Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 923594, 14 pages
doi:10.1155/2012/923594

Research Article

Analysis of Mobility and Sharing of WSNs By IP Applications

Dennis J. A. Bijwaard,[1,2] Paul J. M. Havinga,[2,3] and Henk Eertink[4]

[1] *Inertia Technology, Offenbachlaan 2, 7522 JT Enschede, The Netherlands*
[2] *Ambient Systems, Colosseum 15d, 7521 PV Enschede, The Netherlands*
[3] *Pervasive Systems Research Group, University of Twente, P.O. Box 217, 7500 AE Enschede, The Netherlands*
[4] *Novay, Brouwerijstraat 1, 7523 XC Enschede, The Netherlands*

Correspondence should be addressed to Dennis J. A. Bijwaard, dennis@inertia-technology.com

Received 15 July 2011; Revised 6 October 2011; Accepted 13 October 2011

Academic Editor: Yuhang Yang

Movement of wireless sensor and actuator networks, and of nodes between WSANs are becoming more commonplace. However, enabling remote usage of sensory data in multiple applications, remote configuration, and actuation is still a big challenge. The purpose of this paper is to analyse and describe which mobility support can best be used in different scenarios, and how shared usage of mobile WSANs by multiple IP applications can best be scaled up. This paper describes logistic and person monitoring scenarios, where different types of movements take place. These mobility types and their implications are categorized and analysed. Different degrees of support for these mobility types are analysed in the context of the mobility scenarios. Additionally, different schemes are analysed for shared use of mobile WSANs by multiple applications. In conclusion, guidelines are provided for dealing with mobile and overlapping WSANs and the most promising scheme for shared use of mobile WSANs by IP applications.

1. Introduction

In this paper we analyse the mobility and sharing of internet-enabled wireless sensor and actuator networks (WSANs) by applications. Example applications are remote monitoring of goods that are transported between warehouses, monitoring of persons with health-related problems, and remotely controlling lights or motors (actuation). We focus on the following WSANs types (based on the taxonomy presented in [1]) where mobility and sharing of sensor data can be a concern.

(i) *Body Sensor Network (BSN).* BSNs are sensor networks consisting of few wireless sensor nodes on or around a living being's body connected to a more powerful device such as a smart phone. Monitoring of vital signs, tracking, and data collection have been the main objectives of these sensor networks. Interaction with sensor-enabled objects [2], such as a dumbbell or ball, is an interesting upcoming usage area. BSNs are small-scale, use different types of sensors, and are usually limited to single-hop wireless communication. Due to the fact that various types of personal information can be collected by these networks, both security and privacy are major concerns. Reliable data processing and timely feedback are of high importance. Applications using the sensor data can run on the mobile phone or on a server on the internet (e.g., via connectivity provided by general packet radio service (GPRS) or universal mobile telecommunications system (UMTS)).

(ii) *Structure Sensor Network (SSN).* SSNs consist of medium to large numbers of wireless nodes usually attached to buildings (e.g., office), structures (e.g., bridges), and infrastructure (e.g., rails) or deployed in specific venues (industrial sites). SSNs may be deployed both indoors and outdoors. Wireless nodes can also be attached to objects moving inside the structure and between structures. SSNs usually extend their wireless coverage with multiple hops of wireless communication and often use a variety of sensors.

(iii) *Vehicle Sensor Network (VSN).* The sensor data from within a moving vehicle (e.g., a car, boat, train, and plane) can also be transferred wirelessly (e.g., via GPRS) to a central server, be monitored remotely and/or merged with data from

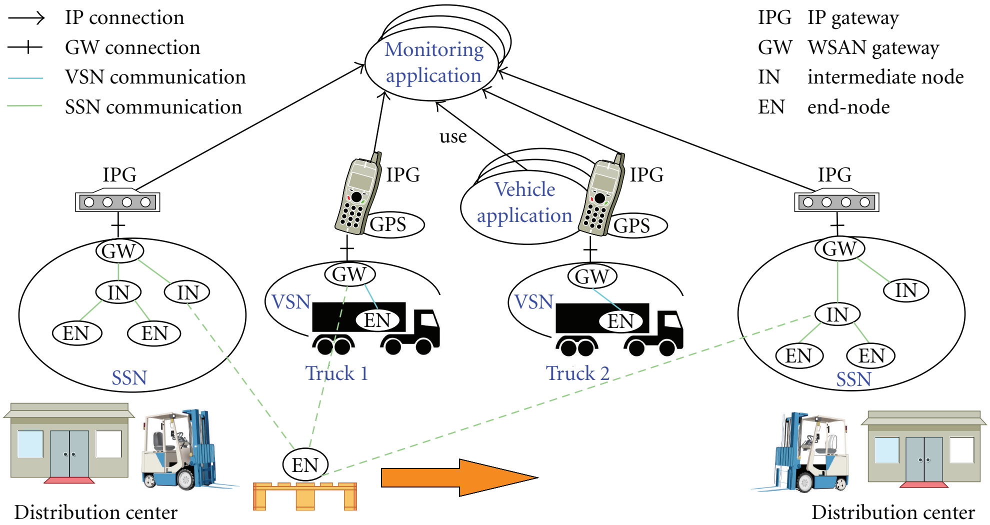

Figure 1: Monitoring moving goods in logistics.

other sensor networks. In warehouse logistics, VSNs are often used together with SSNs, for example, when monitored goods are transported in a truck from one warehouse to the other.

Other WSAN types are the environmental sensor network (ESN) that monitors conditions in the environment, the transport sensor network (TSN) that contains both VSN and wirelessly interconnected vehicles, and the participatory sensor network (PSN) consisting of smart phones with embedded sensors.

We analyse the different movements that can take place in and across WSANs. Furthermore, we analyse the movement of Internet-connected WSANs and applications that use them. These IP applications can use sensor information from the WSANs as well as configure and actuate the elements of individual nodes. The purpose of our analysis is to gain insight in the different types of mobility and to determine how they can best be supported in different usage scenarios. A lot of research has been done on mobility within WSANs (e.g., in [3–5]). However, in this paper, we focus on mobility issues of nodes that move between WSANs, WSANs that move in each other's range, and IP applications that use the sensor information. Additionally, this paper analyses ways to share multiple mobile WSANs in an IP application and how multiple IP applications can use the same WSANs. A number of issues related to shared WSAN usage were described by Shu et al. [6], and some solutions have been proposed for sharing WSANs [7, 8]. The purpose of the analysis of shared WSANs usage is to determine which sharing scheme can best be used with different numbers of attached IP applications, where both applications and WSANs can be mobile.

This paper is organized as follows. In Section 2, these WSAN types are used in mobility scenarios where IP application(s) use the WSANs. In Section 3, the types of mobility related to WSANs and IP applications are further detailed, and the consequences of these mobility types are analysed. Section 4 further analyses how to support these mobility types in the scenarios. Section 5 describes and analyses different schemes for handling sharing of mobile WSANs. The article concludes with the most promising scheme to be used for shared mobile WSANs.

