# Analysis of Mobile WSNs over IP

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

[1] Inertia Technology, Offenbachlaan 2, 7522JT Enschede,
dennis@inertia-technology.com
[2] Pervasive Systems, University of Twente, P.O. Box 217, 7500 AE Enschede
P.J.M.Havinga@utwente.nl
[3] Ambient Systems, Colosseum 15d, 7521 PV Enschede,
[4] Novay, Brouwerijstraat 1, 7523 XC Enschede, Henk.Eertink@novay.nl

**Abstract.** 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. 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.

## 1 Introduction

This paper analyses the different movements that can take place in and across Wireless Sensor and Actuator Networks (WSANs) and of attached devices that provide connection to one or more IP applications. These IP applications can use sensor information from the WSAN as well as configure and actuate the elements of individual nodes. The purpose of this analysis is to gain insight in the different types of mobility and to determine which setup works best in different usage scenarios. A lot of research has been done on mobility within WSANs (e.g. in [1, 8, 9], this paper focusses on mobility issues of: nodes that move between WSANs, WSANs that move in each other's range, and moving IP applications that use the sensor information.

This paper is organized as follows. In section 2 the WSAN types are described where mobility is a concern. In section 3 these WSAN types are used in scenarios where both mobility and shared use by IP applications take place. In section 4 the types of mobility related to WSANs and IP applications are further detailed and the consequences of these mobility types are analysed. In section 5 the level of support for these mobility types required by the scenarios is further analysed. The article concludes how mobility of WSANs can best be handled.

## 2 Considered mobile WSAN types

In this paper we distinguish the following WSANs types (based on [6]) where mobility and sharing of sensor data can be a concern:

- **Body sensor network (BSN)**: BSNs are sensor networks consisting of few wireless sensor nodes on or around a living being's body integrated with 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 [3], such as a dumbbell or ball, is an interesting upcoming usage area. BSNs are small scale, heterogeneous (in terms of different types of sensors) and require single-hop 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)).
- **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), 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 require protection mechanisms against both physical and electronic attacks. They may be both single and multi hop (depending on their scale) and are often heterogeneous (in terms of both sensor nodes functionality and type of sensors).
- **Vehicle sensor network (VSN)**: The sensor data from within a moving vehicle (e.g. a car, boat, train, plane) can also be transferred wirelessly (e.g. via GPRS) to a central server, and be monitored remotely and/or merged with data from other sensor networks.

## 3 Mobility scenarios

Four scenarios have been defined where different types 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.

### 3.1 Moving vehicle sensor network

In this scenario, goods in a distribution center are tagged [4] with a sensor node that travels with it when it moves with a truck to another distribution center.

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 loose its connection to the monitoring application when travelling through low-coverage areas (for instance 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 re-routed to a closer-by destination.

### 3.2 Moving vehicle application

In this scenario, truck 2 in figure 1 will have a GPRS connection to the Internet, and the vehicle application may loose 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 monitor the condition of goods in the truck, and compare 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.

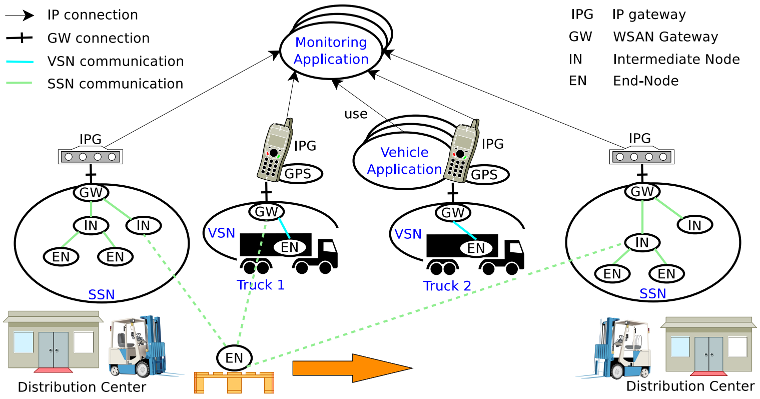

**Fig. 1.** Monitoring moving goods in logistics

### 3.3 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 (for example 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.

### 3.4 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 the she carries, see 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.

