Internet Protocol over Wireless Sensor Networks, from Myth to Reality

Paulo Alexandre Correia da Silva Neves
Instituto de Telecomunicações, Portugal
Department of Informatics, University of Beira Interior, Covilhã, Portugal
Superior School of Technology, Polytechnic Institute of Castelo Branco, Castelo Branco, Portugal
Email: pneves@est.ipcb.pt

Joel José Puga Coelho Rodrigues
Instituto de Telecomunicações, Portugal
Department of Informatics, University of Beira Interior, Covilhã, Portugal
Email: joeljr@ieee.org

***Abstract*— Internet Protocol (IP) is a standard network layer protocol of the Internet architecture, allowing communication among heterogeneous networks. For a given network to be accessible from the Internet it must have a router that complies with this protocol. Wireless sensor networks have many smart sensing nodes with computational, communication and sensing capabilities. Such smart sensors cooperate to gather relevant data and present it to the user. The connection of sensor networks and the Internet has been realized using gateway or proxy-based approaches. Historically, several routing protocols were specifically created, discarding IP. However, recent research, prototypes and even implementation tools show that it is possible to combine the advantages of IP access with sensor networks challenges, with a major contribution from the 6LoWPAN Working Group. This paper presents the advantages and challenges of IP on sensor networks, surveys the state-of-art with some implementation examples, and points further research topics in this area.**

***Index Terms*— wireless sensor networks, Internet connectivity on wireless sensor networks, Internet protocol, ubiquitous networks**

I. Introduction

Many smart sensing nodes that cooperate to sense the environment may constitute a wireless sensor network (WSN), providing sensing services to an ever-growing application space. Each node has a wireless radio to communicate, a processing unit and memory to process tasks and an autonomous energy unit, a battery. WSN applications started with initial military applications (a common ground with many of the technologies we use today), to many other application areas such as environmental observation, health monitoring, structural monitoring, habitat monitoring, smart classroom, and tracking among others [1]. A growing interest is drawn to enable ubiquitous applications using WSN, enabling sensing services that can effectively used in behalf of the user, such as smart spaces and augmented reality.

WSN may have thousands of small smart sensors with computational capability and memory, one or more sensors and a limited power supply. The limited power supply and computational power are the main constraints at the smart sensor level, dictating the feasibility of a given network protocol. Several applications do not allow battery recharge, such as deployment in harsh environments. Moreover, recharge circuitry uses board space and provides for extra weight and cost. Typically, the nodes of a WSN cooperate and drive information to a special more powerful node: the sink node. Many different sensors can be used such as temperature, light intensity, accelerometer, and pressure, among others.

The main goal of a sensor network is to provide sensing services to the user or other systems. The Internet has 1 billion users worldwide, so it makes sense to provide WSN services to this ever-growing community [2]. The Internet of computers is becoming the Internet of machines or "the tangible Internet", a global network that will not only connect computers, but all kinds of processor-enabled machines, such as domestic appliances, mobile phones, and hopefully WSNs.

The connection of WSN to the Internet has been achieved using a proxy-based approach. In this approach sensor nodes communicate through dedicated WSN protocols, whereas the sink acts as a proxy to the Internet, converting IP to/from the dedicated WSN protocol. This approach allows existing networks to be connected with minimal changes|.

Another approach is to use IP as the protocol for the sensor network itself, avoiding the need to use a proxy. However, there is a common belief that IP is not suited for sensor node hardware limitations, mainly due to energy considerations (header overhead), protocol complexity and memory needs. We will prove with this paper that not only IP is feasible for WSN, but also a significant number of implementation attempts exist and more are expected to surface as research continues.

The Internet Protocol (IP) [3] suite is the de-facto routing protocol in the largest of all world networks - the

Manuscript received Feb. 22, 2009; revised Sept. 1, 2009; accepted Nov. 17, 2009.

doi:10.4304/jcm.5.3.189-196

Internet. Though not perfect, it clearly served us well for nearly 30 years in its version 4 specifications, so much that IPv4 is commonly named IP. With the introduction of version 6, the addressing space grew to a number close to 2^{128} addresses, leading to $667x10^{23}$ addresses per square meter of earth surface. This protocol will empower the next generation of networks, where more heterogeneity is expected on the Internet.

The motivation to connect sensor networks to the Internet draws from remote access to data, making ubiquitous computing realistic. Eventually WSN and ubiquitous computing will somehow merge [4]. As an example, an Internet-connected WSN is monitoring a parking lot; a given application can consume data to guide a user to the nearest available space. Moreover, it can even reserve a parking space; provide expected occupation time, among other interesting features, all tightly coupled to provide transparent services to the user.

To the best of the authors' knowledge, no other paper surfaces the current approaches on the application of the IP protocol over WSN. In [5] authors provide an overview of the myths that drove away IP from WSN, however, the paper focus is on presentation of a system architecture, which is also present afterwards. As a result, a great motivation is drawn to the writing of this paper.

The rest of the paper is organized as follows. Section II elaborates on some background knowledge of the main technologies that this paper focuses on: WSN, routing protocols for WSN, IP version 4 and 6, and body sensor networks. Section III presents the main challenges for applying IP as the routing protocol for WSN. Section IV elaborates on the current research and system implementation. Section V concludes the paper and point relevant topics for further research.

