Communication Networks
University of Bremen
Prof. Dr. rer. nat. habil. C. Görg

Master Thesis

Opportunistic Routing in Multi-Sink Mobile Ad Hoc Wireless Sensor Networks

of

Artūras Lukošius
Matr.-no. 1966797

Bremen, September 26, 2007

Supervised by:
Prof. Dr. rer. nat. habil. Carmelita Görg
Dr.-Ing. Andreas Timm-Giel
Dipl.-Ing. Bernd-Ludwig Wenning

Ich versichere, daß die vorliegende Arbeit – bis auf die offizielle Betreuung durch den Lehrstuhl – ohne fremde Hilfe von mir durchgeführt wurde. Die verwendete Literatur ist im Literaturverzeichnis vollständig angegeben.

I certify that I have conducted this work on my own and no other supporting material has been used other than those which are listed as references.

Bremen, den 26. September 2007

(Artūras Lukošius)

PREFACE

"Communications without intelligence is noise; Intelligence without communications is irrelevant". - Gen Alfred Gray, USMC[1]

Today wireless communication becomes more and more popular. A large variety tending from Wireless Personal Area Networks (WPAN), with ranges from 10 meters to Wireless Regional Area Networks (WRAN), extending even up to 40 kilometres, and Satellite Communication, allow to build any specialized or general purpose network.

Dimensions of the communication elements become smaller and smaller every year. New integrated circuits technologies reduce power consumption drastically, at the same time providing high-speed computing power. With such equipment, many tasks, which were impossible to solve due to limitations of cost and low efficiency, became possible now.

Small size, light-weight devices are intentionally meant to be mobile. Mobility gives a lot of freedom, but necessarily involves a lot of complexity in the intelligent part.

One of the most important measures of the fast growing and developing world is energy. Energetic resources are limited. Power consumption must be as low as possible, thus necessarily requires optimization. Data routing algorithms must be adaptive and aware of contextual information. The redundant overhead should be minimized.

Wireless sensor networks are still under hard development. Many scientists and research companies worldwide compete with the limitations and try to provide efficient products to the market.

[1] "USMC: A Complete History (U.S. Military Series)". Jon T. Hoffman, Hugh Lauter Levin Associates, Inc. (September 2002)

ABSTRACT

This thesis introduces the opportunistic routing and analyses a new algorithm for Wireless Sensor Networks - a new routing technique for ad hoc mobile multi-hop wireless networks.

The routing algorithm is created based on a mobility scenario. The network consists of multiple nodes and multiple sinks. All of them are mobile. A source node generates data packets, which must be routed to the nearest sink. Sinks send high power periodic beacon packets. When nodes move, the received signal strength of the received beacon packet changes. Nodes calculate their mobility direction according to this difference of power levels. Then these beacons are forwarded to the neighbour nodes with normal power. Data packets are routed according to the obtained mobility information, such as mobility gradient, neighborhood availability. According to this knowledge, an efficient direction of data packet routing is predicted. Decision is done by every node which participates in the routing process. In other words, each node evaluates the opportunity of packet handling to the neighbour nodes.

The opportunistic routing algorithm is implemented and simulated in the OPNET simulator. The model is built on top of a partly implemented IEEE 802.15.4 model. Implementation of non-beacon, unslotted CSMA/CA medium access layer is part of this work.

The comparison of results is done with respect to the AODV routing protocol. An AODV model was implemented as hybrid structure of IEEE 802.15.4 MAC and AODV routing over IP.

The scope of the analysis is energy consumption, end-to-end delays and goodput of the opportunistic routing protocol.

Keywords: *ad hoc networking, AODV, evaluation, IEEE 802.15.4, mobility model, multiple sinks, OPNET, opportunistic routing, simulation, wireless sensor network.*

TABLE OF CONTENTS

CHAPTER 1

1. Introduction

A Wireless Sensor Network (WSN) is a network of wireless embedded system elements, which consists of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants at different locations [1]. WSNs belong to the Low-Rate Wireless Personal Area Network (LR-WPAN) type. Here, the word "personal" means short range communication. Every device in the network is called a sensor node. It includes the processing unit (micro controller), the radio unit (low-power transceiver) and the sensing unit (a board with sensors).

Nodes may communicate in ad-hoc way in order to extend the communication range and maintain network scalability. The main WSN limitations are battery capacity, bandwidth and computing power. Hence, packet routing techniques [2] must be applied to provide long-range and large-scale communication in WSNs.

Routing in ad-hoc networks selects the optimal path to send a message from a source to a sink. The shortest routing path does not always refer to an optimal routing. Plenty of routing algorithms are available today and each of them tries to solve the routing task, with different requirements and parameters. Most of the algorithms are valid in static networks or allow only a limited node mobility.

Network mobility and node mobility introduce a new challenge into the research area. The deployment of sensor nodes changes frequently and a routing algorithm must adapt to these conditions. It should take into account the information about the packet routing opportunity in each case. Opportunistic routing is aware of the communication context information. It adapts to the current conditions and predicts the future behaviour. In order to extend the maximum network lifetime, the context information must play the most important role.

This thesis introduces a new complex network structure with multiple mobile data sinks. Most routing algorithms are capable to work only with a single data sink, thus such algorithms are not suitable for a multi-sink scenario. Network mobility is exploited by the opportunistic routing algorithm as desired advantage. Intermittent connectivity of nodes means that nodes are in the communication range of each other only at certain periods of time. By exploiting mobility, it is possible to extend a virtual communication range by routing a packet to the node, which moves in the direction of the nearest sink. After some time, it will reach that sink and will route the transmitted packet.

The thesis is organized as follows. After introduction, the second chapter describes the main principles and challenges of the Wireless Sensor Network, gives an overview of available routing techniques and the main routing protocols.

In the third chapter, the IEEE 802.15.4 standard is presented. In this chapter some details about the Physical and the Medium Access Control (MAC) layers are shown. Operational modes of the IEEE 802.15.4 MAC are described in more detail.

The opportunistic routing is presented in the fourth chapter. This chapter provides the introduction to the opportunistic routing and existing opportunistic routing protocols. Because mobility is involved, two different random mobility models are also part of this thesis.

The main is the fifth chapter. The modelled opportunistic routing algorithm is presented and analysed in detail in this chapter. Both the detailed model structure and programming model are presented in the separate subchapters.

The sixth chapter covers the simulation procedure and the evaluation of simulation results of the previously described model. Also, the comparison of simulation results with some results achieved with the AODV routing algorithm is presented in this chapter.

Conclusions and outlook finalise this thesis report.

CHAPTER 2

2. Wireless Sensor Networks

Wireless Sensor Networks (WSN) are large scale networks of sensor nodes. The number of wirelessly communicating nodes can reach thousands of separate devices including sensoric equipment and data collection tools. The areas of application of WSNs are practically unlimited. The initial motivation for WSNs was battle field surveillance for military purposes. Now WSNs are applied for monitoring of the environment in local and wide areas in the context of temperature, humidity and other metrics. This provides a possibility to have precise statistical data about any changes during time. With a short duty cycle, wild and hardly reachable areas can be monitored for several years without a battery replacement. Environmental pollution reduction can be done with a help of adaptive traffic control, exploiting information about the highest amounts of pollutants in certain city areas during a day. WSNs are also applied in automative control, inventory tracking, surveillance, security, health monitoring and other civil tasks, etc.

The following properties, which describe WSNs, are:

- ad-hoc/coordinated communication,
- distributed organization,
- variable density,
- mobility of nodes, dynamic network topology,
- source-sink structure,
- intermittent connectivity, node failures,
- large area of network deployment.

A wireless sensor node is an element of a WSN, having such properties:

- small size,
- battery powered,
- low power consumption,
- low data rates,
- low cost,
- sensing/monitoring equipment,
- intelligent structure.

2.1 Principles

The principle of a Wireless Sensor Network is rather simple. An example of a deployed wireless sensor network is shown in Figure 2.1. Usually, the number of sensor nodes is large. Nodes have limited communication range, thus simultaneous transmissions are possible. Due to limited transmitter range, a message must be forwarded in multiple hops in order to reach the remote sink node, which is separated by a long distance from the originating source node. When all nodes are stationary, messages are routed easily as routes are also static. The only limitations in this case are interference of simultaneous transmissions, noise and collisions of packets if limited energy is not accounted.

In case of a monitoring scenario, all sensed data from one or several source nodes is sent periodically to a single sink or, in more complex scenarios, to multiple sinks. Data aggregation can be done in order to reduce traffic and power consumption. Monitoring applications do not require large amounts of data to be transmitted. When a source node sends a message containing sensed information, it must propagate through the network towards the best sink node by hopping from node to node. This hopping procedure is managed by routing protocols. Some of them are described in detail later in this chapter.

Nodes can communicate in ad hoc way or can be controlled by network coordinator. For large-scale, widely deployed networks, ad hoc interconnection mode is more affordable, because the construction of a large wireless sensor network can be simplified by self-organization and self-configuration methods.

A wireless network can be realized in the real world by specialized hardware. WSN hardware has an embedded hardware structure. In Figure 2.2, the structural diagram of a wireless sensor node is shown. A controlling element of a wireless sensor is the Micro Controller Unit (MCU). Strict requirements for it are short wake-up time, low power consumption, high computing speed. The MCU includes Flash and SRAM memory, needed for special purposes; also required interfaces, such as USB, SPI, RS232. The most popular micro controllers are produced by Texas Instruments, Intel, Atmel, Microchip, Philips. An embedded operating system and other implemented software is written into the MCU flash memory. The MCU controls the connected transceiver and provides an arbitration for analog and digital sensors.

The next important part is the RF transceiver (including the antenna). It is controlled by the MCU. Wireless sensor networks are described in the IEEE 802.15.4 standard, hence the transceiver hardware must follow the rules covered by this standard. RF transceivers, produced by Chipcon, are widely used in the development and evaluation

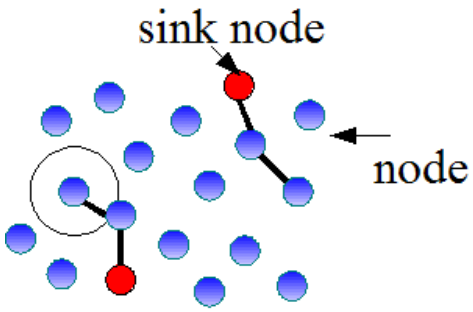

Figure 2.1: Example of an ad hoc wireless sensor network

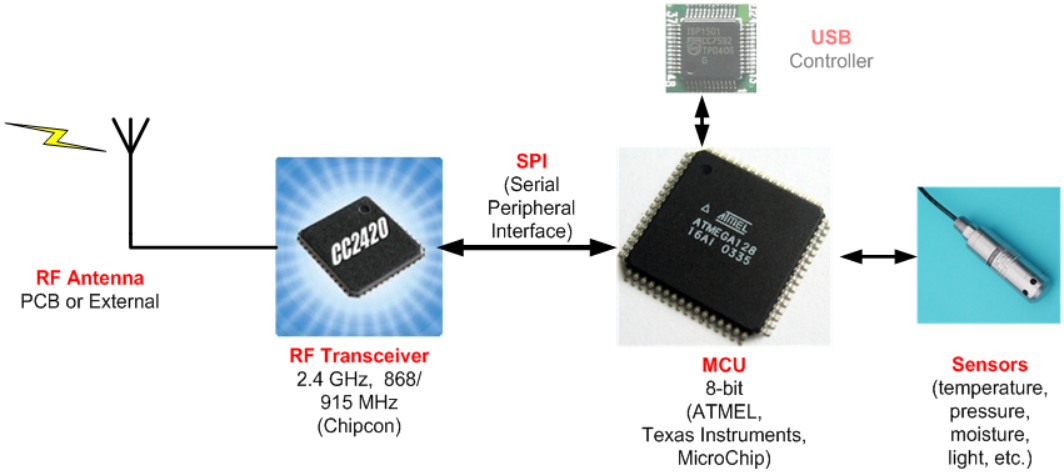

Figure 2.2: Hardware structure of a wireless sensor node

boards. Low power consumption is one of the main requirements for transceivers, because the largest amount of energy is spent for radio transmission and reception.

The low power consumption requirement can be met with the help of routing protocols. A routing scheme type depends on the scenario in which it is used. Efficient power consumption is always the main task. The total number of required transmissions to send one data packet from a source to a sink must be minimized.

2.2 Challenges and Requirements

The main requirements for Wireless Sensor Networks are low power consumption, long network lifetime, low data rates, in-network stability, mobility tolerance, scalability, etc.

Routing algorithms must overcome some requirements called routing challenges [2]. The main challenges are:

- energy consumption,
- node deployment,
- data reporting method,
- sensor/link heterogeneity,
- fault tolerance,
- scalability,
- mobility,
- quality of service (QoS).

Wireless sensor networks consist of a huge number of sensor nodes. Mainly all of them are battery powered. Routing algorithms should always be power aware because sensor network lifetime is equal to sensor node lifetime, i.e. when the first node in a network dies, the network can be considered as dead.

Manual node deployment is difficult when the number of nodes increases noticeably but, in this case predefined routing paths are possible. Random deployment is less costly, nodes form an ad-hoc infrastructure. But this increases the complexity of routing algorithms.

The data reporting method can be variable. Time, event, query or hybrid driven reporting is possible. In sensor networks, sensor nodes can operate as nodes, cluster heads, base stations, etc. It means, a sensor node must be heterogeneous. This can be achieved by involving various routing techniques. Interference, power lack, error and physical damage always threatens sensor nodes. Fault tolerance must always be taken into account. Number of active nodes in a network is variable. A high number of active nodes can cause infinite queues. Mobility tolerance in target detection and tracking as well as adaptive routing techniques are needed. Quality of service requires limited delays. All these challenges place routing on the sharp edge.

The following points summarize the requirements for routing in wireless sensor networks:

- low power consumption,
- maximum network lifetime,
- low data rates,
- in-network stability,
- mobility tolerance.

The routing protocol is a critical issue. Each sensor must exploit available information from the surrounding nodes and context of the transmitted information itself. Different adaptive routing algorithms which exploit context information are available. Context awareness and opportunistic routing belong to the advanced adaptive routing type. Advantages can be discovered in mobile networks where the topology changes frequently and where nodes can have intermittent connectivity.

2.3 Available Techniques

Wireless sensor networks are one the most active developement branches today. As mentioned before, wireless hardware of the WSN elements and requirements for the specalized software is standardized.

ZigBee™ [3] is a closed-source specification for wireless connectivity, focusing on standardizing and enabling interoperability of products within home control, building automation and industrial control and monitoring. The ZigBee™ Alliance is an association of companies working together to enable reliable, cost-effective, low-power, wireless connected, monitoring and control products, based on an open, global standard. Today there are over 150 companies participating in the ZigBee Alliance: Texas Instruments, Motorola, Philips, Samsung, ATMEL, Analog Devices, etc.

All Alliance companies are working on development of ZigBee™ hardware (low power micro controllers and transceivers, micro controllers with integrated transceivers). Additionally, gateway products are in discussion to link ZigBee™ with existing home, building automation, and industrial WLAN/WPAN networks.

The ZigBee™ stack has a structure similar to the standard ISO/OSI model. The company Figure8Wireless (bought by Chipcon in 2005) has developed the ZigBee™ Z-Stack solution, targeting ZigBee™ Alliance standards. Z-Stack occupies the layers from Network to Application. The lower ones belong to the IEEE 802.15.4 standard, which is described in detail in the next chapter.

TinyOS [4] is an open-source operating system, designed for wireless embedded sensor networks. Its component-based architecture supports the concurrency intensive operations required by networked sensors with minimal hardware requirements.

TinyOS has a big advantage over ZigBee™: TinyOS is fully available for every user, hundreds of contributed projects are included. TinyOS is platform independent software. The programming language used in TinyOS is stylized C (NesC). Implementation code can be simulated on a PC in a TinyOS simulator, written in Java. Telos, Tmote Sky, Mica, Mica2, MicaZ and other platforms are supported by TinyOS.

2.4 Routing Protocols

Routing protocols [5] are specific routing algorithms with properties used in different routing topology classes, such as flat, hierarchical and location-based routing. Some features of the best known routing algorithms are shown in Table 2.1. This table describes each routing protocol in power, mobility, position, negotiation and information aspects. These aspects can be accepted as context measures. If a context attribute is included into the protocol, this protocol is context-aware.

Context awareness is a process where context information is treated with evaluation of a feature called context attribute. Context can be divided into these groups of awareness:

- power/energy,
- mobility,
- information,
- privacy,
- quality of service (QoS).

Ad hoc routing protocols can be divided into reactive, proactive, hybrid, hierarchical, geographical, power aware, multicast, geocast and other routing types. The simpliest the most popular are reactive and proactive routing types. Reactive routing discovers route on demand, proactive maintains the route tables periodically even when there are no pending messages to send. An example of simple reactive routing is shown in Figure 2.3. First, flooding of route requests is performed. Routes are formed from these requests and replies. Then data messages are routed to the destination following the built path. Ad Hoc On Demand Distance Vector Routing Protocol (AODV), Multipath

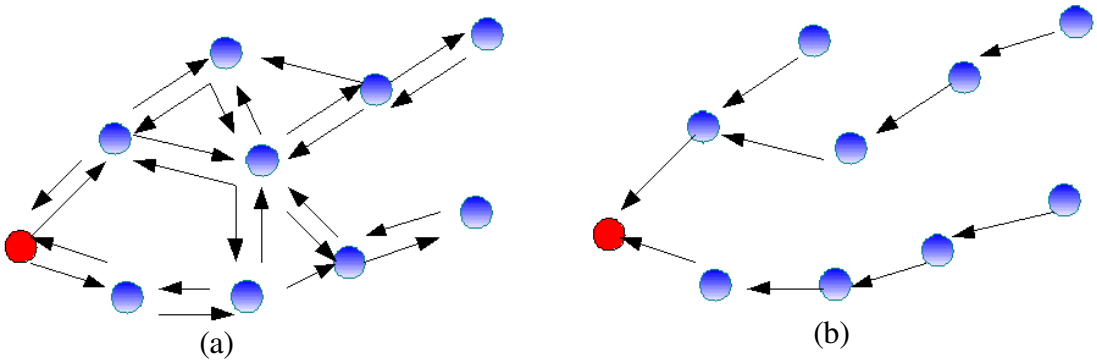

Figure 2.3: Example of reactive routing

	Class	Power usage	Mobility	Position	Negotiation	Information
SPIN	Flat	Ltd.	Possible	No	Yes	Yes
Directed Diffusion	Flat	Ltd.	Ltd.	No	Yes	Yes
GBR	Flat	N/A	Ltd.	No	No	Yes
LEACH	Hierarchical	Max.	Fixed BS	No	Yes	Yes
TTDD	Hierarchical	Ltd.	Yes	Yes	No	No
GEAR	Location	Ltd.	Ltd.	No	No	No
GOAFR	Location	N/A	No	No	No	No
SPEED	QoS	N/A	No	No	No	No

Table 2.1: Routing protocols

On-demand Routing Protocol (MOR) and Temporally-Ordered Routing Algorithm routing protocol (TORA) belong to the group of reactive routing protocols. Hierarchical State Routing protocol (HSR) and Optimized Link State Routing Protocol (OLSR) belong to the proactive routing type. There are too many available routing protocols to be listed here. The best resources are decribed in [5], [6] and [7].

