DOI 10.3233/MIS-2012-0138
IOS Press

Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things

Antonio J. Jara*, Miguel A. Zamora and Antonio Skarmeta
Department of Information and Communication Engineering, University of Murcia, Murcia, Spain

Abstract. The Internet of Things (IoT) requires scalability, extensibility and a transparent integration of multi-technology in order to reach an efficient support for global communications, discovery and look-up, as well as access to services and information. To achieve these goals, it is necessary to enable a homogenous and seamless machine-to-machine (M2M) communication mechanism allowing global access to devices, sensors and smart objects. In this respect, the proposed answer to these technological requirements is called Glowbal IP, which is based on a homogeneous access to the devices/sensors offered by the IPv6 addressing and core network. Glowbal IP's main advantages with regard to 6LoWPAN/IPv6 are not only that it presents a low overhead to reach a higher performance on a regular basis, but also that it determines the session and identifies global access by means of a session layer defined over the application layer. Technologies without any native support for IP are thereby adaptable to IP e.g. IEEE 802.15.4 and Bluetooth Low Energy. This extension towards the IPv6 network opens access to the features and methods of the devices through a homogenous access based on WebServices (e.g. RESTFul/CoAP). In addition to this, Glowbal IP offers global interoperability among the different devices, and interoperability with external servers and users applications. All in all, it allows the storage of information related to the devices in the network through the extension of the Domain Name System (DNS) from the IPv6 core network, by adding the Service Directory extension (DNS-SD) to store information about the sensors, their properties and functionality. A step forward in network-based information systems is thereby reached, allowing a homogenous discovery, and access to the devices from the IoT. Thus, the IoT capabilities are exploited by allowing an easier and more transparent integration of the end users applications with sensors for the future evaluations and use cases.

Keywords: Internet of Things, machine to machine, 6LoWPAN, address management, global communications, end-to-end addressability

1. Introduction

Flexibility, ubiquity, and scalability are the three required features within the current technological Era, focused on the ubiquitous computing [1] and the Internet of Things communications [2]. Flexibility is required due to the wide range of heterogeneous environments located around the world. The application areas defined usually cover a wide range of domains, including user-centric solutions such as e-health [3]; solutions more indirectly related to the user such as environmental monitoring [4]; those totally focused on the user, like Intelligent Transport Systems [5]; and finally, the development of a mix of solutions not focused on the user combined with user application domains, such as smart cities [6]. These solutions can range from simple sensors under the road for parking areas, or in the floor to measure humidity, to more complex systems, such as smart meters to measure pollution, air quality, and environmental

[*] Corresponding author: Antonio J. Jara, Department of Information and Communication Engineering, University of Murcia, Murcia, Spain. Tel.: +34 868888771; Fax: +34 868884151; E-mail: jara@um.es.

factors, and can even include clinical devices in e-Health and solutions for Ambient Assisted Living environments [7].

Flexibility, ubiquity and scalability are properties found in the current Internet, and that is why the aforementioned challenges can be solved not only with the new capabilities to link Internet with everyday sensors and devices, but also with the exploitation of data captured from the Future Internet through the so-called Internet of Things (IoT).

Future Internet and the IoT represent unprecedented growth in the number of devices and users connected to the Internet. Therefore, the devices should be as autonomous as possible in satisfying the so-called 'self-* functionalities', such as self-management, self-healing, and self-discovery. These properties are especially challenging in the Internet of Things, where many devices are mobile and, consequently, can change their location in the network.

For that reason, this research is focused on operating on top of the Future Internet infrastructure, i.e. IPv6. Thereby, users and clients discover and use homogenous IP-based resources, with protocols and technologies that are very well-known and are already deployed. However, other technologies such as IEEE 802.15.4, and Bluetooth Low Energy, are not based on IP networks, and have different limitations. For those technologies, other uses out-of-IPv6-network mechanisms have been defined: device location is not performed with IP locators, discovery messages are carried over a path not intended for general data communication, and so on.

As previously mentioned, our principle goal is to avoid the out-of-IPv6-network mechanisms in order to homogenize the discovery and use of resources through the Future Internet infrastructure, i.e. through the IPv6 network. This makes services reachable through homogenous and interoperable technologies, such as WebServices, and the discovery of services can be conducted through network-based Information Systems that are already deployed, such as the Domain Name System with the Service Discovery extension (DNS-SD).

The contribution of this paper is a way to provide any sensor, device or platform with IoT capabilities, from the common networking point of view. In other words, this means the evolution of consumer devices, as well as communication with the capabilities offered by the Future Internet, based on IPv6 protocol and technologies, such as IPv6 over Low Power Area Networks (6LoWPAN). In this regard, 6LoWPAN allows Internet extension to small and smart devices, making it feasible to identify and create connections among people, devices, and the things surrounding us.

Consequently, this extension to Internet, based on IPv6 and global connectivity, offers a homogeneous support and end-to-end capabilities. Furthermore, the technologies and current technologies/protocols from 6LoWPAN and IPv6 can be extended and re-used, e.g.: directory systems based on Domain Name System Service Discovery (DNS-SD), which can extend the current Resource Directory from M2M platforms and projects, such as SENSEI [8], in a global way.

Since original IPv6 and 6LoWPAN are not extensively supported by sensors and devices, such as legacy devices, nor by the environmental sensors currently deployed, this work instead proposes a mechanism for efficient support of global communications in machine-to-machine (M2M) scenarios, called Glowbal IP.

Glowbal IP is the result of scientific research on the two main open issues found in Internet of Things scenarios with applications and use-cases, oriented to connectivity with external servers, mobile user applications and interoperability scenarios.

The first concern is that most of the sensors and technologies currently deployed in smart cities, and industrial, building automation and smart grid scenarios lack 6LoWPAN support and IPv6 capabilities. As a result, current technologies must be extended to enable IPv6 capabilities, either with new hardware or with dramatic changes in the communication stack. These options are usually neither feasible nor scalable, and are not cost-effective for big deployments where it is not supported maintenance mechanisms such as Over-the-Air (OTA) firmware updates. Therefore, the main design challenge for Glowbal IP was to define a solution to be laid over the existing application layer, in order to avoid any changes in the current communication stacks, or any need for additional capabilities. Glowbal IP will be a part of the application to extend the addressability and determine end-to-end sessions for these technologies and devices.

A second problem was found with 6LoWPAN performance, which is the reference technology to integrate IPv6 in smart devices with limited capabilities due to its ability to link the Internet with everyday devices. In general terms, we found that the RFC4994 [9] overload was too high for global communications, since it requires in-line consideration of the full address; however, changes made by the new RFC6282 [10] to minimize the problem were insufficient, since it still requires a complex context management for an overload reduction that is not significant. We therefore concluded that even the technologies currently supporting IPv6 for smart things offer less than optimal header compression.

As a result, 6LoWPAN devices prepared to optimize performance within global communication, as well as other smart devices, can only be powered with 6LoWPAN or native IPv6. This work, however, proposes a new adaptation protocol called "Glowbal IP" which provides an Access Address Identifier (AAID), and an AAID-IPv6 address translation mechanism for different technologies, in order to adapt any device to the Internet of Things architecture via IPv6. In this respect, AAID simplifies all the parameters from IPv6 communications (source address, destination address, source port and destination port) in a single 4-byte communication identifier. Thus, the mentioned IPv6/UDP header overload that occurs in devices based on 6LoWPAN can be reduced with global IP addressing.

Therefore, Glowbal IP reaches an effective frame format for global communications, and a mechanism to support global communications with the Future Internet architecture, i.e.: with other IPv6 end nodes in networks that do not support IPv6 or 6LoWPAN. The main advantages from Glowbal IP are the reduction of the overhead of 6LowPAN networks for global communications, and the integration of legacy systems that cannot implement IP protocols due to various issues such as limited payload size e.g. Bluetooth Low Energy, or because it was not considered during the deployment, therefore it is offered a solution adaptable and transparent to the exiting deployments and communication stacks.

This document is organized as follows: Section 2 presents related works that deal with aspects such as IPv6 and 6LoWPAN, as well as their limitations, and the capabilities to define network-based information systems to discover resources and services by means of the Domain Name System Service Directory; Section 3 describes the Glowbal IP protocol, with the different format and entities involved in the mapping; Section 4 demonstrates the advantages of Glowbal IP to enable network-based Information Systems through DNS-SD and WebServices; Section 5 describes how the protocol has been implemented and evaluated; Section 6 explains Glowbal IP's advantages and capabilities; and Section 7 offers conclusions and future lines of research.

2. Related works

This section describes the works related to Glowbal IP from two perspectives. First, it describes the advantages of integrating IPv6 in the Internet of Things, as well as the limitations from current approaches, i.e. 6LoWPAN. Second, it describes the capabilities to build advanced network-based information systems, such as resource and services directories, over the Future Internet architecture, by using technologies such as DNS-SD.

2.1. Future Internet (IPv6) and the Internet of Things

The Internet of Things (IoT) is the main justification for the Future Internet, where IPv6 is the fundamental technology. It is estimated that the Future Internet will reach from 50 to 100 billion connected things by 2020 [11], while the IPv6 address space supports 2^{128} unique addresses (approximately 3.4×10^{38}); specifically, it can offer 1.7×10^{17} addresses on an area about the size of the tip of your pen. As a result, it makes it feasible for sensors and consumer devices to evolve towards the communication capabilities presented by the Future Internet with IPv6 protocol, by means of new technologies. It can be found several stacks and implementations for the integration of IP in wireless sensor networks [12], but the most extended and standardized is IPv6 over Low Power Area Networks (6LoWPAN). This extends the Internet to small and smart devices. Therefore, it will allow systems to identify and connect people, devices, and the things around us.