II. Technological Background

This section provides some insight on WSN, considering their routing protocols, their application on body sensor networks, and surfaces IP in both fourth and sixth versions.

A. WSN

WSN first depicted in military applications, to track enemy movement and survey battlefield areas. With the promise of low node cost, powered by MEMS (micro electromechanical systems) technology, WSN began its application to broader areas like environmental monitoring, building automation and monitoring, underwater surveillance, up to healthcare monitoring [6]. The new application areas pose different challenges when compared with military applications, such as patient safety on healthcare applications or signal acquisition on underwater applications, among others. However, some challenges are horizontal, such as energy constraints, wireless communication coverage and bandwidth, and limited computing resources.

Another very interesting application of WSN is in biofeedback. Several sensors are placed on the human body directly or through wearable clothing. These sensors monitor health parameters such as heartbeat, body temperature, Electrocardiogram (ECG) and may be wirelessly connected to a sink node. The sink node is responsible for capturing the reading of all sensors, sending the data to an interface device, such as a mobile phone or PDA [7]. This kind of network is commonly known as a body sensor network (BSN), since its scope is body-wide [8]. The connection of BSN to the Internet is also mandatory for remote access.

The smart sensor nodes (also referred as motes) of a WSN have one or more sensors, a processing unit with RAM and program memory, a limited power supply, and a wireless transceiver, as depicted in Figure 1. In terms of energy, the majority is spent on wireless communication. Sometimes a bit transmission uses 1000 times the power of computing an instruction. Energy is of major importance, with some designs featuring some sort of energy harvesting, as in [9]. As the node operates, energy is depleted; as nodes begin to fail the network coverage shrinks, eventually rendering it useless [10]. As a result, a great effort is drawn on employing power-efficient routing protocols.

Among the challenges that this kind of network presents, apart from the energy constraints, we find node placement, node mobility, node resources (also considering energy), and data aggregation. Node placement clearly depends on the application. For a healthcare application, node placement must be very precise and difficult to control without human intervention, while on a military application it may be impossible to control, e.g. dropped from an aircraft. Node mobility is not supported on many designs. However, some applications like healthcare where a patient travels along the hospital, or sensors placed on animals to study their behavior, node mobility has to be considered.

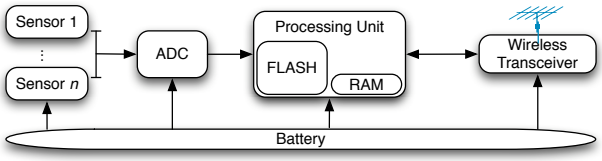

Figure 1. Typical block diagram of a wireless sensor network smart node.

Node resources are scarce, and on a flat network, every node plays every role: communication, sensing, and computation. On a non-flat design a clustered or hierarchical network and some nodes may be only relaying information. Since a node must be cheap enough for the overall network to be cost-efficient, hardware resources must be bound. It is common to find 8 or 16-bit microcontrollers, 4-10KB of RAM and 48-256KB of Flash. Examples of such equipments can be found in Crossbow Technology (http://xbow.com).

B. WSN Routing Protocols

Routing in WSN is of major importance, since nodes need to communicate to each other for the information to reach the sink node, constituting a multi-hop network. Due to the previously outlined challenges that WSN presents, research for dedicated routing protocols has evolved.

Good surveys on routing protocols developed specifically for WSN exist and may be found on [11, 12]. In [11], authors discuss system architecture and design issues that influence the performance of a given protocol. These are network dynamics, node deployment, energy considerations, data delivery models, node capabilities and data aggregation/fusion.

Routing protocols for WSN can be classified by type, based on their main characteristics. Then, the following three categories may be considered: data-centric protocols, hierarchical routing protocols, and location-based routing protocols [11]. Some other protocols are based on network flow or quality of service (QoS) modeling. The evaluated protocols feature energy considerations, but still lack on QoS and real-time applications.

The concept of data-centric protocols relies on a sink node that queries sensor network areas for specific data (data-centric). The query must clearly indicate the required data, through e.g. attribute-based naming. Among the protocols based on this approach are SPIN, Directed Diffusion, Rumor Routing, Energy-aware routing, and Gradient-based routing, among others. Directed Diffusion clearly made a leap forward on this type of protocols, with some others following the same approach or similar concept.

Hierarchical protocols introduce multi-tier routing on WSN. If a single tier is used on a large WSN, energy may be depleted faster on the intermediate nodes. Hierarchical routing takes advantage of network clustering, where several sensing nodes elect a typically more powerful node to communicate with the sink in their behalf.

Several cluster heads communicate with each other to reach the sink, relieving nodes from multi-hop communication, thus saving battery life. This kind of protocols also can take advantage of data aggregation on cluster heads, relieving the sink from lower-level data aggregation, thus minimizing needed computing power.

Examples of hierarchical routing protocols are the LEACH (Low-Energy Adaptative Clustering Hierarchy), PEGASIS (Power-Efficient GAthering in Sensor Information Systems), and TEEN (Threshold Efficient sensor Network protocol). LEACH is one of the most popular hierarchical routing algorithms for sensor networks, while PEGASIS introduces improvements on the LEACH protocol.