The Sensor Protocol for Information via Negotiation (SPIN) [5][2] is shown first in Table 2.1. It belongs to the flat routing type. Sensor nodes disseminate information from node to node and each node is a potential Base Station (BS). This allows fast query of data from any sensor node. Assuming a region, where a number of nodes can have similar data which are not necessary to transmit. The nodes instead use so called meta-data to identify the main data to be sent. Hence, only advertisements of data are sent over the network and can be requested by the BS. This allows less redundancy. Queries can be time driven. Advertisement and request are repeated in some periods of time. A BS can also initiate a transmission. SPIN is an adaptive routing protocol as it can adapt energy consumption by remaining energy level indicators (energy awareness).

The SPIN family includes a lot of protocols. The main versions are SPIN-1 and SPIN-2. SPIN-1 is a three step protocol using three types of sensor messages: data advertisement of new data (ADV), data request (REQ) and transmission of requested data (DATA).

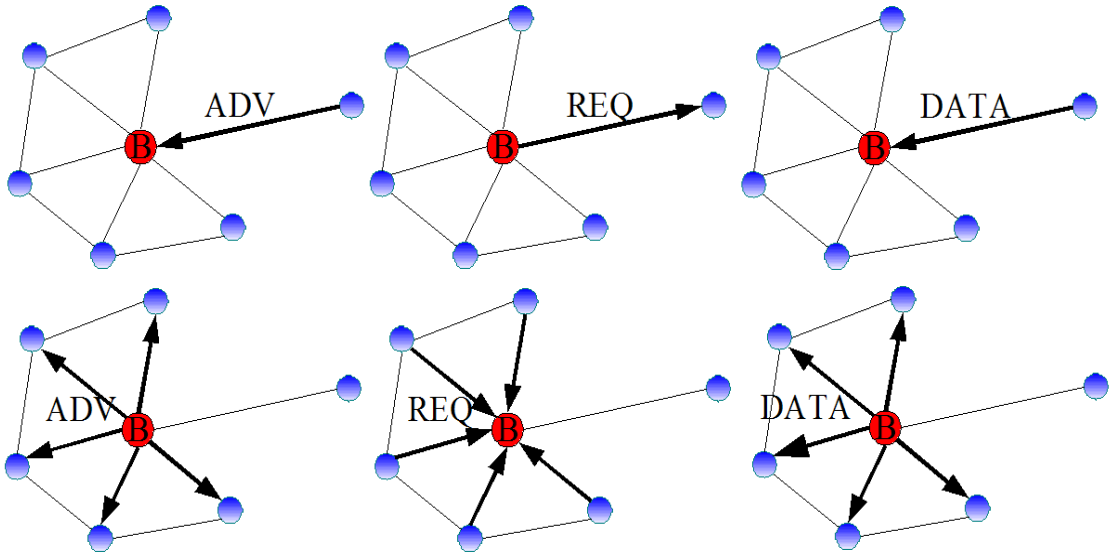

Figure 2.4: SPIN algorithm

The procedure is shown in Figure 2.4. A sensor node advertises new data by an ADV packet to the BS. The base station indicates the data as important and sends a data request REQ. Then the BS advertises new data to all surrounding nodes by ADV. Again the advertised data contains important information and is requested by all neighbor nodes which is not necessarily the case and data transmission is initiated (DATA). SPIN-2 is the same as SPIN-1 except for an energy threshold that is included. A node indicates its participation in conversation if the personal energy level is not lower than a low energy threshold. It participates only in case when all three steps ADV, REQ and DATA energy consumption will not decrease below the given energy threshold.

Classical flooding of sensor data from overlapping areas causes redundancy which is called implosion and energy wasting. The SPIN protocol allows mobility as neighbor nodes make local decisions and adapt the behavior to current context information. Advantages of the SPIN protocol are energy saving, possible mobility and no implosion, because data redundancy is eliminated in a query-driven fashion. Data from overlapping areas are processed by negotiation. The main disadvantage of SPIN is that this algorithm has no guarantee of data delivery.

The Directed Diffusion Routing Protocol also belongs to the flat routing type. It has similar context properties as SPIN. Only the elimination of redundancy is made by data aggregation. Similar data is grouped (in-network aggregation), which minimizes the amount of transmitted messages. Directed diffusion is an application-aware protocol. The BS indicates interest of data and the nodes make a gradient of information. The interest diffuses hop-by-hop in a network and is sent back when the interest coincides with available data. The gradient strength can be different in the different sectors of sensor nodes. Different from SPIN, data communication is done node by node where each node has the capability to perform data aggregation. Hence, there is no necessity to make a spanning tree of routing paths. This could be problematic in environment monitoring as it requires continuous transmissions to the BS.

The Gradient Based Routing (GBR) protocol [2] is similar to directed diffusion except that the number of hops from the BS is memorized as the interest propagates. Then, the packet is sent to the link with least number of hops (largest gradient).

In the hierarchical routing, sensor nodes with the most energy are exposed as Cluster Heads (CLH). They act as routers of information between clusters and inside a cluster. A cluster head performs data aggregation, multi-hop routing, channel allocation, etc. Hierarchical routing protocols are energy efficient protocols in sensor networks where energy consumption of sensor nodes is not uniform. The Low Energy Adaptive Clustering Hierarchy (LEACH) and the Two-Tier Data Dissemination (TTDD) protocols belong to this type of routing. LEACH uses cluster heads to control cluster operation. The cluster head is fixed and switched to another sensor node when power dissipates. The TTDD base stations can be mobile and data is delivered between the BSs. Sensor nodes are assumed to be stationary and location-aware.

Location based routing exploits node locations. The distance between neighbors is estimated by the Received Signal Strength Indicator (RSSI). Information about the node location is exchanged. The Geographic and Energy Aware Routing (GEAR) uses a similar functionality as directed diffusion, only the diffusion gradient is limited according to the routing zones specified by node locations. Interest can only be sent into regions that are needed. Most of the location based routing algorithms exploit the location data and other context attributes are not used.

One of the routing protocols, not listed in the Table 2.1, is the Sensor Context Aware Routing (SCAR) protocol, which exploits movement and resource prediction techniques to smartly forward data towards the right direction at any point in time [8]. SCAR uses a probabilistic approach (prediction theory). This approach also can be named adaptive routing. Mobile neighbor nodes can be the best carriers to forward information to the sink. The probability of jumping to one of these mobile neighbors is predicted. Nodes exchange mobility, collocation with sinks, battery level and rate of connectivity. All these context attributes are set into the goal function. Nodes calculate the probability of data delivery and exchange this information. Multiple neighbor nodes can be chosen as carriers. The source node sets up a list of neighbors with decreasing order according to the probability of delivery (jumping). A replica is sent to the node with the highest probability. Messages from neighbors are buffered. The choice of the best carrier is done with the best neighbor to reach the sink. Context information is exchanged between nodes (node ID, probability of delivery and available slots in a buffer).

The opportunistic routing type is used in this work. It is an advanced version of the geographical routing type. Due to its high importance, it is described in detail in Chapter 4.

CHAPTER 3

3. Overview of the IEEE 802.15.4 Standard

IEEE 802.15.4 [9] is a simple packet data protocol designed for lightweight wireless networks. Its architecture representation is shown in Figure 3.1. This standard was not developed specially for Wireless Sensor Networks (WSN), but still can be used with WSNs because the main requirements are related. Low power consumption, low cost, low data rate are typical requirements for WSNs. The IEEE 802.15.4 protocol describes physical and Medium Access Control (MAC) layers. It is closely related with the ZigBee (see Chapter 2.3) standard. The ZigBee Specification was released in 2004, which is publicly available and describes upper network and application layers.

Wireless channel access is controlled by MAC via Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and optional time slotting. Communication between sensor nodes is performed with message Acknowledgment (ACK) and an optional beacon structure. Beacon-enabled and non-beacon operational modes are possible with the use of slotted and unslotted CSMA/CA accordingly. These two modes are described in details in the following subchapters. Multi-level security with 32-bit or 64-bit encryption can ensure security of data communication.

The IEEE 802.15.4 standard's main advantages are long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics. Configured for maximum battery life, it has the potential to last as long as the shelf life of most

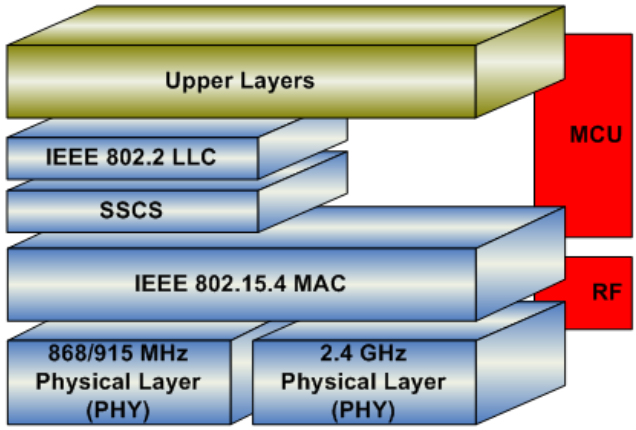

Figure 3.1: IEEE 802.15.4 architecture

batteries. This is very important if a large number of node devices is used, where a frequent changing and recharging of batteries is impractical. Depending on the power consumption allowance, a transmission range can reach from 30 up to 100 meters and even more.

The architecture layers reach and include Logical Link Control (LLC). LLC is standardized in 802.2. LLC connects the MAC layer with upper layers through SSCS (similarly to data link layer). Sometimes LLC is not used as separate layer, only some functions of LLC are implemented in software and are arbitrated by upper layers.

IEEE 802.15.4 supports multiple network topologies including Star, Cluster Tree and Mesh types. The PHY layer contains an RF Transceiver, operating with one of the specified frequency bands. The MAC layer provides access to the physical channel. Two modes of MAC operation are predefined in this standard: beacon-enabled and non-beacon enabled mode. Normally, PHY and MAC are part of a transceiver, only control and data interchange are in responsibility of software in the MCU.

The main topics from this standard are described in detail in the following subchapters.

3.1 Network Topologies

Depending on the application requirements, the WPAN may operate in one of three topologies:

- the star topology,
- the peer-to-peer topology,
- cluster tree topology.

The former two are shown in Figure 3.2. In the star topology, the communication is established between end devices and a single central controller, which is called the Personal Area Network (PAN) coordinator. A PAN coordinator can be used to start, stop

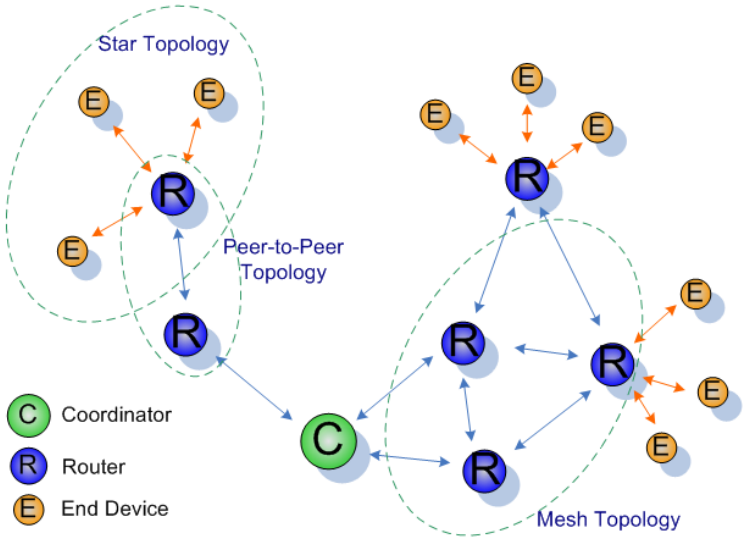

Figure 3.2: Star and peer-to-peer network topologies

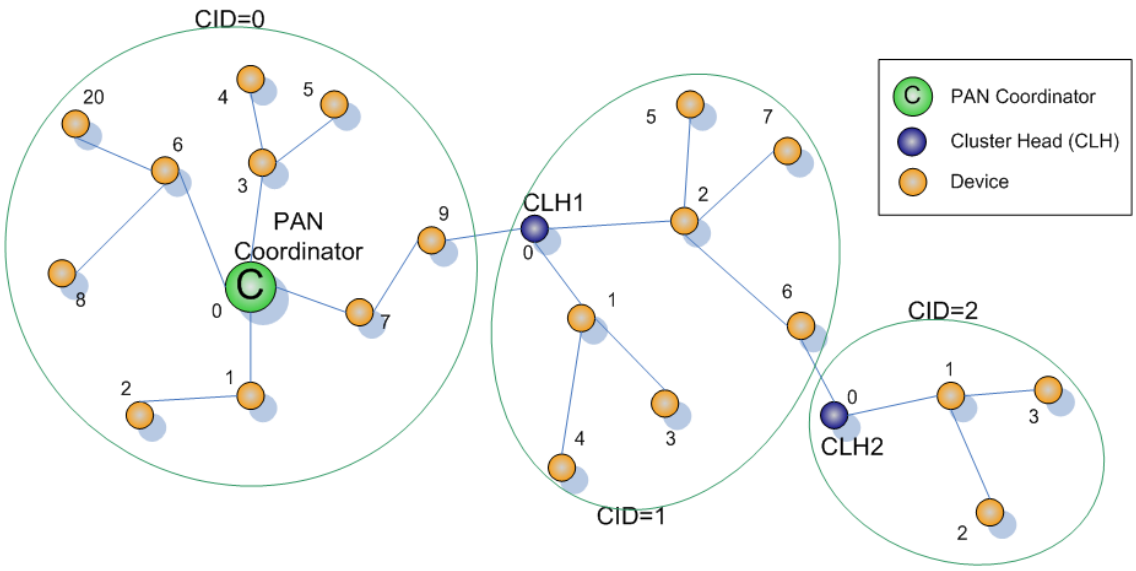

Figure 3.3: Cluster-tree network topology

or route communication in the network. According to the IEEE standard, two types of devices are supported by LR-WPAN: Full Function Device (FFD) and Reduced Function Device (RFD). A FFD can be a PAN coordinator, a router or a simple device. It supports the full set of special functions and the full protocol stack. Routing and coordination tasks are performed by the FFD. RFDs have limited functionality and basically are simple. The main tasks of RFDs include sensing and data transmission of monitored information to the prescribed FFD. All devices operating on a network of any topology have 64-bit extended addresses, which are unique for every device. This address is used for direct communication inside the PAN, or short 16-bit addresses can be assigned by the PAN coordinator during device association with the PAN. The PAN coordinator is the primary controller of the PAN, which can be mains or battery powered. Other devices are preferred to be battery powered. Applications that benefit from a star topology are home automation, personal computer peripherals, toys and games and personal health care.

The peer-to-peer topology also includes the PAN Coordinator or router. However, it is different from the star topology. The difference is that devices can communicate directly as long as they are in communication range of each other. The peer-to-peer topology allows more complex network formation, such as mesh networking. Application of peer-to-peer topology is done in the areas of industrial control and monitoring, logistics, tracking, intelligent agriculture and security applications. A peer-to-peer network can be ad hoc and self-organizing. The network structure allows multiple hops from any device to any other device on the network for message routing. Routing is not the part of the IEEE 802.15.4 standard.

An example of the use of the peer-to-peer communications topology is the cluster-tree network topology, shown in Figure 3.3. The cluster-tree network is a special case of a peer-to-peer network. Most of devices are FFD. An RFD may connect to a cluster-tree network as a leaf node at the end of a branch. It may be associated with only one FFD at a time. The first FFD, that appears in the network, is elected as the PAN coordinator and provides synchronization services to other devices or other coordinators (cluster heads). The PAN coordinator is a Cluster Head (CLH) labeled as CLH0 and forms the first

cluster with a Cluster Identifier (CID) equal to zero - CID0. Clusters are interconnected by a leaf nodes that appear at the cluster edge. This node must be FFD or at least must support packet relay functions. The IEEE 802.15.4 standard does not define how cluster-tree networks are constructed. The network layer in the ZigBee Specification uses primitives provided by the IEEE 802.15.4 standard to construct cluster-tree networks.

3.2 The IEEE 802.15.4 Physical Layer

PHY is the first layer in the IEEE 802.15.4 stack. It communicates over transmission media using 3 bands, which are divided into 27 channels. One band has a worldwide allowed carrier frequency of 2.4 GHz, 16 channels, 250 kbps bitrate with O-QPSK signal modulation. In the United States, a second band with 868.3 MHz carrier frequency is used: 1 channel, 20 kbps bitrate with BPSK modulation and a third one is used in Europe, 902-928 MHz: 10 channels, 40 kbps bitrate with BPSK modulation. Hardware designers should be aware of this when selecting the right band.

The physical layer has the special purpose to perform channel analysis and to transmit/receive packets. It activates and deactivates the radio transceiver. A wireless sensor node can enter a sleep mode if the beacon-enabled mode is active. This will save energy, but a strict synchronization and coordination scheme must be applied in this case. In non-beacon enabled mode, a sleep mode control is even complex and must be managed by advanced power control algorithms in the MAC layer. Energy Detection (ED) of the channel and the Link Quality Indication (LQI) for received packets are common tasks of the PHY layer. The Clear Channel Assessment (CCA) is a technique for CSMA/CA that ensures an idle channel at the start of data transmission. Channel frequency band selection is also defined in the physical layer part. Acknowledged and unacknowledged data transmission and reception is performed according to specifications in IEEE 802.15.4.

An example of the 2.4 GHz frequency band, divided into 16 channels is shown in Figure 3.4. Every channel frequency sub-band is calculated according to the formula which is given in [9]:

$$Fc = 2405 + 5\,(k - 11) \text{ in MHz, for } k = 11, 12, ..., 26 \qquad (3.1)$$

WLAN and Bluetooth standards have similar physical channel structure. But there is no possibility of connection between ZigBee and WLAN (IEEE 802.11) or Bluetooth (IEEE 802.15.1) due to different specifications covered in the standards. For this reason it is necessary to use gateways in order to backbone the different networks together.

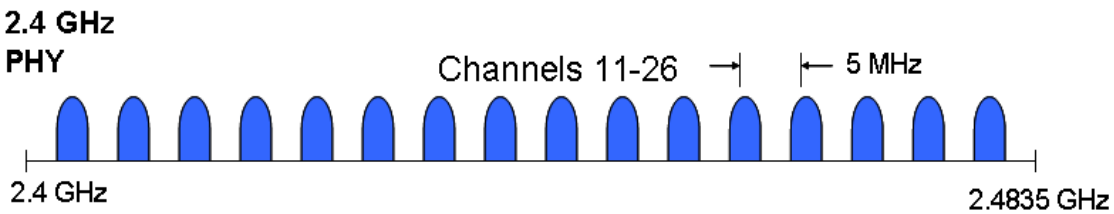

Figure 3.4: 2.4GHz wireless band channels

3.3 The IEEE 802.15.4 Medium Access Layer

Medium Access Layer (MAC) is the second layer in the IEEE 802.15.4 protocol stack. This layer provides an interface between the physical layer and upper layers. MAC is similar to that of IEEE 802.11. It employs CSMA/CA channel access protocol, has contention free and contention access periods. RTS/CTS is disabled in order to reduce collisions. MAC can operate in two modes: beacon-enabled mode and non-beacon enabled mode. MAC addresses can have a length of 64 bits, which allows a network size up to 2^{64} nodes and short 16-bit addresses for local addressing.