2. Mobility Scenarios

WSANs can bring clear benefits to large-scale enterprise systems by delegating part of the business functionality closer to the point of action [9]. Healthcare, wellbeing, and sport-related person monitoring with WSANs is another area that gains research attention [10]. We have defined four scenarios where different types of mobility take place when nodes, complete WSANs, or IP applications using the sensor data are moving. Two scenarios are described where a truck with monitored goods moves between distribution centres and two where a monitored person moves around. For both trucks and monitored persons, an IP application can run on the internet or be directly attached to the WSAN while using information from another IP application running on the internet. Both a smartphone and router can be the IP gateway (IPG) for WSANs and applications.

2.1. Moving Vehicle Sensor Network. In this scenario, goods are tagged [11] with a sensor node. This sensor node travels with it when it moves with a truck between distribution centres. The trucks have a VSN deployed, and the distribution centres have an SSN deployed, see Figure 1. All sensor data, including global positioning system (GPS) location, are provided to the monitoring application. The VSN in truck 1 may lose its connection to the monitoring application when travelling through low-coverage areas (e.g., tunnels), and the IPG will roam to other GPRS network providers when going abroad. The monitoring application would typically offer realtime insight in the conditions of the goods, both when in storage and during transit. Based on condition deterioration, the truck could be rerouted to a closer-by destination.

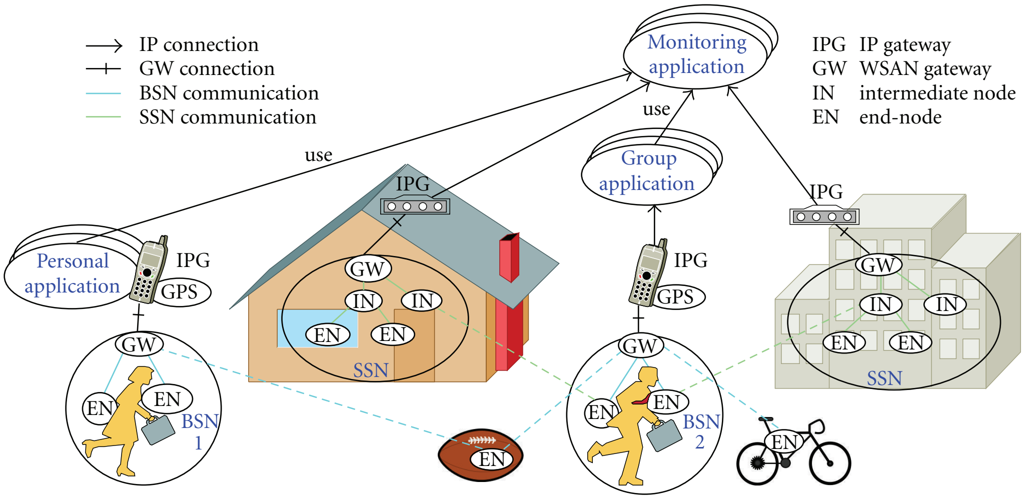

Figure 2: Moving BSN and personal applications.

2.2. Moving Vehicle Application. In this scenario, truck 2 in Figure 1 will have a GPRS connection to the Internet, and the vehicle application may lose connection to the monitoring application when travelling through low-coverage areas, and the IPG will roam to other network providers when going abroad. An example vehicle application could be monitoring the condition of goods in the truck and comparing the measurements with the inventory list to see if nothing is lost, misplaced, or spoiled. Via the monitoring application, the vehicle application could check historic conditions of the goods and location of missing goods or replacements.

2.3. Moving Body Sensor Network. In this scenario, a man with BSN 2 and smartphone moves between two houses with WiFi coverage and deployed SSN. The man uses objects that have sensor nodes attached that are compatible with the BSN. The BSN is used by a group application running remotely on the Internet (e.g., monitoring health status and location and may use other monitoring applications), see Figure 2. The smartphone will use the cheapest available Internet connection for communication to the Internet, such as WiFi.

2.4. Moving Personal Application. In this scenario, a woman with BSN 1 and smartphone moves between two houses with WiFi coverage and deployed SSN and uses sensor information from these SSN nodes. The BSN is used by a personal application running on the smartphone that she carries, see Figure 2. The smartphone will use the cheapest available Internet connection for obtaining measurements from a monitoring application. This monitoring application provides real-time sensor information from buildings based on GPS location.

3. Analysis of Mobility Types

Since WSAN nodes and its gateway can be attached to different moving objects, multiple types of mobility can occur within and across WSANs. Additionally, a device that hosts an IP application using the sensor data can move. A wireless node can be an endnode that is usually equipped with sensors and/or actuators or an intermediate node that can extend the coverage area of the WSANs.

This paper makes a distinction between the following WSAN nodes: the *gateway* that makes it available to applications, *intermediate nodes* that extend the coverage of the WSAN gateway, and *endnodes* that can connect to the intermediate nodes or gateway. Although the paper assumes that the endnodes do not change to intermediate nodes (like in the Ambient WSANs [12]), most of the mobility types described also apply when they do (such as with the Collection Tree Protocol (CTP) [13]). In the CTP, an endnode can join the WSANs via another endnode, turning the latter into an intermediate node.

The *wireless resources* used by a WSAN are characterised by one or more radio channels and the type of radio transmission. Example radio transmission types are probabilistic such as in carrier sense multiple access (CSMA), using timeslots such as in-time division multiple access (TDMA), and frequency hopping such as used in Bluetooth. Different WSANs are defined to be *compatible* when nodes of the WSANs can communicate with both gateways: they use the same WSAN protocol; use the same wireless resources; share the same encryption key.

We distinguish the following types of mobility related to WSANs.

(i) A moving IPG: network mobility takes place when the IPG starts using another wireless or wired network technology or starts using a different network provider on the same network technology. The implication of this change is that the Internet Protocol (IP) address of the IPG changes which will break connections when there is no transparent mobility support (like mobile IP (MIP) [14, 15]) in place. For short-lived connections like via HTTP, this connection break will result in a time-out. Movement can also make the IPG unreachable when there is no

Table 1: Mobility consequences for compatible WSANs and their nodes (data link layer).

					Static			
			WSAN		interm. node		endnode	
		Associated	In	Out	In	Out	In	Out
Moving	WSAN	—	Reallocate	Ok	Option	Lost	Option	Lost
	Interm. node	Yes	Alternative	Lost	Alternative	Lost/alternative	Option	Lost/alternative
		No	Option	Lost	Option			
	endnode	Yes	Alternative	Lost	Alternative	Lost/alternative		
		No	Option		Option			

network coverage or when it moves into a private or protected network. The moving IPG affects

(a) an attached WSAN: the IPG provides the WSAN with Internet connectivity for applications that want to use information from, configure, or actuate nodes in the WSAN. Examples are moving BSNs and VSNs. The implication of movement can be (un)reachability and (dis)connection of IP applications,

(b) an attached IP application: an IP application can use sensor data from nearby or remote WSANs via TCP/IP. The IPG movement can break existing connections from the IP application to the WSAN and make others possible.