Another routing approach in WSN is location routing. This kind of routing takes advantage of the knowledge of smart sensor location to send queries to specific regions. The location information can also be used to minimize the impact of communication on energy consumption, taking shorter paths requiring less transmission power. Most of these protocols come from ad hoc networks, but may be well applicable to sensor networks. MECN (Minimum Energy Communication Network), GAF (Geographic Adaptive Fidelity), and GEAR (Geographic and Energy-Aware Routing) are examples of location protocols.

None of the identified protocols were developed with Internet connectivity as a main goal. As a result a proxy-based scenario is the only solution for Internet connectivity, as opposed to smart sensor node stack based IP implementation.

C. Surfacing IP version 4 and IP version 6

Since IP over WSN is the focus of this writing, we surface both IPv4 and IPv6 protocols in this section. IPv4 was developed in the early seventies to ease communication between restrict and closed number of researchers and academics in the United States [13]. Later RFC 791 presented the Internet Protocol, a protocol for wired computer networks that is able to connect different networks by the means of a compatible router. The age of the Internet was just beginning, and back then no one predicted the number of users Internet has today.

The version 4 of the IP protocol survived until now with a great success, in spite of its limitations. However, the introduction of several mobile Internet access devices pushes IPv4 addressing space boundaries. The Internet Engineering Task Force (IETF) began working on the successor of IPv4 around the early 1990's. In 1993, the IETF started the Internet protocol next generation (IPng) for proposals investigation and recommendations for the future IPv6.

The use of network address translators allows the reuse of IPv4 addressing space inside a given network, a solution adopted by many Internet service providers (ISP) for household utilization. Such amend allows IPv4 to be used even today, even with billions of Internet-enabled devices. However, we all eventually adopt IPv6.

D. Body Sensor Networks

A very interesting application area of WSN is healthcare promotion and biofeedback. In this area, WSNs are known as wireless body sensor network (WBSN), since the objective is to place sensors on the human body to study health parameters.

Much research is focused on the development of biosensors [14, 15], medical systems [16, 17] and development of suitable interfaces [18-20]. This presents a very challenging and interesting application area that can also benefit from the integration of IP.

The raw sensor data is transferred to a more powerful node, the sink. Data must be processed, stored and presented to the medical staff and/or patients. The feasibility of such networks depend on their ability to operate for weeks on a 24/7 basis without intervention, operation under extreme temperatures and provide lower cost than current solutions [21]. This kind of networks plays well with remote monitoring, thus also drawing great benefit from Internet connectivity.

III. IP OVER WSN

This section provides an overview with the motivation and challenges for the implementing the IP protocol on WSN. The use of IP on WSN is more than a mere academic research thrust; it provides significant advantages and tackles the need for the augmentation of the Internet to provide more ubiquitous services. However, such advantages come with a price, namely on

the addressing of some new challenges that a protocol created for wired networks presents.

A. Background

Two basic architectures emerged when connecting WSN to the Internet, a proxy-based solution or integration of IP at the smart sensor level (also referred as IP stack). As may be seen in Figure 2, the sensor network has another routing protocol different from IP, and the sink acts as a protocol-mapping device, which connects the network to the Internet.

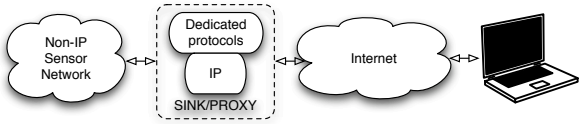

Figure 2. Connecting WSN to the Internet using a proxy-based solution.

This transformation can be performed at the application level [22]. For example, the sink node may query the sensor network using dedicated protocols, store data locally, while performing data aggregation. This approach may be shown in Figure 3, scenario (a). When an Internet host requires data, it communicates via IP protocol with the sink that sends data from the local database to the requiring host.

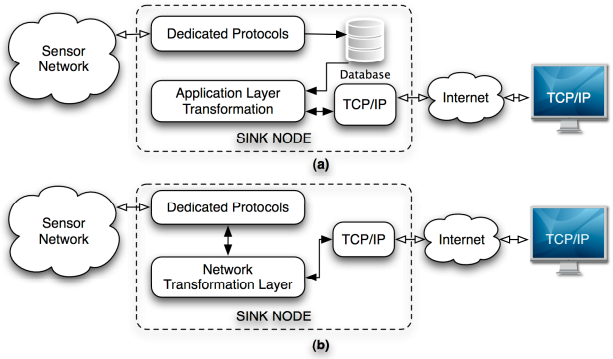

Figure 3. Different approaches for proxy-based WSB connection to the Internet: (a) with proxy database, and (b) without memory.

Another proxy-based solution may be applied at the network level, where a sink performs protocol transformation without the use of a local database, depicted by the scenario (b) of Figure 3. When an Internet host sends a query to the sink, the sink queries the sensor network. While this approach may lead to freshness of data, it may also lead to delays since the database is not present to provide some buffer effect.