The 6LoWPAN adaptation layer was indicated to carry IPv6 datagrams over constrained links, such as the one defined in the IEEE 802.15.4 standard [13], taking into account the limited bandwidth, memory, or energy resources that are expected in applications such as wireless sensor networks [14]. IEEE 802.15.4 represents a Maximum Transfer Unit (MTU) of 127 bytes. This is reduced to 102 bytes after taking into account the IEEE 802.15.4 MAC header with extended MAC addressing IEEE EUI-64bits. It is further reduced by an additional 21 bytes [15] after accounting for link layer security (AES-CCM-128 for integrity and confidentiality). This leaves from 81 to 102 bytes of actual payload, depending on security level.

6LoWPAN defines a Mesh Addressing header to support sub-IP forwarding, a Fragmentation header to support the IPv6 minimum MTU requirement, and stateless header compression for IPv6 datagrams. Specifically, the defined 6LoWPAN headers, one for the IP header, and another one for the UDP header (LOWPAN_HC1 and LOWPAN_HC2, respectively) are able to reduce the relatively large IPv6 and UDP headers down to several bytes.

LOWPAN_HC1 and LOWPAN_HC2 are insufficient for most practical uses of IPv6 in 6LoWPANs, where global communications are involved [16,17]. LOWPAN_HC1 is most effective for link-local unicast communications, where IPv6 addresses carry the link-local prefix and an Interface Identifier (IID) directly derived from IEEE 802.15.4 addresses. In this case, both addresses may be completely elided. However, even though link-local addresses are commonly used for local protocol interactions, such as IPv6 Neighbor Discovery, DHCPv6, or routing protocols, they are not commonly used for the application layer, where communication with external clients and servers is required.

To solve the problem found with RFC4944 [9], a new encoding format, LOWPAN_IPHC, was developed for RFC6284 [10] for effective compression of Unique Local, Global, and multicast IPv6. This new encoding format is based on shared state within contexts. But, although usable, this is still inefficient. Figure 1 presents stack overhead for the RFC4944 and for the RFC6282 with contexts.

Figure 1 shows that 6LoWPAN has an overload of 26–41 bytes, meaning that the final available payload is reduced to half of the original size, i.e. 61 to 76 bytes from the original 127 bytes. Therefore, it is reduced to less than 50% of the original frame size from IEEE 802.15.4 of 125 bytes.

2.2. Directory systems for the Internet of Things

Two different levels of discovery can be defined: *resource discovery*, the discovery of devices on the network; and *service discovery,* the discovery of the services, methods and functions offered by a specific resource.

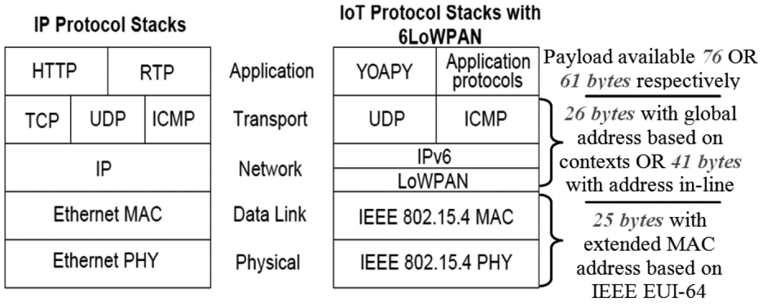

IP Protocol Stacks
IoT Protocol Stacks with 6LoWPAN
HTTP
RTP
Application
YOAPY
Application protocols
Payload available 76 OR 61 bytes respectively
TCP
UDP
ICMP
Transport
UDP
ICMP
26 bytes with global address based on contexts OR 41 bytes with address in-line
IP
Network
IPv6
LoWPAN
Ethernet MAC
Data Link
IEEE 802.15.4 MAC
25 bytes with extended MAC address based on IEEE EUI-64
Ethernet PHY
Physical
IEEE 802.15.4 PHY

Fig. 1. Future Internet and Internet of Things stacks.

Resources are reachable through technologies such as 6LoWPAN, Bluetooth Low Energy and, from our point of view, any technology offering IPv6 support. At least when they are not reachable, they are identifiable through technologies such as Radio Frequency Identification (RFID), and Near Field Communication (NFC).

Resource discovery is the process by which the user is able to find devices offering services according to his criteria and interests. It can differ from the resources that the user can explicitly request or from a more sophisticated discovery where the network is more pro-active, and it notifies the user about the availability of these new devices [18].

Resource discovery will provide descriptive information, such as the resource type or family, and some attributes to describe it. In addition, it will provide the information that the user will need to reach them, i.e.: a locator such as a URL or IP address.

Resource discovery management requires dynamic updates to the system with the new resources included in the network, as well as the ability to integrate the updates over mobile [19] in order to be consistent with the real resources reachable at a specific moment, and security [20] to protect resources and services that one may want to access through controls.

Service discovery is focused on the description of those services provided by technologies, such as those that are Web-based, i.e.: XML, Web Services, or other technologies such as JSON, and DNS Service Directory.

These services include printing and file transfer, music sharing, servers for pictures, documents and other file sharing, as well as services provided by other resources. With the expansion towards the Internet of Things, other, simpler services can be considered, such as the environmental status consultation for temperature, humidity and lighting, a pressure value for a parking sensor, or the value of glucose for a medical device.

Different techniques can be found for resource and services discovery and the Internet of Things. Right now, the most common approach is the definition of M2M platforms [21], such as ThingWorx, Pachube, Sen.Se, and SENSEI, where the devices are registered in the platform, and are reachable from the Internet through WebServices such as SOAP and REST. The problem with this static approach is that it is limited to the information on the platform and the manually registered devices and, for that reason, defining more scalable solutions must be required. This makes it possible for resources entering the network to be available by registering with the discovery system, without any interaction with the user, on a directory system that is homogenous and consultable simply over the Internet, without the need to use a specific M2M platform.

This capability for autonomous registration and the discovery functionality to be dynamically adapted with the inclusion of new devices in the network is necessary for the above-mentioned IoT to be flexible and ubiquitous. It is also necessary for the scalability required to manage every resource connected to the network, whose number is continuously increasing. It is not feasible to continue considering IoT solutions that require a manual and static management of resources, with fixed registration over specific directory systems from the M2M platforms.

Some naming systems such as Lightweight Directory Access Protocol (LDAP) [22], Universal Description, Discovery, and Integration (UDDI) [23], and Domain Name System (DNS) [24] offer resource and service directory capabilities, and more specific resource discovery technologies could be added, such as UPnP, JINI, Service Location Protocol (SLP), and Rendezvous or Bonjour protocol over DNS-SD.

The solution considered for the Internet of Things has been DNS-SD because an independent directory for the resource is needed. Consequently, other approaches based on multicast queries such as SLP – with direct discovery of resources – are not feasible for the IoT. That solution does not work properly because, for one, the resources are not discoverable while they are sleeping, and they need sleep in order to optimize their power consumption and lifetime. It also does not work properly because the overload from multicast for this kind of mesh topology network is not appropriate and, finally, because continuous requests to the node overloads the end-device.

Rendezvous protocol from ZeroConf Architecture, which is used for Bonjour in MAC OS, or AVAHI in Linux OS are based on the DNS-SD from the IETF ZeroConf working group [25] to store the information and multicast DNS (mDNS) in order to query the DNS-SD records.

DNS-SD and mDNS present a solution where no additional infrastructure is needed, and merely requires that resources be enabled with an IP address. The solution is focused on the re-use and extension of existing Internet standards. This can be found with a multicast approach, such as the first stage Service Location Protocol and JINI protocols through multicast, particularly multicast DNS (mDNS), and the DNS service discovery (DNS-SD) to leverage existing Internet protocols. In our approach, following the objective from Glowbal IP to enable all resources with IPv6 addresses, and the re-use and extension of current Internet technologies, we will focus on DNS-SD, as we will describe in Section 4.

Section 4 will also describe the use of common Web technologies for the definition of services, the same way UPnP leverages common Web technologies such as HTTP, SOAP, and XML, to provide access to resources and services. More specifically, WebServices is used for the Internet of Things [26]. It is based on RESTFul and CoAP [27], which is a lightweight version of REST, and the description of services in the DNS-SD [28] follows the semantic [29] and naming conventions that describe how services will be represented in DNS records, as defined by Web Linking description, in particular the version of Link format defined under the CoRE IETF working group [30].

3. Glowbal IP protocol

Taking into account not only IoT heterogeneity, but also the facts that 6LoWPAN (RFC4944 and RFC6282 version) represents low optimization for global communications and that several technologies do not offer native IPv6 support or 6LoWPAN, a more optimized adaptation must be considered. This adaptation for global communications should be compatible with IPv6 and 6LoWPAN, allowing IPv6 to connect to networks with non-IP support, such as Bluetooth and LoWPANs, with only IEEE 802.15.4.

The protocol proposed here provides for an Access Address/Identifier (AAID) which simplifies every parameter from IPv6 communications (source and destination address/port, 36 bytes) in a single 4-byte communication identifier. Thus, the 41 bytes from the IPv6/UDP headers based on 6LoWPAN with global IP addressing can be significantly reduced. This achieves an effective frame format for global communications, and also a mechanism to support global communications in networks that do not have native support for IPv6.

This section will describe the Glowbal IP protocol, its motivation and objectives, the implementation details with its header format description, the tables involved in mapping between Glowbal IP identifiers and IPv6 addresses, and finally some examples of how it can enable IP connectivity to allow interoperability with the rest of the IPv6-based devices connected to the Future Internet Core Network.