(ii) A moving WSAN: a WSAN gateway that may have associated nodes. When the WSAN moves in range of another WSAN, matching wireless resources may require changing these resources in one of the WSANs to avoid bandwidth degradation and possible collisions. When compatible WSANs move in range, the nodes may associate to both of them. When a compatible WSAN moves in range of an intermediate or endnode, that node may join the WSAN. When the WSAN moves out of range of an associated intermediate or endnode, the association will be lost.

(iii) A moving intermediate node (with or without connected nodes)

(a) Within a WSAN. For instance, an intermediate node attached to a forklift can extend the radio coverage of the WSAN in the direction it moves and allow endnodes to communicate. When this intermediate node moves in range of a compatible WSAN gateway or an other intermediate node, it has the option to join that WSAN; when it moves out of range, it will lose the connection when it was associated. When the intermediate node moves in range of a compatible endnode, that endnode may join the WSAN. When the intermediate node moves out of range of an associated endnode, the endnode will lose its association,

(b) Across WSANs. For instance, an intermediate node attached to a forklift moving between the coverage areas of different compatible WSANs and picking up goods with attached endnode(s). The intermediate node can join the other WSAN when it is out of range of the other one and can choose the WSAN when it is in range of both. When it comes in range of another node, that node can choose to join it when it goes out of range of a node, that node will lose its association unless there is an alternative intermediate node or gateway in range.

(iv) A moving endnode

(a) Within a WSAN. The node may have to communicate via different intermediate nodes depending on their radio coverage. When an endnode moves in range of a compatible WSAN or connected intermediate node, it can join it. When it moves out of range of such a WSAN, it will be disassociated. When it moves out of range of a compatible intermediate node, it will be disassociated unless there is an alternative intermediate node or gateway in range,

(b) Across WSANs. For instance, an endnode that is placed with goods transported between WSAN-enabled distribution centres (see Section 2). When an endnode moves in range of a compatible WSAN or intermediate node, it can join it. When it moves out of range of such a WSAN, it will be disassociated. When it moves out of range of an intermediate node, it will be disassociated when there is no alternative in range.

Table 1 summarizes the mobility consequences on the data link layer when a WSAN, intermediate or endnode moves in or out of range of another compatible WSAN, intermediate, or endnode. Before this movement, the moving entity can be associated or not, for WSANs this does not apply. When WSANs come in each other's range, they may need to reallocate their wireless resources when they use the same ones. When an intermediate or endnode comes in range of another WSAN, it has the option to associate with that WSAN (denoted as "option") or choose it as an alternative link. When an intermediate or endnode moves out of range of an intermediate node, it may still have an alternative to use, else the association with the WSAN is lost.

Table 2: Mobility consequences for WSANs used by IP applications (network layer).

			Static IPG with attached			
			WSAN		Application	
		Connected	In	Out	In	Out
Moving IPG With attached	WSAN	Yes			Alternative Option	Lost/reroute
		No				
	Application	Yes	Alternative Option	Lost/reroute		
		No				

Table 2 summarizes what happens when an IPG with attached WSAN or IP application moves in or out of range of another IPG with attached IP application or WSAN, respectively. It assumes a bidirectional connection between the WSAN and the IP application. Moving in range here means that an IP connection becomes possible; moving out of range here means that the IP connection breaks (e.g., when no mobility protocol like MIP is in place and the IPG changes IP address). The moving IPG can have an attached IP application or WSAN that is connected or disconnected. When a connection breaks after moving, it may be reestablished by setting up an alternative route or it may be lost when this is not possible. When a connection becomes possible after moving, this is denoted as "option."

3.1. Remarks on WSAN Mobility Types

(i) Clearly, there are a number of options for connected nodes when another compatible WSAN comes in reach; how they deal with this can vary per WSAN type. In Section 4, we analyse this further for the given scenarios.

(ii) Table 1 merely describes the case where compatible WSANs and its nodes are considered. When incompatible WSAN protocols, wireless resources, or encryption are used, nodes cannot use these links. The gateway may still need to reallocate resources when the other WSAN operates on the same channel. Section 4 analyses different ways to support overlapping WSANs.

(iii) Without mobility support, complete WSANs and IP applications will disconnect when the IPG changes IP address. For seamless mobility, a number of mobility schemes can be used (described in Section 5).

(iv) WSAN nodes can potentially listen to messages in each of the WSAN they become part of, so they can also transfer information from one WSAN to another. Section 4 describes how data protection can be provided.

4. Analysing the Mobility Scenarios

In this section, the mobility scenarios from Section 2 are analysed in the light of the different mobility types described in Section 3 and the level of mobility support that can be offered.

Important properties for mobility support in the scenarios are the following

(i) *Security/Privacy.* Security of WSANs is a complex issue. Cryptographic credentials can be used to authenticate a node in a network and to encrypt the traffic; examples of these credentials are keys and passwords. Keys can be symmetric, where one key is used for both encryption and decryption or asymmetric, where a pair of keys is used for encryption and decryption. [16] provides a set of guidelines to handle security in WSANs, however asymmetric encryption becomes possible in WSANs [17].

(ii) *Interference.* Networks that use the same wireless resources can potentially interfere with each other. This interference can take different forms. When the WSAN protocols use timeslots, misalignment may cause collisions in two slots for every message, while timeslot alignment limits this to maximally one collision per message. When the WSANs use probabilistic Media Access Control (MAC) protocols, the chance for collisions will increase since there are more nodes. When a combination of timeslots and probabilistic MAC protocols are used, all timeslots are likely to suffer packet loss. Adaptive MAC protocols (like [18–20]) could be used to reduce TDMA interference.

(iii) *Overlap Awareness.* When a WSAN is aware of the presence of another WSAN, it can adapt itself accordingly. The first step to become aware is detecting an increase of interference. Next, a scan can be done to detect periodic traffic and silence on the radio channel. The detected periodic patterns can be used to adapt the WSAN traffic to reduce interference. Scanning can also be used to detect familiar WSAN types. When received messages can be decoded and are of nonregistered intermediate nodes, there is a good chance that a compatible WSAN is nearby.

(iv) *Wireless Resource Adaptation.* When a WSAN is aware of an overlapping WSAN, it can adapt its wireless resources to reduce interference. Examples of WSAN adaptation are channel change, synchronisation and distribution of timeslots between WSANs, turning off the gateway, and changing mode of operation (e.g., change from gateway to intermediate node).

(v) *WSAN Mobility.* What do nodes need to do to switch to another WSAN? Clearly, this depends greatly on the WSAN type, for instance, in the following cases.

(a) In the Ambient WSAN [12], all nodes have a unique 6-byte MAC address. The endnodes (called SmartPoints) can send messages (using CSMA) when they have compatible network keys. The intermediate nodes (called MicroRouters) need the (symmetric) network key to announce them selves to the gateway and to get (TDMA) timeslots assigned.

(b) In a IPv6 over low-power wireless personal access networks (6LoWPAN) network [21], the MAC address (2 upto 8 bytes) is used for node identification, and communication can be beacon less (pure CSMA) or beacon enabled (a hybrid of CSMA and TDMA). Nodes need to register themselves using the 6LoWPAN-customized neighbour discovery protocol, which makes a unique node address available in the WSAN and makes the WSAN network prefix available to the node. MIP can be used to make a node uniquely addressable when it moves between different WSANs. 6LoWPAN networks can utilize the symmetric keys of the 802.15.4 MAC.