Another solution is to integrate an IP stack on the smart sensor and directly use IP as routing protocol inside the network, as Figure 4 depicts. This is the scenario we are interested on in this paper. This scenario presents specific challenges as above mentioned in Section 3.2. Another motivation comes from the fact that IP protocol presents several advantages that mainly draw from the decades that is being used with success on computer networking, with various mechanisms and protocols already developed, validated and operationally deployed [22]. Moreover, tools for network management, commissioning, configuring and debugging developed for IP-enabled networks could also be used [23]. IP brings an open standard to WSNs, and presents a very attractive learning curve (availability of bibliography published on the subject), almost transparent Internet integration, network maintenance and scalability.

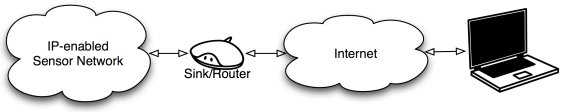

Figure 4. Connecting WSN to the Internet at the smart sensor level.

B. Challenges

Several reasons supported the idea that IP cannot be used directly at the smart sensor level, reserving the routing for dedicated protocols. In this subsection we provide a vision of the major challenges with some discussion.

Header overhead. IP adds significant amount of data on the header block of the packet, introducing undesirable overhead. Since the majority of energy is spent on wireless communication, this may be a very limiting factor for the use of IP on the smart sensor node. The minimum IPv4 header has 20 bytes plus the payload. Extensions can be used that further enlarge the size of the header.

IPv6 uses a different approach, where a fixed 40 bytes header (double the one in IPv4) is used. The header size increase is mostly due to 128-bit addresses instead of 32-bit addresses of IPv4, even though IPv6 header is optimized leaving some IPv4 header bits behind. As a result header overhead may increase. To tackle this challenge, header compression must be used. The compression can be applied to the addresses (by using link-local addresses for instance) or even applying the compression mechanisms defined by the 6LoWPAN specification.

Addressing Scheme. IP addressing scheme relies on the knowledge of the source address and a destination address, and both must be unique inside a given network. While IPv4 can use dynamic host configuration protocol (DHCP) for address attribution, it contributes for more protocol overhead; while IPv6 provides an intrinsic mechanism for stateless auto-configuration. In IPv6 both anycast and multicast addresses also make it possible to address a group of nodes with a single address. Anycast delivers a packet to the nearest interface of the identified group alone, while multicast delivers to all the network interfaces of the identified group.

While traditional computer networks hosts communicate to transfer data among applications, WSNs are intended to provide sensing services. In many applications, it is desirable to know the sensed data, not the address of the smart sensor(s) that produced such data. As a result, the most important asset is the data produced by the smart sensor, and typically a data-centric approach is preferable to address-centric. However, when considering body sensor networks, an address-centric approach may be preferable, since typically no redundant sensors are used, mainly because of patient discomfort and setup time. As a result, this special kind of WSN may benefit from a unique addressing scheme.

Limited Bandwidth. Small smart sensors have limited wireless bandwidth; 250kbps is very common in IEEE 802.15.4 implementations [24]. The more bits must be transmitted, the longer the data transmission will take, and longer the latency for medium access. With limited bandwidth one wants to waste as minimum as possible in overhead bits, let it be for header, error control, or others. IP may pose significant challenges, since it was developed for wired connections. To tackle this challenge header compression mechanisms

Limited Energy. One of the distinct factors of WSNs is the limited energy of the nodes, since nodes must be small and cost-effective. Wireless communications on the nodes consume the maximum amount of energy, involving both transmission and reception [25]. In some cases the energy cost of one bit transmission corresponds to 1000 processor instructions or more. In many scenarios it is not viable to provide battery replacement or even recharge. Then, when a node looses power it dies. When a given number of nodes in a network die, the network ceases to provide sensing services, rendering it useless.

This challenge is tackled with a conjunction of several mechanisms. The first is header compression. With transmission of fewer bits, energy wasted on transmission of a single packet is minimized. The second mechanism is stateless auto-configuration of IPv6. This mechanism allows the association of an IPv6 link-local address to an interface, which may be enough for a given network. Link-local addresses in IPv6 start with FE80.

Implementation Challenges. One of the implementation challenges is the internetworking between layer 2 protocols and IP. Since a specification for Ethernet exists and most computer local area networks use this protocol, the problem is solved. A growing interest is given to IEEE 802.15.4 standard and mechanisms must be implemented to internetwork with IP. Other implementation challenges are related to development of suitable security mechanisms, and specification of ad-hoc networking and auto-configuration for ad-hoc deployment. In this specific challenge the 6LoWPAN specification provides an overlay network layer that can transmit IPv6 data over IEEE 802.15.4 frames. 6LoWPAN is presented with some detail in section IV.A. Also the work from Adam Dunkels addresses some implementation challenges with the first IP stack for 8-bit microcontrollers [26].

Transport Protocol. IP protocol does not guarantee reliability in packet transmission, employing a best-effort approach. When one considers IP on its usefulness for global Internet connection, one considers transmission control protocol (TCP) as the transport protocol to achieve reliable packet transmission. However, TCP is not energy-aware and requires acknowledgment packets to be sent towards the transmitting host; which wastes valuable bandwidth and energy resources.

