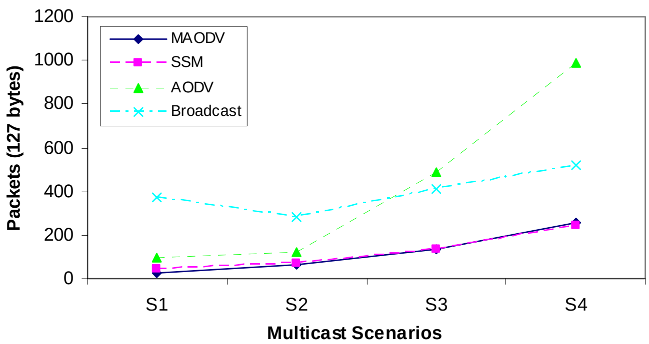

Figure 6. Number of data packets forwarded by intermediate devices

Another conclusion is that if few receivers are present, the unicast and the multicast approaches lead to similar results, contrary to the broadcast approach. In the latter approach, even if only few sensor nodes request the middleware component, all the packets are sent to all nodes. However, this is reversed when the number of receivers increases: broadcast becomes a better solution when compared with the unicast approach.

Finally, the last results relate to the main limitation in a WSN: energy. It is important to realize that a WSN may become useless if one or more sensor nodes "die", i.e., if sensor nodes become unable to communicate and/or forward communications due to energy exhaustion. Therefore, it is necessary to use a protocol that uses as low energy as possible. Figure 7 presents the energy levels after the injection of the four middleware components. These values were achieved by summing the remaining energy of all sensor nodes at the end of the simulation.

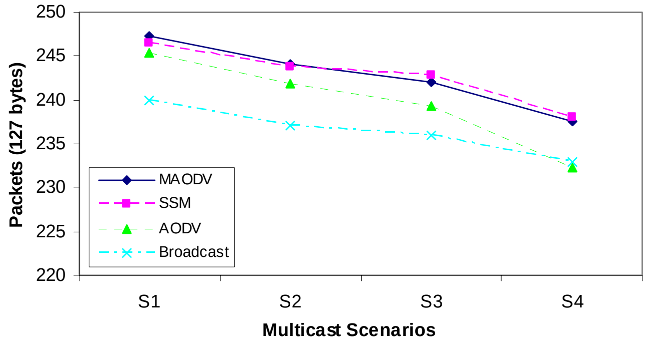

Figure 7. Remaining energy after the software components distribution

The multicast protocols led, once again, to the best results, when compared to the AODV and broadcast protocols. Due to their characteristics, the multicast protocols used less communication resources, since they are based point-to-multipoint paradigms.

As the simulation results have shown, multicast has significant advantages in WSN environments, over broadcast and unicast. It reduces the number of transmitted packets required to update a specific middleware component. Therefore, this will represent a decrease in the energy spent by each node. Looking at the scenarios used in the simulations, the best results were achieved when the number of multicast receivers was high. In this case, the unicast approach used more bandwidth and resources, since it requires one-to-one communication. In scenarios where few receivers existed (e.g., in scenario S1), the gains were not so high, when compared to the unicast protocol, although it still leads to better results than the ones obtained with broadcast.

We can also conclude that SSM is also a good choice for WSNs. This is important because if this protocol will be used in future IP networks it can also be extended to WSNs.

V. CONCLUSIONS AND FUTURE WORK

The full potential of Wireless Sensor Networks can only be explored if Internet connectivity is provided. In order to do this, IP must, somehow, be supported in WSNs.

Although sensor nodes have stringent energy and processing limitations that constitute an obstacle to the use of a fully-fledged IP protocol, simplified versions are already being used. In this respect, exploring the use of IPv6 is also promising, because IPv6 uses simpler headers and offers native support for mobility and multicast.