(c) In the Inertia WSAN [22], the endnodes have a 2-byte address assigned; this address is used in the registration message to the gateway to obtain a TDMA timeslot. There are no intermediary nodes, since this network is primarily targeted at small body area networks. Objects with a node attached can be used by multiple WSANs in sequence. The messages are not (yet) encrypted.

(d) BSNs can also be constructed using Bluetooth which uses frequency hopping for radio transmission. Bluetooth is single hop (research is done on multihop scatternets) and usually uses a powerful device like a smartphone or PC as master. For switching to another network, the master of the other BSN needs to pair with the device and connect to one of its services. When pairing is done beforehand, the master could be programmed to autoconnect to a specific service, which would enable mobility of devices between masters.

(vi) *IP Mobility.* No transparent mobility scheme like MIP is considered in the scenario analysis; different IP mobility schemes for IP-enabled WSANs will be compared in Section 5.

(vii) *Costs.* Different wireless communication technologies have different associated costs. Using WiFi is generally cheaper or even free, while mobile data roaming via GPRS can vary from a relatively cheap data bundle to very costly when exceeding the bundle and when crossing nation borders. Internal WSAN communication is considered free of charge in this paper.

(viii) *Protocol Robustness.* Protocols that are not robust against foreign messaging will suffer most from interference. Methods to detect broken packages vary from a cyclic redundancy check (CRC) check to encryption where decryption is likely to fail for broken packets. Techniques like forward error correction can be used to add redundancy to the messages to be able to reconstruct some of the broken messages when there is interference.

(ix) *WSAN Compatibility* (as defined in Section 3).

4.1. Moving Vehicle Sensor Network. In order to get a complete measurement trace from the moment the sensor node comes out of storage in the first distribution centre until it arrives with the truck in the other distribution centre, measurements need to be merged at IP level in the monitoring application. In order to correctly correlate the measurements, an indication is required that the VSN gateway is in range of the SSN gateway. One indication is the fact that sensor nodes that were first reporting via the VSN start reporting via the SSN. Another indication is correlation of the GPS coordinates of the truck and the distribution centres. A third indication could be the detection of the SSN by the VSN gateway.

The most prominent changes that can occur when a VSN moves are the following

(i) The VSN moves in range of the SSN and potentially other VSNs (i.e., other trucks). When the WSANs use the same radio channel, there can be interference. When the WSANs are compatible, nodes may report via the other WSAN.

(ii) The VSN moves out of range of the SSN and potentially other VSNs. In this case, the nodes that remain in coverage of the VSN need to associate with it in order to transmit.

(iii) The VSN moves in range of intermediate and endnodes. When these nodes are compatible with the VSN, they may associate with it.

(iv) The VSN moves out of range of associated intermediate and endnodes. These nodes will no longer be able to transmit via the VSN so need to associate with the SSN or another VSN.

(v) The IPG in the truck may connect to different IP networks, for example, when it moves from one country to the other. Additionally, Internet connectivity can be temporarily unavailable.

(vi) The GPS coordinates of the truck and a distribution centre will differ when the truck is on the road and be similar when the truck is close by.

From the changes above, an issue becomes apparent when compatible WSANs come in range, that is, nodes that can report to both WSANs. The SSN should be capable to handle a few more nodes from the truck (since the nodes may go to storage anyway), however the VSN has a limited Internet connection and could have a harder time with additional nodes. Moreover, the monitoring application would have a harder time distinguishing the additional nodes reporting to the VSN from the ones that are really being transported by that truck. Therefore, the following solutions are proposed to restrict this freedom of the nodes.

(i) When a compatible WSAN is detected, the VSN gateway could be switched off. However, this could give problems when multiple VSNs are close together, since they may all decide to switch off. Furthermore, the nodes in the truck may not be able to reach the SSN from within the truck.

(ii) When a compatible WSAN is detected, the VSN gateway could be switched to intermediate node mode, so that it extends the coverage of that WSAN. However, this will put more load on the SSN and there may be a limit to the number of supported intermediate nodes (e.g., 64 in the Ambient network).

(iii) Without detection, the WSANs can be separated by using different network keys, and only the nodes that need to be mobile between the WSANs can have multiple keys (i.e., the nodes that go from storage to transport to another storage). The nodes can decide themselves when they start using the other network key for transmission, for example, switch to the SSN when the VSN link degrades.

Of course, also interference will be a concern for WSANs that use the same wireless resources. When using timeslots, this can partly be resolved by synchronizing and/or distributing timeslots. Alternatively, the VSN could be changed to use noninterfering wireless resources or different network key before it reaches the distribution centre, for instance by detecting similarity in GPS coordinates of the truck and distribution centre and consulting via the monitoring application what resources are used by the SSN.

Additionally, since the IPG can change its IP address, it will need to a mechanism to still report the measurements to the monitoring application. Obviously, the IPG could buffer measurements and send them after reconnecting to the monitoring application.

4.2. Moving Vehicle Application. The most prominent changes that can occur when a truck with vehicle application moves are the following.

(i) The IPG may connect to different GPRS or UMTS networks and optionally other wireless networks like WiFi.

(ii) IP connectivity of the IPG can be temporarily unavailable when there is bad or no wireless network coverage.

The implication of network attachment changes is often that the IP address of the IPG changes or becomes unavailable, which will break existing connections from the vehicle application or VSN to other IP applications on the Internet. When there is no connection, it will be impossible to connect to the monitoring application to fetch SSN measurements; in other cases, the connection needs to be reestablished.

Moreover, IP applications on the Internet that are using data from the vehicle application may be confronted with a changed IP address or unreachable IPG and associated connection breaks. The IP address of the IPG can be unreachable when not connected, when in a private area network, and when a restrictive firewall blocks the Internet traffic.

4.3. Moving Body Sensor Network. The most prominent changes that can occur when a BSN attached to a smartphone moves are:

(i) The BSN moves in range of the SSN and potentially other BSNs (i.e., other persons). When the WSANs use the same radio channel, there can be interference. When the WSANs are compatible, nodes may report via the other WSAN.

(ii) The BSN moves out of range of the SSN and potentially other BSNs. In this case, the nodes that remain in coverage of the BSN need to associate with it in order to transmit.

(iii) The BSN moves in range of objects with endnodes. When these nodes are compatible with the BSN, they may associate with it and transmit their measurements.

(iv) The BSN moves out of range of associated objects with endnodes. These nodes will no longer be able to transmit via the BSN.

(v) The smartphone may connect to different wireless networks and Internet connectivity can be temporarily unavailable.

(vi) The GPS coordinates of the smartphone and an SSN will differ when the person is out of range and be similar when he/she is close by.

The following mobility support options can be considered in this scenario. (Note that data protection is an important privacy aspect in BSNs.)