Another alternative is the use of the user datagram protocol (UDP). This protocol is sometimes used on non mission-critical sensor networks, avoiding the acknowledgement mechanism of TCP. A discussion on some variations of TCP can be found on [27].

IPv4 or IPv6. IPv4 currently still manages to satisfy the great majority of computer communication needs across the Internet, mainly due to several mechanisms like network address translation (NAT). However, IP addresses are becoming short, so IPv6 rises as a solution. Moreover, features inside IPv6 provide functionality only found on IPv4 plus one or more added mechanisms.

The IPv6 protocol may even aggravate the expected overhead of IP for WSN. However, a detailed study proves that overhead increases by a very small amount [28]. The paper presents both simulation and prototype results, pointing several advantages of using IPv6 on such hardware constrained devices, like auto-configuration and stateless mechanisms, the growing adoption of IPv6 and increase in addressing space.

IV. Current Approaches

This section reviews the most relevant efforts to bring IP to WSNs. The first part presents an overview of the first approaches, while the second part presents and discusses some 6LoWPAN implementations. Finally, section C presents some real implementations on the field.

A. Breaking the walls

Breaking the walls presents initial work on IP over WSN, that progressively put IP on the WSN space. The first breakthrough was the introduction of a full TCP/IP stack on very limited hardware, through the work of Adam Dunkels [26]. In this work two implementations are presented, one for very limited 8-bit architectures (uIP) and other with more functionalities (lwIP), conform to a subset of RFC 1122. While lwIP provides a full-scale, but simplified, implementation of IPv4, ICMP, TCP and UDP, uIP only can handle one interface, does not implement UDP, focusing on IP, ICMP and TCP protocols.

Adam Dunkels *et al.* present possible approaches for the header overhead problem, by applying header compression techniques. The use of an application overlay network implements a data-centric routing with address distribution based on sensor location. The Distributed TCP caching mechanism enables lower energy consumption, each node is able to cache a single TCP segment, enabling single-hop retransmissions [29].

Another work on header compression presents a layered approach that dissociates the network from the transport compression, enabling compression on different links, domains and even networks [30]. Performance evaluation is drawn for a tree-shaped sensor network with one sink node, and shows energy consumption gains from the proposed header compression architecture.

In [5] some challenges are identified and the architecture of IPSense, a system that allows IPv6 over WSNs. IPSense features flexible addressing, enhanced mobility, and a clustering mechanism with sensor routers. Sensor routers are responsible for communication management with the sink node, aggregating several sensor nodes, and are also faced as gateway points for

other networks to communicate, thus alleviating the very constrained sensor nodes.

A TCP/IP implementation is described by Xiaohua Luo *et al*., but is based on a proxy approach [31]. The base station converts external TCP/IP requests to an Active Message, while sensor nodes implement a protocol called SIP – Sensor Internet Protocol. This approach lightens the computational requirements on the sensor nodes, but the sensor network itself does not use TCP/IP. The SIP protocol assumes that motes never need to communicate with external hosts, so only respond to queries. The base station is responsible for receiving TCP/IP requests from Ethernet, 802.11b wireless network or Bluetooth, translating into an Active Message.

B. 6LoWPAN

A task force named 6LoWPAN Working Group (WG) from the Internet Engineering Task Force (IETF) is working on a standard protocol definition: 6LoWPAN [23]. The main goal is to enable IPv6 packets over low power wireless networks, with emphasis on the IEEE 802.15.4 standard, supporting small/pico sensor network nodes. The group aim is to define an encoding mechanism that is layer 2 and 3 agnostic.

Initial implementations of 6LoWPAN show that a mere 32KB Flash ROM is needed. Moreover, the WG has managed to ditch DHCP and NAT by using Zero-Conf and Neighbor Discovery capabilities of IPv6. Also, stacked headers are used to minimize header overhead, through header compression.

The working group successfully addresses the header overhead problem of IPv6, removing the need for configuration servers (namely, DHCP and NAT), use of EUI-64 and 16-bit unique addresses within the personal area network (after an association event) [32]. However, in order to use 16 bit addresses, a PAN coordinator must dole the address in an association event, limiting the validity to the lifetime of the association.

Zach Shelby considers IP-enabled WSNs as the Wi-Fi of the embedded world [33], namely IP over IEEE 802.15.4. The paper refers the 6LoWPAN initiative as a means to achieve the desired functionality, namely with the use of NanoSensors™.

According to [34] management tools must take into account the special characteristics of WSNs. The LNMP network management protocol provides network management with simple network management protocol (SNMP) support. Coordinator nodes capture the state of sensor nodes and relay data to the gateway, which filters state data from the list of reporting coordinators. SNMP protocol is supported on the external networks, and the gateway acts as a proxy between SNMP and the local management framework.

Even with 6LoWPAN communication between different networks can result in relatively high overhead due to the bits needed for addressing hosts. The 6GLAD [35] architecture proposes a twice-NAT and reverse network address translation mechanisms. The twice-NAT features both source and destination IP address modifications, and by means of reverse NAT mapping on the WSN gateway, mapping IPv6 addresses to node's short addresses inside the network, allowing the use of less bits for addressing.