3.1. Motivation and objectives

The main motivations for defining the Glowbal IP protocol have been the overload resulting from 6LoWPAN for global communications, as stated above in Section 2.1. Another motive has been to make IP connectivity feasible for non-IP enabled technologies and new IoT technologies, such as Bluetooth Low Energy (BT-LE), which has a limited payload of 19 to 27 bytes.

Based on those motivations, Glowbal IP's objective is to provide connectivity to the Future Internet Core Network based on IPv6 for devices such as IEEE 802.15.4 sensors, which have no support for 6LoWPAN in their stacks. In addition, the purpose is to provide connectivity to other technologies which do not provide any global communication capability in their stack, although they are able to communicate with the Core Network through other interfaces located on their platform. Bluetooth, for example, can be located through handset devices. These handheld devices offer connectivity with the Internet through their GPRS/GSM network interfaces. Therefore, they can be used as a gateway to manage a personal network, where each device is connected to a smart phone through Bluetooth Low Energy, Bluetooth 2.1 or Near Field Communication (NFC) by means of its active mode NDEF Push Protocol (NPP) [31] that can be addressed and can communicate globally. This work is focused on networks based on IEEE 802.15.4, but ongoing work will focus on extending Glowbal IP for Bluetooth Low Energy as well.

Glowbal IP technologically provides current sensors from deployed environments – where IPv6 is not provided – with an adaptation mechanism to make end-to-end connectivity feasible.

Furthermore, it allows interoperability among different scenarios and technologies deployed providing, in turn, an easier mechanism based on the Internet that helps integrate sensors from external providers through a transparent IPv6-based reach. In addition, to these integration heterogeneous multi domain networks [32], it will be addressed in the future issues such as multi-homing, and mobility, which are also some capabilities from IP technologies [20,33–35].

3.2. AAID: Access Address Identifier

Access Address/Identifier (AAID) is a 32-bit address that is generated at the time the connection is set up. The access address identifies a connection between a node and a client.

The sensors can configure/negotiate the AAID with the gateways/Border Routers for a communication process. The usual overload derived from IPv6 address size occurs only at initialization. After initialization, AAID simplifies the parameters from the IPv6 communication (source address, destination address, source port and destination port) in a single 32-bit communication identifier (4 bytes). This reduces the IPv6/UDP headers overload based on IPv6, and even 6LoWPAN with global IP addressing.

In order to make this process more compatible and extendible, AAID has not been considered as an additional network layer; instead, it has been included as part of the current application layer (payload), making this end-to-end connectivity transparent for current end-nodes, and for the communications stacks already defined.

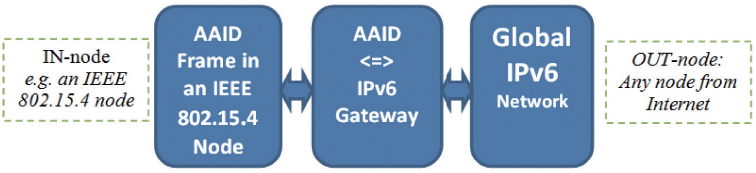

IN-node
e.g. an IEEE 802.15.4 node
AAID Frame in an IEEE 802.15.4 Node
AAID <=> IPv6 Gateway
Global IPv6 Network
OUT-node: Any node from Internet

Fig. 2. AAID translation from Intranet of Things to Internet of Things.

Translation is carried out by the gateways, as shown in Fig. 2.

As we can see, global connectivity is reached through the AAID to IPv6 gateway, which is called an AAID gateway. This AAID gateway's features are similar to the Border Routers from 6LoWPAN, where the Border Router also performs the adaptations in a similar way as the method defined for Glowbal IP.

Finally, with regard to the AAID generation mechanism, a simple hash process is defined based on CRC-32 bits, since this offers low complexity. It can be automatically calculated by the end-node and by the AAID gateway. The hashing is calculated over the session information, as it is defined in Eq. (1).

$$\text{AAID} = \text{h(source IP, destination IP, destination Port)} \tag{1}$$

This AAID value belongs to each node, and is used for the session only. Therefore, it does not presenting aliasing problems, as described in the following section for the Local to Global mapping tables (L2G).

The complexity of AAID generation and management lies in supporting multi-homing and mobility where a different AAID is generated for each of the different gateways, since they assign a different IP source for this AAID node. Therefore, a synchronization mechanism is required for all the AAID gateways involved.

For mobility purpose, it is mainly required a synchronization of the previous AAIDs established in the previous AAID gateway, and the new visited AAID gateway, in order to avoid recalculate them for the new IP address. Therefore, it will be required the transfer and synchronization of the AAID records and information associated in the L2G tables during the binding transfer as part of the mobility protocol.

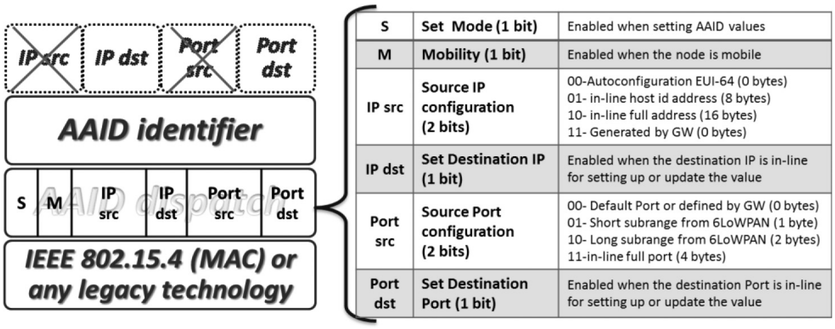
Mobility and multi-homing support is currently being considered for Glowbal IP, and the required fields in the header format and dispatch have been defined in order to report this situation. More specifically, however, this extension of Glowbal IP for mobility and multi-homing support is part of the ongoing work.

3.3. Glowbal IP header format

Glowbal IP is not actually presenting a network header since it is considered part of the payload. Therefore, it can be considered as a session layer over the application layer.

As it has been mentioned, the IPv6 source is generated through mechanisms such as stateless auto-configuration. Therefore, explicit indication is not necessary.

Regarding source port, it can be found two options; on the one hand, it can be considered that each device has a unique application; in this case it is not necessary to indicate the source port either. However, on the other hand, it can considered different applications, such as ports for management applications, e.g. Simple Network Management Protocol (SNMP), control applications for supervisor or privileged use access, and finally user applications. In addition, this should not be limited the capabilities of applications in the future in order to offer a high flexibility for the Internet of Things. For that reason, Glowbal IP offers both options, in the case of working with ports, it is generated an AAID for each one



S	Set Mode (1 bit)	Enabled when setting AAID values
M	Mobility (1 bit)	Enabled when the node is mobile
IP src	Source IP configuration (2 bits)	00-Autoconfiguration EUI-64 (0 bytes) 01- in-line host id address (8 bytes) 10- in-line full address (16 bytes) 11- Generated by GW (0 bytes)
IP dst	Set Destination IP (1 bit)	Enabled when the destination IP is in-line for setting up or update the value
Port src	Source Port configuration (2 bits)	00- Default Port or defined by GW (0 bytes) 01- Short subrange from 6LoWPAN (1 byte) 10- Long subrange from 6LoWPAN (2 bytes) 11-in-line full port (4 bytes)
Port dst	Set Destination Port (1 bit)	Enabled when the destination Port is in-line for setting up or update the value

Fig. 3. AAID format and meaning fields.

of the ports, since it is part of the AAID generation mechanism, see Eq. (1). Finally, regarding security, it is highly interesting in order to manage policies, where specific ports can be reserved for management, and consequently controlled to now allow access from external network, allow only access to specific hosts, or apply an advanced control access.

Right now, the applications are moving around the denominated Web of Things, where the Internet of Things nodes are embedded Web Services server, which deals with all queries regarding the announcement of CoAP methods.

Glowbal IP offers the option of indicating the IPv6 source, in order to be more flexible and for specific use-cases where an end-node uses static addressing is required.

AAID requires information regarding the IP network layer, mainly for the destination node. These factors about specification of source information will simplify AAID management, particularly during mobility and multi-homing.

The IPv6 header format consists of three main parts:

- *AAID dispatch:* Indicates the control information for AAID management, as well as information from the original IP/UDP header in-line. Specifically, the fields provided are:
  - *Set bit* (*S*)*:* This bit indicates the definition of a new session from the AAID gateway to the AAID node, or vice versa. It is usually accompanied by a set of in-line fields, such as destination port, destination IPv6 address, etc.
  - *Mobility/Multi-homing bit* (*M*)*:* This tells the AAID gateway to check with the other AAID gateways, through the back end or the overlay, that this node does not have pending sessions from another location.
  - *IP source format* (*IP S*)*:* These bits indicate whether the IP source address is based on autoconfiguration through the mechanism defined in the RFC 4862 (00); whether it requires the use of a specific host id (01) to keep a fixed address in a local domain; whether it is a state-full address, regularly used by this node (10); or whether it has been delegated to the AAID gateway (11) to use any of the mechanisms described in Section 3.4 for generating the source IP address in the L2G table.
  - *IP destination set* (*IP D*)*:* This bit shows its configuration or lack thereof. This function is usually enabled in conjunction with the S bit.
  - *Port source format* (*Port S*)*:* This is based on the same format as the one for 6LoWPAN in RFC4944, where specific sub-ranges of ports are defined in order to reduce the number of bytes that are required to specify the source port. In addition, as already mentioned, the determination of the port from the AAID gateway can be taken into consideration to simplify the process.