(1) *WiFi Usage.* Based on costs, the smartphone will have preference for WiFi to send BSN messages to the group application. instead of the more costly GPRS. Of course a new connections needs to be established to the group application. When multihoming is supported, the GPRS connection could be kept open while using WiFi. When moving out of WiFi range, GPRS will be used again and the WiFi connection to the application will break.

(2) *Secured Object Use.* since objects can potentially listen, store, and forward information, communication of more sensitive BSN sensor data should be encrypted.

(3) *Separate Uplink.* Since the BSN and SSN need to connect to different applications, they use a separate IP connection. The BSN should use encryption for privacy-sensitive messages, and its uplink should use encryption towards the application. Inter-BSN traffic is impractical for normal usage, so BSNs should use different encryption keys for privacy.

(4) *BSN Messages via Compatible SSN.* When BSN and SSN are compatible, BSN endnodes may use any intermediate SSN node or gateway to send their information upstream. The information could be encrypted such that only a specific application can decrypt it, for instance, by using the public key of the application for encrypting the message payload. The connection details for the destined application should somehow be conveyed to the IPG of the SSN gateway. This makes this a more customized and therefore less attractive option.

(5) *Dual-Stack BSN Endnodes.* They are endnodes that can communicate both with the SSN and incompatible BSN. This can also be used to send messages with encrypted payload upstream. Here, the BSN message destination also needs to be conveyed to the SSN gateway.

WiFi usage and encryption are a must for lowering communication costs and enhancing privacy. A separate IP uplink for the BSN and SSN messages is considered more practical than sending BSN messages via a compatible SSN.

4.4. Moving Personal Application. The most prominent changes that can occur when a person with personal application on a smartphone and attached BSN moves are the following.

(i) The smartphone may connect to different wireless networks, and Internet connectivity can be temporarily unavailable. In case of WiFi, local access to the IPG of the SSN may become possible.

(ii) The BSN can come in range of a SSN.

(iii) The BSN can get out of range of the SSN.

The following options can be considered for a moving application (on a smartphone) that uses its attached BSN and nearby SSN data.

(1) *Intranet Access to SSN Data.* Local access to SSN data may be possible in the associated Intranet when the smartphone is allowed to use this network. The SSN needs to advertise itself in some manner to enable discovery by the smartphone application.

(2) *Public SSN Server.* The SSN sends its sensor data to a publicly reachable server on the Internet from which applications can fetch it when they have the proper credentials. Retrieval could, for example, be based on the current GPS coordinates of the smartphone.

(3) *Direct Access to SSN Nodes.* Intercepting sensor information from the SSN in a BSN endnode is not really feasible, since SSN nodes direct their readings only towards the gateway and sleep most of the time to save energy and bandwidth (so requests could take very long). It would also require a compatible WSAN.
The first two options are both viable. Direct access to SSN nodes is not really an option.

4.5. Conclusions for WSAN Mobility Scenarios. The following conclusions can be drawn for the WSAN mobility scenarios.

(i) Support for moving endnodes between compatible VSNs and SSNs is feasible when all WSANs are controlled by one party (e.g., using [12, 21]). When multiple parties are involved, these WSANs are likely to use different encryption keys or protocols. For more flexibility, the endnodes could be equipped with multiple keys so that they can operate in all WSANs that they have keys for. The downside of this is that the network keys could potentially be obtained from each endnode, therefore the encryption should preferably work such that the encryption key only makes it possible to send something towards the gateway, not to decrypt all WSAN traffic. This can be accomplished by encrypting with the public key of the receiving gateway or the application. When using multiple applications, a group key could be used for the applications or the WSAN gateway (or its IPG) could do the encryption. In the latter case, traffic from the gateway to applications can then be encrypted separately.

(ii) In order to reduce interference from overlapping WSANs, the moving one could adapt its wireless resources before the overlap, for example, when similar GPS coordinates are detected.

(iii) In order to reduce interference from overlapping compatible WSANs, the moving one could turn off its gateway [12] or change to intermediate node mode.

(iv) In order to avoid endnodes of compatible WSANs to move between one another, they can use different network encryption keys so that only nodes that have both keys can move to the other WSAN and choose when changing WSAN is most appropriate.

(v) As discussed, merging SSN and BSN directly proves troublesome, especially for obtaining SSN measurements from nodes that often sleep. It is therefore more practical to merge BSN and SSN data at the application layer.

(vi) Encryption needs to be in place when BSN nodes send privacy-related information, else foreign objects can store and forward it.

(vii) WSAN protocols should be robust against foreign protocols, in order to coexist with other WSANs that use the same wireless resources.

5. Schemes for Shared Usage of Mobile WSANs

In this section, schemes are analysed where multiple applications use the same WSAN data [6–8], while the IPG of both the application and the WSAN can change IP address while moving. For handling mobility of a WSAN and connected applications, a number of options can be considered. The following properties are used for comparing them; a number of them originate from the scenarios analysis and others from deployment and complexity concerns.

(i) *Multi-Move.* Is simultaneous moving of source and destination supported?

(ii) *Smart Buffering.* Can intelligent buffering be done for applications when connections fail? Alarm messages and recent measurements can better be sent first since they usually have higher priority than older measurements.

(iii) *Overhead.* Is there inherent overhead in the approach?

(iv) *Duplication Node.* Where are messages destined for multiple recipients duplicated (or broadcasted)? Obviously, closer to the recipients is more efficient, especially when different recipients require different data rates [23]. Options are endnode, gateway, server, router, proxy, or relay.

(v) *Maturity.* Is the scheme still in research or is it already available?

(vi) *Deployment Needs.* What is necessary to deploy this on the current Internet?

(vii) *Access Control.* Who checks whether a destination is allowed to get the content? Depending on the number of destinations, the source may need to be taken out of the loop.

(viii) *Request Method.* Can application requests like configuration and actuation be transferred to the source using the methods of the mobility scheme or is an additional method required?

The combination of the properties overhead, duplication node, and access control give an indication of the scalability of a scheme. For instance, when a scheme has much overhead and duplication and access control are done at the source, it is not very scalable. The scalability increases when access control and duplication can be done closer to the destinations and when the overhead decreases.

5.1. IPv6 Mobility. 6LoWPAN turns the WSAN into an Internet Protocol version 6 (IPv6) network and addresses mobility of nodes with MIP [24]. This maintains reachability of all nodes in the WSAN when they move inside or across WSANs. However, WSAN nodes are often not reachable since they are sleeping to save energy. The 6LoWPAN gateway may then send additional information when a connection is broken because of sleeping duty cycle. Furthermore, 6LoWPAN assumes the application will handle resending to each individual node in case of failure. 6LoWPAN uses network mobility (NEMO) [25] for mobility of the complete WSAN. This means that the whole WSAN can change its point of attachment, since the network prefix of the WSAN has MIP support.

There are a number of issues with 6LoWPAN for WSANs.

(i) Traditionally, WSAN nodes just sent their readings towards the gateway, and an application can connect with the gateway to receive the sensor readings and for configuration. In 6LoWPAN, the gateway is an IPv6 router, and an IP application that is interested in the readings, that needs to register its IP address with each individual node (unless multicast can be used as destination, and applications can join the multicast group). This makes the binding between the application and nodes very tight which hinders scalability.