As written in IEEE 802.15.4, the medium access layer perform the following tasks:

- beacon generation if the device is the PAN Coordinator,
- synchronization to these beacons,
- association and dissociation from the network,
- device security,
- CSMA/CA channel access control,
- Handling of Guaranteed Time Slot (GTS) mechanism,
- control between peer-to-peer MAC entities.

Frames supported by MAC are: Data, ACK, Beacon and MAC Command frames. All frames are used for reliable communication. Reliable delivery of data is ensured by using ACK frames. Acknowledgements are transmitted to every received packet which has set the acknowledgement request flag as enabled. In IEEE 802.3, acknowledgements are performed by TCP layer. All addresses of network participants are held in the Coordinator memory. The Advanced Encryption Standard (AES-128) can be used to ensure the security of transmitted data and control packets. Data encryption consumes lot of processing power, hence different levels of encryption complexity must be used.

Transmission of two consecutive frames is separated by an Inter Frame Spacing (IFS) period (see Figure 3.5 [9]). The MAC layer requires some amount of time to process data received from a physical layer. If a transmitting frame requires acknowledgement, IFS will follow the ACK frame. The length of IFS depends on the transmitted frame length. If it is a long frame, Long IFS (LIFS) follows the ACK frame in case of acknowledged transmission and Short IFS (SIFS) in case of a short transmitted frame. LIFS and SIFS are used without t_{ack} in unacknowledged transmission. Slotted CSMA must take it into account for all transmissions in a Contention Access Period (CAP).

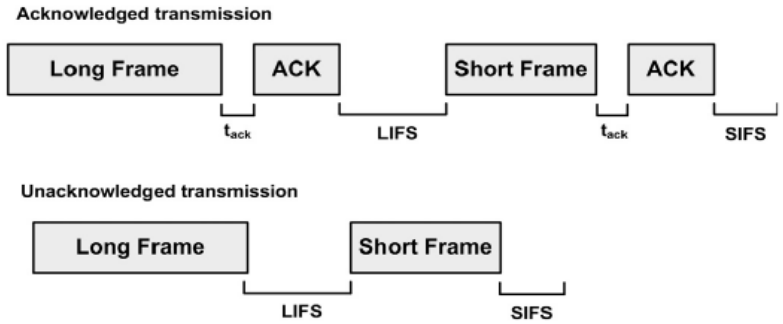

Figure 3.5: Inter Frame Spacing (IFS)

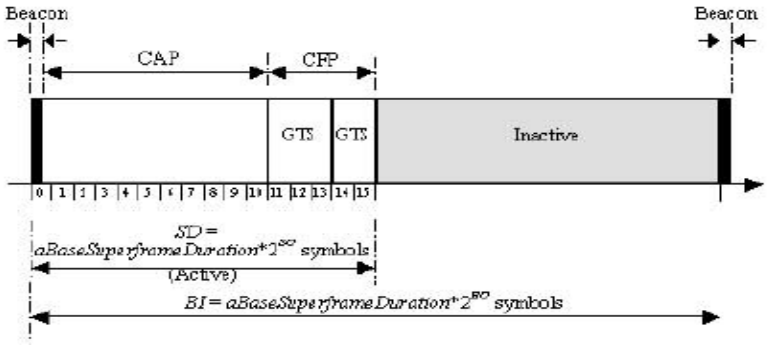

Figure 3.6: Superframe structure

3.3.1 Beacon-Enabled Mode and Slotted CSMA/CA

The IEEE 802.15.4 beacon-enabled mode exploits a superframe structure. All devices in the network must follow the rules of this superframe in order to communicate reliably. Devices must be associated with the PAN Coordinator. The PAN Coordinator sends periodic beacon frames, containing information about superframe parameters, which define active and inactive periods.

The Superframe structure is shown in Figure 3.6 [9]. The active period is divided into 16 equal time slots, followed by an inactive perdiod. There are two types of superframes, with and without Guaranteed Time Slot (GTS). GTS is located in the Contention Free Period (CFP). The PAN Coordinator can define up to 7 GTS frames in one superframe. A CFP is defined when QoS is necessary to be supported. GTS slots have the purpose for low latency applications or when a specific bandwidth must be guaranteed. During inactive periods no transmissions are allowed, hence all of them must be finished before the start of this period, if the inactive period is defined in the superframe structure. The superframe starts with a beacon frame and finishes before the next following beacon. The duration is called Beacon Interval (BI).

Communication can be restricted by the PAN Coordinator, so that only during CAP, devices are allowed to transmit messages. Then every device must compete among the others according to the Slotted CSMA/CA.

The slotted CSMA/CA mechanism (see Figure 3.7) is used only in the beacon-enabled mode. CSMA/CA is based on a backoff period which is a random waiting time before a packet can be transmitted to the radio channel. In the beacon-enabled mode, access to the channel can be done only at the boundaries of these backoff periods. And these boundaries must be aligned with the superframe slot boundaries. This is done because superframe slot boundaries are interdependent with each other.

Slotted CSMA/CA has three main scheduling parameters. The Number of Backoffs (NB) is the number of backoffs until the device can access the radio channel. The Backoff Exponent (BE) is the number of waiting periods before the channel can be accessed. The Contention Window (CW) is the number of backoff periods that is necessary to wait until transmission is allowed. Initially, this value is set to 2 and decreased by 1 each time when a backoff period expires. If the channel was busy during channel access, this value is reset back to 2.

The slotted version of CSMA/CA algorithm starts with an initialization of scheduling variables. If the battery extension is enabled, then BE is set to the minimum value of 2 and the *macMinBE.* Otherwise BE is set to the *macMinBE.*

Then the algorithm locates a backoff period boundary and starts a random delay to avoid collisions. The delay is chosen randomly from 0 to $2^{BE} - 1$ backoff units. Clear Channel Assessment (CCA) is performed on the backoff period boundary just after the expiration of the backoff period. If the accessed channel is free, then CW is reduced by one and this procedure is repeated until CW = 0. If at this point the channel is still idle, the transmission of the waiting packet starts immediately. If during this cycle the channel in one of the CW periods was busy, CW is reset back to 2, NB is increased by 1

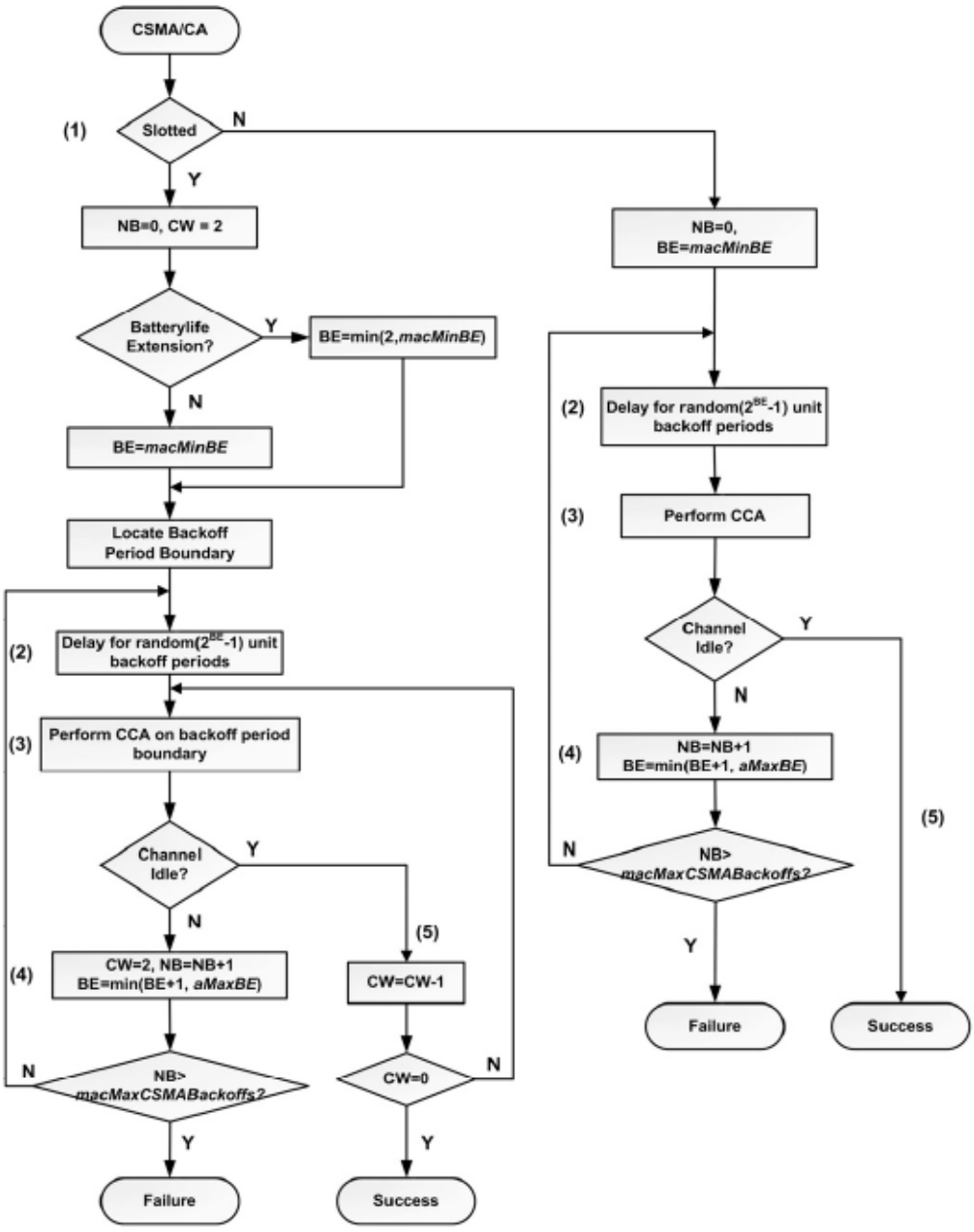

Figure 3.7: CSMA/CA algorithm

and BE is selected as minimum of BE + 1 and the maximum number of the Backoff Exponent. If NB does not exceed *macMaxCSMABackoffs* value, cycle 2-4 is repeated, otherwise it is indicated as a failure. When a failure occurs, MAC layer drops the current packet and may indicate this to the upper layers as link failure.

3.3.2 Non-Beacon Enabled Mode and Unslotted CSMA/CA

In the previous chapter the beacon-enabled mode was defined. The other type without beacons and without superframes is called non-beacon enabled mode (see Figure 3.7 [9]). This is the simplified version of MAC protocol which even allows the ad hoc structure without the PAN coordinator. With PAN Coordinator, devices must poll the PAN Coordinator for pending data.

All data transmissions in this mode are carried with the Unslotted CSMA/CA. Only the ACK frames are sent without this mechanism.

The right side of Figure 3.7 shows the structure of the Unslotted CSMA/CA algorithm. CW value is not used in this case. After variable initialization, the random backoff delay is started without alignment to the backoff boundaries. This is simply because it is not used. After this delay period, the CCA is performed. In the step 3, the channel is checked immediately for idleness. If the channel is found to be idle, an immediate transmission of a packet is started, otherwise the cycle is repeated in similar way to that of the Slotted CSMA/CA.

Acknowledgments are handled differently in beacon and non-beacon mode. In the non-beacon-enabled mode, an ACK must be transmitted in 192 μs after receiving the last byte of a valid frame demanding an ACK.

This mode of IEEE 802.15.4 MAC operation is chosen for this master thesis, because ad hoc node communication is affordable. The main advantages of this mode are simple implementation, no complex coordination, scalability of the network and independent communication.

CHAPTER 4

4. Opportunistic Routing in Wireless Sensor Networks

Many routing protocols were proposed for the packet routing in Wireless Sensor Networks. Most of them try to search a single path for the whole time. In mobile networks, the topology of nodes changes frequently and there could be several or even no available routes. If the communication coverage is small enough, an intermittent connectivity between sensor nodes exists. Mobile neighbor nodes can be exploited as opportunistic elements for packet forwarding. Node mobility is the key to the extension of the communication range between nodes.

This chapter presents the opportunistic routing, the new technique for wireless sensor networks. First the definition of the opportunistic routing is presented and the influence of the spatial diversity for the opportunistic routing is analyzed. Several opportunistic routing protocols and mobility models are described in the last subchapters.

4.1 Definition

Opportunistic routing exploits a redundancy of nodes to transmit a packet to nodes that are available for routing. It is based on the idea of geographic routing. Opportunistic routing still exploits location information, but the forwarding node is elected differently, according to the protocol which is used in each case.

The advantages of opportunistic routing appear in denser networks, where the number of potencial forwarding nodes is larger. This provides a high neighborhood cardinality. In order to have an efficient routing algorithm it is necessary to use cross-layering by integrating MAC and network layers. The netwrork layer sets up a list of available candidate nodes and sends it to the MAC layer. The final decision is made in the MAC layer according to the node connectivity, channel conditions, reliability, etc. Optimal transmission can be done only when the conditions are favorable.

Opportunistic routing is powerful and well-suited to Wireless Sensor Networks, where nodes have intermittent connectivity and the availability of neighbor nodes for packet forwarding is disrupted. Promiscuous opportunistic routing algorithms can negate its advantages in dense networks. This is because the adaptation of a MAC layer to the neighborhood availability can increase energy costs even more than that of a geographical routing with repeated transmissions. Opportunistic routing algorithms should exploit proactive collection of information about their surrounding neighborhood. In any case it is necessary to analyze the performance and behavior of

opportunistic routing algorithms to realize, under which conditions each of them makes sense.

4.2 Spatial diversity

Routing techniques can help to reduce power consumption. Traditional routing algorithms exploit only a single path. Examples are geographic routing and AODV. Disadvantages of this type of routing are a susceptibility to node failures, hot routing spots and bottlenecks at the cross paths of different routes. These algorithms are simple and easy to implement.

Multi-path routing is more complex. Probabilistic routing and diffusion protocols belong to this type. Multiple paths allow to increase the global network lifetime, because the traffic load is distributed through a network according to the fading channel conditions. Due to a fast changing channel it is necessary to supply rights for channel arbitration to the MAC layer. Routing is performed at this level according to the specified forwarding region provided by the NET layer.

The transmission range of a wireless sensor node in 2D analysis is approximated as a perfect circle with a radius proportional to the transmit power. In 3D it is a sphere, which has perfect omni-directional propagation of a radio signal. However, real antennas are non-perfect and the radiation of a radio signal is not equal in all directions.

The MAC layer can exploit the spatial diversity, when it specifies the forwarding

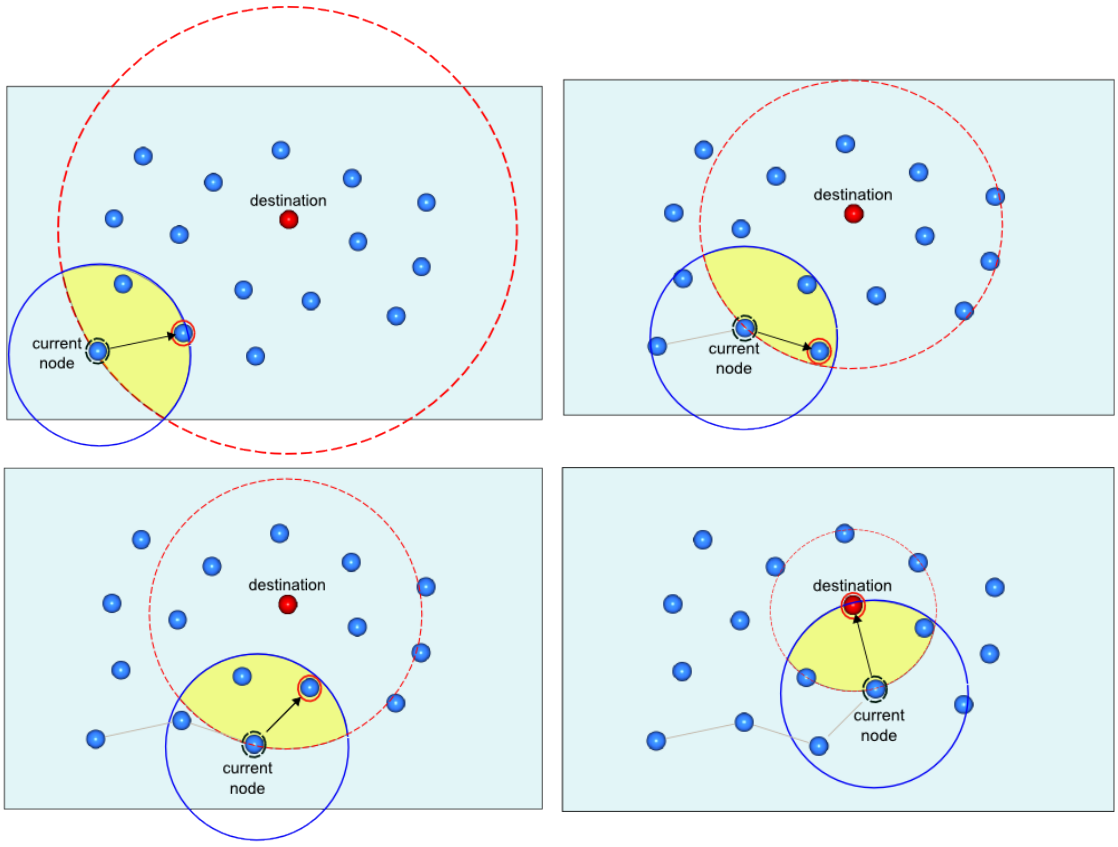

Figure 4.1: Spatial diversity in WSNs

region, containing neighbor nodes which are closer to the destination, instead of simple flooding or broadcasting of a packet to all surrounding neighbors. The receiving neighbor nodes are included in the MAC packet header.

An example, exploiting this spatial diversity, is shown in Figure 4.1 [10]. Nodes know their locations and the location of the destination. The source node initiates the transmission of a data packet to the destination. The forwarding region is elected according to the geographic information of node locations and the transmission range. The optimal forwarding region is the lens of nodes that appear in the intersection area of the source node transmission range and the circle, having a radius length equal to the separating distance between source and destination nodes.

When the Network layer selects a forwarding region containing nodes that appear in that area, it sends the list of node addresses to the MAC layer. The MAC layer selects the next forwarding node by the availability information, which is obtained according to the past behavior of a neighbor node and so on. Then the packet is routed to the elected candidate node and this node becomes the current node, which must repeat the same procedure. This cycle is repeated until the destination receives the data packet. If a candidate node cannot receive a packet due to unfavorable conditions, the new candidate is elected. If a packet is stuck at some node, this packet is dropped.