  - ∗ *Port destination set* (*Port D*)*:* This bit shows its configuration of its lack of it. This function is usually enabled in conjunction with S bit

- *AAID identifier*: This defines the 32 bits of the AAID identifier.
- *In-line fields:* Finally, the fields which are in-line for the setting phase of the AAID are closed. We must underscore that the in-fields are only done for the initialization packet, while the rest of the session only performs the dispatch and AAID. In other words, this means only 5 bytes will identify all communications, instead of the usual 26 to 41 bytes from 6LoWPAN.

3.4. Link Layer to Global IPv6 Mapping Table (L2G Table)

In addition to the foregoing issues regarding AAID management with multiple gateways, there is another crucial goal to be met: maintaining uniqueness across the gateways for an AAID association. To this end, the Link Layer to Global IPv6 mapping Table (the L2G table) defines a relationship between the AAID and the MAC address from the device. The only requirement is to guarantee the AAID uniqueness inside a specific device; in the event that an alias conflict (aliasing) takes place between two sessions from the same device, a simple solution can be applied to avoid it, such as a plus one mechanism, i.e. adding one unit to the AAID number when there is some conflict with a previous AAID.

This potential conflict does not require more complex management, since both the AAID gateway and the AAID sensor are aware of the current AAID node sessions, even in scenarios with mobility and multi-homing.

The L2G table stores the mapping between the Link Local address based on MAC EUI-64, the short address in the case of IEEE 802.15.4, and the assigned IPv6 global address.

In the specific case of IEEE 802.15.4, the mapping process can be automated by means of the stateless auto-configuration defined in the RFC4862 [36], where the Interface Identifier for IEEE 802.15.4, defined in the RFC4291 [37], is based on the MAC EUI-64 identifier assigned to the device. The global address for the end device is then created with the combination of the IPv6 prefix and the EUI-64 address. This is equivalent to the mechanism used to build addresses through the Neighbor Discovery protocol, where the Router Advertisement reports the IPv6 prefix, default router address, hop limit, and MTU.

It is assumed that the communication between the AAID node and the AAID gateway is based on extended link layer addressing, i.e. MAC EUI-64 addressing. However, as for the presented for MAC EUI-64 addressing, it can be also considered the mapping with the 16-bit short address. In this situation, a "pseudo 48-bit address" should be built, as indicated in RFC4944, and extended to EUI-64 with the procedure from RFC2464 [38].

Once the IPv6 address has been built for the AAID node, the AAID for each session can be calculated following Eq. (1).

Figure 4 is an example of the L2G table located in the AAID gateway. This scenario functions as a bridge between the adapted network based on IEEE 802.15.4, and the global IPv6-based network.

As we can see, only the native addressing, the calculated source IP, the destination IP address and destination port for the session are indicated for the L2G table, together with the assigned AAID identifier at the end. Section 5 describes AAID gateway implementation and evaluation of the AAID mapping performance.

3.5. Interoperability scenario

IoT consists of a wide range of different scenarios with significant technological differences that prevent direct interoperability. Bearing in mind the foundations of the Future Internet and the Internet

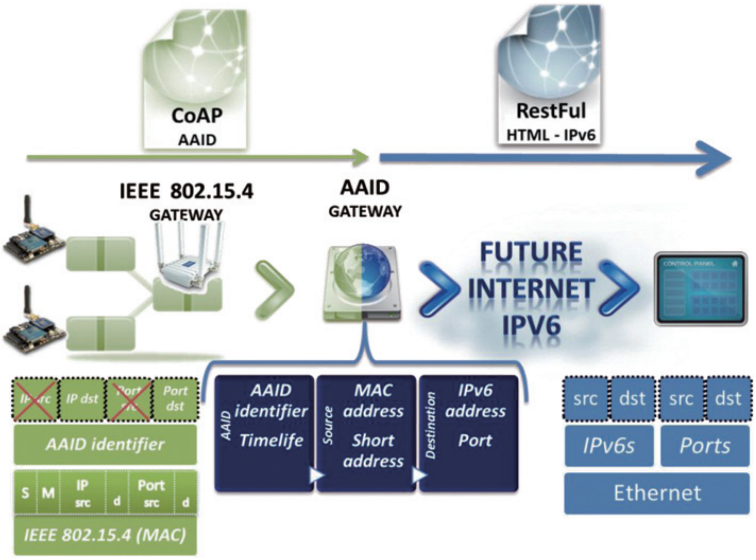


Fig. 4. L2G table for mapping between AAID-based network and IPv6-based network.

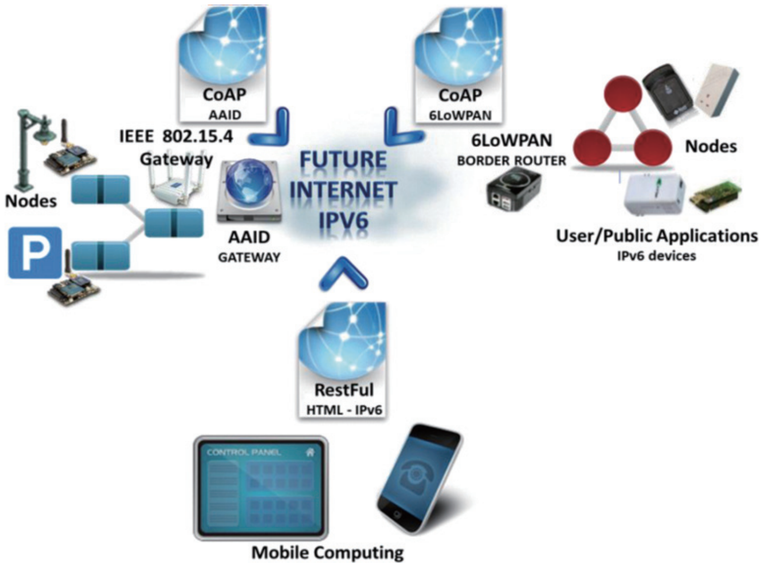


Fig. 5. Inter-operability scenario among Glowbal IP, IPv6 and 6LoWPAN.

of Things, it is therefore imperative to achieve multi-scenario interoperability. This characteristic is one of the advantages offered by the Glowbal IP protocol proposed here.

Figure 5 shows an interoperability scenario, where there are sensors supporting 6LoWPAN and RestFul through Contiki OS, such as Telos B motes, as well as sensors with native IPv6 support, such as SunSpots. It is connected with applications from the user or public management as well, and accessed through the Future Internet network in a transparent and homogeneous way.

The rest of the platforms/technologies/machines that do not offer direct IPv6 or 6LoWPAN support can be adapted in a similar way with AAID over their native application layer (payload). The sensors

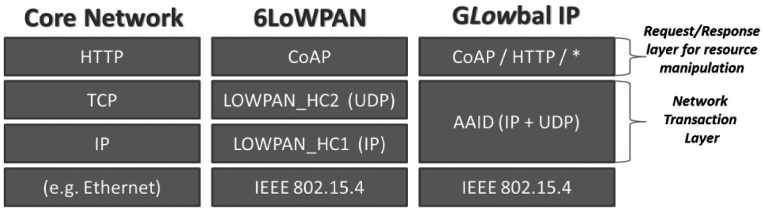


Fig. 6. Different WebServices and application stacks over 6LoWPAN, native IPv6 and Glowbal IP.

considered are the Waspmote nodes, which are highly extended in smart cities and environmental monitoring deployments. Waspmotes only support IEEE 802.15.4. But, these nodes are able to reach IP connectivity through Glowbal IP.

In addition, it is not required to reprogram the communication stack from the nodes, such as it is required to add 6LowPAN support. Thus, Glowbal IP is very useful for deployments where the nodes can be only be reprogrammed OTA for the application layer software, such as it is found in some deployments based on Internet of Things for smart cities such as SmartSantander. Thereby, Glowbal IP is defined in the applications embedded inside the nodes, which is more feasible, scalable and safes that reprogramming the nodes with a full communications stack.

Finally, Glowbal IP allows interoperability with the Future Internet core network, and consequently enables interoperability among scenarios with IPv6 technologies.

4. Enabling network-based Information Systems with Glowbal IP

4.1. WebServices support with Glowbal IP

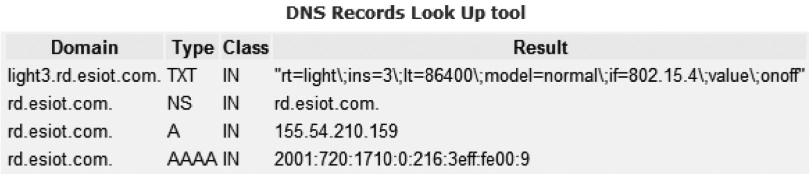
Homogenous access to information and management by way of WebServices such as RESTFul/CoAP and SOAP lightweight is highly interesting and desirable in order to define solutions that are based on the so-called Web of Things [39].

WebServices protocols, such as RESTful and other application packets, are encapsulated after AAID, which only identifies the session to which the packet belongs. Therefore, it also opens an opportunity for the Web of Things and remote Web Services with the end-node. The next table shows the adaptation and homogeneity among IP, 6LoWPAN and AAID, providing the upper layers with connectivity support.

Subsequently, for transactions and transport, HTTP over TCP could be applied in the current Internet architecture; CoAP over 6LoWPAN in the current Internet of Things, based on 6LoWPAN; and finally, the proposed adaptation for non-IPv6 networks, i.e. CoAP, HTTP or any protocol over the Access Address/Identification (AAID), which, as it has been mentioned, encapsulates UDP information (porting) and IP information (addressing).

