# Managed Ecosystems of Networked Objects

Jeroen Hoebeke, Eli De Poorter, Stefan Bouckaert, Ingrid Moerman, Piet Demeester

*Ghent University - IBBT*
*Department of Information Technology (INTEC)*
*Gaston Crommenlaan 8 Bus 201*
*B-9050 Ghent, Belgium*
Tel.: +32 9 33 14900
Fax: +32 9 33 14899
E-mail: {firstname.lastname@intec.ugent.be}
URL: http://www.ibcn.intec.ugent.be , http://www.ibbt.be

**Abstract** Small embedded devices such as sensors and actuators will become the cornerstone of the Future Internet. To this end, generic, open and secure communication and service platforms are needed in order to be able to exploit the new business opportunities these devices bring. In this paper, we evaluate the current efforts to integrate sensors and actuators into the Internet and identify the limitations at the level of cooperation of these Internet-connected objects and the possible intelligence at the end points. As a solution, we propose the concept of Managed Ecosystem of Networked Objects, which aims to create a smart network architecture for groups of Internet-connected objects by combining network virtualization and clean-slate end-to-end protocol design. The concept maps to many real-life scenarios and should empower application developers to use sensor data in an easy and natural way. At the same time, the concept introduces many new challenging research problems, but their realization could offer a meaningful contribution to the realization of the Internet of Things.

***Keywords*** *Future Internet, Internet of things, sensors, virtualization, clean-slate, network architecture, end-to-end communication*

## 1 Introduction

Advancements in computing, communication systems and miniaturization have lead to the advent of low-power wireless sensors and actuators and the integration of sensors into mobile devices such as smart phones. These sensors enable us to take measurements, collect physical world information, inject this information in the virtual world where it can be further aggregated and processed and, eventually, be used to act again upon the physical world. As such, communication

evolves to a world in which existing communication devices, sensors, actuators and other smart devices and objects can cooperate, enabling person-to-object and object-to-object Internet-based communication. This opens up many new and exciting Internet services in a wide range of application domains: logistics, transportation, smart buildings, environmental monitoring, participatory sensing, security and surveillance, control and automation, traffic management, e-health, location-based services, etc. It becomes clear that these sensor and actuator networks will become a cornerstone of the Future Internet, enabling many novel services and opening up new business opportunities. This requires generic, open and secure communication and service platforms. Communication platforms must enable the smart, secure and manageable interconnection of an ever-increasing variety of communication devices and resources, access networks… Service platforms must guarantee that the wealth of information can be discovered, aggregated, delivered, stored… and turned into value for the Future Internet applications.

To achieve this, these sensors and actuators should be seamlessly integrated into the Internet, which is not possible today due to the structural limitations of the Internet protocols that have not been designed with the characteristics of such lightweight devices in mind. Therefore, sensor and actuator networks are now merely seen as an add-on, as an extension to the current Internet realized by implementing intelligent gateways. This limits flexibility in deployment, usage and the advent of novel services. The systems are not open, intelligence in the end devices that want to make use of the sensor data is limited, communication between diverse geographical locations is complex, etc. This hinders the realization of the targeted communication and service platforms of the Future Internet. We believe that a seamless integration can provide an answer. This does not mean opening up access to sensor data to the whole world, since many scenarios require restricted and secure access to distributed sensor data, involving only a limited group of objects that need to collaborate. It therefore means that objects that need to cooperate should be able to communicate securely and in an end-to-end manner, resulting in a smart communication and service platform that can fulfill the need of many, but not all, application scenarios. This novel proposal for communication of groups of Internet-connected objects will be the subject of

this paper and is encompassed by the concept of "managed ecosystems of networked objects" (MENO).

In section 2, we motivate the need of a seamless integration of sensors and actuators (and networked objects in general) into the Future Internet by looking at today's communication with sensor nodes and identifying the limitations and shortcomings, and by identifying the demands imposed by application scenarios. In section 3 we present a novel possible solution for this challenging problem through the realization of managed ecosystems of networked objects. This general concept tries to address the identified problems by creating secure virtual environments of all involved parties in an automatic fashion in order to offer secure and restricted access to sensors and actuators from other resources such as computers, smart phones, cloud services, etc. On top of this virtual network, a seamless integration will be achieved through the design of a well-chosen set of novel clean-slate end-to-end protocols for sensor data discovery, access and communication, together forming an ecosystem. From the start of the design, we highlight the need to take into account the specific limitations and characteristics of the most limited end devices. In section 4, we present some scenarios and illustrate how they can benefit from the MENO concept, followed by some more general benefits. An overview of the requirements and research challenges involved by this novel concept and the related work in these fields is described in sections 5 and 6. Finally, section 7 concludes this paper.

## 2 Background and motivation

It is clear that smart objects such as sensors and actuators will become a cornerstone of the Future Internet, enabling many novel services and opening up new business opportunities. This requires generic, open and secure communication and service platforms. Communication platforms must enable the smart, secure and manageable interconnection of an ever-increasing variety of communication devices and resources. Service platforms must guarantee that the wealth of information can be discovered, aggregated, delivered, stored and turned into value for the Future Internet applications. Today's efforts in realizing these platforms take one of the following paths:

- Integration of the virtual world in the Internet at the service level [1-2][13-14]: The Internet and sensor networks remain shielded, using heterogeneous networking technologies, but generic glue is provided at the service level (e.g. web query to gateway, gateway that publishes sensor data in the Semantic Web), integrating the virtual world with the physical world and concealing the differences in network communication in the Internet and in the sensor networks. The network communication is taken for granted.
- Connectivity between all objects in the Future Internet by porting Internet protocols to the sensor world [5-12]: Internet protocols are ported to objects such as sensors (e.g. http and COAP, IPv6 and 6LowPan, XML and sensorML) for compatibility reasons, resulting in suboptimal protocols and network communication together with translations, filtering or adaptation layers at gateways, proxies or firewalls.
- Clean-slate design of a new Internet architecture such as done by e.g. [25]: a complete redesign of the current Internet paradigms to interconnect everything with everything. This implies the design of new solutions at the scale of the Internet. This approach is very challenging due to its extreme scale. Therefore, it is particularly difficult to come up with a one-fits-all solution and has a high change of failure to reach actual deployment.

Today's efforts for integrating sensor and actuator nodes into the Internet, except for the clean-slate design, make heavily use of gateway functionality as shown in Figure 1.