(ii) The burden of reaching sleeping nodes is placed on the IP application(s) that use them. Since the time window for sending messages to a WSAN node can be very small, this may be infeasible from remote application locations because of unpredictable latency on the path towards the WSAN. It is therefore advised to let the WSAN gateway handle reachability of nodes.

(iii) 6LoWPAN requires both IPv6 and a home agent (HA) with support for NEMO. Neither of those are currently widely deployed.

(iv) Every WSAN node will need to do access control for configuration and actuation from applications.

(v) When security is required, every WSAN node will need to do network or application layer encryption to secure the path towards the IP application, independent of data link layer security that may already be in place.

(vi) When multiple applications require sensor information from the same node, that node needs to send the information twice (unless there is multicast support), which doubles bandwidth both within the WSAN and its uplink.

(vii) Transmission control protocol (TCP) connections are a bad match with dynamic WSAN nodes that are often sleeping and since packets may also be dropped because of congestion or because the node battery drained or the node moved outside range. It is often better to send a new measurement than to retry an old measurement that got dropped because of collisions.

(viii) There are still numerous challenges related to security in 6LoWPAN [26], not to mention combining security with nodes that move between WSANs.

There are a number of things that the gateway could potentially handle transparently when it uses packet inspection to preprocess requests towards nodes and responses from nodes.

(i) Access control on behalf of nodes.

(ii) Buffer requests to sleeping nodes until they wake up.

(iii) Handling interest of an application, for instance, by using IP multicast.

(iv) Replication of sensor readings to multiple applications.

(v) Converting TCP connection towards a node to (UDP) packets, and injecting UDP packets from

Table 3: 6LoWPAN Mobility.

	Multimove	Smart buffering	Overhead	Duplication node	Maturity	Deployment needs	Access control	Request method
6loWPAN	Ok	–	Low	Endnode	–	IPV6, HA + NEMO	Endnode	Same

Table 4: Mobility using instant messaging.

	Multimove	Smart buffering	Overhead	Duplication node	Maturity	Deployment needs	Access control	Request method
SIMPLE, XMMP, IRC	Ok	–	Medium-high	Gateway	++	Client API, server	Server	Same
PSYC	Ok	–	Low	Server	+/−	Client API, server	Server	Same

the node to an existing TCP connection towards an application.

Most of these options turn the gateway from a simple IPv6 router to a stateful router that requires deep packet inspection and making real-time packet modifications. Moreover, transparent network layer security with nodes will make many of these options impossible without sharing key material between nodes and the multiple WSAN gateways they need to attach to.

Because of all these issues, complicated solutions and lack of IPv6 and IP multicast deployment, for the time being it makes more sense to look for a WSAN mobility scheme that does not require full IP access to individual WSAN nodes and allows efficient usage by multiple applications. The results for 6LoWPAN are summarized in Table 3.

5.2. Instant Messaging. When communication between an IP application and WSAN is seen as instant messaging over IP, it can make use of existing instant messaging solutions. Since these solutions have either a publicly reachable server or distributed ones, both the WSAN and IP application can move while sending messages. Most instant messaging approaches offer encryption of the connection to the messaging server or the messages themselves. Only a limited number of instant messaging protocols are suitable for integration in applications (i.e., are an open standard [27]) popular ones are Internet Relay Chat (IRC) [28], Protocol for SYnchronous Conferencing (PSYC) [29], SIP for Instant Messaging, and Presence Leveraging Extensions [30], (SIMPLE) and Extensible Messaging and Presence Protocol (XMPP) [31]. Most of these protocols are not designed for reliability, but reachability is good for all of them since they all provide one or more ways to traverse through firewalls. The messages in these protocols are quite large because they are text based, especially in SIMPLE and XMPP.

Unfortunately, only few instant messaging solutions (e.g., PSYC) offer efficient ways to send to multiple recipients. The results for instant messaging are summarized in Table 4.

5.3. Mobile Stream Endpoints. When communication between an IP application and a WSAN is seen as a bidirectional message stream, a number of mobility schemes can be envisaged. The results for mobile stream endpoints are summarized in Table 5.

Transparent Mobility. MIP could be used to transparently support mobility for both sides of this bidirectional stream. A drawback of this approach is that the WSAN needs to duplicate its sensor messages to each application, and that there is no good support for intelligent buffering when there is a connection outage, since MIP transparently keeps connections open even when there is temporarily no Internet connection.

Nomadic Mobility. A bidirectional connection could be setup between the WSAN and each application. The overhead can be low when a compact asynchronous protocol is used or high when a synchronous protocol with verbose messages is used (such as Simple Object Access Protocol (SOAP) [32]). In cases of connection loss, the WSAN would queue the messages that could not be sent and resend them in another order when the connection is reestablished later (possibly from a new IP address). Big drawbacks of nomadic mobility are the following.

(i) The WSAN and application may not be able to find one another when they move at the same time.

(ii) Communication is duplicated when multiple applications use one WSAN.

(iii) The WSAN will need to do access control for every application.

(iv) Bidirectional messaging does not work very well with web services when only one communication endpoint is publicly reachable. This would involve some sort of polling to get the requests from the other direction.

Nomadic Mobility with Public Server. Nomadic mobility can be enhanced using a publicly reachable server towards which both WSANs and applications set up a bidirectional stream. This enables both WSANs and applications to be mobile and at the same time reduces messaging that would

Table 5: Mobility using stream endpoints.

	Multimove	Smart buffering	Overhead	Duplication node	Maturity	Deployment needs	Access control	Request method
MobileIP	Ok	–	Low	Gateway	+/–	HA	Gateway	Same
Nomadic	—	+/–	Low-high	Gateway	++	Self-contained	Gateway	Same
Nomadic with server	Ok	+/–	Low-high	Server	+/–	Self-contained	Server	Via server
session mobility	Ok	+/–	Low	Gateway	+/–	SIP server	Gateway	SIP message

Table 6: Mobility of content source.

	Multimove	Smart buffering	Overhead	Duplication node	Maturity	Deployment needs	Access control	Request method
IP multicast	—	–	Low	Router	++	Router(s)	Router	Separate
Content-based routing	—	++ with proxy	Low-medium	Server	++	Client API, server(s)	Server	WSAN subscribes
Cache and forward routing	Ok	++	Low	Proxy	–	Multiple IP tunnels	Proxy	Separate
Partial sessions with relays	Ok	+	Low	Relay	–	SIP server and relays	Appl. server	SIP message

otherwise be duplicated at the source, that is, the WSAN only has to send sensor information once and the server duplicates it to all connected applications. An example is the asynchronous Ambient middleware [12]. With web services, the bidirectional messaging drawback worsens, since all interested applications will have to poll for updated sensor data and the WSAN will have to poll for configuration and actuation requests.