Figure 6 shows the relationships among the different stacks for the network transaction layer, which involves networking and transport, as explained in previous sections. However, it also takes into account the application layer for the request/response of the different resources, as well as services from resources. For this purpose, the most common technology is the Web of Things, which defines the use of REST for the Core Network, and a light version of REST for 6LoWPAN, called CoAP. In the case of Glowbal IP, any of them can be considered since it is independent from the network layer, although CoAP is more frequent due to its advantages for constrained devices.

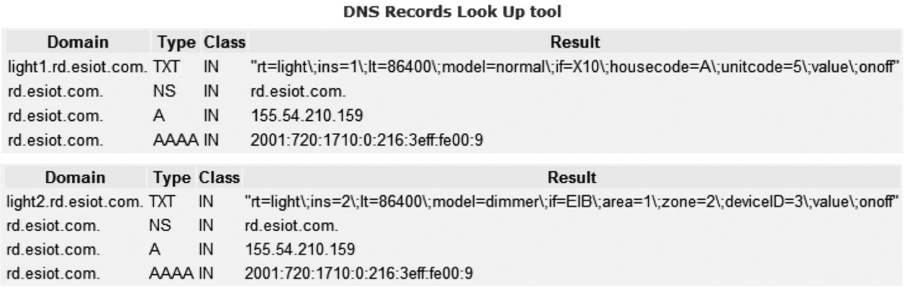
To do so, the sensors are extended with RESTFul methods and attributes. Web Services offers interoperability and homogenous access to services, regardless of the technology from the underlays.



DNS Records Look Up tool

Domain	Type	Class	Result
light3.rd.esiot.com.	TXT	IN	"rt=light\;ins=3\;lt=86400\;model=normal\;if=802.15.4\;value\;onoff"
rd.esiot.com.	NS	IN	rd.esiot.com.
rd.esiot.com.	A	IN	155.54.210.159
rd.esiot.com.	AAAA	IN	2001:720:1710:0:216:3eff:fe00:9

Fig. 7. DNS-SD for a thing based on IEEE 802.15.4 accessed through Glowbal IP.[1]



DNS Records Look Up tool

Domain	Type	Class	Result
light1.rd.esiot.com.	TXT	IN	"rt=light\;ins=1\;lt=86400\;model=normal\;if=X10\;housecode=A\;unitcode=5\;value\;onoff"
rd.esiot.com.	NS	IN	rd.esiot.com.
rd.esiot.com.	A	IN	155.54.210.159
rd.esiot.com.	AAAA	IN	2001:720:1710:0:216:3eff:fe00:9

Domain	Type	Class	Result
light2.rd.esiot.com.	TXT	IN	"rt=light\;ins=2\;lt=86400\;model=dimmer\;if=EIB\;area=1\;zone=2\;deviceID=3\;value\;onoff"
rd.esiot.com.	NS	IN	rd.esiot.com.
rd.esiot.com.	A	IN	155.54.210.159
rd.esiot.com.	AAAA	IN	2001:720:1710:0:216:3eff:fe00:9

Fig. 8. DNS-SD for a thing based on X10 (top) and EIB/KNX (bottom) accessed through Glowbal IP.

For example, the same set of sensors is considered with different technologies, even when the physical sensor comes from a different manufacturer, such as IEEE 802.15.4, X10 and EIB/KNX. For example, a common set of RESTFul services interface has been defined for the attributes of a light. This will prove scenario independence, since both can be accessed at the same way, by defining the appropriate IPv6 address. *See* next section, and Figs 7 and 8, where all the light sensors offer the same “onoff” and “status” CoAP methods in order to change the status, and then consult the respective status.

4.2. Discovery support with Glowbal IP

Discovery allows resources to become aware of services from the rest of the resources without explicit management from the user. This means that a user, and even another resource, can discover and potentially use a resource without prior knowledge of it, and of its capabilities and services.

Section 2.2 discussed a wide range of discovery systems, most of which are in use today. It concluded that the majority of them look for a homogenous way to locate devices, and the solution used to locate resources is IP. We should emphasize that IP addressing is not directly used on a regular basis; the URL or device name is offered instead, although, at the end, it is an IP-based locator. Therefore, Glowbal IP presents the advantage of continuing to use the already extended discovery systems for the Internet of Things.

The chosen solution for discovery is DNS-SD and mDNS, which is an evolution of DNS. It is mainly focused on the naming aspects for resources, although it also offers the description of the resource and services through the use of its records. Note that this solution defines neither new operations nor new DNS record types. Therefore, it is fully compatible with the current DNS deployment.

Originally, DNS-SD defines DNS pointer (PTR) records to indicate the type of service using the form _type._protocol.domain for a specific IP locator. These pointers are originally defined by the reverse DNS

[1] The different TXT records can be tested for light1.rd.esiot.com, light2.rd.esiot.com, and light3.rd.esiot.com through the DNS tool: http://www.hscripts.com/tools/HDNT/dns-record.php.

Table 1
Link Format and DNS-SD description for the resource

Link format	DNS-SD
Resource Instance (ins=)	{instance}
Resource Type {rt=}	{ServiceType}
<uri> (It is already obtained from the AAAA entry)	TXT path=
Interface Description {if=}	TXT if=
Additional attributes (e.g. the CoAP methods){xxx=}	TXT xxx=

protocol. Through these reverse DNS records, the user is able to find all resources in a specific domain, e.g.: "example.com," by issuing a query for _http._tcp.example.com.

In this case, _http denotes the application-layer protocol that the user is looking for services based on HTTP, while _tcp indicates that the service runs over TCP/IP stack, and example.com denotes the domain to which the query is directed. Furthermore, DNS-SD is extended with mDNS in order to carry out the queries, and use the ".local." domain to operate over link-local multicast.

The aforementioned pointer records contain the service instance names in a format for matching the query. For example, a query for printers might return the URL for the printer available in the domain. DNS-SD overloads this request so that when the client passes a service type in the query, the query returns service instance names.

In addition to the reverse directory, the type of service can be determined, where RFC2872 [40] defines a group of very well-known services, and "TXT" records which will be associated with that service to define the attributes or keys, such as model, ID, type, status, or more specific information for each service.

With regard to the Internet of Things, a simplification of this DNS-SD through the CoRE IETF working group has been defined. For example, this simplification only considers the discover resources by requesting "/.well-known/core".

From the CoRE point of view, the DNS-SD can be seen as a repository for Web Links. The use of Web Linking for description and discovery of resources hosted by constrained web servers is specified by the CoRE Link Format.

Discovery is performed by sending a native query to the DNS-SD through the mDNS protocol, or it can be used through the CoAP interface, where parameters such as Resource Type (rt) are defined to filter the kind of device. It should be pointed out that the functionality through DNS-SD native protocol and CoAP is equivalent, but the CoAP extension is also considered in order to make the discovery process simple and homogenous for devices with constrained capabilities to implement an additional protocol for the DNS.

Specifically, the attributes for a specific device are defined using the well-known CoRE Link Format interface or any other description format over one "TXT" record.

In particular, the CoRE Link Format defines the following attributes for the "TXT" record: Resource Type "rt", Instance attribute "ins", assuming that we can find multiple instances of the same resource type in an environment, e.g.: multiple lights and temperature sensors can frequently be found. In addition, other parameters are considered, such as Interface "if" in case multiple technologies are available on the platform, and other parameters such as lifetime "lt", domain "d", and context "con".

Table 1 presents the differences between the CoRE Link Format used for the Internet of Things and the original DNS-SD. As we can see, DNS-SD uses multiple TXT entries, while Link Format uses only one, allowing for a reduction in overload for the transmission of each record, due to the restrictions in the payload size for the Internet of Things communication technologies.

An example of this access via CoAP is the following request for the resource type Temperature over a determined resource directory, such as:

GET /rd.esiot.com?rt=Temperature

The result could indicate the CoAP method "temp" over the URL node1.esiot.com for the asked resource type Temperature.

<coap://node1.esiot.com/temp>;rt="Temperature"

In this particular case, native access from DNS will be understood to request the records. Figure 1 shows the example of a device connected by way of a native interface "if" IEEE 802.15.4, with the CoAP methods "value" to consult the current status of the sensor, and the method "onoff" to change the status, as well as common fields defined by the CoRE Link Local format, such as the resource type "rt", and instance "ins".

In addition to this basic approach, in this work we have defined an extended set of parameters for the "TXT" record. We should highlight that it has a capacity of up to 65536 bytes. For example, Fig. 8 presents the look-up for a light under rd.esiot.com. In particular, the light2.rd.esiot.com, which is a resource type of dimmer with EIB/KNX technology, and the location for the specific technology, which is accessed through the platform (presented in Section 5) is Area: 1, Zone: 2 and DeviceID: 3. Therefore, this offers an extended description of the sensor and its status. All of these values can be consulted through CoAP methods, as defined with the CoRE approach as well.

Furthermore, it should be noted that DNS has some limitations regarding automatic updates, and dynamic and fluid interactions with devices. In order to stay synchronized with the current status of the sensor, the management of the domain has been integrated inside the AAID gateway, that is, the manager for the mapping between the IPv6 address and the specific device. Automatic updates and synchronization with the DNS values are performed, together with the real status from the network. As presented in Section 5.2, these functions have been specifically implemented in the Border Router from the Internet of Things network, which is the same gateway where the AAID gateway is located.

It can be located outside the AAID gateway/Border Router as well, but this could cause the above-mentioned synchronization problems. If DNS-SD is not located at the gateway, it can define multiple ways to discover this resource directory location, such as using DHCP.