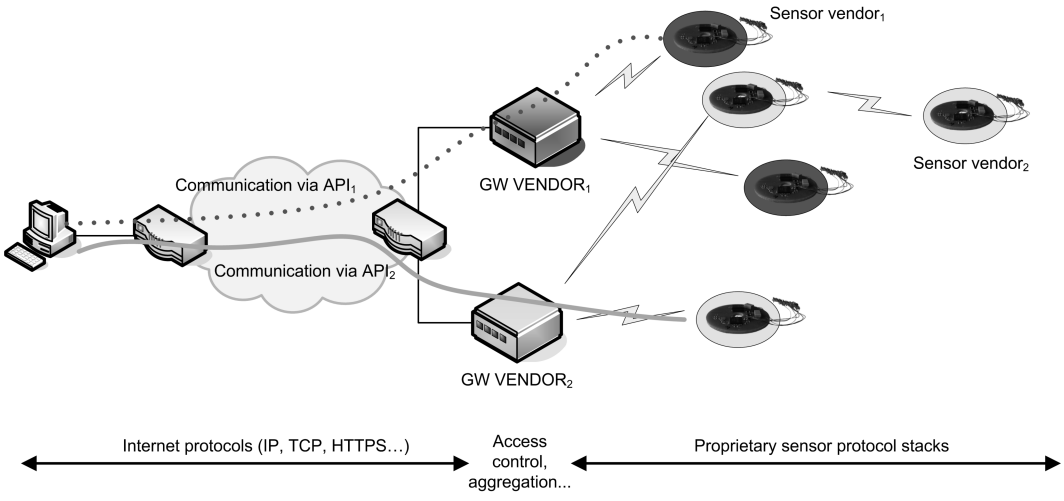


Figure 1: Today's communication with sensor nodes

Dedicated, often vendor-specific, gateways make access to sensor data possible through specifically implemented functionality. The gateway implements the necessary protocols to talk with the sensors and makes (some of) the data available to the outside world, i.e. the Internet, via specific application programming interfaces (APIs). The use of a dedicated gateway has certainly some advantages. Most importantly, the gateway represents a single dedicated point of communication, configuration and access control and is as such, for a single vendor, the easiest way to bring their sensor applications to the market. However, this form of communication has several limitations and disadvantages, which will become more prevalent with the increase of new sensor nodes, their distribution over different geographical locations and the flexibility people desire in the future for integrating sensor knowledge in their applications and for bringing more and more intelligence to end terminals and services in order to create new and innovative services. The following paragraphs list a number of these limitations or disadvantages.

**Protocol translation and centralization of intelligence**: the gateway translates the sensor network protocols to Internet protocols and vice versa. This means that for every sensor application, the gateway must implement the appropriate translation functionality in order to be able to interpret the new type of sensor data. Adding a new type of sensor node can require an upgrade of the gateway. Also, since the gateway is the only one that can directly see the sensor data, the gateway represents the first, and often only, place where intelligent decisions, full control or operations on the raw data can be executed. Intelligence for users is limited to the offering of the gateways and it is not straightforward to shift this intelligence to protocols, to the application endpoints or to the end user terminals in the IP world. This hinders real end-to-end interaction and the possibility for moving intelligence and service capabilities towards the edges of the network, up to users' terminals and things. Having this possibility would stimulate the advent of novel Future Internet services.

**Complexity for application developers**: an application developer that wants to make use of sensor data has to implement the vendor-specific API offered by the gateway and is limited by that interface. Interacting with gateways of different

vendors or with gateways at different locations increases complexity when developing applications and reduces the speed and flexibility of designing novel applications. As such, designing applications that heavily rely on physical world information retrieved from different locations and sensors from different vendors is a tedious task. This hinders the emergence and growth of new companies that offer innovative services based on the readability and controllability of objects via the Internet. Compare it to the success of the current Internet, which has been caused by its unified way for global end-to-end communication and the ease with which Internet applications and services can be designed that reach people over the entire world. Similar unified and end-to-end concepts are needed to facilitate the development of applications that span and integrate the Internet and the embedded world consisting of sensors and other tiny embedded objects.

**Vendor lock-in**: sensor nodes from a specific vendor require a gateway from the same vendor, since the implemented protocols are mostly proprietary and even when they are based on standards, they have often been modified causing incompatibilities with other products that implement the same standard. This limits customer flexibility, since the number of gateways increases with the number of vendors from whom sensor nodes are purchased, forcing customers to stick with the same vendor. This is a deliberate choice of these vendors in order to bind their customers to them by controlling the hardware, the services running on them and the way these services can be used. In addition, it also makes the entrance for young startups to the sensor market more difficult, since they are always tied to the combination sensor and gateway, the only viable market model today. An open architecture for integrating sensors into the Internet would mitigate many of these problems, leading to a decoupling of hardware and the services making use of that hardware. Through such an architecture, some companies can focus on building new sensors, while other companies (or individual application developers) can focus on the delivery of services making use of that hardware, pushing the advent of a new range of Internet enabled services.

**Sensor node distribution and mobility**: the deployment of sensor nodes at different geographical locations requires the installation and configuration of

multiple gateways and the awareness of this by the applications using sensor data. There are no mechanisms to realize the automatic connectivity between different locations. Further, since sensor nodes are bound to a specific gateway, they cannot easily migrate from one gateway to another. This, together with the diversity in APIs, makes it difficult to establish communication among networked objects located in diverse geographical locations and to design applications that can operate transparently from this geographical diversity, heterogeneity of the underlying networks and vendor-specific properties.

**Communication focus**: existing solutions mainly focus on the internal communication, i.e. the communication within the sensor network, and on the interface of the gateway to the outside world, mostly in the form of a web service that exposes the collected and processed data to the outside world. No attention is given to the communication between the gateways and other interested parties, which could be other sensor networks. This part of communication will become more and more important with the advent of what is called the "Internet of Things", where it is assumed that many Internet-connected objects will have to cooperate in a secure and distributed fashion and over heterogeneous networks.

As said, it is envisioned that sensor networks will become a cornerstone of the Future Internet, enabling plenty of new services and giving added value to traditional services. From the above discussion it is clear that in order to fully unleash their potential, a seamless integration of these sensor networks within today's IP-based and tomorrow's Internet is required. It is our general observation that the currently designed systems are not always open and often limit intelligence in the end devices that want to make use of the sensor data, that (secure) communication between diverse geographical locations is complex, deployment and management of the objects remains difficult and that sensors are still mostly seen as an add-on and not as a main Internet component. Consequently, seeing sensor networks just as an add-on, by implementing gateways, will limit flexibility in deployment, innovation in services and will degrade performance as has been shown in the above list with limitations and disadvantages.

We therefore question the usefulness of today's gateways, since they result in an architecture that impedes end-to-end communication that would really be beneficial to unleash the full potential of bringing physical world information into the virtual world. However, we do not question the usefulness of gateway-like devices when they assist in realizing and optimizing end-to-end communication without imposing any additional restrictions. Therefore, we believe that easy deployment, end-to-end connectivity and characteristics, an open architecture and networking protocols, and unified concepts for sensor data retrieval and usage are some of the main objectives to strive for in future architectures for Internet-connected objects such as sensors, actuators and other embedded devices.

# 3 Concept and benefits

To reach the above objectives the following considerations need to be taken into account. Although the Internet connects everything to everything in a unified way, in several important scenarios (today and in the future) its service usage only involves a limited set of devices. In scenarios such as transport networks, site monitoring, Personal Networking… restricted and secure access to a specific group of sensors, possibly distributed or mobile, is required. Opening up access to sensor data to the whole world is not desirable, nor is centrally controlling all access. As such, in these scenarios, communication and service consumption is confined within a limited environment consisting of sensor nodes and other networked objects such as laptops, mobile phones, virtualized machines or resources in a cloud. What we therefore want to strive for is, by making use of the ubiquitous Internet connectivity, to build an open network architecture that enables end-to-end communication between groups of Internet-connected objects and to optimize this communication taking into account the characteristics of the most limited devices: a unified solution for seamless communication at the scale of the objects that need to cooperate and not at the scale of the whole world.

The creation of a secure virtual environment of the involved parties in a distributed and automatic fashion is an interesting solution to offer this secure and restricted access to sensors and other embedded objects. This allows interaction between all sensors and other networked objects that need to cooperate. This approach is also in line with ongoing efforts related to network virtualization,

which are targeted at providing flexibility, promoting diversity and promising increased manageability and security in the Future Internet. However, so far these efforts have always excluded sensor nodes, as these have not been considered as an integral part of the Internet. This virtual environment will run on top of the physical networks, will make use of Internet connectivity and will conceal the heterogeneity of the underlying networking technologies. In addition, this virtual environment should be fully self-organizing and secure, dealing with security, mobility and connectivity aspects.

The great thing about such a virtual environment is that it creates a playground in which novel clean-slate end-to-end protocols can be developed and deployed tailored to the characteristics of the devices and data flows, which are strongly different from the characteristics encountered in today's IP world. IP and its higher layer protocols succeeded in solving the interconnection and interoperability issues of different networks. However, taking into account the advent of lightweight devices such as sensor nodes, it is clear that the standard IP protocols (e.g. IP, TCP, HTTP…) are too heavy for these devices and that they have been developed with a completely different mindset. In addition, a lightweight version of them is also not the best design approach, since real end-to-end connectivity and easy sensor data access and usage impose totally different requirements than those that have been used so far. To overcome these structural limitations, a clean-slate design approach is needed within this virtual environment and this virtual environment perfectly offers everything what is needed to introduce such disruptive technologies independent from the limitations of the existing Internet and to achieve a seamless integration of these sensor and actuator nodes. This achievement of real end-to-end communication between all cooperating objects will facilitate the design of novel services, pushing intelligence to the end points and opening up a new range of Internet enabled services.

These clean-slate end-to-end protocols need to support the efficient and intelligent distribution of sensor data within the virtual environment that consists of very heterogeneous devices. This requires novel addressing, routing, transport and data processing capabilities. For example, looking at how sensor data is distributed,

multicast must be a fundamental part of the design and not an add-on on top of unicast functionality. Also, the efficient propagation of sensor data can benefit from intelligent processing in the more powerful devices. Although all objects participate on equal grounds in the virtual environment, more powerful devices can take up a more important role because of their advanced capabilities. However, the devices that can take up this role can vary and their role is not as dominant as in the case with today's sensor gateways. It is only meant to assist the realization of efficient end-to-end connectivity, without imposing any other restrictions.

Next to this, it is of uttermost importance to come up with completely new primitives for application developers in order for them to use sensor data in a natural way and without bothering about sockets, ports… For example, automatic discovery must allow them to discover the sensors present in the virtual environment and the functionality they offer, similar to what is possible today with plug-and-play devices in LAN type networks. (e.g. UPnP, Bonjour…). User friendly naming of sensor nodes, semantic descriptions of sensor data types or groups of sensor nodes must give application developers a means to flexibly and directly talk to sensors and to retrieve and use their data. Introducing this flexibility requires a completely new design approach. The approach of grouping devices into a virtual environment allows taking such a design approach, opening up new possibilities for designing novel end-to-end connectivity and easy sensor data access and usage and taking the fundamental characteristics of the devices and the data flows into account.

Finally, depending on the scenario or over time, the gathering, storage and processing of sensor data can greatly vary in required processing capabilities and storage requirements, putting severe stress on traditional computing devices such as PCs, which have not been designed to scale accordingly. Also, the collected data sometimes needs to be enriched with input from external services or the users in the virtual environment want to offer a subset of the collected and processed data as a service to users outside the virtual environment. To this end, cloud resources can be integrated in this virtual environment. Cloud computing is a paradigm of computing in which dynamically scalable and often virtualized

resources are offered as a service over the Internet, without requiring technical expertise from the users. By bringing resources from the cloud into the proposed secure virtual environment, these resources can make use of the clean-slate protocols, to easily gather the sensor data from several locations in the virtual environment, while benefitting from the security and self-organization of the virtual environment. According to the users' needs, these resources take care of the computing and processing in a very flexible way, due to their inherent nature to automatically scale according to the needs. In addition, the cloud resources brought into the virtual environment, can offer a service through which the collected and processed data can be offered in a controlled way to external partners, establishing interaction with the outside world where it can be used to create novel applications and services. This illustrates that the idea of virtualization and clean-slate protocol design does not at all contradict with technologies being investigated and introduced today. On the contrary, it opens up new ways of using these technologies and linking them to the physical world in an efficient way. It also illustrates that these virtual environments are not isolated islands, but that they represent an abstraction of cooperating objects, an abstraction of which the result of the internal cooperation can be exposed to the outside world.

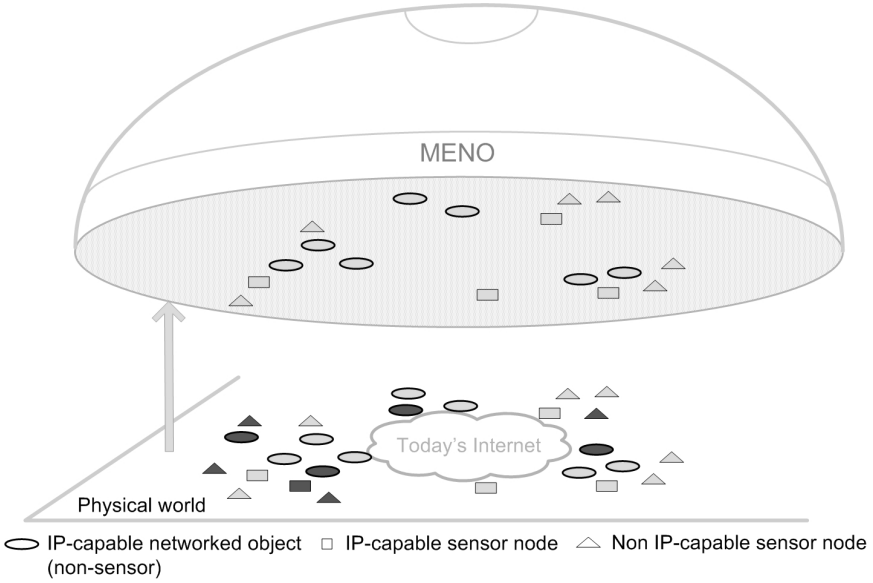


Figure 2: Abstract representation of the MENO concept

All the above ideas and observations, have led to the idea of combining network virtualization and clean-slate protocol design for sensor data access and usage. This idea has been captured in the general concept of Managed Ecosystems of Networked Objects (MENO). Figure 2 shows an abstract representation of this concept. Such an ecosystem is defined as a completely independent, managed, observable, virtual environment of interdependent, networked objects that cooperate in harmony.

- Objects: any device that can communicate, ranging from lightweight embedded sensor nodes over powerful IP devices to virtualized machines and cloud resources
- Interdependent: all objects rely on each other for a common goal and as such represent a logical grouping
- In harmony: seamless, end-to-end operation, requiring a clean slate design from networking to application API
- Virtual environment: objects can be physically distributed, but form one logical network through network virtualization
- Completely independent: can fulfill its function without the need for any interaction with the outside world and is protected from this outside world
- Managed: flexible creation and control of ecosystems
- Observable: properties of the ecosystem can be exposed to the outside world in order to offer services to the outside world

If we look into more detail, we define the following layers as shown in Figure 3.

- The physical network encompassing a wide range of heterogeneous networking technologies (Wi-Fi, Ethernet, 802.15.4, UMTS…), with, currently, Internet as the unified means to communicate between all devices that implement the IP protocol. Connectivity to sensors is realized by devices that bridge the IP world and the sensor world and that implement both networking stacks.
- Using the connectivity of the physical network, a secure virtual logical network is built on top of this physical network, encompassing all devices that need to cooperate in order to achieve a specific goal.
- Within the limited scope of this logical or virtual network, end-to-end communication between all participants is realized through the design of novel end-to-end protocols that support the efficient and intelligent

distribution of sensor data. Augmented with solutions for naming and semantics, this layer offers a powerful API and primitives to application developers for the design of new applications.

- On top of this powerful API, application developers can design new applications and services with reduced effort.

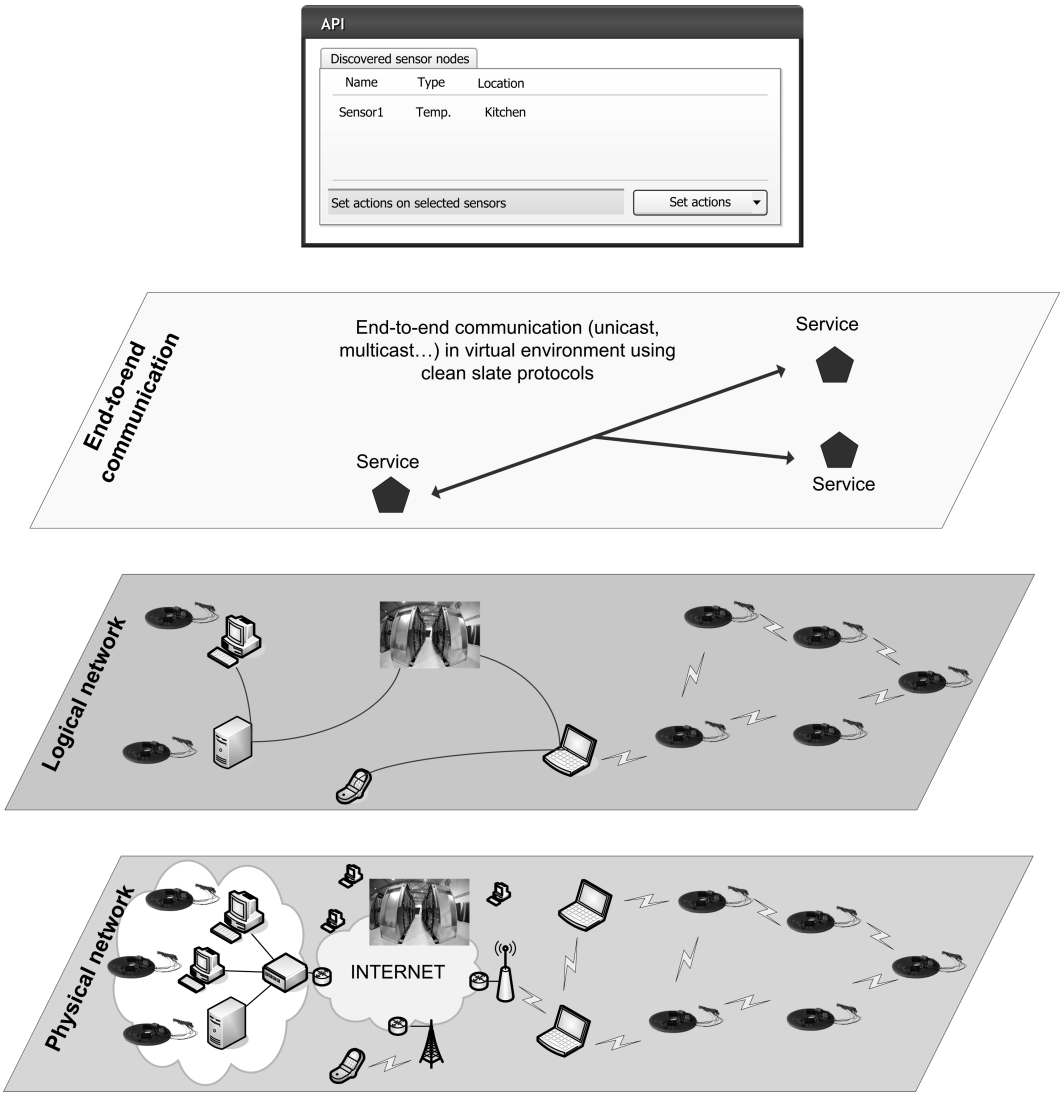


**Figure 3: Layered view of the MENO concept**

From the above description, we can derive the following benefits of the proposed concept. First of all, the virtual environment creates an environment in which all participants can easily and directly communicate without bothering about security, connectivity or mobility. This offloads a great deal of complexity from the protocols running on top and allows the configure-plug-and-play integration of new objects into the ecosystem, thereby matching the use case or communication

needs. The virtual environment offers a local, smaller scale, environment in which direct end-to-end communication can be realized without bothering about gateway APIs. It inherently supports multiple geographically distributed sites and mobility. The latter property is especially interesting when thinking about moving virtual resources, mobile sensors… Finally, the security features of the virtual network ensure that all cooperating objects are shielded from the outside world, a property that is desirable in many scenarios.

Next, on top of this virtual environment, direct access to all objects, including sensors, is realized through clean-slate end-to-end protocols that bypass the limitations of today's Internet protocols. These clean-slate protocols are designed taking the characteristics of lightweight devices such as sensors into account. The end-to-end approach allows the seamless and direct integration of sensors and actuators and empowers end users with the intelligence they need to collect and process physical world data the way they want. Further, the design of protocols within the scope of this virtual environment leads to an optimized solution within a small world, opposed to a generic solution for world-wide access and connectivity to sensors, which would lead to complex architectures. Naming, semantics and new primitives for application developers will empower them to use sensor data in an easy and natural way, which will speed up and stimulate the design of services and applications.

We also argued that our idea does not at all contradict with technologies being investigated and introduced today, but opens up new ways of using these technologies. Exposure of ecosystem data to the outside world ensure that ecosystems do not exist in isolation, but that they can be linked to existing Internet services.

It is also interesting to note that the proposed clean slate approach is restricted to a virtual network environment. The use of virtualization can be seen as an evolutionary approach. When this concept is realized, immediate deployment of the developed solutions on top of the existing Internet is possible through the network virtualization layer that is capable of operating on top of heterogeneous networks. This accelerates the uptake of the newly designed solutions. Later, it

could be possible that virtualization technology becomes an inherent part of the Future Internet design. In that case the developed end-to-end solutions could prove interesting to be deployed directly on top of the Future Internet. Finally, the proposed concept is a generic approach, which has the advantage that it can be used in several scenarios that require cooperation between groups or a selected set of Internet-connected objects, including sensors and actuators.

# 4 Scenarios

As already stated, the MENO concept offers a generic approach in which Internet-connected objects that need to communicate and collaborate are integrated into a virtual network that offers powerful primitives for the design of novel applications and services. Within this virtual network, the most limited devices, i.e. sensors and actuators, can be directly addressed in a natural way and at a local scale, enabling the flexible development of applications, while communication is optimized within the local scope of the virtual network. The result is an integrated end-to-end system offering generic functionality that fits the need of many application scenarios at a local scale and that fits the requirements of many sectors. The availability of such a platform could therefore quickly lead to practical and usable solutions and could stimulate the usage of sensors in sectors where the uptake of these devices is rather limited. In addition, it provides an answer to the need of generic platforms for the Future Internet that capitalize on sensor networks, since currently many of the existing solutions are proprietary or strongly vertically integrated limiting their usage to very specific industries. In the following Table 1, we will give some examples of scenarios that can be supported directly by the generic MENO concept.

It is clear that the MENO concept can be mapped easily onto several scenarios. Of course, there will be scenarios that require different approaches such as centralized localization services based on sensor data coming from sensors embedded in millions of phones. These scenarios will benefit from more centralized architectures such as presented in [1] or architectures that integrate with the current Internet service architecture or Semantic Web [2]. The MENO concept can provide a solution for many, but not all scenarios. Depending one the requirements of the scenario the one or another solution has to be selected. The

same can be observed in the current Internet service architectures, where for example sometimes a choice has to be made between a centralized or peer-to-peer system.

Table 1: Scenarios that can be mapped to the MENO concept

| **Use case 1: Home scenario** | **Use case 2: Transport scenario** |
|---|---|
| Homes are increasingly equipped with sensor nodes (HVAC, fire detection, cameras, passive monitoring, burglar detection…). By integrating all these sensors and the devices of the residents into an ecosystem, they can obtain direct and efficient access to all their sensor data, maintain control over their data and control the house remotely, from wherever they are and in a secure way using for example intelligent applications on their mobile devices. The ecosystem can expose a subset of the data to relevant parties (fire brigade, police, care givers…) | Monitoring of trucks of a transport company equipped with different sensors (camera, temperature, pollution, driving behavior, location, road conditions…): all data can be accessed and collected efficiently and securely via an ecosystem. Cloud resources can be integrated, allowing the collection of huge amounts of sensor data and the enrichment of data with external information. The company can use the data for internal purposes, but can also make the data available to third parties (customers, government, insurance company…) |
| **Use case 3: Site monitoring** | **Use case 4: E-health scenario** |
| A large company that wants to monitor its different sites (toxic waste, gasses, smoke, cameras, fire detection…) can integrate all objects that need to cooperate in an ecosystem. Secure and efficient access to the data is possible, corresponding to the needs of the users. Again data can be stored in cloud resources integrated in the ecosystem and some of the data can be exposed to the outside world (government, insurance company, people living nearby…) | An ageing population and decrease of workforce in the healthcare sector is stimulating new living forms such as villages with adapted houses under the supervision of care centers. These houses will be equipped with sensors for monitoring and provisioning of care. By integrating them into ecosystems, data can be collected more efficiently and decisions can be taken more intelligently, while maintaining security and respecting privacy of the residents. |

# 5 Requirements and research challenges

The overall requirements that need to be fulfilled and objectives that need to be realized in order to implement the proposed MENO concept are summarized in Figure 4 and will be further elaborated in the following sections, together with the research challenges they involve.

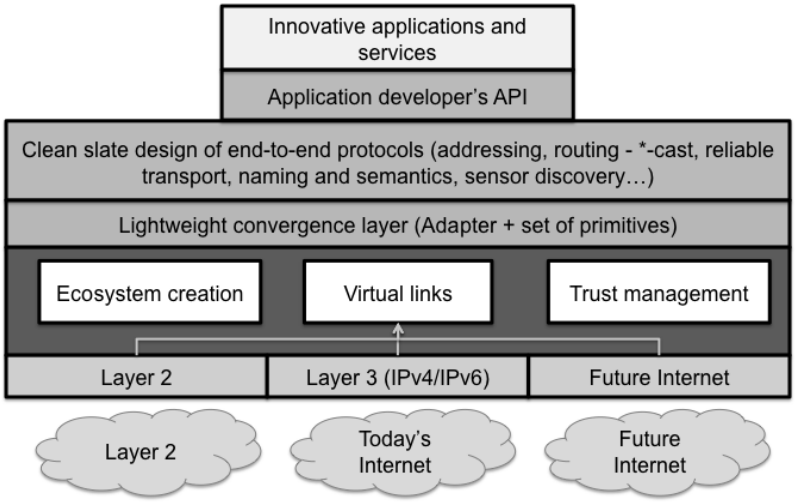


**Figure 4: MENO requirements and objectives**

## Ecosystem creation and management

The ecosystem creation and management is responsible for the creation of the virtual environment in which only a selected set of sensor nodes, IP devices and other Internet-connected objects are allowed to participate. This implies that virtual links need to be established between the different members of the ecosystem. The creation of virtual IP networks on top of the current Internet is not new [3-4], but extending these virtualization efforts to lightweight devices such as sensors imposes new research challenges. First of all, new solutions need to be found to integrate sensor nodes into the ecosystem. Since only a selected set of objects is allowed to join the ecosystem, they need to share some common trust relationship. Novel solutions to implement lightweight trust relationships on devices with very limited processing and memory capabilities need to be investigated. Easy management solutions to add objects to or revoke objects from the ecosystem are also part of this research. The creation of virtual links over the existing Internet is relatively straightforward. Many solutions for the establishment of tunnels exist. Also, solutions for establishing secure links on top of layer 2 connectivity can be found in literature. Again, the challenge is to extend these solutions to sensor and actuator nodes while taking into account the specific characteristics of these nodes (e.g. limited memory and processing, sleep schemes…).

The creation of a virtual environment alone is not sufficient. On top of this virtual environment a lightweight convergence layer needs to be designed. This layer has

to hide the underlying virtual links and the heterogeneity of the underlying networks. It should offer a common language between all objects in the ecosystem in order to be able to create real end-to-end solutions on top of it. Such a layer can be realized in the form of a virtual adapter that allows the sending of raw datagrams to all or specific virtual links. In addition link properties should be exposed to the upper layers in a standardized way, again hiding the heterogeneity of different link technologies. The design must be lightweight, since it must run on devices with limited capabilities. It provides the starting point for the design of clean-slate protocols and introduces a common language between all objects in the ecosystem independent of the underlying networks and of the device capabilities. An example is given in Figure 5.

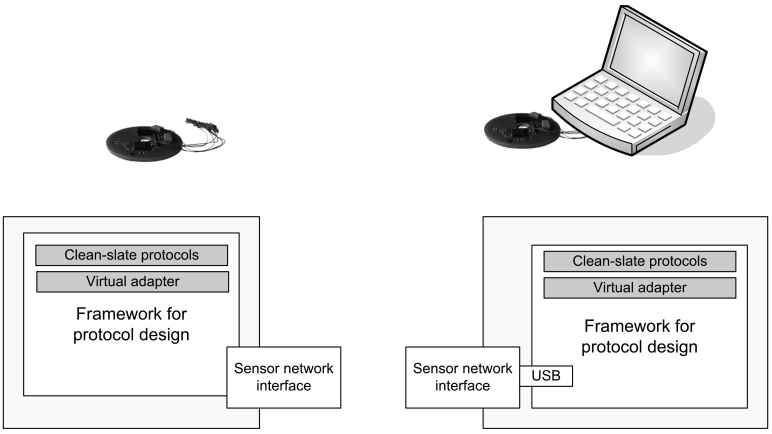


Figure 5: Virtual adapter concept to introduce a common language between all objects

## Clean-slate design and APIs

As already stated, on top of this lightweight convergence layer, any new protocol can be developed and implemented from scratch. This approach enables a clean slate approach for the design of end-to-end solutions for communication between groups of sensor nodes and networked objects, tailored to the specific characteristics of the sensor nodes and the corresponding data flows, characteristics that are strongly different from the characteristics encountered in today's IP world. Therefore, the characteristics of the sensor nodes and the corresponding data flows need to be studied and should drive the design of protocols for the efficient and intelligent distribution of sensor data. The following provides a non-exhaustive list of possible topics that need to be studied to achieve this goal.

- Novel addressing scheme that allows the addressing of individual nodes, groups of nodes, all nodes that are interested in the data of a specific node…
- Support for all communication types encountered: unicast, broadcast, anycast, convergecast, multicast
- Intelligent routing and forwarding schemes where more powerful nodes take up a more important role: label-based routing, application labeling, time stamps, aggregation of data, support for quality of service, hierarchical or cluster-based routing
- Transport protocols tailored to the needs of applications and supporting the reliable delivery of data in an end-to-end manner
- Sensor indexing and caching by more powerful nodes in view of traffic and routing optimizations
- Modular protocol design approach (both for the networking components as the packet construction) in order to allow customization and reconfiguration of networking functionality
- Introduction of energy-saving mechanisms in the protocols
- Design of networking primitives and powerful APIs in order to configure, manage and use the networking functionality and networking services
- Support for traffic and application dependent packet handling

From this list it is clear that there are many challenges that need to be investigated in order to come to an optimal design that takes into account the limitations of the least powerful nodes and optimally exploits the intelligence of the more powerful nodes. Next to the efficient and intelligent distribution of data, it is of uttermost importance to come up with new primitives for application developers in order for them to use sensor data in a natural way and without bothering about sockets or ports. Topics that need to be investigated here are:

- User-friendly naming schemes allowing the naming of individual members of the ecosystem, groups of nodes, types of sensor data… and the possibility to automate the assignment of names
- Semantics: the search, interpretation and transformation of sensor data or related sensor data from different sensors (representing an entity such as a building, vehicle…) is only possible by giving it explicit semantics, which

need to be lightweight. Solutions for representing sensor information are needed, preferably in a semi-automatic way.

- Flexible discovery systems and mechanisms to search for sensor data taking into account the naming and semantics
- Design of primitives and application developers APIs in order to quickly and easily design intelligent applications that can make use of the power of the underlying protocols.

It is clear that the MENO concept introduces a large number of research challenges, spanning several research fields. In the following sections we will highlight some of the past and current efforts in these fields and will point out where the MENO concept needs to advance these efforts or where it can build upon these efforts.

# 6 Related work

Traditionally, sensor networks were not IP-enabled. Hence, when these sensor networks were integrated into IP-based infrastructures, gateways or proxies were deployed at the boundaries of these domains. These gateways act as protocol-translators between the non-IP communication protocols in the sensor network and the IP communication in the Internet and work at application level [5]. However, the use of protocol translation gateways breaks the end-to-end communication paradigm and has proven to be inherently complex to design, manage and deploy [6-7]. Furthermore, when a new sensor protocol is developed, a new gateway needs to be implemented. Therefore, and in order to increase interoperability between sensor nodes from different vendors, a trend has emerged to access these networks with IP. In [5], it is stated that an all IP sensor network is not feasible, mainly because of the fact that the sensor nodes are resource-constraint. A first attempt to implement an IP stack on sensor nodes is uIP [8], an open source TCP/IP stack capable of being used with tiny 8 and 16 bits microcontrollers. uIP has evolved to include a low-power link built on IEEE 802.15.4, showing that a reduced version of IP was feasible for WSNs. uIP does not offer multicast functionality, a functionality that is very important looking at the data flows in sensor networks. Based on the success of uIP, a working group was created by the IETF: 6LoWPAN [9]. This standard describes an adaptation layer between IPv6 and IEEE 802.15.4. IPv6 header compression is used to

enable efficient communication. This solution still uses a gateway for connection between the sensor network and the IP network, but by standardizing the protocols, the translation is much simpler and can be done at network level, without entirely loosing the end-to-end concept. This standard is supported by the IPSO alliance, which is about using IP (IPv4 or IPv6) for interconnecting smart objects [10].
The design of a complete IPv6-based network architecture for wireless sensor networks is given in [11]. To connect a sensor network with other IP networks, border routers are used. These mainly forward IP datagrams at the network layer, without the need to maintain any application-layer state. A similar approach is used in IPSA [12].

It is clear that all these solutions take the same design approach: look how the IP world works and bring it to the sensor world by stripping of functionality and introducing gateway translations where needed. We believe that this is not the most optimal solution, since this approach starts from solutions developed with the requirements of the most powerful devices in mind and these do not at all fit those imposed by sensor nodes. It offers a workable short-term solution, but in the longer term we believe a novel design is needed as proposed by the MENO concept.

The previous solutions are mainly dealing with bringing the IP network connectivity to the sensor world. Next to this, many initiatives exist that want to offer complete sensor network integration frameworks. A very good summary of these frameworks is given in [13]. There are frameworks that want to provide access to sensor data by collecting the data into a database (IrisNet and JWebDust), by establishing a data collection network (Hourglass) or by creating a centralized broker (Janus), which can be consulted by applications to discover or access sensor data. Some of them even look at the integration with IMS (e-Sense and Ubiquitous Sensor Networks). Other initiatives such as Sensor Web Enablement (SWE), SenseWeb and the SPITFIRE project [2] focus on web applications and present solutions for making sensor networks accessible and controllable by web-based applications. Looking at all these frameworks, we can observe that they make use of centralized brokers that are connected with

gateways or proxies at the border in the different sensor networks, that they make use of a n-tiered architecture, that they introduce intermediate brokers or agents or that they continue to make use of the dedicated sensor gateways or sinks. In all cases, there are one or multiple levels of indirection in order to get the sensor data. At some points (e.g. naming, semantics…), similar functionality will be needed in the MENO concept, but it wants to go a step further by really looking into complete end-to-end solutions, directly between the sensor nodes and the more powerful devices.

Another framework, which is being developed in the SENSEI project [14], wants to develop a global scale framework, aiming to bring the sensor world to the rest of the Internet and let applications access a large variety of connected geographically distributed sensor networks. In that respect, the MENO concept is different. Its purpose is not to make sensor data accessible to the whole world, but to group all the involved actors in the targeted application scenarios and to optimize sensor communication within these closed groups through the design of novel end-to-end protocols.

This grouping will be realized through the creation of secure and self-organizing virtual networks. The concept of multiple co-existing logical networks (also called virtual networks, overlay networks) appeared in literature several times in the past and in many different forms [3-4]: Virtual LANs, Virtual Private Networks, Virtual Private Ad Hoc Networks or P2P application level overlays… These solutions make use of IP or assume IP Internet connectivity and are not designed to include sensor nodes, which is required by the MENO project. Of course, adding sensor nodes to a virtual network will pose new challenges that will impact the design. Most importantly, since only trusted nodes may become part of the ecosystem, one should be able to install a trust relationship also on sensor nodes and execute the resulting security algorithms on these nodes to guarantee confidentiality, integrity and data freshness. This is challenging, since sensor nodes have limited storage, computation, power resources and mostly operate wirelessly over a short range. For example, the processing speed of the micro controllers in sensor nodes often does not allow advanced security mechanisms, whereas these will be used in other parts of the ecosystem. Since storage and

memory are limited, the code size of the security algorithms must be limited or reduced. It is clear that a lightweight solution that offers a sufficient security level is required for sensor nodes to securely join the ecosystem. Concerning public key cryptography techniques in sensor networks, these were considered to be too computational, but in [15] it has been shown that it is feasible with the right selection of algorithms, namely elliptic curve cryptography [16], since it requires smaller key lengths for a given level of security than for example RSA public key cryptography and is thus more suited for sensor nodes. This is also confirmed in [17] and demonstrated by [18]. Also the impact of this type of cryptography on the lifetime of the sensor has been studied [17,19] The alternative is symmetric encryption such as 3DES or AES, which is often supported by the sensor hardware itself and which is based on a shared key, leading to the problem of the distribution and renewing of these keys. To solve this key management problem, several solutions have been proposed based on random pre-distribution schemes, such as [20], based on multiple keying mechanisms such as the LEAP protocol [21] or based on the common trust with a third node as in the PIKE system [22], but in general it is assumed that public key cryptography solutions facilitate much simpler security protocols, mainly because of their benefits for key distribution.

Finally, in order to design the solutions for this concept and to deal with aspects such as modularity, very flexible development frameworks are needed that are suited for networking and protocol design. Many frameworks exist of which we give two examples here. Click Router [23] is a software architecture for building flexible and configurable IP routers on rather powerful devices, but can be used for implementing any network level packet processing functionality, which is required to create virtual networks. The information driven framework IDRA [24], targeted on the design of sensor protocols, is very promising for heterogeneous ecosystems. By decoupling the protocol logic and the packet structure, modules can access the information of any network module and protocols can be designed quickly. It includes cross-module information exchange repositories, system-wide QoS control and an adaptive protocol selector that selects the most optimal network modules based on the network context.

The above overview gives a birds eye view on the current state-of-the-art, shows where the MENO concept should advance and where it can build upon existing knowledge.

# 7 Conclusions

The Internet becomes more and more "sensorized". It becomes clear that these sensor and actuator networks will become a cornerstone of the Future Internet, enabling many novel services and opening up new business opportunities. This requires generic, open and secure communication and service platforms. In this paper, we have shown that today's solutions impose many limitations at the level of cooperation of these Internet-connected objects and the possible intelligence at the end points. This is mainly caused by the lack of possibilities for end-to-end communication between these cooperating objects. To this end we propose the MENO concept, which aims to create a smart network architecture for groups of Internet-connected objects by combining network virtualization and clean-slate end-to-end protocol design. This design nicely maps to many real-life scenarios and should empower application developers to use sensor data in an easy and natural way, which will speed up and stimulate the design of novel and more intelligent services and applications, creating new business opportunities. Of course, this concept introduces at the same time many new challenging research problems, but by addressing these problems and realizing the potential of this concept, we hope to contribute to the realization of the Internet of Things.

# References


1. A. J. Perez, M. A. Labrador, S. J. Barbeau, G-Sense: A Scalable Architecture for Global Sensing and Monitoring, IEEE Network, 24(4), 2010, pp. 57-64.
2. FP7 SPITFIRE project, http://www.spitfire-project.eu/
3. N. M. Mosharaf Kabir Chowdhury, R. Boutaba, Network Virtualization: State of the Art and Research Challenges, IEEE Communications Magazine, 47(7), 2009, pp. 20 – 26.
4. J. Hoebeke, G. Holderbeke, I. Moerman, Bart Dhoedt, P. Demeester Virtual Private Ad Hoc Networking, Wireless Personal Communications, 38(1), 2006, pp. 125-141.
5. Marco, Z. and Bhaskar, K., Integrating Future Large-scale Wireless Sensor Networks with the Internet, USC Computer Science Technical Report CS 03-792, 2003.
6. A. Dunkels, JP Vasseur, IP for Smart Objects, white paper, 2008.

7. K. Mayer, W. Fritsche, IP-enabled Wireless Sensor Networks and their Integration into the Internet. Proceedings of the First International Conference on Integrated Internet Ad Hoc and Sensor Networks, InterSense '06, France, 2006, Vol. 138.
8. uIP TCP/IP stack, http://www.sics.se/~adam/uip/index.php/Main_Page.
9. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007.
10. S. Chakrabarti, Z. Schelby, 6LoWPAN Neighbor Discovery: A Highlevel Overview, white paper, 2009.
11. J. W. Hui, D. Culler, IP is Dead, Long Live IP for Wireless Sensor Networks, Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems, SenSys '08, USA, 2008, pp. 15-28.
12. M. Chen, S. Mao, Y. Xiao, M. Li, V.C.M. Leung, IPSA: a novel architecture design for integrating IP and sensor networks, Int. J. Sensor Networks, 5(1), 2008, pp. 48–57.
13. FP7 SENSEI project, D1.3, State of the Art – Sensor Frameworks and Future Internet.
14. FP7 SENSEI project, http://www.ict-sensei.org/.
15. D. J. Malan, M. Welsh, M. D. Smith, A Public Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography, 1st IEEE Conference on Sensor and Ad Hoc Communications and Networks, USA, 2004.
16. A. J. Menezes, Elliptic Curve Public Key Cryptosystems, Boston, Kluwer Academic Publishers, 1993.
17. F. Amin, A. H. Jahangir, H. Rasifard, Analysis of Public-Key Cryptography for Wireless Sensor Networks Security, Proceedings of World Academy of Science, Engineering and Technology, Vol. 31, 2008.
18. L. Uhsadel, A. Poschmann , C. Paar, Enabling Full-Size Public-Key Algorithms on 8-Bit Sensor Nodes, Proceedings of ESAS 2007, Vol. 4572 of LNCS, 2007, pp. 73-86.
19. K. Piotrowski, P. Langendoerfer, S. Peter, “How Public Key Cryptography Influences Wireless Sensor Node Lifetime”, Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks, USA, 2006, pp.169 – 176.
20. D. Liu, P. Ning, R. Li, Establishing Pairwise Keys in Distributed Sensor Networks, ACM Transactions on Information Systems Security, 8(1), 2005, pp. 41-47.
21. S. Zhu, S. Setia, S. Jajodia, LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks, Proceedings of the 10th ACM Conference on Computer and Communications Security, USA, 2003, pp. 62-72.
22. H. Chan, A. Perrig, PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, Proceedings of IEEE INFOCOM 2005, Vol. 1, pp. 524-535.
23. E. Kohler, R. Morris, B. Chen, J. Jannotti, M. F. Kaashoek. The Click Modular Router, ACM Transactions on Computer Systems, 18(3), 2000, pp. 263-297.
24. E. De Poorter, I. Moerman, P. Demeester, An Information Driven Sensornet Architecture, The Third International Conference on Sensor Technologies and Applications, SensorComm 2009.
25. FP7 IoT-A project, http://www.iot-a.eu