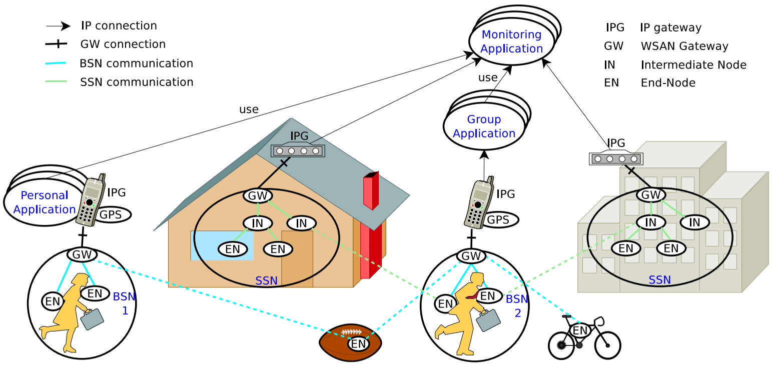

**Fig. 2.** Moving BSN and personal applications

## 4 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 end-node that is usually equipped with sensors and/or actuators, or an intermediate node that can extend the coverage area of the WSAN.

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 **end-nodes** that can connect to the intermediate nodes or gateway. Although the paper assumes that the end-nodes do not change to intermediate nodes (like in the Ambient WSAN [2]), most of the mobility types described also apply when they do (such as with the Collection Tree Protocol [5] (CTP)). In the CTP, an end-node can join the WSAN via another end-node, 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 transmission. Examples transmission types are: probabilistic as in Carrier Sense Multiple Access (CSMA), and/or using timeslots as in Time Division Multiple Access (TDMA) and/or frequency hopping.

We distinguish the following types of mobility related to WSANs:

- 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)) is 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 network coverage, or when it moves into a private or protected network. The moving IPG affects:
  - an attached WSAN. The IPG provides the WSAN with Internet connectivity for applications that want to use info 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.
  - 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.
- A moving WSAN, i.e. 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. Nodes may jump from one to the other WSAN. When moving out of range of another WSAN, the nodes that move with it can stay associated or will associate when they were not yet, non-moving nodes will associate to the non-moving WSAN. When the WSAN moves in range of an intermediate or end-node, that node may decide to join the WSAN when the wireless resources are compatible. When the WSAN moves out of range of an associated intermediate or end-node, the association will be lost.
- A moving intermediate node (with or without connected nodes)
  - 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 allows end-nodes to communicate. When this intermediate node moves in range of a WSAN gateway or other intermediate node, it has the option to join that WSAN, when it moves out of range it will loose the connection when it was associated. When the intermediate node moves in range of an end-node, the end-node may join when the intermediate node is itself joined. When the intermediate node moves out of range of an

end-node, the end-node will loose its association when it was associated via the intermediate node.
    - across WSANs, for instance an intermediate node attached to a forklift moving between the coverage areas of different WSANs, and picks up goods with attached end-node(s). The intermediate node will join the other WSAN when it is out of range of the other one, an 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 loose its association unless there is alternative intermediate node or gateway in range.
- A moving end-node
    - within a WSAN, the node may have to communicate via different intermediate nodes depending on their radio coverage. When an end-node moves in range of a WSAN or connected intermediate node it can join it. When it moves out of range of a WSAN, it will be disassociated. When it moves out of range of an intermediate node, it will be disassociated unless there is an alternative intermediate node or gateway in range.
    - across WSANs, for instance an end-node that is placed with goods transported between WSAN-enabled distribution centres (see section 3). When an end-node moves in range of a WSAN or intermediate node, it can join it. When it moves out of range of 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.

### 4.1 Remarks on WSAN mobility types

- Clearly there are a number of options for connected nodes when another WSAN comes in reach, how they deal with this can vary per WSAN type. In section 5 we analyse this further for the given scenarios.
- When different WSAN protocols or wireless resources are used, nodes can not use these links. The gateway may still need to re-allocate resources when the other WSAN operates on the same channel. Section 5 shows different levels of support for overlapping WSANs.
- Without mobility support, complete WSANs and IP applications will disconnect when the IPG changes IP address.
- 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 5 describes how data protection can be provided.

## 5 Analysing the mobility scenarios

In this section the mobility scenarios from section 3 are analysed in the light of the different mobility types described in section 4 and the level of mobility support that can be offered.

Important factors for this analysis are:

- **encryption keys**: 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.
- **interference**: networks that use the same wireless resources can potentially interfere with each other.
- **awareness**: when a WSAN is aware of the presence of another WSAN it can adapt itself accordingly. Examples of WSAN adaptation are: channel change, synchronisation and distribution of timeslots between WSANs, turning off the gateway, changing mode of operation (for instance change from gateway to intermediate node).
- **mobility**: what do nodes need to do to switch to another network? Clearly this depends greatly on the WSAN type, for instance in the the Ambient WSAN [2], the IPv6 over Low power Wireless Personal Access Networks [7] (6LoWPAN) network, a unique node-id, equal wireless resources and optionally a symmetric key are required for communcation with the WSAN.