This proposal of the spatial diversity in wireless sensor networks is exploited by different opportunistic routing protocols. The next subchapter overviews some of them in detail.

4.3 Opportunistic Routing Protocols

This chapter presents the most famous opportunistic routing algorithms for wireless networks. Not all of them are suitable for WSNs, although they can be applied.

The Extremely Opportunistic Routing (ExOR) protocol exploits wireless networking advantages. It predicts the most useful forwarder by ranking forwarding nodes by number of hops. ExOR forwards a packet in a sequence of nodes. A next forwarding node is determined after a previous node transmitted its packet. One node from all nodes that received the packet, which is closest to the destination, is elected as the next forwarding node. In such manner the packet approaches the destination. The path is determined during a packet propagation. Each hop moves a packet farther than the hops of the best possible predetermined route [11].

In Figure 4.2, an example of a simple network with delivery ratios is shown. Nodes A to D are placed on the line and are assigned with the delivery ratios relative to the separating distance. The node A initiates a transmission to the node D. It can send a packet directly with the delivery ratio of 0.1 and suffer from multiple retransmissions as

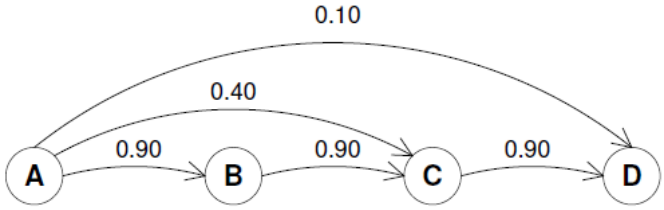

Figure 4.2: Simple ExOR network example, with delivery ratios

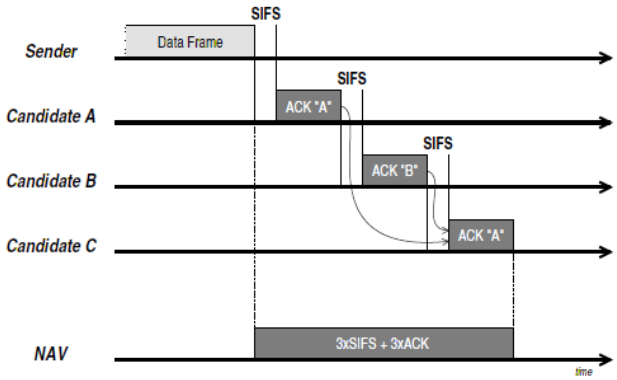

Figure 4.3: Typical ExOR acknowledgment sequence

the probability of a correct packet reception is rather low. The other way is to use multiple hops A-B-C-D. It is wasteful to transmit packet from A to B when C also hears this transmission and so on. If a transmission from A to D fails, B or C can forward this packet. Priorities from higher to lower are assigned as follows: D, C, B. ExOR exploits opportunities to improve performance.

Potential receivers are ranked by forwarding priority according to a simple scheduling structure. Priorities are included in the header of a transmitted packet. Receiving node looks in the header and delays itself for the time relative to the assigned priority. If a higher priority node acknowledges the received packet and forwards it containing an updated header with a new subset of node priorities, the other nodes with the lower priority just drop the old packet.

Packet acknowledgments are used in order to eliminate duplicate forwarding and help nodes to decide which of them is the next forwarder. Typical ExOR acknowledgment sequence of the previous network example is shown in Figure 4.3. MAC layer assigns time slots for the receiving nodes. A receiving node must return an acknowledgment during the assigned time slot. The total duration of all assigned acknowledgments is specified in Network Allocation Vector (NAV). ACK slots are separated by SIFS periods in order to avoid collisions. Node C becomes the new forwarding node, since it heard the packet from A and B lost it. B suggests itself as the best forwarder by sending an ACK including B value. Node C has priority over B (see Figure 4.3), hence it forwards a packet. The probability that A will retransmit a packet is decreased.

The next important opportunistic routing protocol is the Opportunistic Routing in Ad Hoc Networks (OPRAH). This protocol uses the promiscuity of an air interface to find a

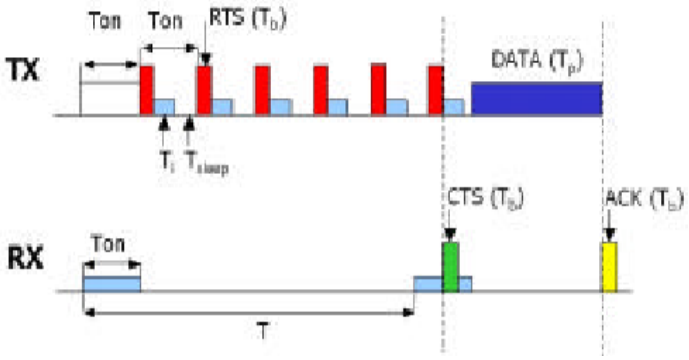

Figure 4.4: TICER scheme

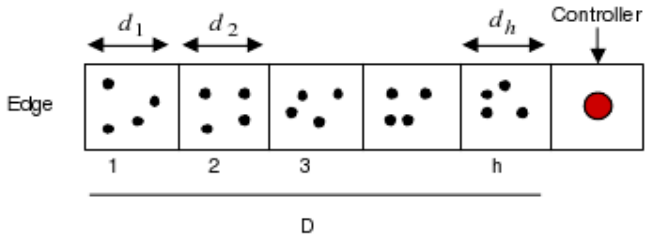

Figure 4.5: Region-based routing. Network model with single sink and routing blocks

more optimal path in a dynamic network [12]. Overhearing other transmissions can cause high power consumption in denser networks, hence OPRAH is not efficient in WSN. OPRAH uses AODV to fill specific route data, not a single route to destination (backward learning). Nodes do not know its geographical locations. All nodes that are closer than the sender node compete for the forwarding of a sent packet. Neighbor nodes are treated as potential relays. The list of these potential relays is created at each node by promiscuous overhearing of transmissions. It is adapted to the mobility and the environment.

Cross-layering structure of a protocol stack is used in the Region-Based Opportunistic routing protocol [13]. Unification of a protocol stack has the advantage of reducing power consumption. Interacting layers have not only the data and control channels, but also include cross functionality, which helps a network to be robust to failures. An asynchronous rendezvous scheme is implemented at the MAC layer. This scheme is called TICER (Transceiver Initiated Cycled Receiver). Nodes exploit a random sleep discipline which allows to save energy. The receiver of a sensor node is enabled periodically (cycled receiver) to monitor the environment every T seconds and is disabled (sleep period) after wakeup time T_{on} (see Figure 4.4 [13]). If the radio channel is idle, RTS is sent to a receiving node. The receiving node sends a CTS signal immediately back to source. The source starts the data transmission after receiving the CTS. If the data was received correctly, an ACK is sent. Then the nodes go back to sleep mode. To reduce collisions, CTS is sent after a random backoff period. To reduce power consumption, T_{on} , RTS, CTS and ACK must be as short as possible. No packets are dropped as the node can process all received data packets, because the traffic amount is low. The network model includes a single controller (see Figure 4.5 [13]). All data packets are routed to this controller. The network is clustered into separate blocks. Messages are routed from one block node to one of the nodes belonging to the next block. The next hop node is the first node that responds to RTS. The forwarding region is selected according the spatial diversity principle, discussed in the previous subchapter.

Opportunistic routing exploits the duty cycling of sensor nodes. Other approaches to this problem are analyzed by such routing protocols: the Energy Efficient Coordination Algorithm (SPAN)[14], the Sparse Topology and Energy Management (STEM)[15], the Geographical Adaptive Fidelity (GAF)[16]. Forwarding of packets to the neighbor, which is closest to the destination is done in Greedy Perimeter Stateless Routing (GPSR)[17].

Geographic Random Forwarding (GeRaF)[18] elects the best node by geographic location. It divides the forwarding region into priority regions. The nodes that appear in

these priority regions and are closest to the destination are assigned with the highest priority.

4.4 Node mobility and Random Mobility Models

Mobile networks are characterized by a node mobility. A mobile network can consist of mobile elements: sensor nodes, sinks, routers. Gateways are stationary in most cases, but can also be mobile. A mobile sink can have a gatewaying functionality in order to communicate with other sinks or dump received data via UMTS, GPRS, etc.

The movement of nodes can be random or predictable. It is possible to describe it by different mobility models. Mobility of nodes is a physical movement, where nodes move independently or relative to the group of nodes. Mobility models are the approximation of movement behaviour. There are three types of mobility: random, predictable and controllable.

Random mobility models, such as random waypoint, random walk, random direction, are used in traditional networking scenarios, where node mobility is not described. Simulation scenarios with described mobility patterns should exploit controllable (highway traffic, city section) and predictable (boundless simulation area, Gauss-Markov, probabilistic random waypoint) mobility models. Problems, that involve group mobility of nodes, can be described by group mobility models (nomadic community, pursue mobility, reference point group).

The next subchapters describe the simpliest and the most popular random mobility models: random waypoint and random direction.

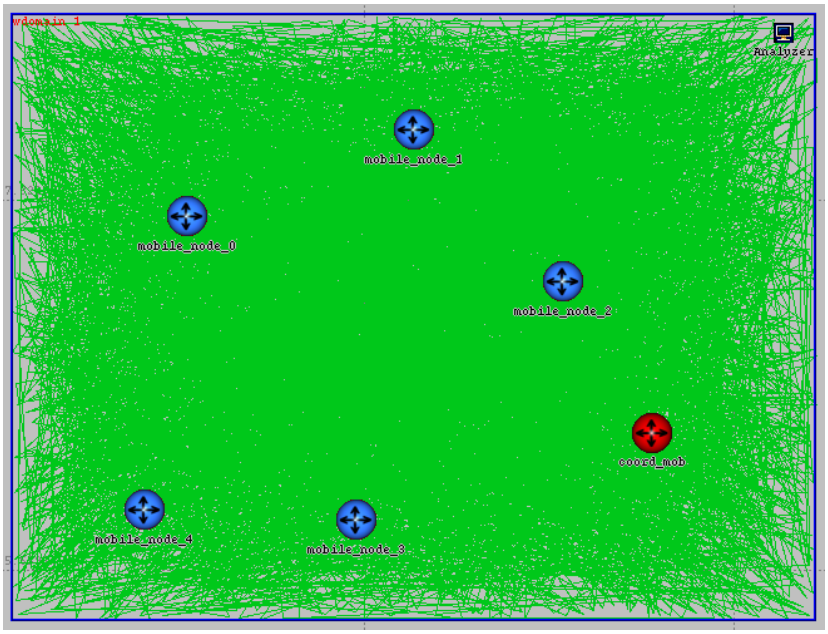

Figure 4.6: Random waypoint mobility model

4.4.1 Random Waypoint Mobility Model

The Random Waypoint mobility model belongs to a random mobility class. It is similar to a random walk model, the difference is that the pause times are included after arrival at the destination point. A mobile node selects a new random point in the simulation area and travels to it with a random constant speed. When a mobile node arrives at the selected destination point, it waits for a random pause time. Then a new destination point is selected. Speed is uniformly distributed in the interval [$speed_{min}$, $speed_{max}$]. Random waypoint is a widely used model.

In order to check the behavior of mobility in the network with random waypoint mobility profile, the simulation is done in the OPNET simulator. The simulation is started with randomly deployed mobile nodes (see Figure 4.6). There is a transient period of an initialization state of a random waypoint model. It is necessary to skip the first 1000 seconds of simulation runtime in order to avoid this transient influence, even if nodes move with a low speed. The initial random distribution of mobile nodes does not represent the behavior of moving nodes in the steady state. If a simulation runtime is relatively long, it is possible to include the transient period as it will not cause a big variance of the final results. More stable results can be obtained in a network with higher speed and longer pause times of mobile nodes.

The next problem of a random waypoint mobility model is that the distribution density of mobile nodes is larger at the center of the simulation area than at the edges. That means that nodes are moving more frequently at the center than to the edges, a mobile network becomes clustered at the center. As an example, see Figure 4.6. In this figure the results of simulation of a random waypoint mobility model are shown. Speed is uniformly distributed in the range [10-20m/s]. The pause time at the destination is constant of 10 seconds. The simulation runtime is 9000 seconds. It is noticeable that the distribution of random destination points is denser at the center. For this reason, the random waypoint mobility model is not suitable in a simulation scenario that requires a

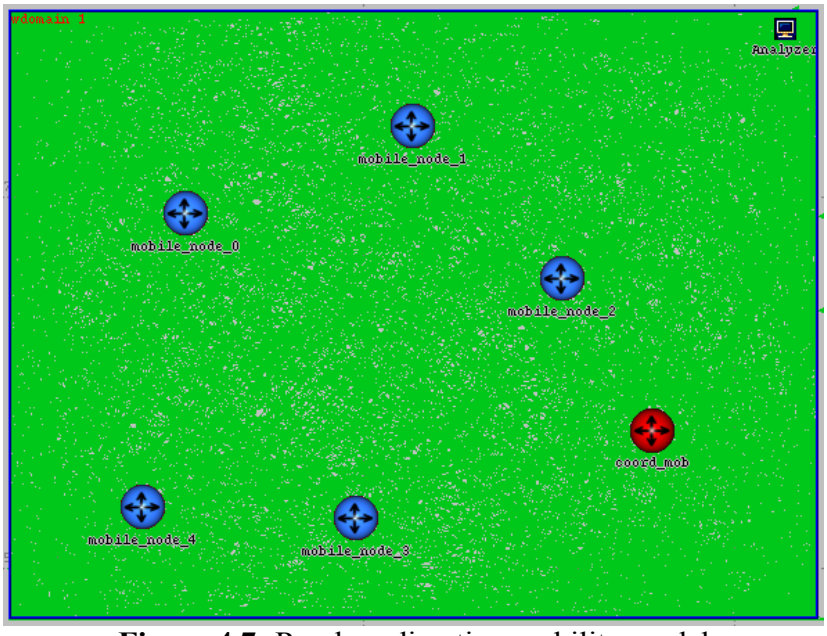

Figure 4.7: Random direction mobility model

homogeneous distribution. The random direction mobility model should be used in that case. This model is described in the following subchapter.

4.4.2 Random Direction Mobility model

The Random Direction mobility model overcomes the mentioned problem of network clustering at the center of a simulation area. This model allows a constant number of nodes crossing the simulation area. Initially, nodes in the network are randomly deployed. A mobile node selects a random direction (random angle) and moves to the simulation boundary with a constant random speed and stops there for a random pause time. Then it selects a new direction according relative to the boundary. Nodes cannot leave the bounded simulation area. For example, if a node is at the left wall of simulation area, it can select random angle in the range [0 - 180 degrees] directed from the left. If the node appears in the upper corner, it can select an angle [0 - 90degrees] directed from down to right.

The random direction mobility model is characterized by a uniformly distributed angle of movement direction. A modified version of this model allows a node to stop on the way to the boundary and to choose a new direction.

An example of standard random direction mobility is shown in Figure 4.7. The density of mobile nodes is homogeneously distributed. Nodes visit all locations. Parameters, that are used for the simulation, are the same as for the random waypoint model which was discussed in the previous subchapter. Mobile nodes stop at the simulation boundary. Long pause time has the influence for the routing length. This length per route will be higher than the average hop count of the most other mobility models [19].

The random direction mobility model is chosen for this thesis. Principles and implementation of this model are presented in Chapter 5.6.3.

CHAPTER 5

5. Simulation Model of The Opportunistic Routing Protocol

In this chapter, the simulation model of the new opportunistic routing protocol is introduced. This model is implemented in the OPNET simulator [20]. The task analysis describes the task of this master thesis. The whole model is analyzed in detail from the structural, opportunistic routing and programming points of view.

5.1 Task Analysis

The main task of this master thesis is the development of a new opportunistic routing method for a mobile WSN with multiple sink nodes.

A mobile network consists of mobile nodes. These moving nodes change their locations, thus causing disruption of the communication between nodes. An intermittent connectivity and knowledge about the nodes' relative movement can be exploited in order to achieve an efficient, reliable routing.

The major part of the work is an implementation of the network layer using the opportunistic routing algorithm on top of existing layer 1 and layer 2 models, covered by IEEE 802.15.4 standard (Chapter 3). In this work, the non-beacon, unslotted CSMA/CA the IEEE 802.15.4 MAC and the IEEE 802.15.4 PHY models are exploited. These MAC and PHY layers are the modified versions of the existing model, available in [21]. Unslotted CSMA/CA is chosen for this work, because it allows ad hoc communication between sensor nodes.

In order to analyze the performance of the proposed opportunistic routing algorithm, it must be simulated in a simulation environment. Many available free simulators [22] are not precise and cannot provide flexible analysis of the simulation model. At the start time of this modeling work, the only available simulation model of partly implemented IEEE 802.15.4 was provided by Open-ZB [23]. This model (v1.0) is created with the commercial OPNET simulator [20], thus the OPNET simulation environment is chosen for the development of the opportunistic routing protocol. This simulator is presented in more detail in Chapter 5.2 and the Open-ZB model is presented in Chapter 5.3.

The network layer containing the opportunistic routing protocol is implemented from

scratch and presented in the following subchapter. Power consumption analysis is done by the battery model, which is also available in [21].

The implemented opportunistic routing model performance must be analyzed. Power consumption, data packet end-to-end delays, route length, throughput and data packet loss are the main statistics which must be taken into account when evaluating the model.

In order to ensure that this model is built according to a delay, reliability and energy efficiency tolerant opportunistic routing scheme, the comparison of simulation results with the well known AODV routing protocol is provided in Chapter 6.

5.2 The OPNET Simulation Environment

Simulation is an easy way to test of a generated scenario. It is possible to change the network size and node deployment without any costs. Simulation statistic results give the possibility to evaluate the performance of the implemented model and parts of the algorithm. Mistakes of design can be easily fixed in a simulation environment opposed to fixing them in real models.