A similar approach for efficient address utilization is the dual addressing scheme (DAS) for IPv6 over IEEE 802.15.4 networks [36]. DAS maps a global IPv6 node address to a link local address to save energy and resources. Also the gateway maps IPv6 global addresses into link local lightweight addresses to reach a specific node inside the network. The proposed scheme is validated through simulation that shows a significant reduction in overhead.

C. Some Implementations

The first attempts to integrate a sensor network in the Internet were proxy-based. The above-mentioned SIP protocol is based on a proxy scheme [31]. The proxy deals with the communication between external hosts and wireless sensors through an Active Message mechanism. The proxy is transparent in terms of TCP/IP operation, since it does not require any changes on the wireless sensors or the Internet hosts. Such approach is still used on ZigBee Bridge for instance [37].

One example of smart sensor stack comes from a sensor network for intrusion monitoring featuring an IP-based WSN with the ESB platform from FU Berlin [38]. In this work authors use the ContikiOS with the uIP stack, providing TCP/IP support. Addresses are distributed based on node location on a grid, which require location information at the sensor level.

An implementation of a TCP/IP stack for Tiny OS based on a code base from HP Labs, featuring IEEE 802.15.4, a port of TCP/UDP/IP uIP stack, Telnet and HTTP (dynamic web pages support) servers. The implementation also features a lightweight version of the protocols SIP, DHCP, NTP and an IMAP-like message service. It also features a Linux-based IEEE 802.15.4 access point through a Telos mote plugged into the computer [39].

ContikiOS, currently on version 2.2.3 presents the uIPv6 stack with 6LoWPAN implementation [40], the evolution of above-mentioned uIP. This version was awarded with the IPv6 Ready silver seal, featuring IPv6 over IEEE 802.15.4 through 6LoWPAN. The stack features IPv6, TCP, UDP, ICMPv6, and neighborhood discovery (ND).

TinyOS (http://tinyos.net), currently on version 2.1, also has a 6LoWPAN implementation (b6loWPAN) with support for stateless auto-configuration, multi-hop routing, and fragmentation for 1280bytes MTU. The implementation features tools like ping, nc6 and tracert6.

V. CONCLUSIONS AND FURTHER RESEARCH TOPICS

In this paper we surfaced the state-of-the-art on the efforts to bring IP over WSN. Motivation is clearly focused on their connection to the Internet in the most transparent possible way, allowing realistic ubiquitous computing applications. IP over WSN is more than a myth; it is a reality. Efforts are aimed at the sensor level, namely the 6LoWPAN group and software resources like TinyOS and ContikiOS.

A sensor network presents many challenges that ultimately result in node failure, leading to dynamic routing of information inside the network. As in traditional IP networks, dynamic routing may be needed. One research topic that must be considered is the search for an optimal dynamic routing protocol such as routing information protocol (RIP), open shortest path first (OSPF), or other to route information.

IP over WSNs is a reality, but the vision of Internet connectivity we have on traditional computing systems, with the required ease of use and auto-configuration is yet beyond reach. We believe a Plug-and-Play like approach for WSN is a very interesting research topic for network deployment.

The development of adequate applications for remote network management taking into account the specificities of the sensor network are yet to be achieved. Such software tools must run on several hardware platforms (personal computer, smart phone, or even dedicated devices), provide accurate and timely information about the network, and also provide a convenient application-programming interface (API) for remote data acquisition.

With IP, a dynamic routing protocol and a convenient set of tools, WSN present an invaluable resource for the vision of ubiquitous computing.

AKNOWLEDGEMENT

Part of this work has been supported by Instituto de Telecomunicações, Next Generation Networks and Applications Group, Covilhã, Portugal, and by the Euro-NF Network of Excellence from the Seventh Framework Program of EU.

REFERENCES

[1] I. Khemapech, I. Duncan, and A. Miller, "A Survey of Wireless Sensor Networks Technology", in *6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, Liverpool, UK, June, 2005.

[2] T. Kim, Y. Han, S. Cheon, I. Kim, J. Oh, and J. Ryou, "Network Traffic Analysis System Based on Data Engineering Methodology using System Entity Structure", in *International Conference on Convergence Information Technology*, Gyeongju, South Korea, 2007, pp. 1752-1757.

[3] R. Braden, Requirements for Internet Hosts - Communication Layers, Internet Engineering Task Force, RFC 1122, October 1989.

[4] J. A. Stankovic, "When Sensor and Actuator Networks Cover the World", *ETRI Journal*, vol. 30, pp. 627-633, No. 5, 2008.

[5] T. Camilo, J. S. Silva, and F. Boavida, "Some Notes and Proposals on the use of IP-based Approaches in Wireless Sensor Networks", *Ubiquitous Computing and Communication Journal*, vol. Special Issue on Ubiquitous Sensor Networks, 2007.

[6] K. Römer and F. Mattern, "The Design Space of Wireless Sensor Networks", *IEEE Wireless Communications Magazine*, vol. 11, pp. 54-61, December 2004.

[7] L. Zhong, M. Sinclair, and R. Bittner, "A Phone-centered Body Sensor Network Platform Cost, Energy Efficiency & User Interface", in *International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006)*, Cambridge, MA, USA, 2006.