Finally, the example for the light1.rd.esiot.com, and light2.rd.esiot.com with EIB/KNX and X10 technology (see Fig. 8) has been presented; this platform offers connectivity with different non-IP technologies, such as EIB/KNX, X10, Bluetooth, IEEE 802.15.4, etc. This allows for managing the information locally, even when it is globally available and accessible through DNS queries.

5. Evaluation

The AAID Gateway has been implemented in a multi-protocol system based on an ARM CPU and an embedded Linux OS, and the AAID node in an IEEE 802.15.4 USB dongle based on Jennic JN5139 chip. Furthermore, the performance and scalability of this system has been evaluated, together with the interactivity and mapping process between the AAID node and the AAID Gateway over the IPv6 network from the University of Murcia.

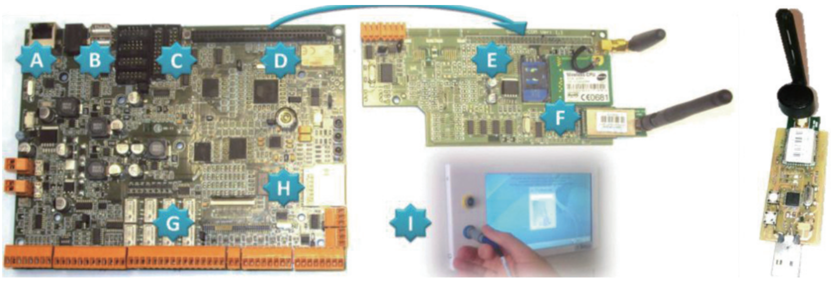


Fig. 9. AAID Gateway on the multiprotocol card (left) and AAID node on the 802.15.4 USB dongle (right).

5.1. Implementing Glowbal IP

The evaluation was conducted on the platform that our research lab developed to build automation and industrial environments. For example, a previous version of this platform was deployed in a building automation solution [41],

This platform consists of a hardware modular solution, based on Linux OS, that allows the upgrade of platform components without requiring reconfiguration of the other components. This characteristic makes this platform more expandable, and offers the option of installing software that has already been tested and made available for Linux, making it more robust. Specifically, it supports capabilities for routing (*route*), router advertisement (*radvd*), policies (*iptables*), and DNS-SD (*bind*).

The implementation of the daemon involved in the AAID gateway makes this adaptation practicable. Specifically, a *tap* interface is built with the addresses assigned to the objects with AAID. Thereby, it is able to collect all the received packets for AAID nodes through a daemon with a RAW socket, *SOCK_RAW option*, listening in promiscuous mode, *ETH_P_ALL option*, in the *tap* interface.

The AAID Gateway platform is presented on the left side of Fig. 9. It is based on the ARM9@400Mhz 32-bit processor, with 256MB LPDDR RAM memory, and 256MB NAND memory, which supports Linux OS. It offers an Ethernet 10/100Mbps (A), 2 USB 2.0 ports (B), 4 Serial RS232 ports (C), Bluetooth 2.1 with HDP profile compliant with BlueGiga (D), GPRS from WaveCom (E), IEEE802.15.4 ZigBee from Jennic (F), 24 inputs/outputs among digitals/analogs/relays (G), a compact flash support for data logging (H), and a touch screen LCD (I). Finally, other capabilities are interesting for continuous sensing, such as real-time watch, 5 high precision timers, 2 analog/digital converters for analog signal processing, a random number generator for security seeds, and IPv6 stack support.

Furthermore, the AAID node is shown on the right side of Fig. 9. It is based on the Jennic JN5139 module. It also has a OpenRISC 32-bit processor, which supports IEEE802.15.4 stack, and ZigBee Pro. It is able to set it up with 6LoWPAN as well, but for this evaluation it has been defined with the basic IEEE 802.15.4 stack. This is connected to the PC through the USB port. Thereby, it is easily programmable and permits debugging the results through the emulated serial port. In addition, it offers an advanced cryptography stack based on Elliptic Curve [42], which is highly relevant for the Internet of Things, due to its security requirements and privacy issues [43,44].

The next section shows the evaluation performed over this platform, where the AAID approach has been implemented.

5.2. AAID mapping performance

The AAID mapping performance has been evaluated in the multi-protocol card shown in Fig. 9 (left). This multi-protocol board is responsible for mapping between the multiple technologies and its corresponding IPv6 addresses, and vice-versa.

This AAID Gateway functionality is divided into the following two modules:

- *Sender module*: This corresponds to the module allocated in the multiprotocol card to manage the traffic generated from the non-IP devices, by way of AAID technology support to the Core Network. This module identifies and knows in-depth the connection and session information for each device, since it manages the L2G table. It is listening to the native interfaces from the technology used for each device – IEEE 802.15.4 in this case, through a serial port – but it can be also accessed through a serial port in board technologies such as X10, EIB, CAN, and Bluetooth. It checks that the AAID is previously used and available in the L2G, or if it is a set message and requires inclusion in the L2G mapping table.
- *Receiver module*: This is also allocated in the multiprotocol card to manage the incoming traffic from the Core Network to the specific technologies and specifications. This module is a daemon which is listening, in promiscuous mode, to the messages received from the global network. Once a message is received, this receiver maps the IPv6 destination address to the correspondent AAID, and follows the mapping specifications in order to detect whether this is from a previous session, or whether it is necessary to set up a new AAID.

In the AAID node, a pre-analysis in the incoming packets is also defined to determine the session from the coming packet, as well as a post-processing, in order to include the AAID information to the payload.

This process has been evaluated with a flow of data packets between a server and an AAID node with 500 consecutive requests (each one with a different port). Over this evaluation, the total time was calculated for processing the mapping and the reply. Therefore, the transmission time has been calculated as the difference between the total time, and the time calculated locally in the AAID GW, and AAID for the processing. The result is divided by 2, to consider only the time for one-way transmission, not for the full round-trip.

The results, shown in Fig. 10, come from the division in processing in the AAID GW, the processing in the AAID node, and the one way transmission time (half of the round-trip transmission time).

Furthermore, a summary of the results has been also defined in Table 2, where the minimum, maximum, and average for each of the considered times were calculated.

With regard to the mapping processing, it is not introducing a high delay. More specifically, the mapping processing in the AAID gateway is practically instantaneous; being only slightly higher in the AAID node due to its constraints, but this also presents an average time of 22 milliseconds. Therefore, carrying out this mapping processing is entirely suitable.

It is important to point out that the transmission times are low, since they were evaluated with a server located at the same network. But, it is not relevant for the evaluation for the AAID mapping.

6. Discussion

This section summarizes how Glowbal IP addresses the requirements from Internet of Things to extend the access and use of the Future Internet infrastructure, homogenizes the access to the services/resources/devices, and extends global access with high level aspects such as interoperability among scenarios, as well as future mobility and multi-homing. Specifically, it can be summarized in five key points, which represent a significant contribution to the current status of the field.

At the beginning, Glowbal IP followed the spirit from Future Internet; IPv6 nowadays is being turned into a key technology for the Internet of Things. Until now, the usual practice was build islands of Wireless Sensor Networks connected to the Internet by way of a Portal Server or a Gateway, where the

Table 2
Summary of the mapping performance for 500 sessions

Description	Minimum	Maximum	Average
Time transmission (half of a round-trip)	9,900 ms	32,920 ms	15,900 ms
Time processing AAID Gateway	0,020 ms	0,110 ms	0,033 ms
Time processing AAID node	20,828 ms	34,170 ms	22,828 ms
Total	22,444 ms	54,965 ms	38,969 ms

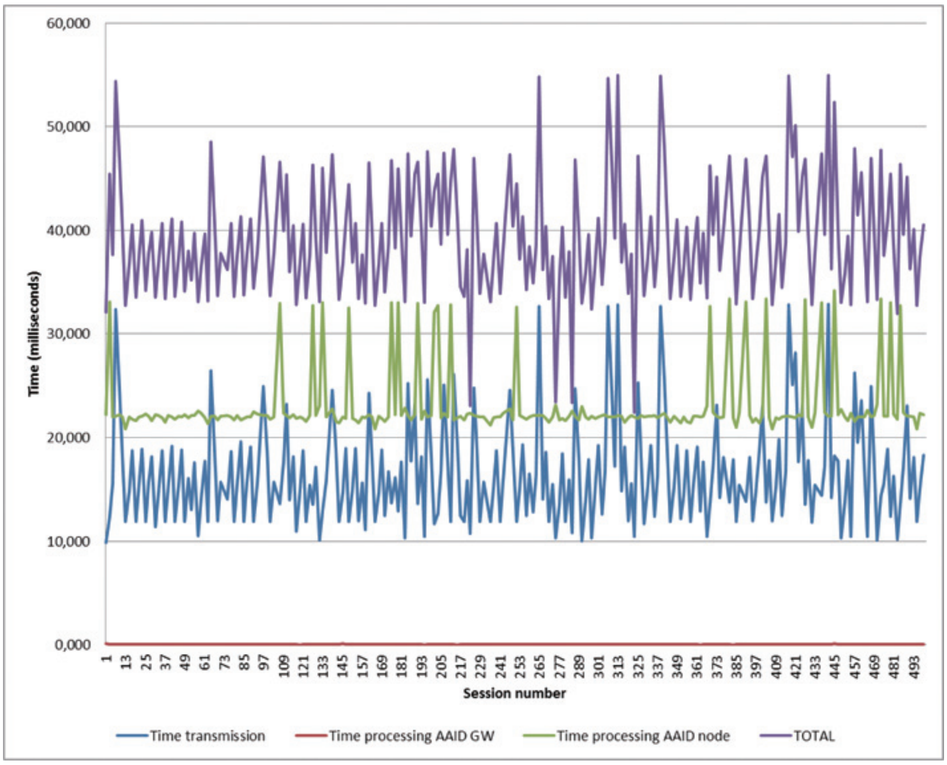


Fig. 10. Performance evaluation for the AAID mapping in AAID Gateway and AAID node.

information is processed and later sent to the defined clients. These approaches offer what literature calls an Intranet of Things. Therefore, in order to move toward a real Internet of Things, it is necessary to provide support for end-to-end and global access, which is located at IPv6 capabilities.