Session Mobility. A session could be set up between the IP application and the WSAN, with for instance the Session Initiation Protocol (SIP) [33, 34]. This session will contain the bidirectional messaging connection between the WSAN and the IP application. A SIP re-INVITE can be used to move the endpoints on either side to another IP address. Just like in nomadic mobility, messages during connection outage can be queued and sent in a different order when the connection is reestablished. The WSAN gateway is expected to handle sending messages to sleeping nodes and will forward all messaging from the WSAN to the application. Since the WSAN gateway is the IP endpoint of communication with applications, it can also easily support network layer security mechanisms such as virtual private network (VPN) and Internet Protocol Security (IPsec) [35]. There are a number of issues with this approach.

(i) Each WSAN will need to do access control for every application.

(ii) The WSAN needs to replicate messages for every attached application, wasting uplink bandwidth.

(iii) Connection setup must be supported at both network ends (possibly private or protected networks).

5.4. WSAN as Content Source. When communication between an IP application and WSAN is seen as a content stream from the WSAN to all interested applications, the messaging could be optimized by bundling communication to groups of applications. The results for mobile content sources are summarized in Table 6.

IP Multicast. IP multicast by the sender enables sending information to multiple recipients that can join the stream. IP multicast has a number of issues.

(i) Mobility of the content source has only recently become a research topic and would typically involve context transfer between routers.

(ii) Configuration and actuation messages towards the source would have to use a different protocol.

(iii) IP multicast is mainly deployed in content distribution networks for pre-defined sources, and a lot of routers in the Internet do not yet support or allow it.

Content-Based Routing. With content-based routing [36–38], routing is done based on elements of the content body instead of the destination. Interested applications can subscribe for different content. Content-based routing has the following issues.

(i) Mobility of the source has only recently become a research topic.

(ii) Routing is often implemented on the application layer, inheriting application protocol overhead.

(iii) Configuration and actuation requires reverse traffic, but WSAN could subscribe for these events.

(iv) Messages are not cached for unconnected clients, however a subscription proxy [39] could be used.

Cache-and-Forward Routing. In cache-and-forward routing [40], interested applications can subscribe to content via a local post office which will look up the source post office via a naming service. The content is sent by the source via cache-and-forward routers towards the destination(s). It allows efficiently sending content by the (mobile) source to multiple recipients. Both the sender and the receivers can be mobile.

(i) Cache-and-forward routing is a future Internet research topic and would require deployment of a number of network elements.

(ii) Configuration and actuation messages towards source would have to use a different protocol.

Partial Session Mobility with Relays. When the session between the WSAN and applications is split in subsession between the WSAN and subsessions between the relay and each application, mobility can be supported for both the WSAN and the applications without duplication at the source (but at the relay instead). The duplication can be further reduced by adding additional relays in different network segments. With SIP, an SIP application server can be used to automate splitting the sessions [41, 42]. The INVITE from an application towards the WSAN is therefore picked up by an SIP application server and split into subsessions.

(i) One subsession between the WSAN and the relay. This subsession is typically set up when the first application subscribes to the WSAN messages using an SIP INVITE.

(ii) Other subsessions between the relay and each application. These subsessions are set up for each application that subscribes.

(iii) To further reduce duplicate message streams, a subsession between a relay and another relay can be set up when multiple applications in the same network segment subscribe to the same WSAN stream. An SIP re-INVITE can be used to split the subsession between the initial relay and the application(s) to one: between the relays and others between the new relay and each application.

A further advantage of splitting the streams is that private and protected networks are less of an issue, since no connection needs to be set up directly between these sort of networks, because a relay will be used that is reachable by both endpoints. Configuration and actuation requests towards the WSAN can likewise be intercepted and be transformed into a configuration or actuation message towards the WSAN after access control is checked and when there is no conflict between multiple applications. For example, when one application requires a temperature update every 5 minutes instead of the default 15 minutes, the WSAN nodes can be configured to send it every 5 minutes, and the relay would forward it in this pace to the requesting application and keep forwarding it every 15 minutes to the other applications.

5.5. Reflection. Currently, only few reasonably mature mobility schemes offer buffering, low overhead and do not need an additional protocol for requests, namely, a nomadic with server when a compact asynchronous protocol is used, session mobility and content-based routing with a proxy. However, session mobility does not scale well since it does access control at the gateway for each application and duplicates messages for multiple applications at the gateway, wasting precious uplink bandwidth. Content-based routing with a proxy does scale well, but does not guarantee reliable communication and source mobility is still a research topic. So, the nomadic with public server with a compact asynchronous protocol provides the best current option. The partial sessions with relay scheme forms a good, but nonmature, alternative when more applications use the WSAN data, since it can add relays in different network segments on the fly. This option is similar in efficiency to cache and forward routing although it uses a session approach instead of post offices and can use its own protocols for sending messages towards the source. The cache and forward routing could also provide a solution for some of the shortcomings of 6LoWPAN, since it makes it possible to cache and forward the sensor messages for interested applications instead of direct IP connections.

6. Conclusions

This paper analysed scenarios in which different WSAN and application movements take place. Moving endnodes between different WSANs can be supported by compatible WSANs but does not allow controlling when the movement takes place. With different encryption in each WSAN, the endnodes can associate with the other WSAN at a convenient moment.

To reduce interference between WSANs, the moving gateway can turn off its gateway or switch to intermediate node mode to make endnodes communicate with the other WSANs. To prevent interference from overlapping WSANs, it is advisable to adapt the wireless resources before the overlap occurs, for instance, by detecting similarity in GPS coordinates of the WSANs.

With different WSAN types, data of overlapping WSANs can best be merged at the application layer. In order to support coexistence of WSANs using the same wireless resources, WSAN protocols should be robust against foreign protocol messaging.

When privacy is required, as is often the case in body sensor networks, messages can better be encrypted with the public key of the receiving gateway (or middleware), which can in turn send it encrypted to one or more applications.

For sharing WSANs among few applications, nomadic mobility with a server using compact asynchronous messaging has the best properties. When the number of applications increases, schemes that bundle traffic towards groups of applications become more attractive.

Acknowledgment

This paper is partially funded by AgentSchapNL as part of the Dutch Point One initiative (free project).

References

[1] N. Meratnia, B. J. V. D. Zwaag, H. W. V. Dijk, D. J. A. Bijwaard, and P. J. M. Havinga, "Sensor networks in the low lands," *Sensors*, vol. 10, no. 9, pp. 8504–8525, 2010.

[2] S. Bosch, R. S. Marin-Perianu, P. J. M. Havinga, M. Marin-Perianu, A. Horst, and A. Vasilescu, "Automatic recognition of object use based on wireless motion sensors," in *Proceedings of the International Symposium on Wearable Computers 2010*, pp. 143–150, IEEE Computer Society, Seoul, Republic of Korea, October 2010.

[3] M. Ali, T. Suleman, and Z. A. Uzmi, "MMAC: a mobility-adaptive, collision-free MAC protocol for wireless sensor networks," in *Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference (IPCCC '05)*, pp. 401–407, April 2005.

[4] H. Pham and S. Jha, "An adaptive mobility-aware MAC protocol for sensor networks (MS-MAC)," in *Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 558–560, October 2004.

[5] D. Zhang, Q. Li, X. Zhang, and X. Wang, "DE-ASS: an adaptive MAC algorithm based on mobility evaluation for wireless sensor networks," in *Proceedings of the 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM '10)*, pp. 1–5, September 2010.