### 5.1 Moving vehicle sensor network

The following levels of mobility support can be offered when the VSN (partly) overlaps with a SSN (depending on the compatibility and awareness in the WSANs):

1. **unaware WSANs**: WSANs that are unaware of each other can potentially disrupt each other when they use the same wireless resources. In this case, the intermediate and end-nodes of both networks may choose to connect to the other sensor network when wireless protocol and encryption keys are compatible.
2. **robust unaware WSANs**: When the WSANs are robust against foreign protocol messaging, they will only suffer a decrease in available bandwidth when they are partly overlapping while using the same wireless resources. When using the same protocol and wireless resources and encryption key, there is no way to stop nodes connecting to the other WSAN and vice-versa.
3. **aware gateway**: VSN gateway turns off and the VSN sensors report to the SSN of the distribution center. This is only an option when the wireless protocol and encryption keys are compatible, and the same wireless resources can be used.
4. **intelligent aware gateway**: the VSN gateway turns into intermediate node. This is an option when compatible wireless protocol and encryption techniques are available, when the same wireless resources can be used, and when an additional intermediate node can be accommodated in the SSN). This ensures better coverage for the sensors inside the truck, but puts more load on the SSN, especially when there are multiple VSN-enabled trucks.
5. **intelligent aware sensor nodes**: the VSN sensor nodes in the truck communicate both to the VSN and the SSN in parallel and may report differently to both networks regarding for instance privacy rules and needs. The communication towards the nodes may become harder, since they will be busy on

the other WSAN part of the time. This will also involve a more complicated scheduler, and multiple WSAN protocol stacks when they are incompatible.

6. **intelligent application**: sensor information is merged elsewhere (i.e. the VSN data is merged remotely with that of both SSNs, for instance in a back-office monitoring application). This requires an indication that the VSN gateway is in range of the SSN gateway to correlate the data, for instance using GPS location. Additionally, the gateways should not interfere too much, for instance use separate channels, different encryption keys, and be robust against foreign protocol messaging.

Additionally, the IPG can change its IP address when it starts using another network technology or another network provider, and no transparent network mobility like MIP is in place. Additionally, Internet connectivity can be temporarily unavailable. This will change the IP address of the IPG or make it unavailable and therefore break existing connections from the WSAN to applications.

Given the required resources in terms of bandwidth and code size on the WSAN nodes and gateway to support mobility awareness and intelligence, and scalability issues with multiple trucks, the following options are the most viable:

- the robust unaware WSANs combined with an intelligent application.
- the aware gateway combined with an intelligent application.

In both cases the different networks can be protected with separate encryption keys. The end-nodes would then require encryption keys for all WSANs they need to operate in, and/or can encrypt its payload such that it can only be decrypted in a specific application.

### 5.2 Moving vehicle application

When the IPG to which the vehicle application is attached moves, the IPG may connect to different GPRS networks and optionally other wireless network technologies like WiFi. It can also mean temporary unavailability of IP connectivity. The implication of this change of network attachment 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.

### 5.3 Moving body sensor network

The following mobility support options can be considered when a BSN attached to a smartphone moves in range of an SSN and WiFi access point (data protection is an important privacy aspect in BSNs):

1. **WiFi usage**: when the smartphone moves in range of the WiFi access point it can use that for sending BSN messages to the group application instead of the more costly GPRS. The implication is that the IP address of the

smartphone changes and the old connection breaks when no transparent IP mobility like MIP is in place. When multi-homing is supported, the GPRS connection could be kept open while using WiFi. When moving out of WiFi range, GPRS will be used again breaking the WiFi connection to the application.

2. **secured object use**: since objects can potentially listen, store and forward information, communication of more sensitive BSN sensor data should be encrypted.
3. **robust and separate uplink**: BSN and SSN are robust for each other's messaging and use a different uplink. The BSN should use encryption for privacy-sensitive messages and its uplink should use encryption towards the application.
4. **compatible WSANs**: when BSN and SSN are compatible, end nodes may use any intermediate 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. Still the destined application for BSN messages should be known to the SSN gateway, since it is most probably different from the application that uses the SSN data.
5. **intelligent BSN end-nodes**: end-nodes that can communicate both with the SSN and incompatible BSN. This can also be used to sent messages with encrypted payload upstream. Here, the BSN message destination also needs to be conveyed to the SSN gateway.