OPNET [20] is an event-driven, network simulation tool, which allows an easy implementation of the all model elements. As an example, the OPNET simulation environment is shown in Figure 5.1. The node model specifies the main blocks and parameters of a node and provides an interface to a network element. The process model defines the states and the state transitions of the node model elements. It abstracts the behavior of the network element. The packet format generator allows to build any

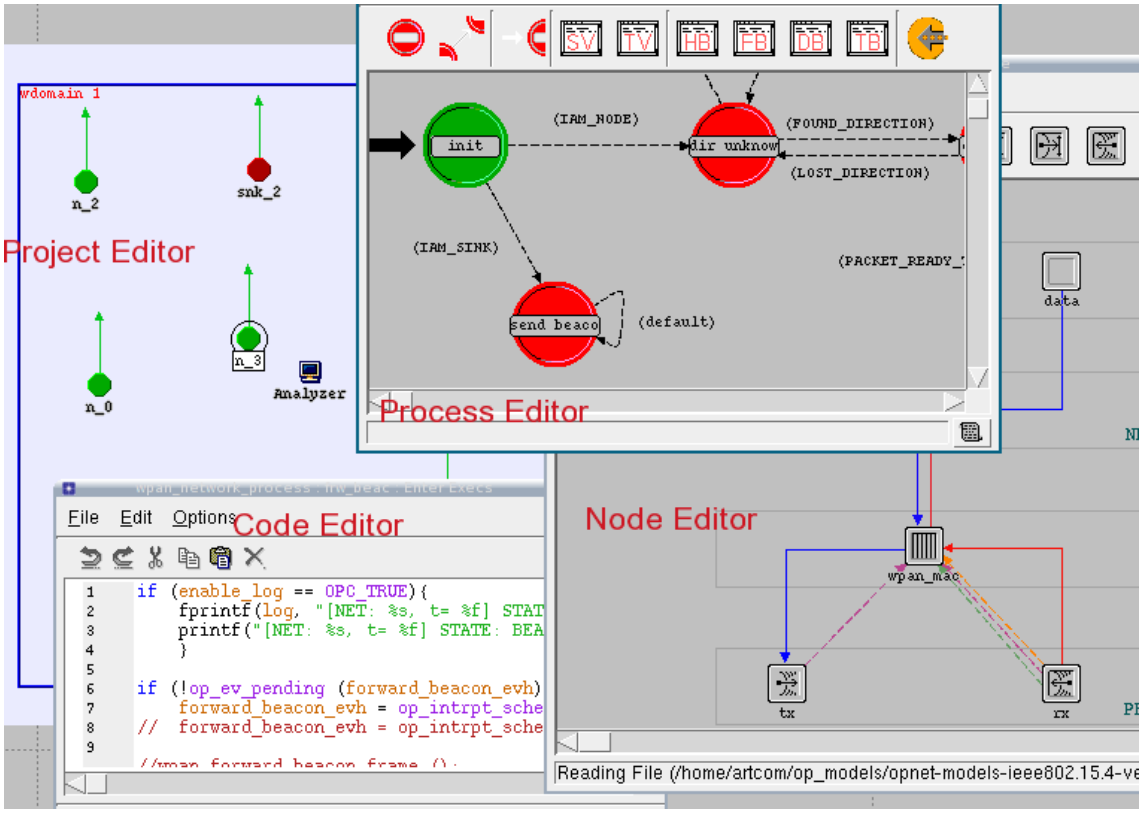

Figure 5.1: OPNET simulation environment

packet consisting of a real byte oriented packets on named unsorted fields. The packets definition can follow exact protocol specifications. It is easy to deploy network elements in the project editor. All parameters can be configured easily. OPNET includes available tools for link setup and mobility profiling. Simulation results can be processed and analyzed with advanced functions.

For modeling of the Opportunistic Routing in Multi-Sink Mobile Ad Hoc Wireless Sensor Networks protocol (ORMMA-WSN), OPNET version 11.5A is used. The wireless module license and mobility tools are exploited. This work includes some parts from the IEEE 802.15.4 WPAN model available in [21].

Statistics collection is performed in the area of energy consumption, propagation delays, packet loss and detailed node statistics.

5.3 The OPNET Simulation Model of IEEE 802.15.4

Open-ZB [23] is an open source implementation of IEEE 802.15.4/ZigBee [9]. The simulation models are available for OPNET and TinyOS. Version 1.0 of the accurate simulation model of the slotted IEEE 802.15.4 is programmed for the OPNET simulator.

The model structure is shown in Figure 5.2 [23]. This model implements PHY and MAC and APP layers. PHY is includes a transmitter and a receiver working at 2.4 GHz frequency, 2 MHz bandwidth and QPSK modulation. The MAC layer contains slotted CSMA/CA, generates beacon frames and synchronizes nodes with a PAN Coordinator. The battery module calculates consumed and remaining energy levels. The APP layer includes a sensory data generator using unacknowledged frames and a MAC command frame generator creating acknowledged frames. The sink module performs statistics of

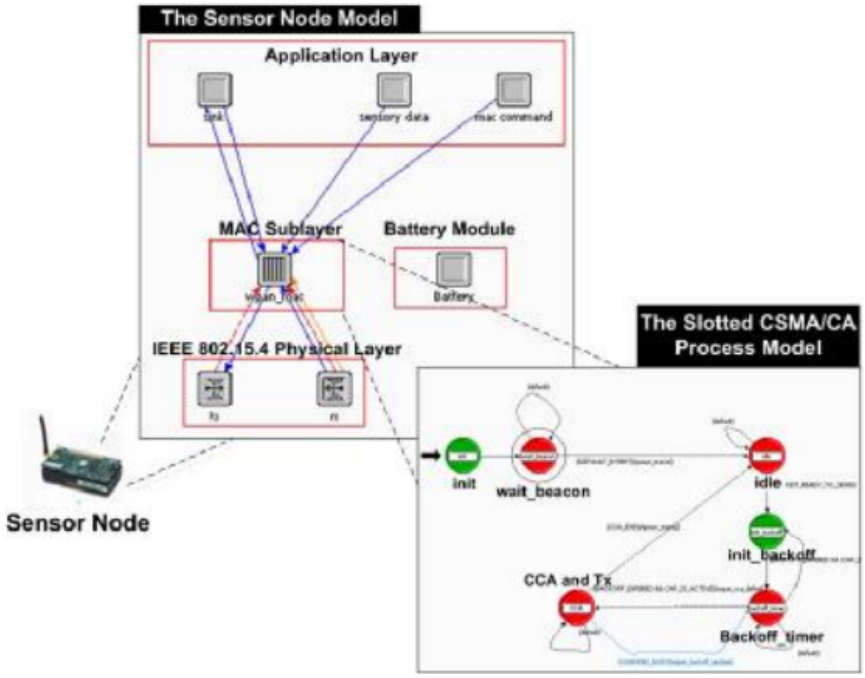

Figure 5.2: Open-ZB IEEE 802.15.4 model in OPNET

the received frames.

The radio model contains the standard OPNET wireless modules, which emulate the radio channel with such elements as interference, noise, BER, propagation delay, etc.

The supported features of the Open-ZB are:

- Beacon-enabled mode (Generation of beacon frames),
- Slotted CSMA/CA MAC protocol,
- Beacon, data, ACK packet frame formats,
- IEEE 802.15.4 PHY characteristics,
- Calculation of power consumption (MICAz model).
- GTS Mechanism (v2.0).

5.4 The Opportunistic Routing Protocol

The Opportunistic Routing (OR) model is based on the idea, that multiple sink nodes transmit periodic higher power beacons and the other nodes extract their mobility information from these beacons. The node mobility is relative to the sink, because nodes do not know about their global position. If a mobile node moves away from a sink, it must give away all pending packets to the most successful mobile node, which appears in its neighborhood.

The OR protocol has the following properties:

- obtaining node's mobility information from beacon signals by RSSI values,
- calculation of the Mobility Gradient (MG),
- building of a neighbor node table including node mobility information,
- forwarding of node's mobility information to the neighborhood,

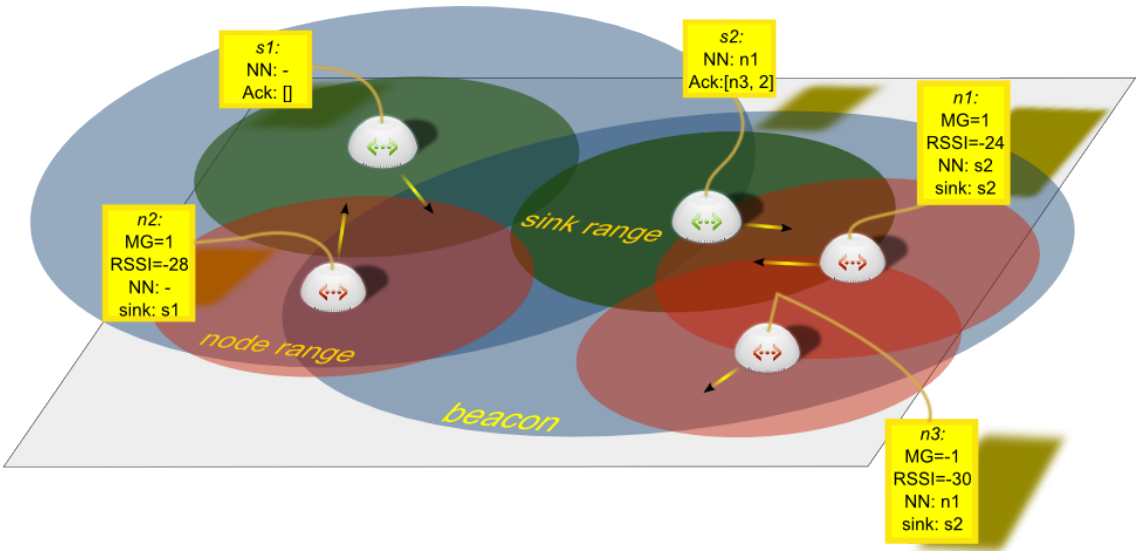

Figure 5.3: Multi-Sink scenario using the opportunistic routing protocol

- evaluation of the neighborhood information,
- election of the best neighbor node and the best sink,
- recovery after the link failure (try to avoid packet loss).

The following scenario in Chapter 5.4.3 describes the Opportunistic Routing in Multi-Sink Mobile Ad Hoc Wireless Sensor Networks (ORMMA-WSN).

5.4.1 Received Signal Strength Indication (RSSI)

The Received (RX) Power indicates the average received signal power of the received packet. It is used to identify the mobility gradient of a moving node.

The PHY layer indicates the RSSI value to the MAC layer. The RSSI is used by ORMMA-WSN for MG calculation and comparison of sink and sensor nodes. The RSSI value increases when the signal becomes stronger. The value is included in the Network packet format.

Nodes periodically receive high power beacons and fill this information into the sink table. Sinks are sorted according to the RSSI value.

5.4.2 Mobility Gradient

The Mobility Gradient (MG) is the information about mobile node's movement direction relative to the sink. Nodes calculate the MG value from two subsequent beacon signals received from the same sink. The sign of difference between the current and the previous RSSI value gives the mobility direction:

$$MG = sign(RSSI_2 - RSSI_1) = sign(\Delta RSSI)\,. \tag{5.1}$$

A negative MG value stands for the movement of the node away from a sink and a positive value means moving towards the sink. When node and sink are not moving or when they move in parallel, MG is zero:

$$\begin{cases} MG = -1, \text{ from sink,} \\ MG = \ \ 0, \text{ constant,} \\ MG = +1, \text{ to sink.} \end{cases} \tag{5.2}$$

Due to fluctuations of the radio channel, the RSSI can change even if there is no relative movement. For this reason, a small MG threshold σ must be used in order to avoid a fast switching of the MG value

$$MG = 0, \ \ if\ \Delta RSSI > \sigma\,. \tag{5.3}$$

At least two beacons are necessary to calculate the node mobility. The beacons must be subsequent or their time difference must not be larger than the allowed period of time between two received beacons, called Sink Expiration Time (SET). After this period, the sink is removed from the table.

The MG value is included in the NET layer packet header. It is one of the most important parameters in the ORMMA-WSN protocol.

5.4.3 The Multi-Sink Scenario

In a usual single sink network, data is routed to one destination. The destination address can be known a priori. When more than one destination is available, nodes must obtain information which destination is the closest or what is the destination with the least cost to route.

The Multi-Sink Scenario, represented in Figure 5.3, uses a network where multiple data sinks are involved, arrows show the directions of movement. The communication range is the same for all nodes and sinks. Sink beacons are sent periodically with higher TX power, hence the beacon coverage is larger. The simulation area is not fully covered by these beacon signals (no full connectivity inside a scenario), thus a node can appear in a silent zone and lose its mobility information. If a neighbor node is in proximity of a sink and the node which lost its MG information, it can help this node to recover by forwarding its mobility information. This method, however, is limited to a maximum of 2 hops and a different approach to solve this problem can be considered as future work. In this work, it is assumed that if node is in a silent zone, it waits for better conditions.

All nodes are mobile. They have intermittent connectivity to neighbor nodes and are moving randomly inside the simulation area. The number of sensor nodes is larger than the number of data sink nodes:

$$N_{sensors} > N_{sinks} .$$

Nodes obtain their collocation with sinks according to the MG information, calculated from the periodic beacon RSSI as discussed before. When a sink is considered as valid (two consequent and not expired beacons), it is written to a sink table. This table is check for expired sinks. When at least one valid sink is in the table, node obtains its mobility information by a calculated MG value. All multiple sinks are included and sorted by their RSSI value. The best sink is the closest sink, thus the one with maximum RSSI value. The best sink is elected after each received beacon signal.

Once a node obtained its mobility information, it must forward this mobility information to the neighborhood. This process is called beacon forwarding. Every beacon is forwarded with normal power. If a network contains a large number of sinks and the inter-sink beacon arrival time is small, this can cause redundant forwarding of beacon packets. Because of this, a short time interval is used to delay beacon forwarding. This can be related with the speed of node mobility. If a node moves faster, this waiting time interval is decreased.

When a neighbor node receives the forwarded beacon, it extracts the mobility information of the forwarding node and fills the neighbor node table accordingly. The same expiration procedure is done as for the sink table. If a neighbor node Beacon Forwarding Interval (BFI) is larger than the Node Neighbor Expiration Time (NNET), the neighbor node is removed from the table.

If a sink receives a forwarded beacon from the neighbor node, it means that this neighbor node is in the sink's communication range. The problem is that the neighbor node cannot know when it is in the sink's range, because the sink beacon power is larger than the power of a node transmission signal, and data communication is only possible in the communication range. The sink must announce the list of neighbors that appear in its range. In this work, the announcement is done by including the list of neighbors in the beacon packet header. Sinks build a neighbor node table like the sensor nodes, but only for this announcement purpose. If a neighbor node BFI is larger than the Sink

Neighbor Expiration Time (SNET), a sink neighbor node is removed from the table. This process is repeated if there are no data packets in the network. If a node senses some data, it initiates the data transmission. If a node is in the sink's communication range and discovered its address in the received beacon, it can send the data packet directly. If the transmission was successful, the packet is acknowledged by the sink. If a node is far away from the sink, the ORMMA-WSN protocol elects the Best Neighbor Node (BNN) each time there is a packet to send. Nodes compare their MG and received RSSI to those of the neighbor node. If, in the neighborhood, there is a node which moves towards the sink (MG = +1) and if the current node is moving away or constant, this current node must give away all pending packets to the neighbor node. This neighbor node is elected as BNN. If, during packet relay, the link breaks, the BNN is reelected. The election procedure is described in more detail in Chapter 5.6.8. Each next hop node makes its own decision about the routing direction, hence there is no reason to include the sink address in the network packet header.

Due to mobility, it can happen that the back route does not exist anymore. Hence the acknowledgments cannot be sent via multiple hops. One proposal for this is that ACK sequence numbers can be included in the beacon packet header. In this way, the source node is able to know whether the packet reached one of the destinations. This can introduce a larger overhead in power consumption (high power beacons) and increase the probability of collisions because of the longer packets transmission time. For this reason, packets are only acknowledged in intermediate hops in the MAC layer. The Network layer does not allow packet loss and uses an infinite buffer. Analysis of the queuing size of routing packets is a part of performance evaluation.

As an example of table parameters, labels are attached to the nodes in Figure 5.3. The sink nodes *s1* and *s2* send periodic beacons. Sensor node *n2* is in *s1* and *s2* beacon range, but not in the communication range. Node *n2* elects sink *s1* as the best sink because it is closer. Node *n2* approaches *s1*, its MG is 1. No neighbors are available. the best sink is *s1*. It is expectable that after some time *n2* will be in the communication range of *s1* and will handle a packet. The right side of the example network contains node *n1* and *n3* in the sink *s2* range. Node *n1* is in sink *s2* communication range and approaches this sink, hence BNN is *s2*. Node *n3* moves away from the sink and can hear the forwarded beacon from *n1*. Node *n3* gives away all pending packets to the node *n1*. And *n1* routes these packets to the sink *s2*. The proposed ACK structure is shown for this example: sink *s2* puts the following ACK value to the beacon header: acknowledgment for *n3*, data packet sequence number is 2.

5.5 Modeling Structure

Mobile sensor nodes are nodes with ad hoc networking capability using the IEEE 802.15.4 non-beacon enabled mode with unslotted CSMA/CA. The mobile node structure is almost the same as for mobile sinks, except that it is not sinking the data but acting as relay.

A mobile node must be powered by a protocol stack in order to communicate with other nodes. This stack employs layers from PHY to the APP layer. These layers are implemented as separate processes of the different modules. The wireless sensor node structure is analysed in Chapter 5.5.1.

For node mobility, a random mobility profile is choosen for every node, the random direction mobility model with a homogeneous node distribution is selected.

The PHY layer is modified in order to have TX power control. The MAC layer with unslotted CSMA/CA is responsible for packet transmission, retransmission and collision avoidance. The ORMMA-WSN algorithm performs the discussed opportunistic model functionality, processes data packets and provides a destination address to the MAC layer. The MAC layer indicates the RSSI of the received packet to the Network layer.

Power consumption is calculated in the separate battery module.

The modeling procedure is as follows:

- Random mobility profiling and random direction mobility model implementation.
- Modification of the available IEEE 802.15.4 MAC model [21].
- TX power control in MAC layer and PHY layer.
- Network layer process model and packet buffer.
- Implementation of table processing functions and statistics collection.
- Application layer process model with beacon and data packet generators and data sink.
- Beacon processing and forwarding, expiration timers and table element removing procedures.
- Mobility gradient calculation.
- Mobility information module implementation.
- Neighborhood information module implementation.
- Network packet buffer handling.
- Packet transmission and ACK waiting procedures.
- Inter-Control Interfaces (ICI) for destination address and RSSI indication.
- Statistics collection wire setup.
- Node module parameterization.
- Setup of the simulation scenario.

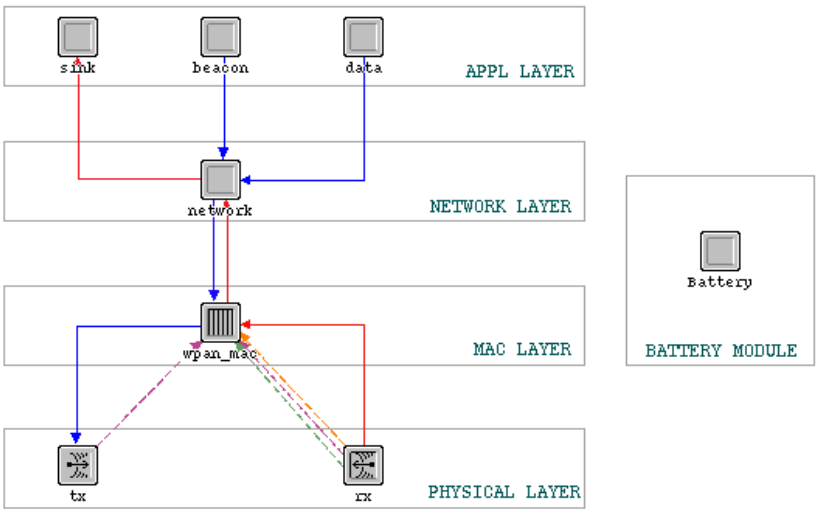

Figure 5.4: Wireless sensor node model

5.6 Programming Model Analysis

The main part of this work is an implementation of the simulation model of the wireless sensor network, consisting of wireless sensor nodes equipped with the IEEE 802.15.4 MAC and the NET layer with the opportunistic routing algorithm. The model is programmed and modeled with the OPNET simulator. Separate parts of the programming model are presented and analyzed in the separate subchapters within this chapter.