The second contribution is opening legacy technologies and already deployed devices to a new range of IPv6-enabled services. Based on the Glowbal IP integration mentioned in the first contribution, a real interconnected physical and virtual object (end-to-end) can be reached by way of IPv6. Thereby, a homogeneous, transparent and scalable access to the devices and services can be achieved. From the Web of Things approach, the RESTFul methods could be applied directly to the end-device, increasing the scalability of the solution, flexibility and allowing for extension of the ubiquitous concept with mobility and global interoperability.

The third contribution is that Glowbal IP supports RESTFul/CoAP at the end-device level, in order to make the solution more scalable than the current approach mentioned, where the portal server is required to translate from native protocol (e.g. Waspmote) to HTTP Push method (e.g. REST). In short, Glowbal IP presents the integration of CoAP methods in the IoT nodes.

The fourth contribution is the interoperability of heterogeneous Smart Things (IoT nodes), systems and scenarios from different IPv6 enabling technologies, such as 6LoWPAN, and native IPv6. The mentioned enablers are supplemented with Glowbal IP for other nodes such as IEEE 802.15.4 and Bluetooth nodes. The interoperability is reached through homogenous RESTFul/CoAP. In addition to the interoperability among scenarios, communication with external sensors is also feasible. Therefore, it also enables cross-domain applications. It is well known that IoT technology is useful in numerous application domains, ranging from environmental monitoring to health monitoring, smart spaces, improvement of industrial processes, and so on. The entry barrier to getting involved in this domain and starting to offer new products or services is not very high: when the plethora of potential applications and low entry barrier is combined, the IoT domain is suitable for agile SMEs to develop a range of new products and services. An easy integration of the current SME solutions with the services and potential offered by IoT is also feasible. All in all, it is opening possibilities to define innovative business models based on end-to-end connectivity and supporting innovative Internet services.

The fifth contribution is the re-use of existing IP technologies such as DNS Service Directory (DNS-SD) and multicast DNS (mDNS) for discovery purposes, in addition to defining the exploitation of network-based information systems through the definition of the resource and service directories in the already deployed DNS servers.

7. Conclusions and future works

This paper has presented the innovative protocol Glowbal IP for the extension of devices already deployed and legacy technologies to IPv6. It allows a user to create global communications and network layer homogeneity through IPv6. In addition, Glowbal IP solves the lack of optimization from 6LoWPAN with regard to global communications, which requires from 26 to 41 bytes for the 6LoWPAN header, while AAID only requires a 5-byte header, when the identification of the session is carried out by way of AAID identifiers.

The research has also shown how to exploit the network-based information systems through the current DNS deployment, with the DNS Service Directory and multicast DNS. This allows a system to describe information in the network about devices such as family, model, features and Web Services offered in order to interact with it.

Finally, this has been evaluated in a multiprotocol card developed in our lab, and this system represents a low delay because the mapping tasks defined Glowbal IP as a suitable technology to be deployed.

Ongoing work is focused, firstly, on the extension of Glowbal IP for mobility and multi-homing, and the connection of islands of discoverability. For these three purposes, we are working on an overlay which offers ancillary support to the capabilities from IPv6 protocols. Secondly, Glowbal IP will be evaluated for Bluetooth Low Energy, due to its capabilities for the Internet of Things. Specifically, this is an interesting technology because it is located in handset devices, and these devices offer connectivity with the Internet through their GPRS/GSM network interfaces. Therefore, they can be used as a gateway for the management of a personal network.

Acknowledgments

This work was made possible by the generous support of the Excellence Research Group Program (04552/GERM/06), from Seneca Foundation; FPU program (AP2009-3981), from the Spanish Ministry of Education and Science; and in the framework of the IoT6 European Project (STREP) from the 7th Framework Program (Grant 288445).

References

[1] C. Endres, A. Butz and A. MacWilliams, A survey of software infrastructures and frameworks for ubiquitous computing, *Mobile Information Systems* **1**(1) (2005), 41–80.

[2] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, *Computer Networks* **54**(15) (2010), 2787–2805.

[3] A. Durresi, M. Durresi, A. Merkoci and L. Barolli, Networked biomedical system for ubiquitous health monitoring, *Mobile Information Systems* **4**(3) (2008), 211–218.

[4] C. Sotomayor, A.J. Jara and A.F.G. Gómez-Skarmeta, Real-Time Monitoring System for Watercourse Improvement and Flood Forecast, Lecture Notes in Computer Science, *Springer Verlag* **6935** (2011), 311–319. ISSN: 0302-9743.

[5] J. Santa, M.A. Zamora, Antonio J. Jara and A.F.G. Skarmeta, Telematic platform for integral management of agricultural/perishable goods in terrestrial logistics, *Computers and Electronics in Agriculture*, ElSevier, ISSN: 0168-1699, Vol, 89, pp. 31–40. doi:10.1016/j.compag.2011.10.010, 2011.

[6] O. Haubensak, Smart Cities and Internet of Things, Business Aspects of the Internet of Things, 2011.

[7] A.J. Jara, M.A. Zamora and A.F.G. Skarmeta, An internet of things-based personal device for diabetes therapy management in AAL, *Personal and Ubiquitous Computing* **15**(4) (2011), 431–440.

[8] Z. Shelby, Embedded web services, Wireless Communications, *IEEE* **17**(6) (December 2010), 52–57, doi: 10.1109/MWC.2010.5675778.

[9] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC4944, September 2007.

[10] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Network, IETF 6LoWPAN Working Group, RFC6282, 2011.

[11] B. Emerson, M2M: the internet of 50 billion devices, Win-Win, Editorial: Huawei, January 2010.

[12] J.J.P.C. Rodrigues and P.A.C.S. Neves, A Survey on IP-based Wireless Sensor Networks Solutions, in: *International Journal of Communication Systems*, Wiley, ISSN: 1074-5351, Vol. 23, No. 8, August 2010, pp. 963–981.

[13] IEEE Standard for Information technology, Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE 802.15.4, 2006.

[14] M. Goyal, W. Xie and H. Hosseini, IEEE 802.15.4 modifications and their impact, *Mobile Information Systems* **7**(1) (2011), 69–92, 10.3233/MIS-2011-0111.

[15] A.J. Jara, L. Marin, M.A. Zamora and A.F.G. Skarmeta, Evaluation of 6LoWPAN capabilities for secure integration of sensors for continuous vital monitoring, V International Symposium on Ubiquitous Computing and Ambient Intelligence (UCAmI'11), 2011.

[16] H.K. Kahng, D.-I. Choi and S. Kim, Global connectivity in 6LoWPAN, draft-kahng-6lowpan-global-connectivity-01.txt, IETF work in progress, March, 2011.

[17] B. Gohel and D. Singh, Global connectivity for 6lowpan draft-singh-6lowpan-global-connectivity-01.txt, IETF work in progress, Feb 2011.

[18] W.K. Edwards, Discovery systems in ubiquitous computing, Pervasive Computing, *IEEE* **5**(2), 70–77, doi: 10.1109/MPRV.2006.28, 2006.

[19] S. Kiyomoto and K.M. Martin, Model for a Common Notion of Privacy Leakage on Public Database, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (*JoWUA*) **2**(1) (2011), 50–62.

[20] A.J. Jara, R.M. Silva, J.S. Silva, M.A. Zamora and A.F.G. Skarmeta, Mobile IP-based Protocol for Wireless Personal Area Networks in Critical Environment, Wireless Personal Communications, Springer London, ISSN: 0929-6212, Vol. 61, No. 4, 2011, pp. 711–737.

[21] A. Herstad, E. Nersveen, H. Samset, A. Storsveen, S. Svaet and K.E. Husa, Connected objects: Building a service platform for M2M, Intelligence in Next Generation Networks, 2009. ICIN 2009. 13th International Conference on, doi: 10.1109/ICIN.2009.5357057M2M platforms, 2009.

[22] J. Hodges and R. Morgan, Lightweight Directory Access Protocol (v3), IETF RFC 3377, Sept. 2002.

[23] P. Mockapetris, Domain Names – Concepts and Facilities, IETF RFC 1034, Nov. 1987.

[24] OASIS, Introduction to UDDI: Important Features and Functional Concepts, Organization for the Advancement of Structured Information. Standards (OASIS), Oct. 2004.

[25] S. Cheshire and M. Krochmal, DNS-Based Service Discovery, IETF Zeroconf Working Group, www.zeroconf.org/ and www.dns-sd.org/, draft-cheshire-dnsext-dns-sd.txt, 2011.

[26] T.R. Sheltami, E.M. Shakshuki and H.T. Mouftah, A web-based application of TELOSB sensor network, *Mobile Information Systems* **7**(2) (2011), 147–163, 10.3233/MIS-2011-0115.

[27] Z. Shelby, K. Hartke, C. Bormann and B. Frank, Constrained Application Protocol (CoAP), draft-ietf-core-coap-06, IETF work in progress, May 2011.