In this paper we have addressed both the use of IPv6 and the use of multicast in WSNs. The results clearly show that WSNs can greatly benefit from both. Specifically, multicast leads to reductions in the number of transmitted packets and, consequently, in energy consumption. In fact, WSNs may become the next successful field of multicast deployment, in addition to the emerging field of IPTV.

Further research will continue to explore the use of multicast in WSNs.

ACKNOWLEDGEMENT

The work presented in this paper was partially financed 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).

REFERENCES

[1] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November 1997

[2] D. Estrin et al. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification" RFC 2362, June 1998

[3] T. Bates, Y. Rekhter, R. Chandra and D. Katz. "Multiprotocol Extensions for BGP-4", RFC 2858, June 2000.

[4] B. Fenner and D. Meyer. "Multicast Source Discovery Protocol (MSDP)", RFC3618, October 2003.

[5] S. Bhattacharyya, "An Overview of Source-Specific Multicast", RFC3569, July 2003.

[6] J. Sá Silva, S. Chandrakar, T. Camilo and F. Boavida, "Assessing and Extending SSM for Highly Dynamic Mobility Environments", Fifth International Conference on Communication, Information and Signal Processing, IEEE Communication Society, Bangkok, December 2005

[7] J. Heidemann, F. Silva and C. Intanagonwiwat, "Building Efficient Wireless Sensor Networks with Low-Level Naming", 2000;

[8] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed Diffusion: a scalable and robust communication paradigm for sensor networks", ACM Press, 2000;

[9] A. Dunkels, T. Voigt and J. Alonso. Making TCP/IP Viable for Wireless Sensor Networks. In Proceedings of the First European Workshop on Wireless Sensor Networks (EWSN'04), work-in-progress session, Berlin, Germany, January 2004.

[10] M. Zuniga and B. Krishnamachari, " Integrating Future Large Scale Sensor Networks with the Internet " , USC Computer Science Technical Report CS 03-792, 2003.

[11] IETF Working group www.ietf.org [12] Camilo, T., Sá Silva, J., Boavida, F., "IPv6 in Wireless Sensor Networks, a New Chalenge", First International Workshop on Convergence of Heterogeneous Wireless Networks, Julho 2005;

[12] T. Camilo, J. Sá Silva, C. Carreto and F. Boavida, "ASSENT: Ant-based System for Sensor Energy-Efficient Networks", Ants 2006: Fifth International Workshop on Ant Colony Optimization, September 2006.

[13] T. Camilo, "IPSense – Multi-Paradigm Routing for Wireless Sensor Networks", in Proc. of the CoNext 2005 - ACM Conference on Emerging Network Experiment and Technology, Toulouse, France, October 2005.

[14] Contiki Operating System, http://www.sics.se/~adam/contiki/, 2005

[15] eGate/WEB stands for Embedded Gate/WEB, ScatterWeb GmbH, Berlin 2005, http://www.inf.fu-berlin.de/inst/ag-tech/scatterweb_net/hardware/egw/index.html

[16] B. Cain and S. Deering, I. Kouvelas and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[17] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", update to RFC 2710, draft-vida-mld-v2-08.txt, December 2003.

[18] K. Dant et all, "Robomote: enabling mobility in sensor networks", in IEE/ACM Fourth International Conference Processing in Sensor Networks, April 2005

[19] M. Ali, T. Suleman and Z. Uzmi, "MMAC: a mobility-adaptive, collision-free mac protocol for wireless sensor networks", in Proc. 24th IEEE IPCCC'05, USA, April 2005

[20] E. Royer and C. Perkins, "Multicast operation of the ad-hoc on-demand distance vector routing protocol", Porc. 5th ACM/IEE Annula Conf. on Mobile Computing and Networking, Aug. 1999

[21] http://www.isi.edu/nsnam/ns/

[22] Y. Zhu and T. Kunz, "MAODV implementation for NS-2 2.26", Carlton University, 2004