5.6.1 Node Model

The wireless sensor node model is presented in Figure 5.4. This structure is the same both for sensor and sink nodes. The node model represents the protocol stack containing different blocks.

The lowest layer is the Physical Layer (PHY). Radio receiver (rx) and radio transmitter (tx) are separated and described by different modules. Data transmission and reception is done in multiple stages of different analysis functions. BER, Signal to noise ratios (SNR), channel matching, pathloss, etc. are calculated for every received packet. This procedure is controlled by a radio model. Packets are exchanged between the PHY and and MAC layers through data stream channels (solid arrow lines). Statistical wires (dashed lines) are used in order to indicate radio channel conditions to the upper layers. RSSI, receiver busy and collision events are indicated by the receiver module. A transmitter busy interrupt is sent when there is a data transmission in the transmitter module.

The transmitter and receiver configuration is shown in Figure 5.5. Parameters are chosen according to the IEEE 802.15.4 PHY characteristics. TX power is set to the default initial value, but can be changed during simulation runtime (TX power control).

name	tx
channel	(...)
rows	1
row 0	
data rate (bps)	250,000
packet formats	wpan_ack_frame_pkt_format,
bandwidth (kHz)	2,000
min frequency (MHz)	2,401
spreading code	disabled
power (W)	promoted
bit capacity (bits)	infinity
pk capacity (pks)	1,000
modulation	qpsk
rxgroup model	dra_rxgroup
txdel model	dra_txdel
closure model	dra_closure
chanmatch model	dra_chanmatch
tagain model	dra_tagain
propdel model	dra_propdel

name	rx
channel	(...)
rows	1
row 0	
data rate (bps)	250,000
packet formats	wpan_ack_frame_pkt_format,
bandwidth (kHz)	2,000
min frequency (MHz)	2,401
spreading code	disabled
processing gain (dB)	channel bw/dr
modulation	qpsk
noise figure	1.0
ecc threshold	0.0
ragain model	dra_ragain
power model	dra_power
bkgnoise model	dra_bkgnoise
inoise model	dra_inoise
snr model	dra_snr
ber model	dra_ber
error model	dra_error
ecc model	dra_ecc

Figure 5.5: Transmitter and receiver module configuration

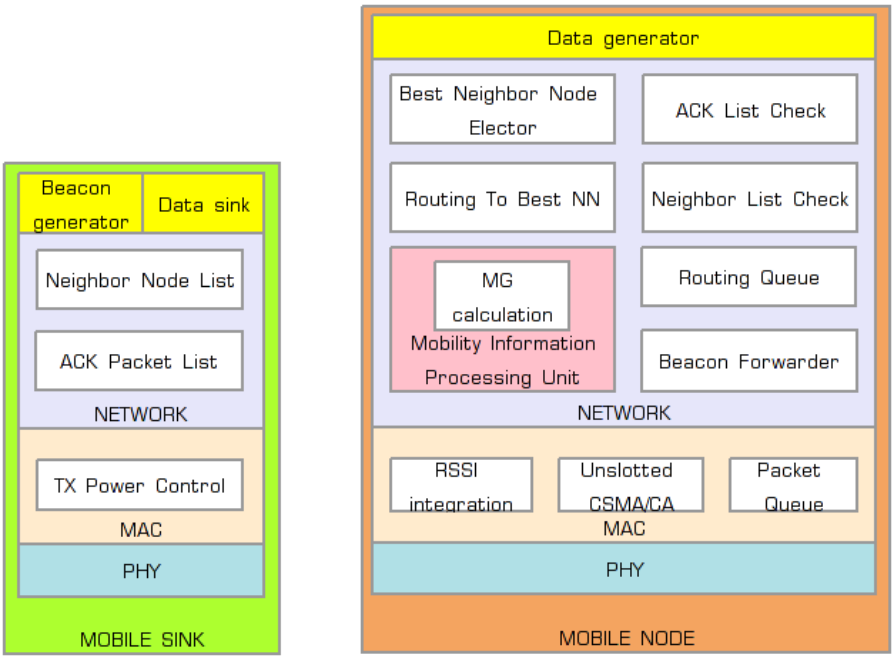

Figure 5.6: Mobile sink node and sensor node programming model

Also it is necessary to define the packet formats which will be supported by the PHY layer. These packet formats are described in the next subchapter.

The next upper layer is the medium access control (*wpan_mac*). This module includes the state process model of the non-beacon enabled MAC with the unslotted CSMA/CA channel access protocol. This allows ad hoc communication between nodes. The MAC layer is the interface layer between PHY and Network layers. The MAC layer has the following functionality:

- Provides the control functions for the PHY layer.
- Packet filtering and handling.
- Channel access control (unslotted CSMA/CA).
- Packet transmission and retransmission.
- Indication to Network layer about RSSI of the received packet via ICI interface which is coupled with the current packet.
- TX power control for high power beacon packets.
- Packet queue arbitration.

The Network layer (network) implements the ORMMA-WSN protocol. This module contains the state process model of the opportunistic algorithm. The node model provides the interface that controls this process model's initial parameters and the relation with other modules in the node model. The Network layer encapsulates beacon and data packets from the Application layer above and provides the received data packets for the data sink module. The Network layer internal programming structure is shown in Figure 5.6. Mobile sink nodes and sensor nodes have different network layers. The opportunistic routing functionality is tightly related with the network layer of a mobile sensor node. The main functions of the ORMMA-WSN protocol are:

- setup of sink and neighbor node tables,
- beacon forwarding,

- mobility information processing,
- packet routing queue arbitration,
- election of the best sink and the best neighbor nodes (Chapter 5.6.8),
- ICI interface providing the destination address to the MAC layer.

The top is the Application layer (APP). A beacon generator (beacon) generates unacknowledged beacon packets. The data generator (data) generates acknowledgement requiring data packets. Initial parameters are controlled from the node model. When the Data packet is received by a node, it must be sent to the data sink module (sink) for statistics.

An additional element in this programming node model structure is the battery module. It has the purpose of calculation of the power consumption by a current node. It is possible to set the initial energy amount in order to evaluate the network lifetime. On the other hand, the total amount of the consumed energy during simulation runtime is also an important metric. This battery module supports the parameters of the MICAz mote specification (see Chapter 5.6.6).

5.6.2 Packet Formats

The packet format is a formalization of data fields oriented into one sequence or string. In this model different packet formats are supported in every layer. The encapsulation and decapsulation procedures allow to transmit packets between two layer entities.

In OPNET, data packet formats are created with a help of the Packet Editor. A packet format is created from the data fields, which can be defined as named data field, unnamed indexed field or data vector. Data formats can be specific (int, double), structures or can be inherited. Data inheritance usually is used for payload encapsulation.

For the PHY layer in Figure 5.4, packet formats are the same as for the MAC layer. In this work, only two MAC packet formats are employed: the MAC packet format (Figure

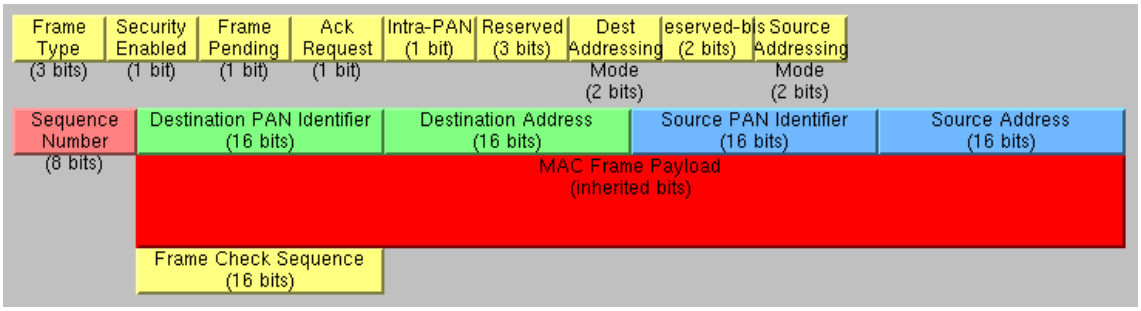

Figure 5.7: MAC packet format

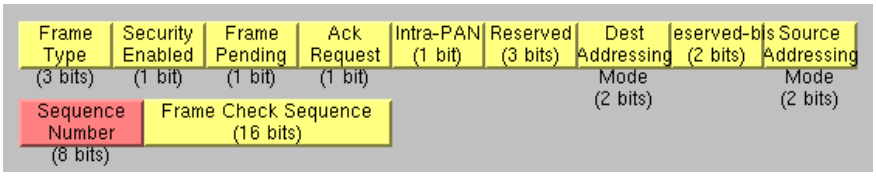

Figure 5.8: ACK packet format

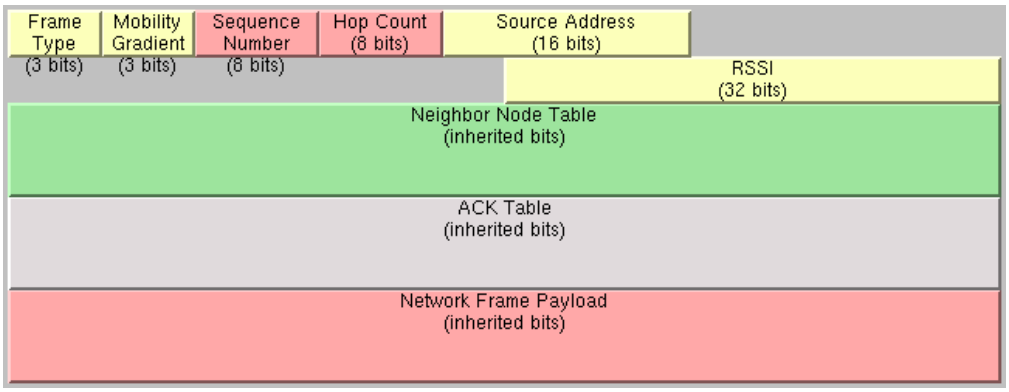

Figure 5.9: Network packet format

5.7) with 16-bit short addressing and the ACK packet format (Figure 5.8). These packet formats are defined in IEEE 802.15.4 and were available in [21]. However, not all fields are exploited by the modified MAC protocol.

In the MAC packet format these fields are used:

- *Frame Type* defines the type of a packet. Value 1 – data packet, 2 – ACK packet.
- *Ack Request* identifies whether the acknowledgment is requested. Value 1 – requested, 0 – not requested.
- *Sequence Number* shows the current packet sequence number. It is chosen randomly by the MAC layer.
- *Destination Address* identifies the receiver node of the transmitted packet. It is a 16-bit short MAC address, which is unique for every node.
- *Source Address* identifies the owner MAC address of the transmitted packet. The format is the same as the Destination Address.
- *MAC Frame Payload* is the inherited packet from the network layer. It is encapsulated in MAC. The size of this field depends on the payload size.

If the *Ack Request* field is set to 1 in the transmitting packet, an ACK packet must be sent to the source node. The following fields are exploited here:

- *Frame Type* defines the type of a packet. Value 2 – ACK packet.
- *Sequence Number* indicates which packet is acknowledged.

For the Network layer, a new packet format was defined. The structure of the Network packet format is shown in Figure 5.9. This packet format consists of the packet header and the inherited payload field from the APP layer. These fields are defined as follows:

- *Frame Type* defines the format of the network packet. Value 0 – beacon frame, 1-data frame (requires acknowledgment in the MAC packet).
- *Mobility Gradient* shows the direction of movement of the sending node. Value 0 – constant, -1 – away, +1 – towards a sink.
- *Sequence Number* is assigned to every data packet, received from APP layer data generator module. This number is used in order to avoid the duplicated reception of data packets.
- *Hop Count* shows the route length of the data packet. A sink node beacon packet has this field set to the value 0.

- *Source Address* identifies the owner of the packet generated at the APP layer. This field shows the source of the generated data if the packet is routed over multiple hops.
- *RSSI* field indicates the current node's relative distance to the sink.

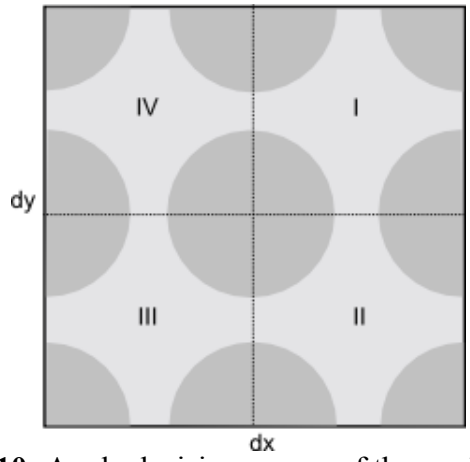

Figure 5.10: Angle decision ranges of the random direction mobility model

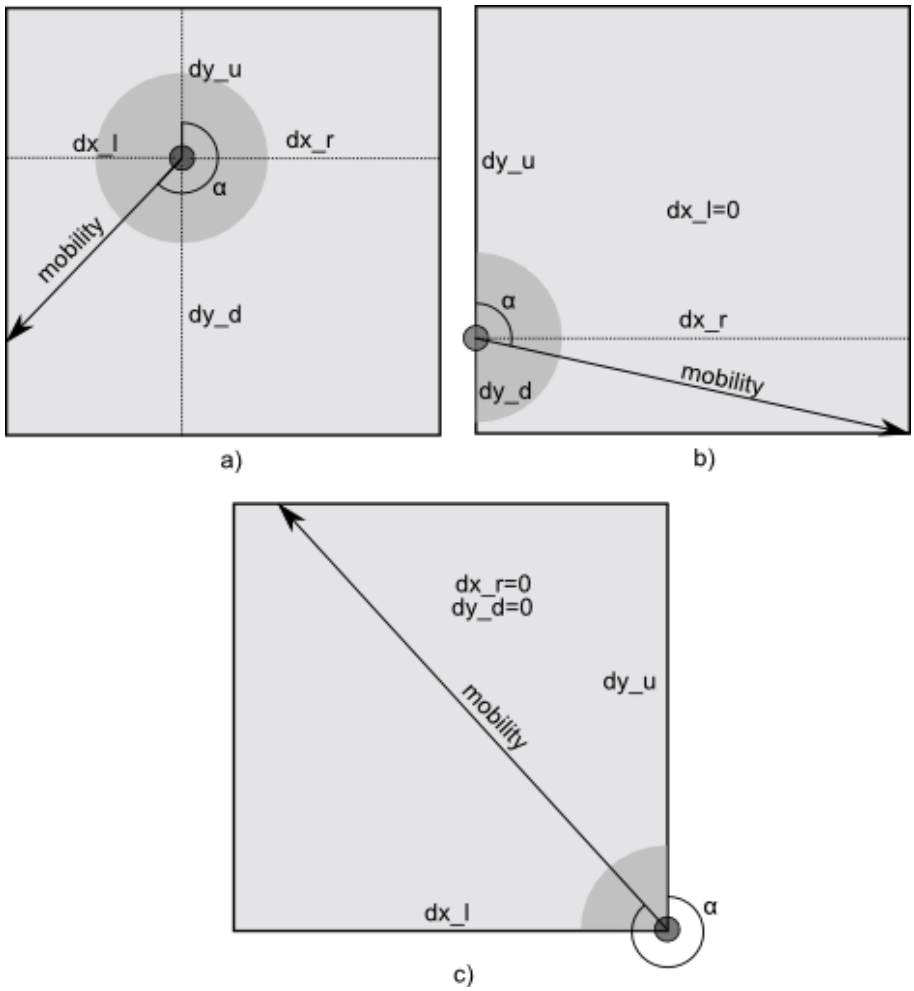

Figure 5.11: Examples of node movement in the Random Direction mobility model

- *Neighbor Node Table* includes the list of neighbor nodes that appear in the sink's range. This field only exists in the sink beacon packet.
- *ACK Table* is the list of ACK sequence numbers to identify which packets were successfully received by the sink. This field is used only in sink beacon frame, but in this work it is not exploited.
- *Network Frame Payload* contains the inherited packet from the APP layer. The field size is equal to the inherited field size. In the beacon packet format, this field does not exist.

5.6.3 Implementation of the Random Direction Mobility Model

The random direction mobility model is implemented in OPNET in order to have a homogenous node distribution in the simulation area. As described in Chapter 4.2.2, this mobility model forces nodes to move to the simulation boundary and stop there for a while before a new movement is randomly chosen.

The implemented model is based on the available random waypoint mobility model in OPNET. Assuming a square simulation area shown in Figure 5.10, where the size is defined by length *dx* and width *dy* a node can only move inside the area which is limited to the defined boundary. During the initial state of the random angle seletion, a node that does not appear at the simulation boundary can choose any arbitrary direction in the range [0..360 degrees]. This range is shown as a darker circle. After the first movement and stop time, a node must choose a new direction which is now selected according to the defined rules in every case. The darker areas show the possible random angle range when a node is facing one of the walls or is at one of the four possible corners in this area.

Examples of node movement in the Random Direction mobility model are shown in Figure 5.11. The node is in the bounded simulation area, at the point defined by the four location parameters: dx_l, dx_r, dy_d and dy_u as shown in the figure. These parameters are related by following formulas:

$$dx_l + dx_r = dx,$$

$$dy_u + dy_d = dy.$$

Location variables change when the node moves. Mobility direction is shown as arrow directed by an angle α from the normal line pointing to the north. This angle is selected randomly from a normal distribution depending on the range of random angle selection, as discussed before:

$$\alpha = a + rand(b - a). \tag{5.4}$$

Here *a* and *b* define the range of the random angle selection [*a..b*]. In Figure 5.11a the first selected angle is in the III quarter (180..270 degrees). It is necessary to calculate the new location [*x*, *y*] at the simulation border where the movement direction from the initial location [x_0 , y_0] reaches the border. It can be calculated like this

$$x = x_0 - dx_l, \tag{5.5}$$

$$y = y_0 - x \tan(\alpha - 1.5\pi). \tag{5.6}$$

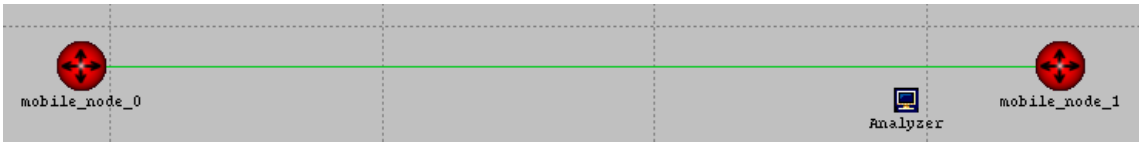

Figure 5.12: Simulation Testbed. Separating distance 100 m

The next location must be calculated in order to calculate the time *t* of movement till the node hits the simulation boundary when node moves with speed *v:*

$$t = \frac{\sqrt{(x-x_0)^2+(y-y_0)^2}}{v}. \tag{5.7}$$

The next cycles are performed in a similar way. When node appears at the corner, the procedure is simplified.