[6] L. Shu, M. Hauswirth, L. Cheng, J. Ma, V. Reynolds, and L. Zhang, "Sharing worldwide sensor network," in *Proceedings of the International Symposium on Applications and the Internet (SAINT '08)*, pp. 189–192, August 2008.

[7] M. Isomura, T. Riedel, C. Decker, M. Beigl, and H. Horiuchi, "Sharing sensor networks," in *Proceedings of the IEEE International Conference on Distributed Computing Systems Workshops*, ICDCS Workshops 2006, p. 61, July 2006.

[8] A. Malatras, A. Asgari, and T. Bauge, "Web enabled wireless sensor networks for facilities management," *IEEE Systems Journal*, vol. 2, no. 4, pp. 500–512, 2008.

[9] M. Marin-Perianu, N. Meratnia, P. J. M. Havinga et al., "Decentralized enterprise systems: a multiplatform," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 57–66, 2007.

[10] A. Avci, S. Bosch, M. Marin-Perianu, R. S. Marin-Perianu, and P. J. M. Havinga, "Activity recognition using inertial sensing for healthcare, wellbeing and sports applications: a survey," in *Proceedings of the 23th International Conference on Architecture of Computing Systems (ARCS '10)*, pp. 167–176, VDE Verlag, Hannover, Germany, February 2010.

[11] L. Evers, M. J. J. Bijl, R. S. Marin-Perianu, R. S. Marin-Perianu, and P. J. M. Havinga, "Wireless sensor networks and beyond: a case study on transport and logistics," Technical Report TR-CTIT-05-26, Centre for Telematics and Information Technology University of Twente, Enschede, The Netherlands, 2005.

[12] D. J. A. Bijwaard, W. A. P. van Kleunen, P. J. M. Havinga, L. Kleiboer, and M. J. J. Bijl, "Industry: using dynamic WSNs in smart logistics for fruits and pharmacy," in *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems (SenSys '11)*, pp. 218–231, ACM, Seattle, Wash, USA, November 2011.

[13] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09)*, pp. 1–14, ACM, New York, NY, USA, November 2009.

[14] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," RFC 3775, IETF, 2004.

[15] C. Perkins, "IP mobility support for IPv4, revised," RFC 5944, IETF, 2010.

[16] Y. W. Law and P. Havinga, "How to secure a wireless sensor network," in *Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information*, pp. 89–95, December 2005.

[17] J. Lopez, "Unleashing public-key cryptography in wireless sensor networks," *Journal of Computer Security*, vol. 14, pp. 469–482, 2006.

[18] G. Haigang, L. Ming, W. Xiaomin, C. Lijun, and X. Li, "An interference free cluster-based TDMA protocol for wireless sensor networks," in *Wireless Algorithms, Systems, and Applications*, X. Cheng, W. Li, and T. Znati, Eds., vol. 4138 of *Lecture Notes in Computer Science*, pp. 217–227, Springer, Berlin, Germany, 2006.

[19] M. Macedo, A. Grilo, and M. Nunes, "Distributed latency-energy minimization and interference avoidance in TDMA wireless sensor networks," *Computer Networks*, vol. 53, no. 5, pp. 569–582, 2009.

[20] T. Wu and S. Biswas, "Reducing inter-cluster TDMA interference by adaptive MAC allocation in sensor networks," in *Proceedings of the First International IEEEWoWMoM Workshop on Autonomic Communications and Computing (ACC '05)*, vol. 2, pp. 507–511, IEEE Computer Society, Washington, DC, USA, 2005.

[21] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," RFC 4919, IETF, 2007.

[22] Inertia Technology, http://inertia-technology.com.

[23] R. Muller and G. Alonso, "Efficient sharing of sensor networks," in *Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS '06)*, pp. 109–118, October 2006.

[24] E. Perera, V. Sivaraman, and A. Seneviratne, "Survey on network mobility support," *Mobile Computing and Communications Review*, vol. 8, pp. 7–19, 2004.

[25] V. Devarapalli, R. Wakikawa, R. Petrescu, and P. Thubert, "Network mobility (NEMO) basic support protocol," RFC 3963, IETF, 2005.

[26] S. Park, K. Kim, W. Haddad, S. Chakrabarti, and J. Laganier, "IPv6 over low power WPAN security analysis," Internet Draft 05, IETF, 2001.

[27] ITU-T, "Open standard," http://www.itu.int/en/ITU-T/ipr/Pages/open.aspx.

[28] W. Kantrowitz, "Network questionnaires," RFC 459, IETF, 1973.

[29] C. V. Loesch, "Whitepaper on PSYC," http://www.psyc.eu/whitepaper.

[30] IETF, "The SIMPLE working group charter," http://datatracker.ietf.org/wg/simple/charter.

[31] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): core," RFC 3920, IETF, 2004.

[32] N. Mitra and Y. Lafon, "SOAP specificiations," http://www.w3.org/TR/soap.

[33] A. Berger and D. Romascanu, "Power ethernet MIB," RFC 3621, IETF, 2003.

[34] A. Roach, "Session initiation protocol (SIP)-specific event notification," RFC 3265, IETF, 2002.

[35] S. Kent and K. Seo, "Security architecture for the internet protocol," RFC 4301, IETF, 2005.

[36] G. Banavar, T. Chandra, B. Mukherjee, J. Nagarajarao, R. E. Strom, and D. C. Sturman, "Efficient multicast protocol for content-based publish-subscribe systems," in *Proceedings of the 19th IEEE International Conference on Distributed Computing Systems (ICDCS'99)*, pp. 262–272, June 1999.

[37] L. Fiege, F. Gartner, O. Kasten, and A. Zeidler, “Supporting mobility in content-based publish/subscribe middleware,” in *Middleware 2003*, M. Endler and D. Schmidt, Eds., vol. 2672 of *Lecture Notes in Computer Science*, pp. 998–998, Springer, Berlin, Germany, 2003.

[38] Elvin, http://www.elvin.org.

[39] P. Sutton, R. Arkins, and B. Segall, “Supporting disconnectedness-transparent information delivery for mobile and invisible computing,” in *Proceedings of the 1st International Symposium on Cluster Computing and the Grid (CCGRID ’01)*, p. 277, IEEE Computer Society, Brisbane, Australia, May 2001.

[40] S. Paul, R. Yates, D. Raychaudhuri, and J. Kurose, “The cache-and-forward network architecture for efficient mobile content delivery services in the future internet,” in *Proceedings of the First ITU-T Kaleidoscope Academic Conference in Innovations in NGN: Future Network and Services (K-INGN ’08)*, pp. 367–374, May 2008.

[41] J. Aartse Tuijn and D. Bijwaard, “Spanning a multimedia session across multiple devices,” *Bell Labs Technical Journal*, vol. 12, no. 4, pp. 179–193, 2006.

[42] S. van der Gaast and D. Bijwaard, “Efficiency of personalized content distribution,” *Bell Labs Technical Journal*, vol. 13, no. 2, pp. 135–145, 2008.