[28] Z. Shelby and S. Krco, CoRE Resource Directory, draft-shelby-core-resource-directory-02, IETF work in progress, 2011.

[29] M. Sabou, Smart objects: Challenges for Semantic Web research, *Semantic Web* **1**(1) (2010), 127–130, doi: 10.3233/SW-2010-0011.

[30] Z. Shelby, CoRE Link Format, draft-ietf-core-link-format-06, IETF work in progress, June 2011.

[31] A.J. Jara, P. López Martínez, D. Fernández Ros, B. Úbeda, M.A. Zamora and A.F.G. Skarmeta, Heart monitoring system based on NFC for continuous analysis and pre-processing of wireless vital signs, *International Conference on Health Informatics*, HEALTHINF, 2012.

[32] A. Durresi, P. Zhang, M. Durresi and L. Barolli, Architecture for mobile Heterogeneous Multi Domain networks, *Mobile Information Systems* **6**(1) (2010), 49–63, 10.3233/MIS-2010-0092.

[33] L.M.L. Oliveira, A.F. de Sousa and J.J.P.C. Rodrigues, Routing and Mobility Approaches in IPv6 over LoWPAN Mesh Networks, in: *International Journal of Communication Systems*, Wiley, ISSN: 1074-5351, Vol. 24, Issue 11, November 2011, pp. 1445–1466.

[34] F.-Y. Leu, I. You and F. Tang, Emerging Wireless and Mobile Technologies, *Mobile Information Systems* **7**(3) (2011), 165–167, 10.3233/MIS-2011-0122.

[35] W. Wu, X. Li, S. Xiang, H.B. Lim and K.-L. Tan, Sensor relocation for emergent data acquisition in sparse mobile sensor networks, *Mobile Information Systems* **6**(2) (2010), 155–176, 10.3233/MIS-2010-0097.

[36] T. Narten and T. Jinmei, IPv6 Stateless Address Autoconfiguration, IETF Network Working Group, RFC 4862, 2007.

[37] S. Deering, IP Version 6 Addressing Architecture, IETF Network Working Group, RFC 4291, 2006.

[38] M. Crawford, Transmission of IPv6 Packets over Ethernet Networks, IETF Network Working Group, RFC 2464, 1998.

[39] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess and D. Savio, Interacting with the SOA-Based Internet of Things: Discovery, Query, Selection, and On-Demand Provisioning of Web Services, Services Computing, *IEEE Transactions on* **3**(3) (2010), 223–235, doi: 10.1109/TSC.2010.3.

[40] A. Gulbrandsen, P. Vixie and L. Esibov, A DNS RR for specifying the location of services (DNS SRV), IETF RFC 2782, http://www.dns-sd.org/ServiceTypes.html, 2000.

[41] M.A. Zamora, J. Santa and A.F.G. Skarmeta, An integral and networked Home Automation solution for indoor Ambient Intelligence, *IEEE Pervasive Computing* **9** (2010), 66–77.

[42] L. Marin, A. Jara and A. Skarmeta, Shifting Primes: Extension of pseudo-Mersenne primes to optimize ECC for MSP430-based Future IoT devices, Multidisciplinary Research and Practice for Business, Enterprise and Health Information Systems, Springer, LNCS, 2011.

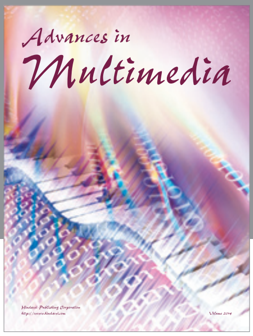
[43] T.A. Zia and A.Y. Zomaya, A Lightweight Security Framework for Wireless Sensor Networks, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* (*JoWUA*) **2**(3) (2011), 53–73.

[44] R. Roman, P. Najera and J. Lopez, Securing the Internet of Things, *Computer* **44**(9) (Sept 2011), 51–58.

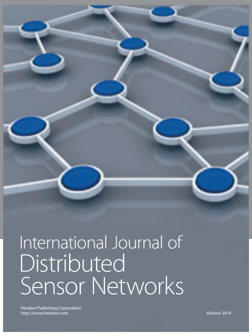
Antonio J. Jara-Valera received his B.S. (Hons. – valedictorian) degree in Computer Science from the University of Murcia (UMU), Murcia (Spain) in 2007, and his M.S. degree in Computer Science from the same institution in 2009, where his Master thesis was about "Internet of Things in clinical environments". He received a second M.S. degree in Computer Science from the University of Murcia in 2010, focused on advanced networks and artificial intelligence, and whose Master thesis was about "Mobility protocols for 6LoWPAN". He has collaborated with UMU's Department of Information Technology and Communication Engineering since 2007, where he currently is working on several projects related to the ZigBee/6LoWPAN and RFID applications in Intelligent Transport Systems (ITS), home automation and mainly healthcare. He is especially focused on IPv6 integration, security and mobility for Future Internet and Internet of Things, which are the topics of his Ph.D. He has published over 40 international papers in this area, and he has worked on different research projects in the national and international area for Internet of Things and IPv6 integration in e-Health, ITS, and building automation.

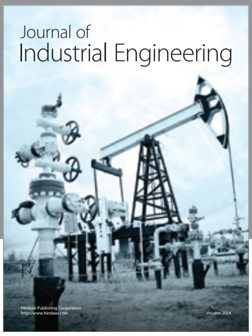
Miguel A. Zamora-Izquierdo received the M.S. degree in automation and electronics and the Ph.D. degree in computer science from the University of Murcia, Spain, in 1997 and 2003, respectively. Since 1999, he has been an Associate Professor with the Department of Information and Communication Engineering, UMU, where he works on several projects related to the remote monitoring and control with a focus on sensors system and embedded system.

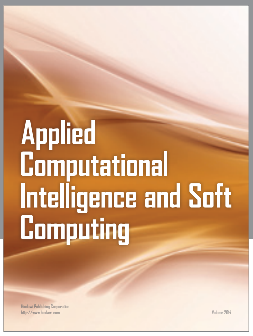
Antonio Skarmeta received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and Ph.D. in Computer Science from the University of Murcia, Spain. Since 2009 he is full professor at the same department and University. Antonio F. Gómez-Skarmeta has worked on different research projects in the national and international area, like Euro6IX, 6Power, Positif, Seinit, Deserec, Enable, Daidalos, ITSS6, and IoT6. He is mainly interested in the integration of security services at different layers like networking, management and web services. Associate editor of the IEEE SMC-Part B and reviewer of several international journals, he has published over 90 international papers and is member of several program committees.

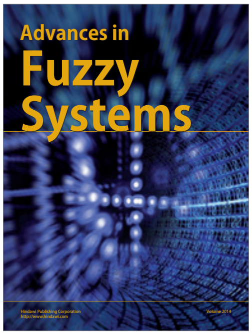

Advances in
Multimedia

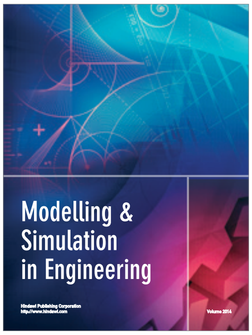
The Scientific
World Journal

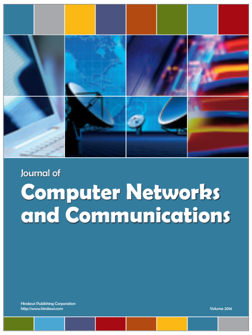

International Journal of
Distributed
Sensor Networks

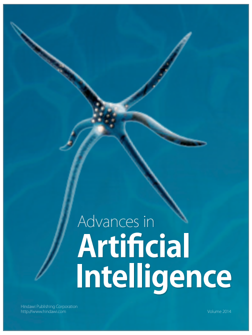

Journal of
Industrial Engineering

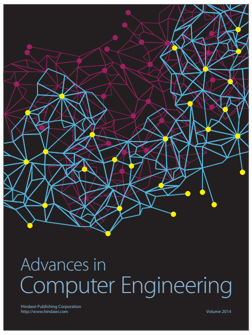

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

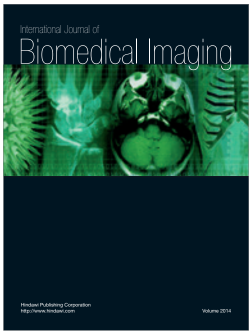

Modelling &
Simulation
in Engineering

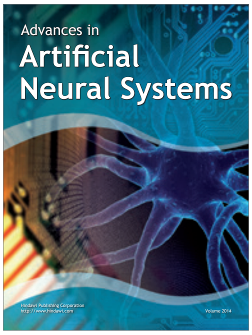

Journal of
Computer Networks
and Communications

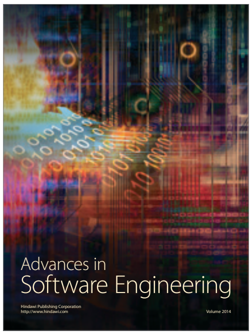

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

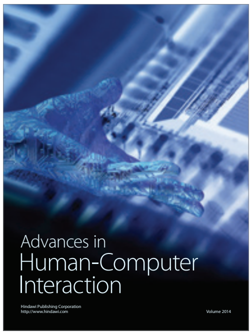
International Journal of
Computer Games
Technology

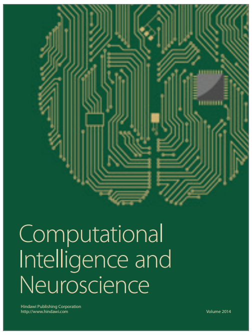

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering