Wireless Personal Communications manuscript No.
(will be inserted by the editor)

Strategies and challenges for interconnecting wireless mesh and wireless sensor networks

Stefan Bouckaert · Eli De Poorter · Benôit Latré · Jeroen Hoebeke · Ingrid Moerman · Piet Demeester

Received: date / Accepted: date

Abstract Wireless sensor networks and wireless mesh networks are popular research subjects. The interconnection of both network types enables next-generation applications and creates new optimization opportunities. However, current single-gateway solutions are suboptimal, as they do not allow advanced interactions between sensor networks (WSNs) and mesh networks (WMNs). Therefore, in this article, challenges and opportunities for optimizing the WSN-WMN interconnection are determined. In addition, several alternative existing and new interconnection approaches are presented and compared. Furthermore, the interconnection of WSNs and WMNs is used to study challenges and solutions for future heterogeneous network environments. Finally, it is argued that the use of convergence layers and the development of adaptive network protocols is a promising approach to enable low end devices to participate in heterogeneous network architectures.

Keywords Wireless sensor network · Wireless mesh network · Cooperation strategies · Future networks

1 Introduction

What started in 1888 with Heinrich Hertz producing the first radio waves, has led to a multi billion dollar wireless industry today. Even though it was only in the late 1990s that second generation mobile telephony and current wireless LANs were available to the general public, many people rely on these

S. Bouckaert, E. De Poorter, B. Latré, J. Hoebeke, I. Moerman, P. Demeester
Ghent University - IBBT, Department of Information Technology (INTEC)
Gaston Crommenlaan 8 bus 201
9050 Ghent, Belgium
Tel.: +32 9 331 49 75
Fax: +32 9 331 48 99
E-mail: stefan.bouckaert@intec.ugent.be

technologies on a daily basis to carry out their personal and professional life. GSM and WiFi are just two examples of the current impact of wireless network technologies, but many more exist.

The success of wireless technologies today caused the international wireless network research community to have high hopes for the future, with many researchers trying to predict what the wireless future is going to look like. The wireless discussion is often entangled with architectural considerations on 'The Future Internet'. While there are many aspects to the different visions, several predictions reappear in virtually every related paper or project proposal:

- A huge number of heterogeneous (wireless) network nodes will be involved. Not only people will carry multiple end-user devices and sensors, the complete environment will be equipped with network nodes. Example applications are environmental information gathering, road state observation, and asset tracking.
- Several (radio) technologies will co-exist and operate together seamlessly.
- An increasing number of technologies such as GPS, WiFi, Bluetooth, ... will be integrated on a single device.
- The large number of devices trigger a massive amount of data.
- This data will be accessible anyplace and anytime, creating an ambient networking experience.
- New (context aware) services will be developed, enabling the end user to use all available technology and data to enrich his or her life.

Although this evolution will not happen overnight, some forms of current generation networks already show similar characteristics. More specifically, when wireless sensor networks are interconnected with wireless (WiFi) mesh networks, a prototype network holding the above characteristics is created. Although plenty of research is available on all aspects of either wireless sensor networks (WSN) or wireless mesh networks (WMN), few information is available on the interconnection of these network types. However, the importance of such research can be motivated:

- Many application scenarios could benefit from a successful and optimal interconnection between WSNs and WMNs. For example, a wireless mesh network can be used as a backbone for collecting sensor data from remote sensor clusters, or, resource intensive calculations with sensor data may be performed on a mesh router instead on a sensor node.
- Studying the sensor and mesh interconnection case can reveal hidden issues that are to be expected in future networks.
- Although wireless sensor and wireless mesh networks each have their own research focus, the networks show many resemblances. Nevertheless, research papers are most often restricted to either one or the other type of network. It is an interesting question whether such separation is always justified, and whether algorithms originally designed for wireless mesh networks can be re-used or adapted for use in wireless sensor networks, and vice versa.

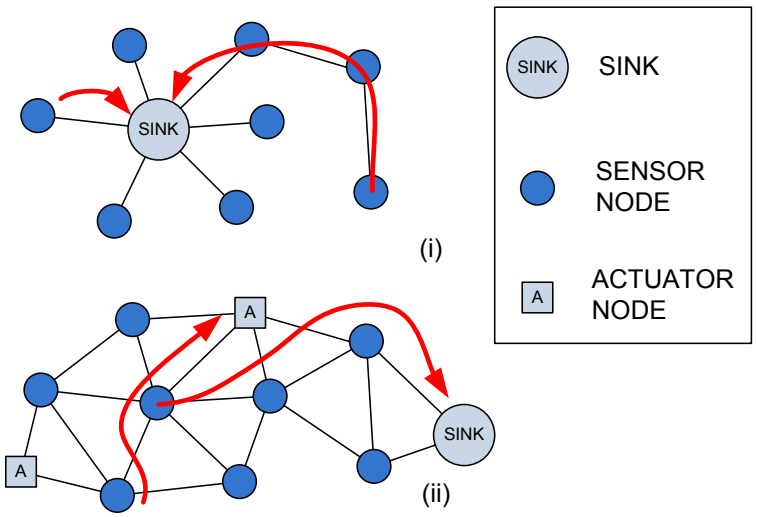

Fig. 1 Wireless sensor network architecture examples.

Therefore, in this article, challenges and strategies for the interconnection of WMNs and WSNs will be explored. The remainder of the article is structured as follows. First, Section 2 details the meaning of WSNs and WMNs in the scope of this article. Similarities and differences between WSNs and WMNs are determined. The research trends in each field are listed. In addition, an example use case illustrates the usefulness of the interconnection, and research challenges are deducted.

Then, existing and new interconnection strategies are presented in Section 3. Section 3.1 investigates the benefits and downsides of traditional gateway based solutions, while Section 3.1 introduces alternative interconnections strategies.

Finally, in Section 4, the prototype case of WMN and WSN interconnection is used as a base to present our long term vision on strategies that can be used to support future wireless network environments.

2 WSNs vs. WMNs

2.1 Characteristics

In order to avoid confusion with WSN and WMN terminology, the interpretation of these terms in the scope of this article is specified as follows;

Sensor devices or *sensor nodes* are network nodes with limited capabilities in terms of processing power, memory capacity and bandwidth, equipped with a sensor and/or actuator chip. As such, a sensor node can be a source of data

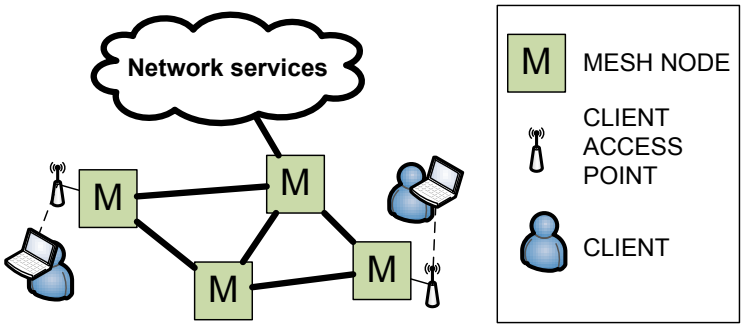

Fig. 2 Wireless mesh network architecture examples.

in a network, but could as well be used as intermediate node to forward data from one sensor device to another, or to a data collection device, called a *sink* (see Fig. 1). Sensor nodes are small sized and limited in cost.

With WSN or wireless sensor networks, all forms of wireless networks between sensor devices are indicated [1,2]. These sensor networks are considered to be self-forming and self-healing, and are used to gather data in places where the use of cabled sensors is hard, costly or undesired. No restriction is made based on network size or topology: both single hop networks between sensor devices or sensor nodes and a sink, and complex multi-hop networks with meshed topologies are considered. Typical examples of wireless technologies used in sensor networks are Bluetooth and ZigBee.

Mesh devices are relatively powerful networked nodes, equipped with relatively powerful wireless interfaces and thus are able to transmit and receive at higher bandwidths than sensor devices. Most authors consider mesh nodes to have limited or no mobility. With WMN or wireless mesh networks, all forms of wireless networks between mesh devices (nodes) are indicated. Again, there are no restrictions on the topology. Mesh networks are often used as a wireless backbone for the interconnection of end user devices. WMNs might also offer additional functionality to the client networks, for example, provide an uplink to the Internet (see Fig. 2). Mesh networks are self-forming and self-healing, and are therefore an ideal solution to provide connectivity in places where cabled networks cannot easily be installed. Furthermore, because of their self-organizing character, mesh networks can be rolled out fast, making them ideal candidates to be used as emergency network infrastructure.

Since WiFi interfaces are already popular with the end users, are cheap to get and operated in license free spectrum, WMNs based on WiFi technology are the most studied networks in (academic) mesh networking research.

Table 1 summarizes typical characteristics of mesh and sensor networks. Because of these different characteristics, WSNs and WMNs each have their research focus. While energy efficiency is not unimportant in WMN research, it is not considered to be the main issue. Research focus is mostly on increasing

Table 1 Typical sensor nodes and mesh nodes characteristics

		Sensor Nodes	Mesh Nodes
General	target form factor	small or tiny $O(mm^3)$	larger $O(cm^3)$
	antenna	integrated	external
	power consumption	$O(mW)$	$O(W)$
	power	small battery or energy harvesting	'unlimited' (external) power source
	price	relatively cheap (a few dollars or less)	relatively expensive ($50 - $500 and up)
	RAM/ROM	(k)Bytes	MBytes
	processing power	very limited	relatively high
Network	bandwidth	low (a few Mb/s and frequently less)	relatively high (several Mb/s)
	interface(s)	single, often proprietary	single or multiple, often standardized
	max packet size	small $O(bytes)$	larger $O(kbytes)$
	IP capabilities	limited or none	IP capable
	sleeping schemes	often used	rarely used
	delay per hop	$O(ms)$ to several seconds	$O(ms)$
	mobility	none to highly mobile	most often limited or none

the efficiency of WMNs in terms of reliability, throughput, delay, scalability or ease-of-use. While similar objectives drive the WSN research, sensor nodes often have a very limited power supply, therefore forcing developers to account for energy efficiency of their protocols. Furthermore, the limited capacities of sensor nodes put larger stress on the code size, code execution time and bandwidth consumption of developed WSN algorithms.

Despite of these differences in focus, many similarities are found in WSN and WMN research:

- The goal of any WSN and WMN, is to create and maintain network connectivity as easy as possible, in order to get as many data, as fast, easy, secure as needed from source to destination node(s), while consuming the least possible number of resources. Resources are the wireless spectrum, node energy, node memory, node processing power, and financial budget.
- Multi-hop networks are created. This usually requires some form of node addressing and a routing protocol.
- Many popular WSN and WMN technologies share the limited $2400MHz$ – $2500MHz$ ISM band of the wireless spectrum.

2.2 WSN and WMN cooperation: example use case

As an example use case, consider the monitoring and tracking of elderly people and caretakers in nursing homes (Fig. 3). This use case is currently under active development within the IBBT-DEUS (Design and Easy Use of wireless Services) project [3], which strives towards designing and implementing easy to use wireless networks. Research is performed in cooperation with a nursing

home. A WSN in a nursing home has several uses. *(i)* Medical monitoring of the residents, possibly using a body area network (BAN, [4]). *(ii)* Portable emergency buttons and sensors, allowing residents to transmit an emergency signal to caretakers from anywhere in the vicinity of the nursing home. If residents know that they are monitored, even when e.g. in the garden, they are more likely to go out. Thus, their mobility increases. The sensor network can be used to provide *(iii)* localization information, which is added to the emergency requests in order to notify a caretaker which is close to the emergency location. *(iv)* Where demented persons are now necessarily restricted to certain areas of the nursing homes when no caretakers are around, in order to keep them from injury or upsetting fellow residents, these restrictions could be limited in case a WSN is able to provide tracking. When a demented person leaves the safe environment of the nursing home, or enters the room of another resident, a caretaker is notified. *(v)* Sensor nodes can be used for wireless building automation, such as to collect information on temperature and humidity. This information is then used to steer the central HVAC installation.

In the same building, a WMN can be installed to provide rooms of senior residents with Internet connectivity, to provide WiFi VoIP coverage, or to connect terminals of caretakers with an information database in the back-end.

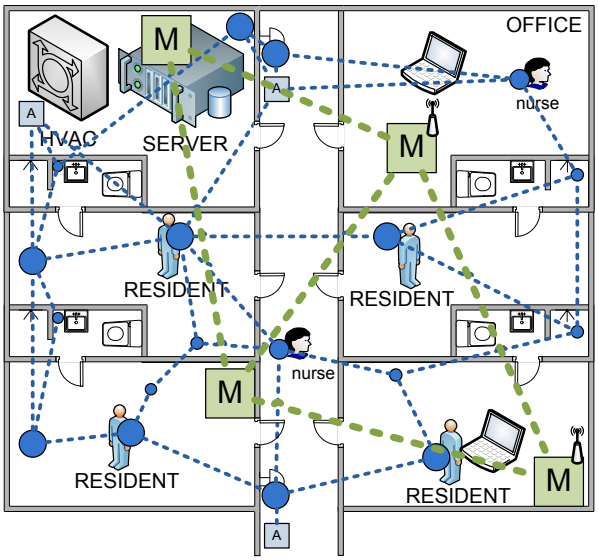

Fig. 3 Part of a nursing home, equipped with several sensors and a mesh network.

Fig. 3 shows WSN and WMN as two individual networks. However, this is a suboptimal situation for following reasons;

First, assume a WMN is already available in the building before deployment of the sensor devices. If a sensor node on one side of the building needs to steer an actuator on the central HVAC installation, intermediate sensor nodes need

to be installed in order to complete the network path. The already available WMN path is thus left unused.

Second, in large or dense deployments, the WSN might not be able to provide all bandwidth needed for delivering large amount of sensor data on its own. Additionally, when long multi-hop paths and sleeping schemes are combined, the packet delay might grow unacceptably large. In these scenarios, a co-located WMN, able to transmit at considerable higher data rates, could reduce the load on the WSN.

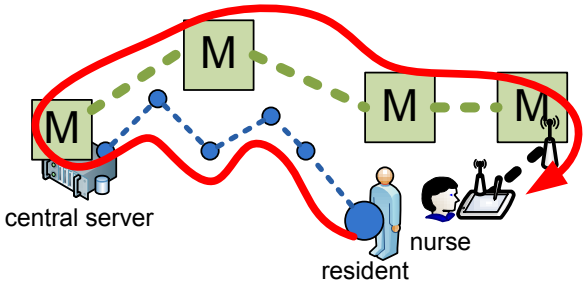

Fig. 4 Nurse with WiFi enabled tablet monitoring real time data at the resident's bedside.

Third, whenever data from the sensor (mesh) nodes is needed on mesh (sensor) nodes, the only possible network path in Fig. 3 passes through the server room, as the server is the only device which interconnects the networks. Especially in large deployments, this results in very inefficient data routing when information from nearby sensors is needed on a WiFi device which is connected through a mesh backbone (see Fig. 4).

2.3 Interconnection challenges

The example from previous paragraph shows that an interconnection between WSN and WMN is useful, both as a way to reduce the load on the resource constraint sensor network, and as a way to allow data from one network to be used on the other network. There are multiple reasons why an effective interconnection is challenging:

– **Different wireless technologies.** A communication link cannot be set up using two different wireless technologies. At least one device or group of devices should be able to receive and send both sensor packets and mesh packets. Unfortunately, even though direct communication is not possible, both networks might interfere. Different packet formats, packet sizes and synchronization strategies make interconnection more complex.

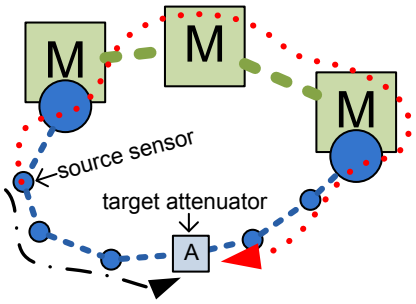

Fig. 5 Example scenario. Both a direct sensor node to actuator node path, as a path through the WMN is available.

- **Different addressing schemes.** While the most popular addressing scheme in WMN deployments is IPv4, sensor networks use simplified addressing schemes.
- **Different routing strategies.** If WSNs and WMNs are connected in a flexible way, allowing data packets to cross technology borders, routing can become complex: one network might follow a reactive routing strategy, and the other network a proactive routing strategy.
- **Security and trust.** In WMN networks, security and trust is most often guaranteed using either pre-shared keys, or by relying on certificate based encryption techniques [5]. Because of the limited capacities of sensor nodes, the security approaches used in WMNs and ad hoc networks are not suitable for WSNs [6]. Some sensor nodes might be unable to implement any security mechanism at all.
- **Backward compatibility.** If a WSN is added to an already existing WMN, should any adjustments to the WMN protocols be made? In general: the less adjustments are to be made on either WSN or WMN protocols, the faster an interconnection can be realized and the sooner an interconnection strategy might be adopted.
- **Metric translation.** If multiple routes from source node to destination node are available in a network, a routing protocol selects the most fit route based on a routing metric. Routing metrics in WMN tend to be based on pure network performance. Typical WMN metric examples such as ETX [7] or WCETT [8] require special probe packets to be sent regularly. While such overhead packets might be acceptable in WMN networks, WSN routing metrics often strive towards optimizing energy efficiency or total network lifetime. If WSN and WMN use different routing metrics, it is not trivial to determine optimal paths through the interconnected networks. For example, Fig. 5 shows how a sensor node trying to contact an attenuator can select a direct path or a path through a WMN. Although sending the packet to the closest mesh node (with a sensor interface) might seem the best solution at first, this might actually not reduce the number of sensor hops in the network.

– **Scalability.** A WSN might be able to offload some tasks to a co-located WMN, thereby increasing its scalability. On the other hand, if WMN and WSN are fully aware of each other's capacity and current state in order to allow optimal packet routing, additional information tables and routing decision steps might have a negative impact on the scalability. The same problem surfaces when remote cluster sensors get interconnected thanks to the presence of a WMN.

It is beyond the scope of this article to propose a solution to all listed research challenges. However, for each of the interconnection strategies of Section 3, some or all of the above issues will have to be solved.

3 Interconnection strategies

3.1 Single Gateway Solution

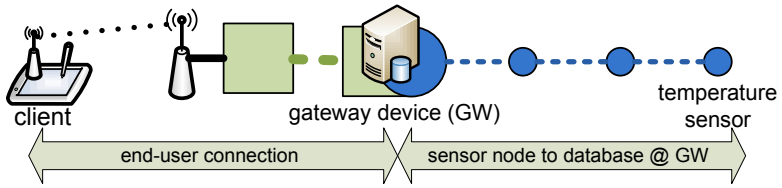

Fig. 6 Traditional single gateway solution for information exchange between networks.

The traditional solution for interconnecting two different network types is use of a gateway device. A gateway is a multi-interface network node, which has the necessary protocols installed to communicate with both network types. In case of WSN and WMN networks, a simple gateway strategy is depicted in Fig. 6. In this scenario, all sensors propagate their values towards a central gateway device, which acts as a sink for the sensor network. The gateway devices stores all received sensor values in a database.

The gateway device also has a mesh interface and WMN protocols, making the server address accessible from a end-user device. Whenever a client device needs to access data, it queries this central database. The client device might also query a specific node or a group of nodes by sending a specific request message over the WMN that is later translated to an appropriate sensor call or multiple sensor calls. This loose coupling of WSN and WMN through the use of a gateway device is easy to implement, and has several other advantages: *(i)* the gateway brings hierarchy into the network. Both networks only need the notion of default gateway to enable the interconnection. *(ii)* A single specialized, powerful device is responsible for the complex translation task, reducing the required complexity in WMN and WSN. *(iii)* Client authorization

can be implemented in the gateway device, thus enabling an administrator to implement centralized access control.

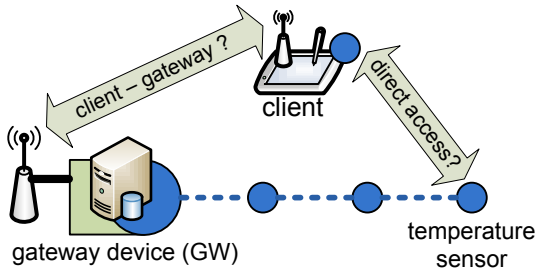

Fig. 7 Example scenario with a two interface client. While the client has a sensor node interface, he might still be forced to go through the gateway.

However, in the context of large scale integrated networks, there is a downside to all above advantages. *(i)* WMN and WSN network have no view on the inner workings or topology of the other network. This makes global optimization of traffic routing hard to achieve. *(ii)* From the WMN perspective, the gateway is the only entry point to the WSN. A large traffic concentration near the gateway node can be expected, and a single point of failure is introduced in the network. *(iii)* While an administrator can easily configure gateway access control in a static network with a predefined set of sensor nodes, mesh nodes and mesh clients, administrator control in dynamic networks with changing user groups is complex and time demanding. *(iv)* Network connections are terminated at the gateways. For every application, proxy services are required to be installed at the gateway, since the WMN nodes cannot directly access the WSN and vice versa. *(v)* The mesh backbone cannot (efficiently) be used for sensor node to sensor node communication.

The example depicted in Fig. 7 can be mapped on the use case of Fig. 4 and illustrates the issues with a single gateway solution. Even if a end-user device does have a sensor interface, the end user will be forced to connect through gateway, as the gateway is responsible for access control. Furthermore, a single gateway is likely to cause vendor lock-in, and might require an additional gateway to be installed for every new application. While this might be the preferred strategy of big companies, using proprietary gateway solutions complicates large scale network integration and hinders innovation by small players on the wireless market.

Consequently, a single gateway solution is more suited for static environments with sensor node to sink traffic patterns, than for future, dynamic environments where a large number of heterogeneous devices continuously interact. Therefore, alternative interconnection strategies are explored in the next paragraph.

3.2 Alternative interconnection strategies

3.2.1 Goals

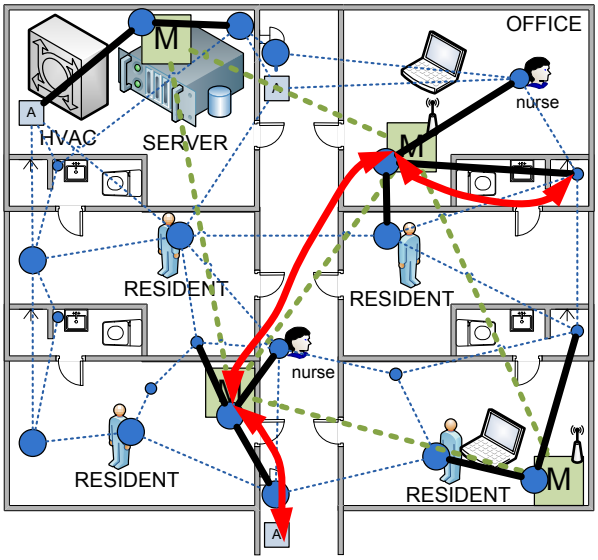

Fig. 8 Reprise of nursing home scenario. Sensor interfaces are added to the mesh routers, enabling sensor node to sensor node communication over the mesh backbone.

To increase the efficiency of WSN and WMN interconnection, three adjustments are required to the basic gateway scenario:

1. The number of gateway nodes should be increased. This is done by adding sensor interfaces to some or all mesh backbone nodes, and guarantees multiple entry and exit points for sensor to mesh to sensor paths.
2. The routing strategies in place should be adjusted to provide optimal routes through the interconnected network. This includes but is not limited to mixed sensor node - mesh node - sensor node paths.
3. The lost functionality of the gateway node should be replaced by (distributed) components across the network.

In Fig. 8, the same use case as in Fig. 3 is depicted, but now with the pursued advanced WSN-WMN interconnection possibilities. A sensor interface is added to every mesh node in the network, allowing transmission from sensor nodes to mesh (gateway) nodes. Ideally, the alternative interconnection strategies should be able to support any communication path in the network. The figure shows an example of a sensor node in the bathroom of a resident steering an alarm actuator in the hallway. The sensor network is able to detect the presence of a WMN backbone, and, instead of forwarding the alarm message over sensor hops only, the message is relayed over the WMN. As a result,

less transmissions by energy limited sensor nodes are necessary. Furthermore, if the power settings of the sensor nodes are kept to a minimum in order to save energy, the WMN backbone might offer a shorter path to the destination, reducing the end-to-end delay. If sleeping schemes are in place in the WSN, the end-to-end delay can be reduced even more.

In the following sections, different interconnection strategies for WSN and WMN are introduced and compared. The strategies are listed based on the complexity of implementation. Wile the first three approaches only enable WSN networks to use the WMN as a backbone, the last two approaches also allow WSN to WMN communication.

3.2.2 Invisible repeater

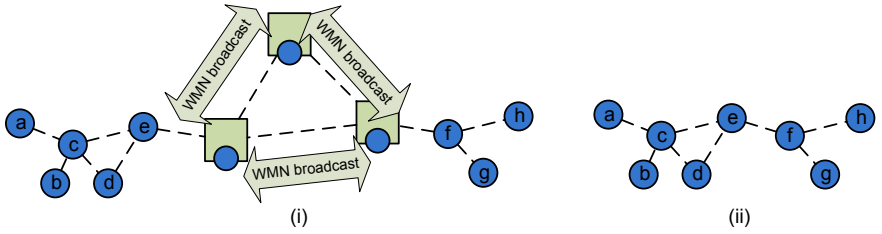

Fig. 9 Invisible repeater. (i) The WMN forwards WSN packets blindly over the mesh backbone. (ii) Resulting topology from WSN viewpoint.

A first and simple solution is the creation of a WMN invisible repeater for sensor nodes. Fig. 9 (i) shows the construction of the invisible repeater solution, in which a WMN router blindly forwards all packets that are received on its sensor interfaces to the other mesh nodes with a sensor interface. The WMN does not process packets that are received by the sensor nodes, and simply acts as an invisible repeater towards the WSN. From the viewpoint of the sensor nodes, this results in the creation of a single large WSN (see Fig. 9(ii)).

While a invisible repeater is easy to implement and is compatible with existing sensor technologies, there are several reasons why the technique is only suitable for a limited number of scenarios. *(i)* Sensor packets that are received at one gateway are sent to every other gateway. This results in a very high number of additional transmissions when a large number of mesh gateway nodes are used. In case N mesh nodes with a sensor interface are available, a single sensor packet received at one of the gateways results in $(N-1)$ sensor packet transmissions at the gateways, increasing the number of packet transmissions in the network. This increases the interference and has a negative impact on the scalability of the solution. *(ii)* Repeaters should be able to detect packets that were forwarded by other repeaters, in order to avoid broadcasting loops. Furthermore, if a single sensor node is able to receive both an original an a forwarded packet, the WSN should also support duplicate detection. *(iii)* If a

multi channel sensor protocol is used, an additional sensor interface is needed for every additional sensor channel to be supported. *(iv)* If the mesh backbone grows large, delay in the WMN might lead to synchronization problems in the WSN.

3.2.3 Virtual sensor device

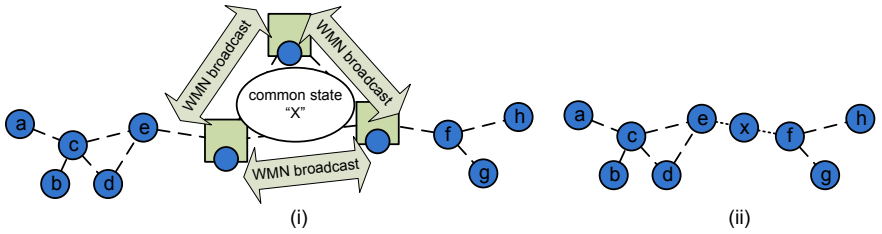

Fig. 10 Virtual sensor device. (i) The WMN acts as a virtual sensor node with extended communication range. (ii) Resulting topology from WSN viewpoint.

A second option to let the WSN use the WMN backbone in a transparent way is an evolution of the invisible repeater. In this scenario, the sensor interfaces are no longer exclusively used as a sniffer and transmission interfaces, but actively participate in the sensor network. However, all sensor interfaces of the gateways are announcing themselves to the outside world as a single sensor node. Thus, the WSN acts as a single, virtual sensor node, with a large communication range. This way, the mesh network is added to the sensor routing tables as a normal (single) sensor entry, providing full backwards compatibility with existing sensor networks.

In order for this technique to work, the mesh network should hold a *common state* of the virtual sensor node. The common state holds, amongst others, a routing table in which every node that can be reached through any of the gateway sensor interfaces is listed. If a sensor packet is sent from the WMN backbone, it is transmitted at every sensor interface of the WMN.

The ability to build a common state and process sensor packets (e.g. update TTL, routing metric, perform energy demanding task of the sensor protocol such as acting as a aggregating node) means that more advanced interaction is possible compared to the invisible repeater solution. As interaction with the sensor interface of the gateways is possible, synchronization with individual sensor clusters can be implemented at the cost of adding more complex algorithms to the common state knowledge in the mesh network.

3.2.4 Multiple termination gateways

Although the virtual sensor device solution overcomes some of the issues with the invisible repeater solution, the forwarding of sensor packets at the sensor

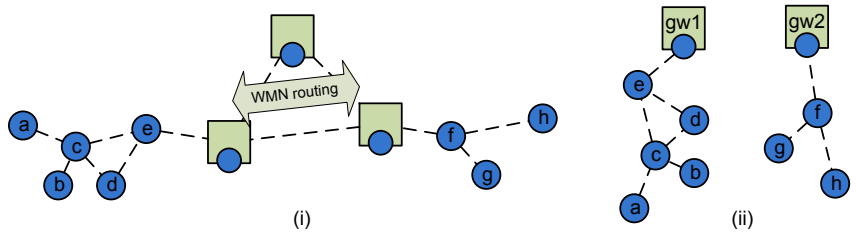

Fig. 11 Multiple termination gateways. (i) All sensor paths are terminated at termination gateways. (ii) Resulting topology from WSN viewpoint.

interfaces of the mesh nodes is still performed unintelligently. Unicast packets which travel over the WMN are broadcast at every gateway, even if the intended receiver of the message cannot be reached through a particular gateway.

Hierarchy can be added to the WSN by configuring the WMN/WSN gateway nodes as explicit sinks for the WSN. Fig. 11 shows how sensor nodes are able to directly contact sensor nodes within their own cluster using only the sensor protocol, or route packets to the gateway for further processing. However, this comes at the cost of added complexity for the sensor nodes, and, in contradiction to the previous solutions, requires a WSN protocol that is specifically designed to work with multiple termination gateways. In order to support optimal routing, sensor nodes should be able to detect whether a certain other sensor can be contacted directly, or whether a path through a gateway node is desirable. If two gateways are available in a single sensor cluster, the sensor routing is responsible for selecting either the direct path, or a path through the WMN. Sensor nodes can register with a gateway node of their choice, and the selection for a specific gateway node may vary over time. To this end, [9] presents a registration method that allows sensor nodes to modify the gateway selection without terminating an existing registration. If the sending and receiving sensor node belong to a different subnet, the packets must pass through gateways by default. Different subnets also require a handover solution in case mobile sensor nodes are used in the network.

The gateway nodes and the WMN can keep track of the location of the different sensor nodes, and thus provide optimal routing of sensor packets over the WMN. Compatibility with existing mesh solutions is maintained by implementing the sensor registration functionalities only at the gateway nodes and have those gateway nodes tunnel control packets and sensor packets over the existing mesh.

The registration protocol of sensors and updates of sensor locations in the WMN will result in additional control overhead. However, since traffic is routed only to the correct gateway over the WMN, the total number of transmissions in the network is reduced. In addition, the sensor nodes do not need to keep track of the all sensor nodes, but can query the gateways for routing information. This increases the scalability of the WSN.

3.2.5 Multiple translation gateways

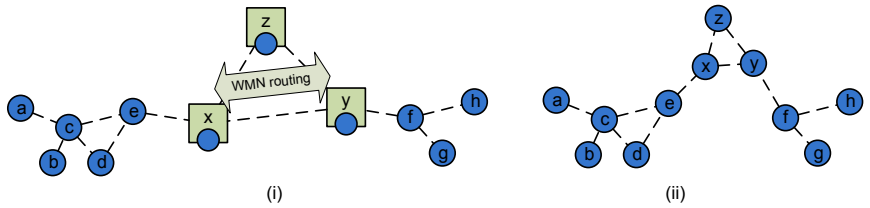

Fig. 12 Multiple translation gateways. (i) Full translation of WSN packets to WMN packets and vice versa. (ii) Resulting topology from WSN viewpoint.

In all previous solutions, the sensor nodes were shielded from the internal workings of the WMN: either the WMN was present but invisible, or, the gateways towards the WMN were known but the underlying WMN topology was invisible, requiring the sensor nodes to query the gateway at regular intervals. Furthermore, the previous solutions do not support end to end communication between sensor nodes and mesh nodes, thus limit the possible interactions between the network types.

In order to allow communication between WSN and WMN nodes, additional applications are installed at the gateways. However, this solution suffers from the same drawbacks as the single gateway solution when it comes to supporting a dynamic networking environment: new applications cannot be added to the network without support from the gateways.

By providing full translation of WSN packets to WMN packets and vice versa, direct communication between sensor and mesh devices is supported, while still allowing the use of the WMN by the WSN for sensor node to sensor node communication. The gateways performing the translation are called *translation gateways*. Transparently translating packets from one technology to an other is a non trivial process, and requires adjustments at several layers of the OSI stack.

A first adjustment to be performed by the translation gateway is *protocol translation* and *packet format translation*. All packet fields an headers need to be in the correct position. Additionally, translation between different representations (e.g. big endian vs. little endian) is needed, and routing protocol strategies (e.g. proactive to reactive) should be translated.

A second requirement is *address translation*. If different addressing schemes are used in WSN and WMN, addresses need to be translated at the gateways. Examples of address translation have been around in literature for quite some time. As an example, NAT-PT [10] specifies address translation between IPv4 and IPv6 networks.

Third, the gateways should provide *metric translation*. Both WSN and WMN might have a notion of path quality, where routing decisions are based on. The quality metric is likely to be different in each network. As such, when

route quality metrics are broadcast in order to build routing tables, it is the responsibility of the gateway to provide proper conversion between two metrics. As a simple example, suppose the quality metric would be hop count. A k hop path in the mesh network might then be translated to an l hop path in the sensor network, with $l < k$, should a developer want to favor the use of WMN links.

Because of the large protocol differences associated with WSNs and WMNs, translating packets will not always be possible for every type of network or for every network protocol or application. In [11], a number of issues with NAT-PT are discussed. The method is therefore especially suited when WSN and WMN protocols show similarities.

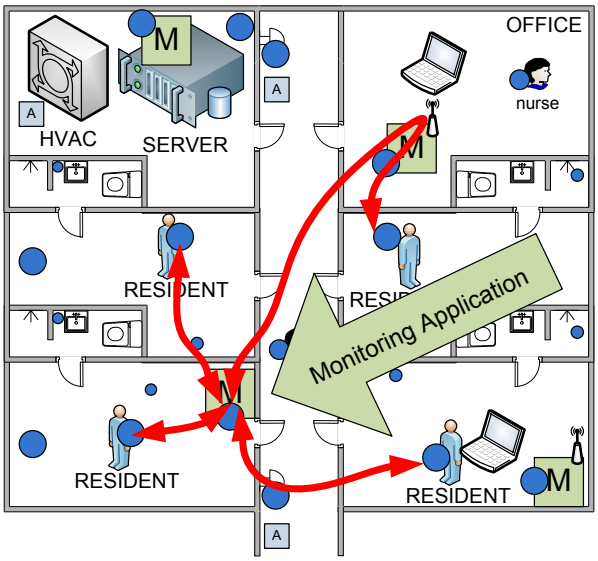

Fig. 13 Gateways and mesh routers are addressable from the sensor network. A medical data monitoring application is installed at one of the mesh routers.

If full translation is possible, optimal use of all possible network path is natively supported. The WSN can route traffic over the WMN, and end-to-end connections between sensor nodes and mesh nodes are possible. Thus, by adding translation gateways to an existing WSNs and WMNs environment, new end-to-end applications between any two devices are supported. For example, a complex or memory demanding monitoring or aggregation application can be installed on one of the mesh routers. Sensor nodes can send measured values to this application for further processing. In the scenario of the nursing home, a mesh application might monitor long term evolution of the medical data of residents, anticipating health issues. This is illustrated in Fig. 13. In the figure, the application is installed at a mesh node/gateway combination, although the application could be installed at a pure mesh node as well. The

ability to deploy decentralized applications on powerful nodes in the network helps to reduce the number of packets that are sent to a single data processing server.

From the sensor node point of view, the scalability of the solution is limited to the scalability of the WSN protocols in absence of the WMN. However, as additional network nodes are now appearing in the topology, the scalability of the WSN becomes increasingly important.

3.2.6 Stack virtualization

Although theoretically promising, the complexity of protocol and packet format translation makes the translation gateway strategy hard to achieve. From the characterization of WSNs and WMNs in Section 2, it is clear that mesh devices are (a lot) more powerful than sensor devices. This also means that in theory, there is no reason why sensor protocols cannot be executed on mesh gateways with an added sensor interface.

Therefore, an additional interconnection strategy is to run a virtual sensor stack on all gateways and all mesh devices. When a sensor packet arrives at a gateway, it is processed by the sensor stack. From the gateway, the packet can be transmitted over a mesh link to any other mesh node, where it again is processed by a (virtual) sensor stack running on the mesh node. The virtual stack contains all relevant WSN protocol needed for processing the packets. However, certain protocols, such as sleeping schemes, might be tweaked in the virtual stack to avoid unnecessary delays when transmitting (encapsulated) sensor packets over mesh links. The schematic representation of the solution is identical to the representation of the translation gateway case (Fig. 12).

The approach is similar to the approach followed in the Akari [12] project. In this project, virtual stacks are enabled in all edge and core components of the Internet, allowing clean slate and legacy protocols to co-exist using the same networking components. This allows the researchers to explore future Internet strategies, while preserving compatibility with the operational Internet.

As with the translation gateway scenario, metric translation is to be supported at the gateways. However, protocol translation, address translation and packet format translation are supported by design thanks to the virtual sensor protocol stack. Unfortunately, in contrast to the translation gateway solution, stack virtualization is not compatible with existing mesh network nodes, as the nodes must support the use of a virtual stack.

3.3 Discussion

In the previous sections, several techniques to interconnect WSN and WMN networks were discussed. While the invisible repeater and virtual sensor device solution provide full compatibility with existing sensor protocols, the broadcast character of the sensor traffic over the mesh results in inefficient use of

Table 2 Overview of the different interconnection strategies

	WSN to WSN	WSN to WMN	Transparent for WSN	Compatibility existing WMN	Metric transl.
invis. repeater	yes	no	yes	yes	no
virtual device	yes	no	yes	yes	no
termination gw	yes	gateway only	no	yes	yes
translation gw	yes	yes	yes	yes	yes
virtualization	yes	yes	yes	no	yes

resources. These methods are therefore especially used as a quick way to interconnect small-scale sensor clusters over existing mesh networks.

The termination gateway solution, the classic approach used in multi-gateway environments, requires sensor network protocols to be specifically designed for the architecture. However, the two tier architecture is a logical way to deal with the heterogeneity of the devices, and increases scalability of the solution. The translation gateway and virtual stack solution support the most advanced connectivity, but are the most complex approaches to implement. Table 2 gives an overview of the the characteristics of the different solutions. The first two columns indicate whether WSN to WSN traffic, and/or WSN to WMN traffic is supported. The third column shows whether sensor protocols should be specifically (re-)designed for the interconnection strategy to work. The table also shows if the wireless mesh routers should be modified (gateway mesh nodes excluded), and if metric translation is required and/or supported.

While the challenges of backwards compatibility, use of different technologies and different addressing schemes, scalability and metric translation were briefly touched upon in the previous sections, it is not within the scope of this article to detail the different topics for each solution. Using the above interconnection strategies does not solve the security issues in case sensor nodes are unable to support security mechanisms. The opposite is true: in case of the invisible repeater and virtual sensor device, forwarding insecure data to other sensor networks increases security risks. While additional encryption techniques might be used in the mesh backbone, the security of the total network therefore still depends on the security mechanisms that are implemented in the sensor network.

4 Future expectations, techniques and challenges

In the previous sections, new and existing interconnection strategies for WMN and WSN networks where given. In this section, additional trends and strategies that might influence future network environments are listed. Section 4.1 explains why in future networking environments, an identical routing and addressing scheme might become feasible. Next, network overlay techniques for WSNs and WMNs are briefly discussed in Section 4.2. Section 4.3 motivates

why adaptive protocols are a promising approach to support future networks. Finally, Section 4.4 lists the lessons learned from studying the WSN and WMN interconnection case that are of general importance to the broader scope of future wireless network research.

4.1 Identical routing and addressing scheme

The evolution of hardware manufacturing processes leads to continuous chip miniaturization, and increases the availability of cheap memory chips. This evolution will one one hand lead to new sensor devices that are more energy efficient and increasingly powerful in terms of processing power and memory capacities, and on the other hand to tiny devices having the same capacities as current generation sensor nodes. For the same reason, wireless mesh devices will become cheaper and smaller. This leads us to believe that for many applications where miniaturization is not the most important issue, most sensor devices will eventually be able to operate using the current generation WMN protocols.

While the processing power of mesh devices will still be higher, certain sensor nodes will be able to hold a larger number of routing entries, allowing WSNs and WMNs to interconnect using an identical addressing and routing scheme. A first step towards the creation of such solution developed within 6lowpan [13] working group of the IETF, where a frame format and compression mechanism for the transmission of IPv6 packets over an IEEE802.15.4 link is defined.

4.2 Overlay networks

An alternative way to use the same addressing and routing schemes is an *overlay network*. In [14], the author describes the use of such overlay network in order to organize and interconnect remote clusters of personal devices over heterogeneous networks. To this end, an abstraction layer is created on top of either the second or third OSI layer, depending on whether a connection to a device in a local cluster, or a connection to a remote device over an IP tunnel over the Internet is set up. The abstraction layer hides the heterogeneity of the underlaying network interfaces from the common addressing scheme, routing protocol, and other upper layer protocols. However, the solution was designed for IP capable devices, and currently does not allow low end devices such as sensor nodes to participate in the network.

Since wireless sensor networks do not support IP, a common network layer for wireless sensor networks is more difficult to define. In [15], the Sensornet Protocol (SP) is defined. The authors describe a convergence layer or 'narrow waistline' below the IP layer, but on top of the MAC layer. The SP layer supports best-effort single-hop broadcasts and hides the link layer specifications. Several cross-layer information points are defined, where higher

layers can retrieve link layer costs and exercise more precise MAC control. However, as of now, the number of practical sensor applications that use a uniform convergence layer is very limited.

4.3 Adaptive networking protocols

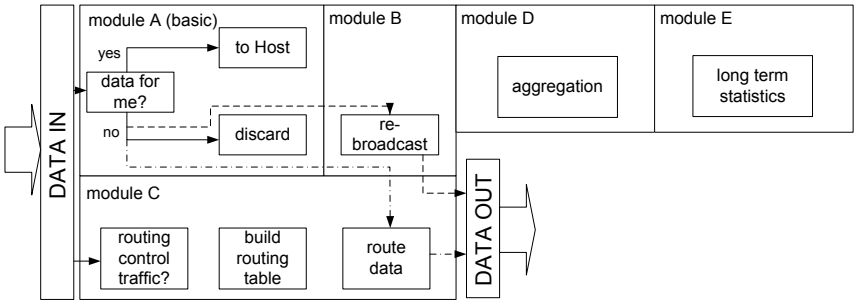

Fig. 14 Example of an adaptive routing approach. Basic nodes only run the basic module *A*. More complex nodes add more functions.

The main problem with any abstraction layer with common upper layer stacks is the inefficient use of the different node types. Future applications will be most effective when every node participating in the network is able to perform those tasks for which it is most suited. Thus, while transparent communication over heterogeneous node types should be possible, not every node type should process a packet in the same way.

Adaptive protocols consist of several modular functional blocks working together to complete a specific task [16,17]. The basic functional block for every task should be installed on both simple and complex nodes. This basic block guarantees that a node is able to handle certain packets. The more complex a specific networking node is built, the more functional blocks can be added, allowing more advanced processing to take place. Consider the example of a routing protocol in Fig. 14. The most basic functional block (module A) is installed at the least capable nodes and has the ability to detect whether a packet is destined to the node itself or not. If the packet is destined to the node itself, it is processed, if not, it is discarded. Module B is added to nodes having sufficient energy to rebroadcast packets destined to other nodes, thus allowing to form the most basic form of multi hop networks. Adding Module C allows nodes to interpret routing control packets and build a routing table, and route packets rather than just broadcast them. The most advanced nodes might add additional modules to support aggregation (module D), build routing metrics based on long term radio statistics (module D), and/or implement any other computational or memory intensive routing tasks.

While a modular routing approach is illustrative, modular security is a more difficult issue for future network environments. If certain basic nodes do not route packets but only produce data, this does not affect the routing in the network as a whole. However, if some nodes cannot process secured packets or produce raw, insecure data, securing data at a later stage does not solve possible security issues. Adaptive security is an interesting future research track. It will remain a continuous challenge to integrate low-end devices in future networking environments.

4.4 WSN and WMN interconnection: lessons learned

From the example case of interconnecting wireless sensor networks and wireless mesh networks, several lessons can be learned that will be of importance in future networking environments. The lessons are complimented with future research directives.

1. The use of isolated gateways as the only way of interconnection should be avoided. Such gateways introduce single point of failures, and are hard to use in dynamic environments with a changing user group or rapidly evolving applications. Furthermore, these isolated gateways cause a high traffic concentration at a single point in the network, resulting in an uneven networking load and contention near the gateway.
2. Every time an interconnection is made, several trade-offs are to be made. A first trade-off is the the level of abstraction versus the amount of information sharing. While a higher level of abstraction increases scalability, it hampers distributed routing decisions. A second trade-off is whether to support backwards compatibility or to apply more drastic changes to an existing network architecture. Solutions supporting backwards compatibility are likely to be more successful on a short term, but eventually limit innovation. Virtualization approaches and the use of convergence layers might be a solution to combine backwards compatibility with clean slate network designs.
3. When different networks, designed for different goals are interconnected, there is currently no objective way to compare the networking metrics of each individual network. Metric translation is not only required for optimal routing, but can also be explored in order to support quality of service across different network types. The standardization of a universal quality metric, determined by each network type in its own way, but globally comparable, is an interesting topic for future research.
4. Adaptive protocols are a promising approach to provide efficient interconnection, while respecting the individual characteristics of each network type. The main difficulty with adaptive protocols is the creation of a basic protocol version that can be deployed on a very basic network node. Current popular protocols such as the IP protocol are relatively complex. Even though the performance of network nodes will increase over time, there will

always remain a class of devices that is unable to run these complex protocols. Therefore, there is a need for novel, simple techniques that are able to provide basic functionalities on the simplest devices an at the same time can be extended to support advanced functionalities on high performance nodes.

5. An important issue in future network environments is how security can be guaranteed. The addition of low end nodes to a secure environment might introduce security risks. The design of simple but effective security solutions for low end devices is therefore extremely important for the future generation of integrated networks.

5 Conclusion

Compared to wireless mesh networks, wireless sensor networks are much more constrained in terms of resources such as bandwidth, processing power and energy. Many use cases exist that profit from the interconnection of sensor networks with mesh networks. A typical example is a nursing home, which can be equipped with a mesh backbone for communication, and a wireless sensor network to provide individual services for the elderly. However, current single gateway solutions do not suffice to interconnect large scale networks, since they are unable to cope with the dynamics of future network environments. The existing and future connectivity strategies presented in this article present an alternative to the single gateway solutions. Because they differ in terms of complexity, scalability and network abstraction level, the applicability of the technique depends on the specific use case.

The interconnection of heterogeneous WSN and WMN networks is a pilot case which can be used to derive directions for the research on future heterogeneous network architectures, where the use of node virtualization and convergence layers enables clean slate design while still retaining compatibility with existing technologies. We feel that one of the major challenges for the development of future network architectures is in the creation of simple but effective protocols for low end devices, and that adaptive protocols are a promising approach to interconnect heterogeneous network nodes, as they allow to exploit the diversity of network nodes that is expected to characterize future network environments.

Acknowledgements Stefan Bouckaert and Eli De Poorter thank the Institute for the Promotion of Innovation through Science and Technology in Flanders (IWT Vlaanderen) for funding this research through a grant.

References

1. I.F. Akyildiz and I. Kasimoglu. Wireless sensor and actor networks: Research challenges. *Ad Hoc Networks Journal (Elsevier)*, 2(4):351–367, October 2004.
2. I.F. Akyildiz, W. Su, Y. Skarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38:393–422, 2002.

3. IBBT. DEUS - Deployment And Easy Use Of Wireless Services. http://projects.ibbt.be/deus, 2009.
4. C. Cordeiro, R. Fantacci, S. Gupta, J. Paradiso, A. Smailagic, and M. Srivastava. Body area networking: Technology and applications. *Selected Areas in Communications, IEEE Journal on*, 27(1):1–4, January 2009.
5. Steve Glass, Marius Portmann, and Vallipuram Muthukkumarasamy. Securing wireless mesh networks. *IEEE Internet Computing*, 12(4):30–36, 2008.
6. Sasikanth Avancha, Jeffrey L Undercoffer, Anupam Joshi, and John Pinkston. *Security for Sensor Networks*, chapter 12, pages 253–275. Kluwer Academic Publishers, January 2004.
7. Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high-throughput path metric for multi-hop wireless routing. In *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking (MobiCom '03)*, San Diego, California, September 2003.
8. Richard Draves, Jitendra Padhye, and Brian Zill. Routing in multi-radio, multi-hop wireless mesh networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, pages 114–128, New York, NY, USA, 2004. ACM.
9. Z. Shelby, P. Thubert, J. Hui, S. Chakrabarti, and E. Nordmark. Neighbor discovery for 6lowpan. *draft-ietf-6lowpan-nd-02 (work in progress)*, March 2009.
10. G. Tsirtsis and P. Srisuresh. Network address translation - protocol translation (nat-pt). *RFC 2766, http://www.ietf.org/rfc/rfc2766.txt*, February 2000.
11. C. Aoun and E. Davies. Reasons to move the network address translator - protocol translator (nat-pt) to historic status. *RFC 4966*, July 2007.
12. Architecture design project for new generation network. http://akari-project.nict.go.jp/eng/index2.htm.
13. Geoff Mulligan. The 6lowpan architecture. In *EmNets '07: Proceedings of the 4th workshop on Embedded networked sensors*, pages 78–82, New York, NY, USA, 2007. ACM.
14. Jeroen Hoebeke. *Adaptive Ad Hoc Routing and Its Application to Virtual Private Ad Hoc Networks*. PhD in Computer Engineering Science, Ghent University, IBCN - INTEC, B-9050 Ghent, Belgium, 2007.
15. David Culler, Prabal Dutta, Cheng Tien Ee, Rodrigo Fonseca, Jonathan Hui, Philip Levis, Joseph Polastre, Scott Shenker, Ion Stoica, Gilman Tolle, and Jerry Zhao. Towards a sensor network architecture: lowering the waistline. In *HOTOS'05: Proceedings of the 10th conference on Hot Topics in Operating Systems*, pages 24–24, Berkeley, CA, USA, 2005. USENIX Association.
16. Robert Braden, Ted Faber, and Mark Handley. From protocol stack to protocol heap: role-based architecture. *SIGCOMM Comput. Commun. Rev.*, 33(1):17–22, 2003.
17. Eli De Poorter, Benoît Latré, Ingrid Moerman, and Piet Demeester. Modular architecture for heterogeneous sensor networks. In *Proceedings of EWSN2007, the 4th European conference on Wireless Sensor Networks, EWSN adjunct poster proceedings, ISBN 1387-2109*, pages pp 21–22, Delft, the Netherlands, January 29-31 2007.