WiFi usage and secured object use are a must for lowering communication costs and enhancing privacy. A robust and separate uplink for the BSN and SSN is the most viable option. Sending BSN messages via a SSN is troublesome, since it needs to be encrypted and somehow addressed to the IP application.

### 5.4 Moving personal application

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 gateway**: the SSN gateway could offer direct IP access to sensor data to nearby applications. Access may be possible in the associated Intranet when the smartphone would be allowed in this network, direct access via the Internet is less likely because of firewalls and private networks that are usually in place. Because of local access, the SSN needs to advertise itself in some manner to be discovered 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 an BSN end node 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 protocol, the same wireless resources and encryption keys.

The first two options are both viable. Direct access to SSN nodes is not really an option.

### 5.5 Conclusions for WSAN mobility scenarios

The following conclusions can be drawn for the WSAN mobility scenarios:

- Support for moving end-nodes between VSNs and SSNs is feasible when all WSANs are controlled by one party. When multiple parties are involved these WSANs are likely to use different encryption keys (or even different protocols). For more flexibility, the end-nodes 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 end-node, so therefore the encryption should work such that the encryption key only makes it possible to send something towards the gateway, not to decrypt everything that is sent inside the network. This can be accomplished by encrypting with the public key of the receiving gateway or the application. When using multiple applications, the gateway (or middleware connected with it) is the best option. Traffic from the gateway to applications can then be encrypted separately.
- It is better to merge BSN and SSN data at the application layer, since obtaining sensor information directly from the SSN proves troublesome and sending private BSN information via the SSN requires usage of SSN protocol and encryption and addressing towards the application.
- Encryption needs to be in place when BSN nodes send privacy-related information, else foreign objects can store and forward them.
- When nodes of different WSAN types move in each other's range, mobility is easier solved at the application layer, unless the WSANs are compatible. In the latter case, the moving WSAN can better turn off its gateway.
- WSAN protocols should be robust against foreign protocols, in order coexist with other WSANs in the same area.

## 6 Conclusions

This paper analysed scenarios in which different WSAN and application movements take place. Moving end-nodes between different WSANs are easily supported when the networks are compatible. When the encryption or protocol is different in the used WSANs, the end-nodes will need to support all of these encryption types. When compatible WSANs move in each other's range, the moving WSAN can better turn off its gateway and let the end-node directly communicate with the other WSAN. Irrespective of the WSAN type, data of overlapping WSANs can best be merged at the IP application layer instead of via each other. In order to support coexistence of WSANs in the same area, WSAN protocols should be robust against foreign protocol messaging. A way to automatically adapt the used wireless resources to be different from the other WSAN is advisable.

When privacy is required, as it is often the case in body sensor networks, encryption can best be accomplished by encrypting with the public key of the receiving gateway (or middleware), which can in turn sent it encrypted to one or more applications.

## References

1. M. Ali, T. Suleman, and Z. Uzmi. MMAC: a mobility-adaptive, collision-free mac protocol for wireless sensor networks. In *Performance, Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International*, pages 401 – 407, april 2005.
2. Ambient systems. ambient-systems.net, Last visited August 2011.
3. 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 *International Symposium on Wearable Computers 2010, Seoul, South Korea*, pages 143–150, USA, October 2010. IEEE Computer Society.
4. L. Evers, M. J. J. Bijl, M. 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, June 2005.
5. 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, pages 1–14, New York, NY, USA, 2009. ACM.
6. N. Meratnia, B. J. v. d. Zwaag, H. W. v. Dijk, D. Bijwaard, and P. J. Havinga. Sensor networks in the low lands. *Sensors*, 10(9):8504–8525, 2010.
7. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. Transmission of IPv6 packets over IEEE 802.15.4 networks. RFC 4944, Internet Engineering Task Force, Sept. 2007.
8. H. Pham and S. Jha. An adaptive mobility-aware mac protocol for sensor networks (MS-MAC). In *Mobile Ad-hoc and Sensor Systems, 2004 IEEE International Conference on*, pages 558 – 560, oct. 2004.
9. D. Zhang, Q. Li, X. Zhang, and X. Wang. DE-ASS: An adaptive mac algorithm based on mobility evaluation for wireless sensor networks. In *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, pages 1 –5, sept. 2010.