[23] NRL's Sensor Network Extension to NS-2, Naval Research Laboratory

TABLE 1 – Multicast groups

Multicast group	Component Size (bytes)	Nº Packets	Start time (sec)	Number of nodes in the group	Nodes' ID
A	500	7	10	10	[1,10]
B	400	5	20	20	[5,24]
C	600	8	30	15	[15,29]
D	800	10	40	30	[20,49]

Jorge Sá Silva received his PhD in Informatics Engineering in 2001 from the University of Coimbra, where is a Professor at the Department of Informatics Engineering (DEI). His main research interests are Mobility, IPv6, Multicast and Sensor Networks. He is a senior researcher at the Laboratory of Communications and Telematics of DEI. He participated in European initiatives such as E-NET and E-NEXT, and international research projects such as EuQoS and WEIRD. He was the Workshop Chair of IFIP Networking2006 and he was also involved in program committees and organization of national and international conferences. He is a member of IEEE, and he is a licensed Professional Engineer. His homepage is at http://www.dei.uc.pt/~sasilva.

Tiago Camilo is a PhD student at Informatics Engineering Department of the Faculty of Science and Technology, University of Coimbra (UC) and member of the Lab. of Communications and Telematics (LCT) of the Department of Informatics Engineering, University of Coimbra. He received an undergraduate degree in Informatics Engineering from Polytechnic Institute of Guarda in 2003. He is an active member of IPv6 Portuguese Task-Force. He participated in European initiatives such as E-NET and E-NEXT, and international research projects such as CONTENT. His homepage is at http://eden.dei.uc.pt/~tandre/.

Pedro Pinto is a MSc student of Engineering Computer Science of the University of Coimbra. He works in Polytechnic Institute of Guarda as network administrator. His main research interests are IPv6, wireless network sensors and Wireless LANs. His homepage is at http://ppinto.pt.to/

Ricardo Ruivo received his graduate in Informatics Engineering in 2006 from the University of Coimbra, where is a System Administrator at the Department of Informatics Engineering.
His main research interests are wireless sensor network, IPv6 and network security issues. He is a licensed Professional Engineer. His homepage is available at http://eden.dei.uc.pt/~rruivo/

André Rodrigues haa a BSc in Informatics Engineering from University of Coimbra and an MSc in Finance from ISCTE Business School. Currently is a Ph.D. student in Informatics Engineering at the University of Coimbra and works as a teacher at the Coimbra Institute of Accounting and Administration (ISCAC), giving classes on networking. His main research interest is Wireless Sensor Networks, more specifically middleware solutions that can adapt to diverse or changing requirements and support mobile nodes and Internet access. He is a researcher at the Laboratory of Communications and Telematics, Department of Informatics Engineering, University of Coimbra.

Filipa Gaudêncio received her MSc degree in Informatics Engineering in 2007 from the University of Coimbra. She is a Professor and the network system administrator in Escola Superior de Tecnologia e Gestão of Instituto Politécnico da Guarda. Her main research interests are Network Management and Security, Sensor Networks, IPv6 and Multicast.

Fernando Boavida received his PhD in Informatics Engineering in 1990, and he currently is Full Professor and President of the Department of Informatics Engineering (DEI) of the Faculty of Sciences and Technology of the University of Coimbra. He is the leader of the Laboratory of Communications and Telematics (LCT) of DEI and the Strategic Director for Communications and Information Technology of the University of Coimbra.
His main research interests are Mobile and Ambient Networking and Scalable Networking (quality of service issues, large scale distributed architectures and management). He was the chairman of the Program Committee of QofIS'2001, IDMS-PROMS'2002, NETWORKING 2006 and WWIC 2007 international conferences. He has been involved in numerous program committees of major international conferences, including INFOCOM 2006 and 2007. He participated in several European initiatives/projects.
He is a senior member of IEEE, and he is a licensed Professional Engineer. He is a member of the Editorial Advisory Board of the *Computer Communications* journal. His homepage is at http://eden.dei.uc.pt/~boavida .