5.6.4 Investigation of the Radio Model

The investigation of the standard radio model in OPNET consists of simulation and verification with mathematical computations. It is possible to describe a very simple mathematical approximation of a radio propagation in the free space. The radio model in the OPNET simulator has a complex structure of a radio tranceiver pipeline which includes 14 intermediate calculation steps, such as transmission delay, link closure, channel matching, gain, noise, interference, error calculations, SNR and error correction.

A simple testbed is shown in Figure 5.12. Two wireless sensor nodes are placed 100 m apart. They operate as sinks and both transmit beacons in 0.03 s intervals. The mobile node 0 approaches the mobile node 1 with a constant speed. Simulation results with different scope parameters are shown in the Table 5.1. It can be noticed that at higher velocities, the transmission range is more limited. The packet size also has an influence on the communication range. Large data packets are more susceptible for data corruption, hence it is necessary to keep the small size of a beacon packet.

The Received Signal Strength Indicator (RSSI) value shows the average power of a received data packet. Normally, the numerical value is small, so it is more convenient to convert it to a logarithmic scale and express it in decibels (dB) or decibel Watt (dBW) compared to 1 W of transmit power signal strength.

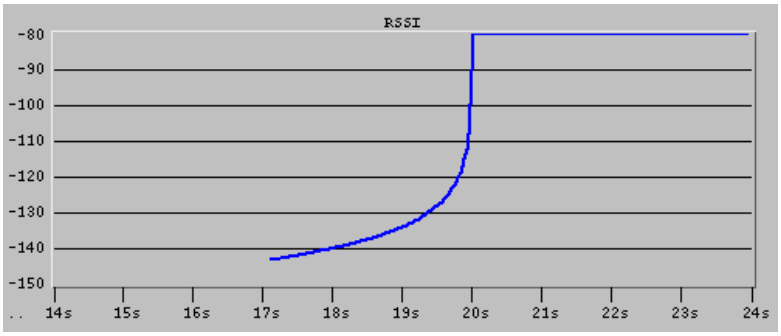

Figure 5.13: RSSI dependence on distance between nodes. Packet size 2000 bits, speed 5 m/s

Min. mean RSSI, dB	Distance, m	Packet size, bits	Node Speed, m/s
-146.75	21.6	230	0.1
-144.57	16.83	1000	0.1
-144.4	16.49	2000	0.1
-146.26	20.44	230	1.0
-144	15.75	1000	1.0
-144	15.75	2000	1.0
-145.22	18.15	230	5.0
-143.28	14.5	1000	5.0
-143.28	14.45	2000	5.0

Table 5.1: Radio model analysis. Simulation results. TX Power 1E-8 W (-80 dB)

Figure 5.13 shows the dependence of RSSI on the separating distance between sensor nodes. Communication between two sensor nodes starts after approximately 17 s when RSSI reaches the minimum value. Above this limit, communication is possible. In this case, it is approximately -143 dB.

In the Network layer, the RSSI threshold value is included. The ORMMA-WSN protocol can exploit this value when a decision about the best neighbor node is performed. This threshold can help to avoid a packet loss, not transmitting a packet when the probability of successful reception is low due to low RSSI.

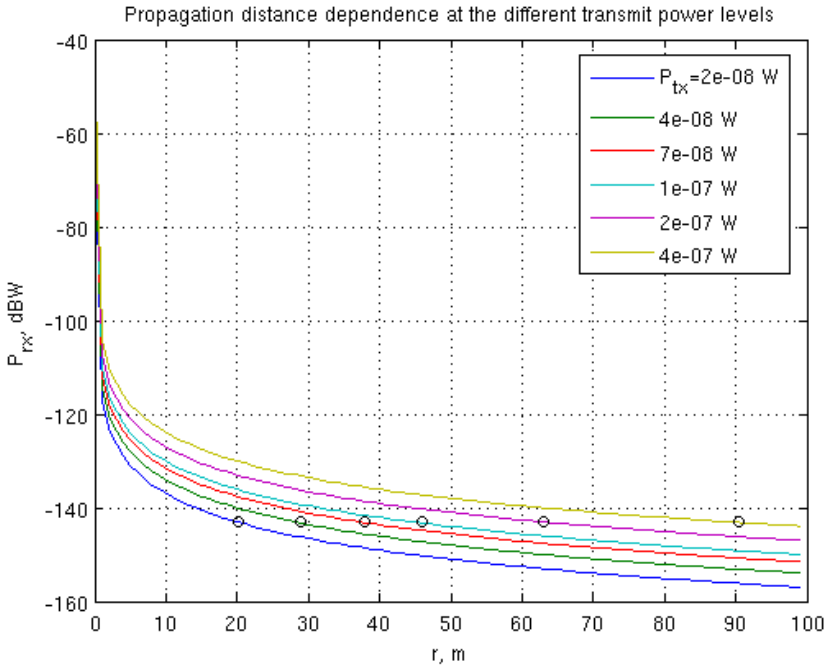

Figure 5.14: Propagation distance dependence at different transmit power levels

The transmitter power can be controlled. The communication distance is measured at the different power levels as shown in Table 5.2. The average minimum RSSI of the received packets is around -143 dB value. This value can be used as the default threshold in the simulation setup.

TX Power, W	Distance, m	min_RSSI, dB
2e-08	20.25	-143.16
4e-08	28.9	-143.26
7e-08	37.9	-143.18
1e-07	46	-143.2
2e-07	63	-143
4e-07	90.4	-143.16

Table 5.2: Transmission range at different TX power levels

The radio model exploits a free space radio signal propagation. The received signal strength P_{rx} depends on transmitter power P_{tx}, propagation distance *r,* wavelength λ and antenna gains. If the antenna gain is not used (i.e. equal to 1), the received power can be calculated as follows:

$$P_{rx} = P_{tx} \left(\frac{\lambda}{4\pi\, r} \right)^2 . \tag{5.8}$$

A comparison of measured (see Table 5.2) and calculated radio propagation signals is shown in Figure 5.14. It can be noticed that calculated propagation distance at the *min_RSSI* level (circle points) of each graph is approximately the same as the measured propagation distance, given in table. Hence, the transmitter power in OPNET can be calculated directly from (5.8) for the required distance *r*.

5.6.5 TX Power Control

The TX power is controlled in the MAC layer. A high power signal is used only for sink beacon packets. In the current version of the implemented model, the *Reserved* field in the MAC packet format is used for indicating the requested TX power ratio (1 - for normal mode, 2 - double power, etc.) to the PHY layer, not the absolute power value. The TX power multiplier value is defined in the node model and is assigned to every node during the simulation initialization step. The implemented functions in the MAC layer separates sink beacon packets and set the *Reserved* field to the multiplier value. This field in only 3 bits long, hence [1..7] multiplier values are allowed. This TX power value can be the same for all nodes or it can be different for each node.

The implemented TX power control is not adaptive. The opportunistic routing is not taking into account the dynamic TX power control according to the RSSI, mobility or neighborhood information. This feature can be considered as a research task for future extensions.

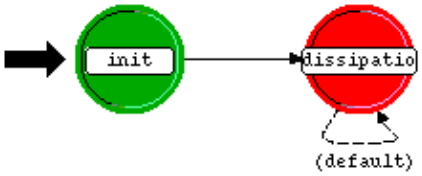

Figure 5.15: Battery process model

5.6.6 Battery Model

Power consumption is one of the most important metrics in wireless sensor networks. A nice work on the advanced analysis of the energy consumption is done in [24].

The Battery model is used for the collection of statistics about energy consumption by the wireless sensor node. This model is taken from the available Open-ZB model in [21]. Its state process model is rather simple (see Figure 5.15). After initialization, the power dissipation procedure is called. An ICI interface is used in order to provide the information about the transmitted and received packets. Packet length and flow direction are used in order to calculate the amount of energy used.

The power consumption parameters are chosen from the MICAz mote specification. In Figure 5.16, the battery model parameters are shown. It is possible to set the required energy levels of Receiving Mode, Transmission Mode, Idle state and sleep mode power consumption. The amount of initial energy is set in Joules or corresponding to the standard capacity of alkaline or rechargeable batteries.

In the model covered by this work, only transmission and reception modes are used. Uncoordinated MAC sleeping structure still has to be implemented. This feature can also be considered as future work.

5.6.7 MAC Layer

The MAC layer state process model diagram is shown in Figure 5.17. The main part of this model includes the implementation of the unslotted CSMA/CA algorithm, which is described in Chapter 3.3.2. This algorithm is responsible for the packet transmission and retransmission. When a packet comes from the NET layer, it is placed in the packet

Battery	
Current Draw	(...)
Receive Mode (mA)	MICAz default
Transmission Mode (mA)	MICAz (0 dBm)
Idle Mode (µA)	MICAz default
Sleep Mode (µA)	MICAz default
Initial Energy	200
Power Supply	2 AA Batteries (3V)

Figure 5.16: Battery model parameters

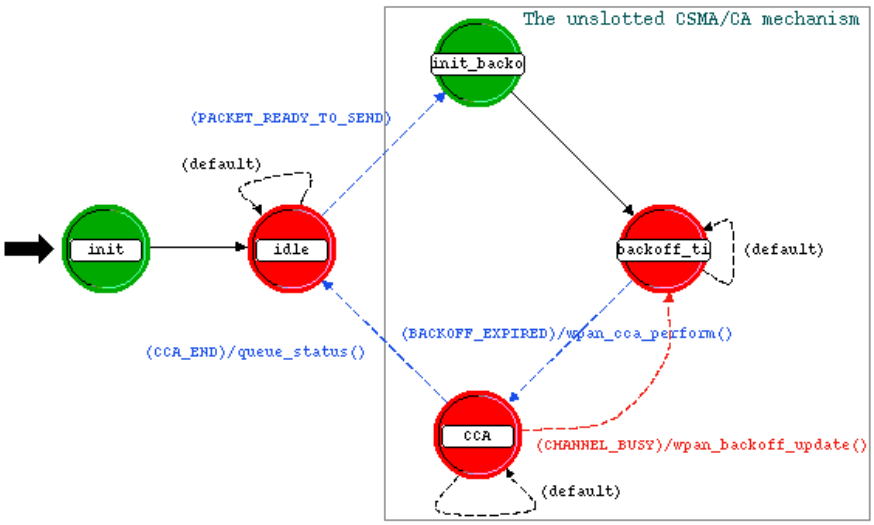

Figure 5.17: MAC process model

queue with FIFO scheduling. When the queue is not empty, the *PACKET_READY_TO_SEND* flag allows the change of state from idle to initialization of a backoff timer. A node waits for a random period of time before it can start the Clear Channel Assessment (CCA) procedure. When the backoff timer expires, the CCA is started. The channel is checked for idleness via the *rx_busy* statistic wire in the node model. If during the CCA, the channel was busy, the backoff procedure is repeated by going back to the *backoff_timer* state and the timer is again updated by selecting a new random period. The *CCA_END* flag is true in the following cases:

- transmission failure,
- transmission successful when sending unacknowledged packet,
- successful reception of an ACK packet,
- failure of waiting for ACK packet,
- number of backoff periods reaches the maximum number of backoff retries.

When a transmission failure or an ACK reception failure occurs, the packet is dropped, i.e. it is removed from the waiting queue at the MAC layer. The indication of this failure is sent to the NET layer via the ICI interface: value of NAK (0). If the acknowledged transmission is successful, the value of ACK (1) is indicated to the NET layer. The routing buffer at the NET layer removes the waiting packet if the ACK value is received.

When a packet is received from the PHY layer, MAC starts packet filtering. If the destination MAC address is equal to the receiving node's MAC address or it is the broadcasting address (0xFFFF), the packet is accepted for further processing, otherwise it is dropped.

Sink beacon packets are sent without CSMA/CA. With CSMA/CA, they would cause a high collision ratio, because in case of a collision, the packet must be retransmitted N times. Node beacon forwarding packets are sent with normal power with unslotted CSMA/CA. ACK packets are sent instantanously without CSMA/CA when an ACK requiring packet is received.

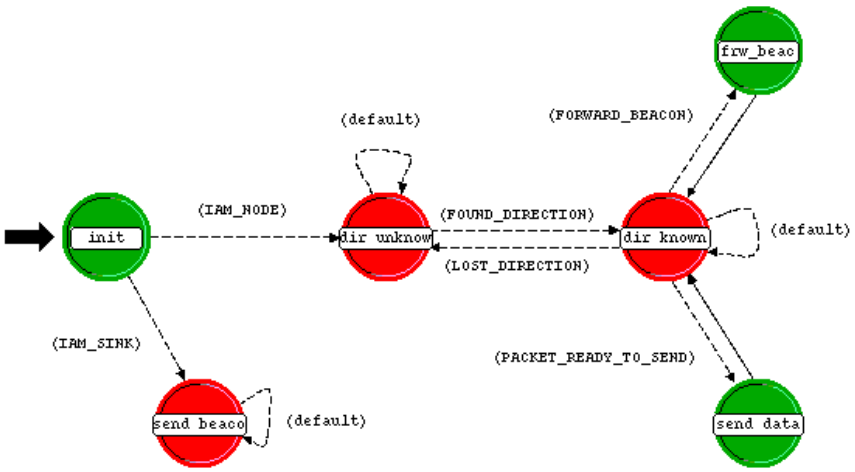

Figure 5.18: Network process model

5.6.8 Network Layer

The NET layer state process model is shown in Figure 5.18. Two node types are sharing the same process model. If the network protocol is run on the sink node, the *IAM_SINK* flag is enabled and the node enters the beacon transmission state. It will remain in this state until the end of simulation. A sensor node employs more complex network state model. The algorithm recognizes a sensor node by the *IAM_NODE* flag. After initialization, a sensor node is in the state that the mobility direction is unknown. In this state a node waits for a number of beacon signals, while it can obtain its mobility information.

The mobility information is calculated according to the mobility gradient (MG) of a node. When a direction is obtained, the process steps into the *direction_known* state, where forwarding of beacon packets and transmission of data or packet routing can be allowed.

Beacon forwarding is a forced state, because the mobility information of a node has higher priority over the data packets. Beacon forwarding can either be controlled by the synchronization to sink beacon signals or the random beacon forwarding can be performed. These two techniques are described in the last two subchapters of the current chapter.

When a beacon from a new sink is received, this sink is listed in the sink table. The sink expiration timer is started with the *SINK_EXPIRATION_TIME* value. This value is equal to the Beacon Interval (BI) by default and can be varied. A sink table example is shown in Figure 5.19. The sink node is characterized by the sink MAC address (*Addr*), mobility gradient (MG) relative to the sink, Beacon Count (BC) value, RSSI indicating

```
[NET: n_2, t= 29.100748] TABLE CONTENTS:

        [Addr:100, MG:-1, BC:25, RSSI:-123.169634, Time:29.000732]
        [Addr:101, MG:-1, BC:25, RSSI:-140.263621, Time:29.005716]
        [Addr:102, MG:1, BC:3, RSSI:-141.411401, Time:29.010732]
```

Figure 5.19: Example of a sink node table

the distance from the sink and the beacon reception time for the expiration timer. Sinks are sorted by the RSSI value. The best sink is the closest sink.
When a forwarded beacon is received, the extracted infomation about the transmitting neighbor node is filled in the neighbor node table, shown in Figure 5.20. A neighbor node expires after the *NEIGHBOR_NODE_EXPIRATION_TIME* if within this period no further forwarded beacons are received from that node. The node is then deleted from the table.

```
NODE NEIGHBOR TABLE:
[NET: n_2, t= 29.112477] TABLE CONTENTS:

       [Addr:1, MG:1, RSSI:-130.573563, Time:28.085703]
       [Addr:5, MG:1, RSSI:-141.227128, Time:28.112303]
```

Figure 5.20: Example of a node neighbor table

As mentioned before, a sink receives the forwarded beacons from neighbor nodes and constructs a table of node addresses that appear in the communication range of the sink. This table is transmitted within a next beacon header. Table elements expire in the same manner as in the neighbor node table.

```
[NET: n_2, t= 29.141149] N-HOOD update: NODE STATE CONTENTS:

       [(Best Sink:102, range:1), MG:1, RSSI:-141.411401, dir_known:1, (Best NN:102, range:1)]
```

Figure 5.21: Neighborhood status information example

Now it is possible to construct the neighborhood status summary. In the Figure 5.21, an example of neighborhood status information of a sensor node is presented. It contains the parameters that characterize the neighborhood: the best sink node address and appearance in that sink range, MG, RSSI and information about the Best Neighbor Node (BNN) and the appearance of that node in its sink range.

The best neighbor node (BNN) is elected according to the MG and RSSI values in the following cases:

- Source node *MG=1* or no NN: source keeps a packet.
- Source node *MG=0* or *MG=-1 and* neighbor node *MG=1*: neighbor node is BNN, source routes packets to this BNN.
- Source node *MG=-1 and* neighbor node *MG=0 and* $RSSI_{nn} > RSSI_{src}$: this NN is the BNN. Routing of packets to the BNN.
- Source node *MG=-1 and* neighbor node *MG=-1 and* neighbor node is in sink range: this NN is BNN, routing of packets to the BNN.
- Source node and NN are in sink range *and* $RSSI_{nn} > RSSI_{src}$: NN is the BNN, routing of packets to the BNN.
- Source node and NN are in sink range *and* $RSSI_{nn} < RSSI_{src}$: source node sends packets directly to the sink node.

Mobility and neighborhood status information are updated periodically. If a link failure is indicated by the MAC layer, the current BNN is removed and a new one is selected if there are available candidates in the NN table.

Data packets are put into a routing buffer (queue). Data packets generated by the APP layer and received from the neighborhood compete in the FIFO manner. Priorities can

be applied for routing packets.

In the network process model (see Figure 5.18), the *send_data* state is occupied when the routing buffer is not empty and the BNN is known. A sensor node prepares a data packet, sets the destination address over ICI coupled with the sendable packet. The buffer managing function sends the packet to the MAC layer for transmission and waits for an ACK or NAK.

Each routing hop node increases the Hop Count value in the packet header. This value represents the route length when the packet arrives at a sink node. The maximum packet lifetime value, which defines the maximum route length is called Time To Live (TTL) interval. It is the maximum number of routing hops allowed for each data packet. If a packet cannot reach a sink by this length, it must be dropped in order to avoid long packet loops. If these dropped packets are indicated to the source node, the retransmission of the dropped data packets can be done by the source node according to the importance of the lost data. A sink node can indicate the successfully received data packets by including the *ACK Table* in the beacon header containing source addresses and the sequence numbers of the received source nodes (see Figure 5.9). The end-to-end packet acknowledgments are not implemented in this work.

Sequence numbers are assigned to every data packet at the NET layer. The *Sequence Number* field in the network packet header has a length of 8-bits. The first generated data packet is assigned to 0 value and all subsequent packets get a sequence number which is increased by 1. When a maximum of 256 is exceeded, counting is started from 0 again.