[8] S.-L. Chen, H.-Y. Lee, C.-A. Chen, C.-C. Lin, and C.-H. Luo, "A Wireless Body Sensor Network System for Healthcare Monitoring Application", in *IEEE Biomedical Circuits and Systems Conference (BIOCAS 2007)*, Montréal, Qc, Canada, 2007, pp. 243-246.

[9] Y. Ammar, A. Buhrig, M. Marzencki, B. Charlot, S. Basrour, K. Matou, and M. Renaudin, "Wireless Sensor Network Node with Asynchronous Architecture and Vibration Harvesting Micro Power Generator", in *Joint Conference on Smart Objects and Ambient Intelligence: Innovative Context-aware Services: Usages and Technologies*, Grenoble, France, 2005, pp. 287-292.

[10] T. Hailun, "Maximizing Network Lifetime in Energy-constrained Wireless Sensor Network", in *2006 Int. Conf. on Communications and Mobile Computing*, Vancouver, British Columbia, Canada, 2006, pp. 1091-1096.

[11] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", *Elsevier Ad Hoc Network Journal*, vol. 3/3, pp. 325-349, 2005.

[12] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", *IEEE Wireless Communications*, vol. 11, pp. 6-28, No. 6, December 2004.

[13] S. Hagen, *IPv6 Essentials*: O'Reilly, 2006.

[14] C. H. Chan, C. C. Y. Poon, R. C. S. Womg, and Y. T. Zhang, "A Hybrid Body Sensor Network for Continuous and Long-term Measurement of Arterial Blood Pressure", in *4th IEEE/EMBS International Summer School and Symposium on Medical Devices and Biosensors*, Cambridge, UK, 2007, pp. 121-123.

[15] P. Cao, S. Jia, X. Wang, and J. Zhou, "Wearable and Wireless Multi-Electrophysiological System", in *3rd IEEE/EMBS International Summer School on Medical Devices and Biosensors*, Cambridge, MA, USA, September, 2006, pp. 83-85.

[16] U. Varshney, "Pervasive Healthcare and Wireless Health Monitoring", *Mobile Networks and Applications*, vol. 12, pp. 113-127, No. 2-3, March 2007.

[17] CodeBlue: Wireless Sensors for Medical Care, URL: http://fiji.eecs.harvard.edu/CodeBlue, Accessed in February 2008.

[18] O. Pereira, P. Neves, and J. Rodrigues, "Mobile Solution for Three-tier Biofeedback Data Acquisition and Processing", in *IEEE Global Communications Conference (IEEE GLOBECOM 2008)*, New Orleans, LA, USA, November 30 - December 4, 2008, pp. 1-5.

[19] T. Gao, C. Pesto, L. Selavo, Y. Chen, J. Ko, J. Lim, A. Terzis, A. Watt, J. Deng, B.-r. Chen, K. Lorincz, and M. Welsh, "Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results", in *IEEE Conference on Technologies for Homeland Security*, Waltham, MA, 2008, pp. 187-192.

[20] D. Yun, J. Kang, J.-e. Kim, and D. Kim, "A Body Sensor Network Platform with Two-Level Communications", in *IEEE International Symposium on Consumer Electronics (ISCE 2007)*, Irving, TX, USA, 2007, pp. 1-6.

[21] P. Kulkarni and Y. Öztürk, "Requirements and Design Spaces of Mobile Medical Care", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, pp. 12-30, No. 3, July 2007 2007.

[22] K. Mayer and W. Fritsche, "IP-enabled Wireless Sensor Networks and Their Integration Into the Internet", in *First International Conference on Integrated ad-hoc and Sensor Networks*, Nice, France, 2006.

[23] G. Mulligan and L. W. Group, "The 6LoWPAN Architecture", in *4th Workshop on Embedded Networked Sensor*, Cork, Ireland, 2007, pp. 78-82.
[24] "Part 15.4: Wirless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) - IEEE Std 802.15.4-2006": IEEE Computer Society, 2006.
[25] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a Survey", *Computer Networks (Elsevier)*, vol. 38, pp. 393-422, No. 4, 2002.
[26] A. Dunkels, "Full TCP/IP for 8-bit Microarchitectures", in *First Int. Conf. on Mobile Systems, Applications and Services*, San Francisco, CA, USA, 5-8 May, 2003, pp. 85-98.
[27] V. Tsaoussidis and I. Matta, "Open Issues on TCP for Mobile Computing", *Wireless Communications and Mobile Computing*, vol. 2, pp. 3-20, No. 1, 2002.
[28] J. S. Silva, R. Ruivo, T. Camilo, and G. Pereira, "IP in Wireless Sensor Networks - Issues and Lessons Learnt", in *Third International Conference on Communication Systems, Software and Middleware (COSMWARE 2008)* Bangalore, India: IEEE Communication Society, 2008.
[29] A. Dunkels, J. Alonso, and T. Voigt, "Making TCP/IP Viable for Wireless Sensor Networks", in *First European Workshop on Wireless Sensor Networks (EWSN 2004)*, Berlin, Germany, 2004.
[30] C. Westphal, "Layered IP Header Compression for IP-enabled Sensor Networks", in *IEEE Conference on Communications (ICC '06)*, Instanbul, Trukey, June 2006, 2006, pp. 3542-3547.
[31] X. Luo, K. Zheng, Y. Pan, and Z. Wu, "A TCP/IP Implementation for Wireless Sensor Networks", in *IEEE International Conference on Systems, Man and Cybernetics*, Hague, Netherlands, 2004, pp. 6081-6086.
[32] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, IETF, RFC 4944, September 2007.
[33] Z. Shelby, "IP-based Wireless Embedded and Sensor Networks: The WiFi of the Embedded World": http://www.sensinode.com/pdfs/sensinode-wp1-why_ip_wsn.pdf, 2008.
[34] H. Mukhatar, K. Kang-Myo, S. A. Chaudhry, A. H. Akbar, K. Ki-Hyung, and S.-W. Yoo, "LNMP - Management Architecture for IPv6 Based Low-power Wireless Personal Area Networks (6LoWPAN)", in *IEEE Network Operations and Management Symposium (NOMS 2008)*, Salvador, Bahia, Brazil, 2008, pp. 417-424.
[35] A. Zimmermann, J. S. Silva, J. Sobral, and F. Boavida, "6GLAD: IPv6 Global to Link-layer ADdress Translation for 6LoWPAN Overhead Reducing", in *Next Generation Internet Networks (NGI 2008)*, Krakow, Poland, 2008, pp. 209-214.
[36] S. Yang, S. Park, E. J. Lee, J. H. Ryu, B.-S. Kim, and H. S. Kim, "Dual Addressing Scheme in IPv6 over IEE 802.15.4 Wireless Sensor Networks", *ETRI Journal*, vol. 30, pp. 674-684, No. 5, 2008.
[37] M. Sveda and R. Trchalik, "ZigBee-to-Internet Interconnection Architectures", in *Second International Conference on Systems (ICONS '07)*, Sainte-Luce, Martinique, France, April 22-28, 2007.
[38] A. Dunkels, T. Voigt, N. Bergman, and M. Jonsson, "The Design and Implementation of an IP-based Sensor Network for Intrusion Monitoring", in *Swedish National Computer Networking Workshop*, Karlstad, Sweden, 2004.
[39] TCP/IP over 802.15.4 stack, URL: http://mail.millennium.berkeley.edu/pipermail/tinyos-devel/2005-August/000767.html, Accessed in July 2008.
[40] M. Durvy, J. Abeillé, P. Wetterwald, C. O'Flynn, B. Leverett, E. Gnoske, M. Vidales, G. Mulligan, N. Tsiftes, N. Finne, and A. Dunkels, "Making Sensor Networks IPv6 Ready", in *Proceedings of the 6th ACM Conference on Networked Embedded Sensor Systems (ACM SenSys 2008)*, Raleigh, North Carolina, USA, 2008.

Paulo Alexandre Neves is a PhD student on Informatics Engineering at the University of Beira Interior under supervision by professor Joel Rodrigues. He received his 5-year B.S. degree (licentiate) in 1998 in Electronics and Telecommunications Engineering from University of Aveiro, 2008; and MsC degree in Electronics and Telecommunications Engineering from University of Aveiro, Portugal in 2001. He also teaches in the Informatics Engineering Department at the Superior School of Technology of the Polytechnic Institute of Castelo Branco, Portugal. He is a PhD student member of the Institute of Telecommunications, Portugal. His current research areas are WSN, integration of the Internet Protocol on WSN, and WSN management. He authors or co-authors more than 15 international conference papers, participates on several Technical Program Committees, and also has two accepted journal publications.

Joel José P. C. Rodrigues is a Professor at the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in Informatics Engineering, MSc degree from the University of Beira Interior, Portugal, and a 5-year B.S. degree (licentiate) in Informatics Engineering from University of Coimbra, Portugal. His main research interests include sensor networks, high-speed networks, and mobile and ubiquitous computing. He is the Editor-in-Chief of the International Journal on E-Health and Medical Communications. He is or was the general Chair of the MAN 2009 and 2010 (in conjunction with IEEE ICC 2009 and 2010), N&G 2010 (with IEEE AINA 2010), Chair of the Communications Software, Services and Multimedia Applications Symposium at IEEE Globecom 2010, Chair of the Symposium on Ad-Hoc and Sensor Networks of the SoftCom Conference and chaired many other technical committees. Hi is or was member of many international program committees (IEEE ICC, IEEE Globecom, IEEE WCNC, IEEE CCNC, IEEE ISCC, IEEE ICCCN, ICTTA, SoftCOM, etc.) and several editorial review boards (IEEE Communications Magazine, Journal of Communications Software and Systems, International Journal of Communications Systems, International Journal of Business Data Communications and Networking, etc.), and he has served as a guest editor for a number of journals including the Journal of Communications Software and System. He chaired many technical sessions and gave tutorials at major international conferences. He has authored or co-authored over 90 papers in refereed international journals and conferences, a book and a patent pending. He is a licensed Professional Engineer and he is member of the ACM SIGCOMM, a member of the Internet Society, IARIA Fellow, and a Senior Member of the IEEE Computer Society, IEEE Communications Society and IEEE Education Society, and a member of several IEEE Technical Committees related with his research areas.