Data packets require an ACK to be transmitted by the receiving end, which indicates the successful transmission. In the case when a data packet is received successfully but the ACK packet is lost, the source node will retransmit the same packet. The probability of duplicate packet reception is therefore high in mobile networks. There exist two ways of duplicate packet filtering. The first is an ACK of ACK packets in IEEE 802.15.4 MAC layer. This way is not efficient because it is necessary to drop the successfully received packet if the ACK to the ACK is not received. Also, an additional overhead of total network output load is expected. ACK packets are sent without CSMA/CA, hence the probability of collision occurrence is also higher.

The second way is implemented in the opportunistic routing model. Sequence numbers in the NET layer help to distinguish which packet is a duplicate. When a data packet is received from a new neighbor node, the source address and sequence number of this packet is written to the *Sequence Number Check* table on the NET level. If a new data packet (different sequence number) is received from the same neighbor node, information about source address and sequence number in the table are updated. In case, when a duplicated packet is received, the previous and current sequence numbers coincide and the data packet must be destroyed. Without this technique, the opportunistic routing model would provide wrong results.

5.6.9 Communication Model

The communication model represents the data packet flow procedure in the communication stack. The APP layer generates a data packet. The NET layer places it into the packet routing buffer (FIFO scheduling) until data packet transmission is

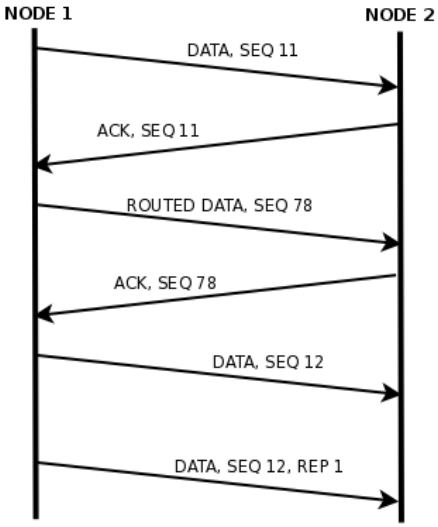

Figure 5.22: Communication flow of data packets

available (*PACKET_READY_TO_SEND* flag). When allowed, the packet is sent to the MAC layer and transmitted with unslotted CSMA/CA. The waiting for the ACK is started. If the ACK is not received, the transmission is repeated N times in the MAC layer. If there is still no ACK, the packet is dropped and NAK is indicated to the NET layer. If the ACK is received, an ACK over ICI is indicated to the NET layer and the current packets are removed from both the MAC packet queue and the NET routing queue. This procedure is performed by a Stop-And-Wait algorithm.

An example of a communication flow of a data packets is shown in Figure 5.22. Every data packet must be acknowledged. The ACK packet must contain the sequence number of the sent packet. Node 1 transmits the data packet with Sequence Number (SEQ) equal to 11 to node 2. An ACK packet with SEQ 11 is received. The current packet is removed. The next packet in the routing queue is a packet received from a neighbor node. Routing of data is started and the MAC assigns SEQ 78. An ACK is received and so on. If a data packet is sent and the ACK is lost, the packet is retransmitted with the same SEQ.

5.6.10 Synchronization to the Sink Beacon Signals

The multiple sink scenario with periodic sink beacon signals requires a synchronization approach. The beacon signal is sent with higher power, hence reaching a broader area. When nodes are not synchronized to the beacon signal (not waiting for it), this causes packet collisions and loss of data. The beacon-enabled mode is described in the IEEE 802.15.4 standard (see Chapter 3) and is suitable only for single sink scenarios.

The proposed technique is shown in Figure 5.23. In this figure, it can be noticed that three sinks *S1*, *S2* and *S3* are sending beacons. Beacons are periodic with a Beacon Period (BP), which can differ from sink to sink. Data is allowed to be transmitted during the inter beacon intervals, so called Beacon Inter Frame Spacing intervals (BIFS). The beacon period is calculated from two consequent beacons received from each sink. When one or more beacons are lost due to the low SNR, bad channel conditions, etc., it

is possible to keep the synchronization valid for some intervals. In this way synchronization is not lost. The number of allowed lost beacons is called maximum beacon recovery interval. It can be variable, but preferable value for high mobility scenarios is 2 or less.

The first step of the synchronization algorithm is to obtain the beacon period information of every available sink and to adjust schedulers to these intervals and restrict data transmission during beacon validity time.

When the first beacon of the sink *S1* is received, the beacon reception time t_{S_1} is notified and the time to the next beacon is counted. The difference of reception times is equal to the beacon period. Beacon Period of sink *S1* is calculated as follows:

$$t_{BP_1} = t_{S_1}(b) - t_{S_1}(b-1)\,, \tag{5.9}$$

where *b* is a beacon number.

When the second beacon of the sink *S1* is received, the next start time of the Contention Free Period (CFP) without data transmission for sink *S1* can be scheduled:

$$t_{CFP} = t_{S_1}(2) + t_{BP_1}\,.$$

When multiple sink beacons are received, the next CFP must be adjusted on the fly. In Figure 5.23 it can be noticed that during the *BP1,* two new beacon signals are received. The same procedure as described above is repeated. When more than one beacon period intervals are known, it is necessary to follow the nearest contention free interval timing values.

The next contention free period for beacon reception from different sinks can be obtained in general from the following formula:

$$t_{next\,CFP} = t_{S_n}(b) + t_{BP_n}\,. \tag{5.9}$$

The algorithm must check if there is enough time to finish the data transmission before the end of data transmission time slot. It always verifies the requested transmission time with the least time left till the next CFP.

5.6.11 Random Beacon Forwarding

Simultaneous beacon forwarding causes high collision rates. All nodes that appear in a sink range receive a sink beacon and try to forward it. Theoretically, CSMA/CA should

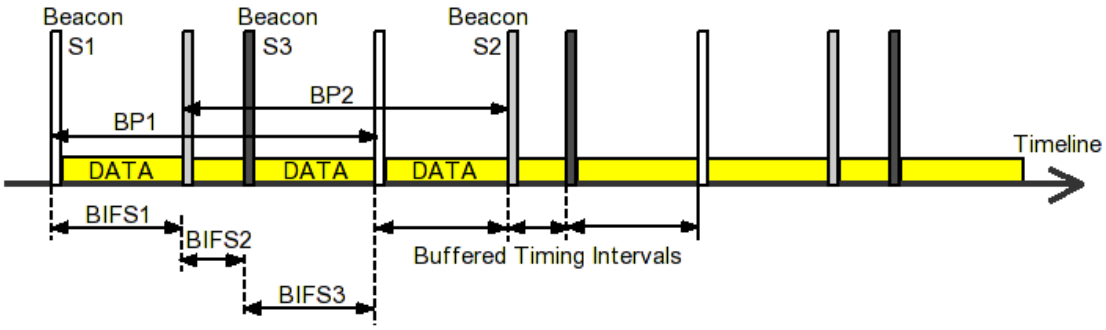

Figure 5.23: Time line of synchronization to beacon signals

avoid collisions. The problem is the random number generator used here. The variance of the random output values is small. This frequently causes the election of the same random backoff intervals in the MAC layer. It means that several nodes will start a beacon forwarding at the same time. On the other hand, when multiple beacons from different sinks arrive in close intervals, it causes a redundant beacon forwarding. This will lead to even greater collision ratios.

A Beacon Forwarding Delay is used in the NET process model. When the beacon forwarding state is entered, the next beacon forwarding time is scheduled by this formula:

$$t_{forward} = t_{simulation} + t_{wait\ beacon} + rand(0.1) \cdot \tag{5.10}$$

Here, the next forwarding time is delayed by the beacon waiting time $t_{wait\,beacon}$ which is the period for collecting several beacons that arrive in close intervals and a random value from a normal distribution. By default this value in (5.10) is chosen as 0.1, although it depends on BP and can be varied.

The results of a random beacon forwarding are shown in Figure 5.24. In the first graph the simultaneous beacon forwarding causes a collision ratio of 20.6%, which is a disadvantageous value. When a random beacon forwarding delay is added, the collision ratio is drastically reduced to 0.81% (see the second graph). Finally, the waiting beacon delay of 0.05 s, equal to the inter-beacon interval, is introduced next to the random waiting time, and the collision is additionally reduced to 0.48% (see the third graph).

The Random Beacon Forwarding technique gives the possibility to reduce the collision ratio to an acceptable level <1%. The algorithm has a simple structure, no additional coordination is necessary.

5.7 AODV Comparison Model

The results of the implemented ORMMA-WSN routing algorithm are to be compared with one of the well known available algorithms. An AODV routing model is implemented in OPNET and is provided with the MANET mobile station. The node model structure is shown in Figure 5.25. AODV is based on the IP routing protocol and employs the WLAN MAC layer.

In order to compare it with ORMMA-WSN, the MAC layers of both the MANET station and the wireless sensor node must be the same. For this reason, PHY and IEEE 802.15.4 MAC with unslotted CSMA/CA layers are attached at the bottom of the *arp* module. The new structure of the modified MANET station is shown in Figure 5.26. The programming structure of control and data channels between layers is similar to the structure described in the previous chapter. All data packets are generated at the traffic source module (*traf_scr*). The AODV protocol tries to find the the best routing path. The IP layer manages the whole communication cycle. The AODV principles are described in [25] and are out of the scope of this work.

The AODV protocol can only work in single sink scenarios. In order to make these two models comparable, a single sink scenario for ORMMA-WSN model must be applied too. However, the performance evaluation of the opportunistic routing model should include multiple sinks to show the advantages.

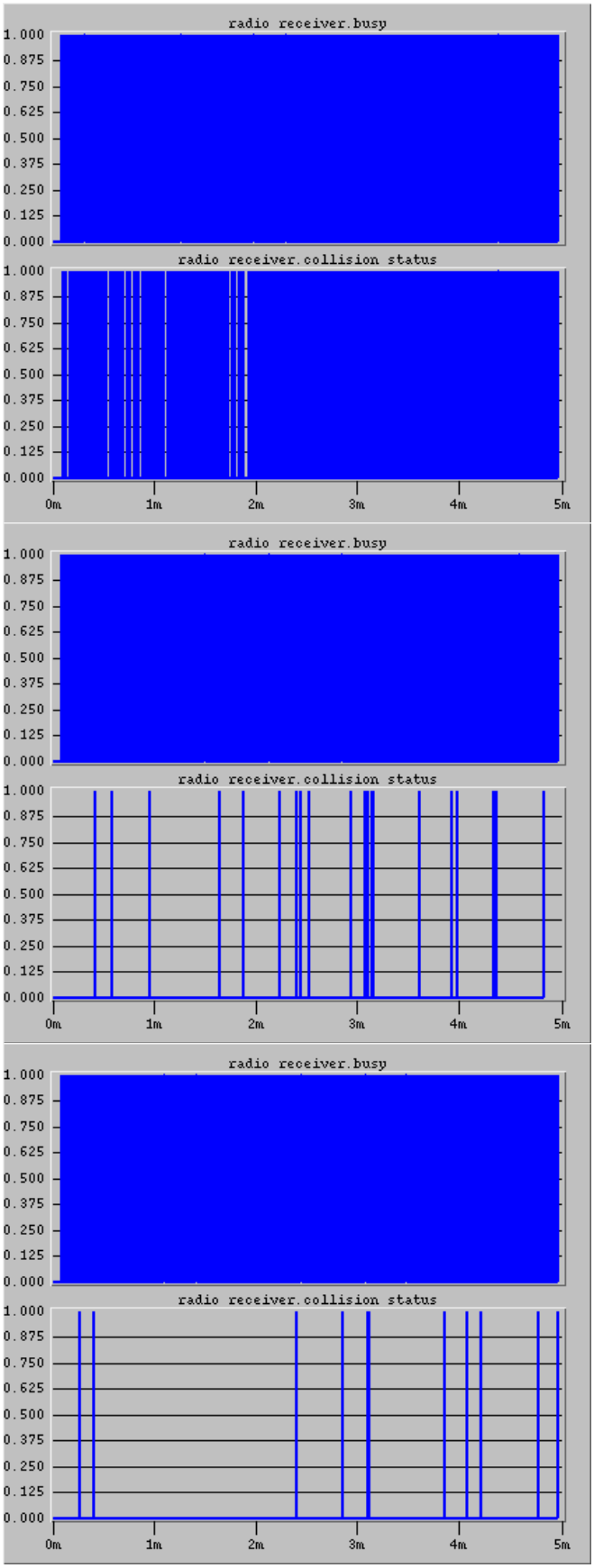

Figure 5.24: Reduced collisions by Random Beacon Forwarding. 2 sink nodes, 6 sensor nodes, BI 1s, inter-beacon interval 0.05s

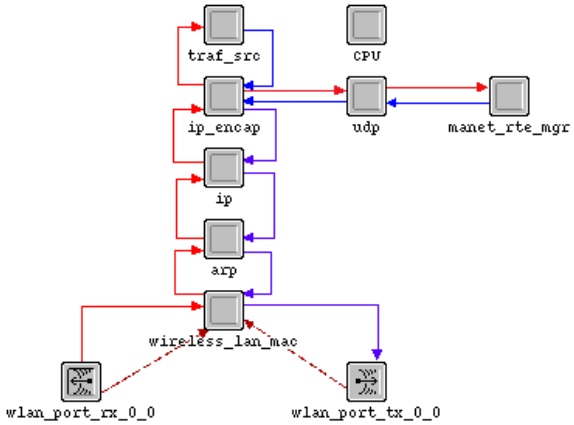

Figure 5.25: MANET node model structure

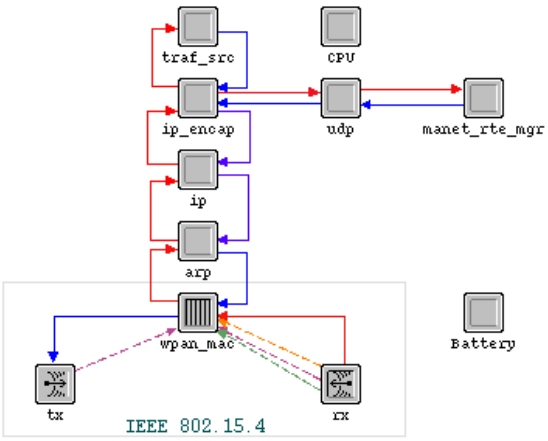

Figure 5.26: Modified MANET node model structure

The next chapter analyses the simulation of the described models in different scenarios and gives an evaluation of the obtained simulation results.

6. Evaluation of Opportunistic Routing Simulation Results

In the previous chapter, the simulation model of the ORMMA-WSN routing protocol was described. A simulation provides the possibility to evaluate the performance of the implemented model.

In this chapter, the ORMMA-WSN is simulated in two different scenarios. The first is used to present the node model operational example and performance statistics. The second provides the comparison of the ORMMA-WSN and AODV protocols. These two protocols are compared with respect to different statistic metrics, such as power consumption, end-to-end delays, route length, etc.

6.1 Multi-Sink Scenario Description

The purpose of the first scenario is to analyze the principles and performace of the ORMMA-WSN protocol. The simulation setup is modelled in OPNET and the layout is shown in Figure 6.1. As decribed in Chapter 5.4, the WSN network consists of mobile nodes. The number of sensor nodes (S) is larger than the number of sink nodes (greater icons). The network analyzer is placed in the middle for collection of the global network statistics. The communication coverages are shown as grey circles. The Beacon Range is represented by black circles with larger radius. The simulation area is limited to the square area. Nodes can move randomly, but only inside this area.

The sink nodes send periodic beacons. The nodes extract the mobility information from these beacons and start the transmission of personal information. Neighbor nodes obtain the forwarded personal information about their neighbors and build the neigborhood knowledge base. Then the data packets can be routed according to the acquired information.

Global and local statistics are collected during simulation runtime. Local statistics consist of process variable changes in every node, such as:

- Radio TX and RX business, idleness, collision occurance, packet loss ratio, bit error rates, etc.

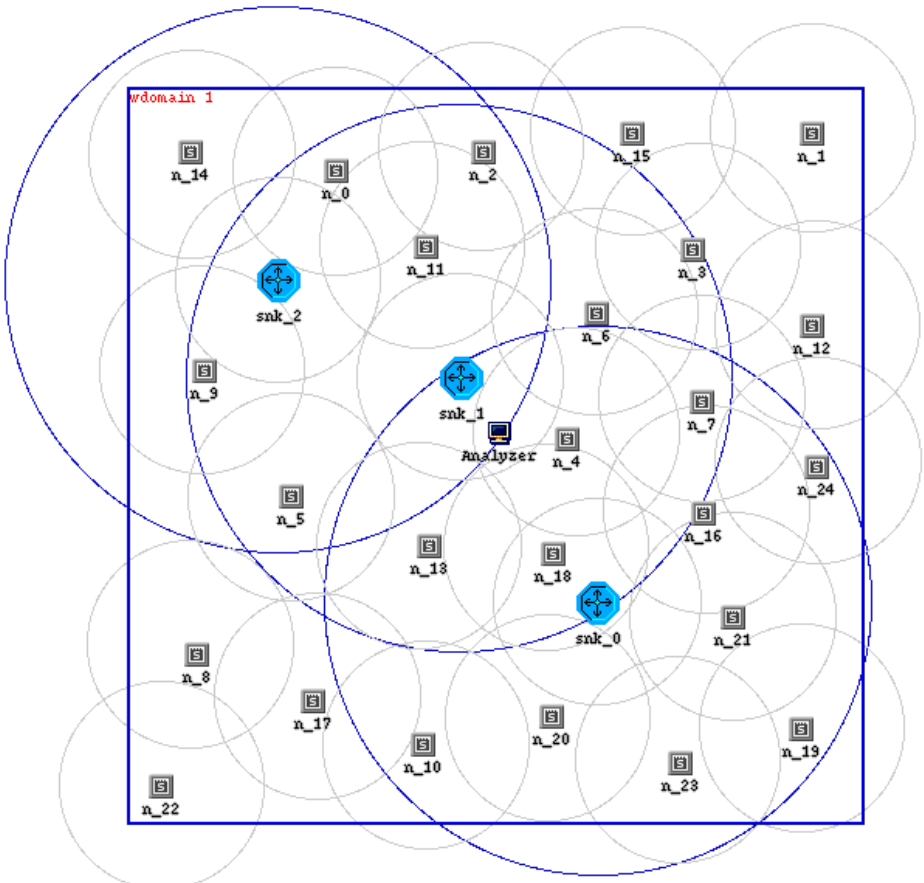

Figure 6.1: Simulation scenario layout

- CSMA, CCA, dropped packets, successful transmission, retransmission attempts, medium access delays, RSSI, queing delay and size.
- Mobility gradient, routing queue size, neighborhood availability, route length, TTL dropped packets.
- Data and beacon generator statistics.

The global statistics show the global network activity. Statistics that fall into this category:

- Packet delay, throughput, power consumption, routing length.
- Most of the local statistics can be collected globally.

6.2 Simulation Parameters

Simulation parameters of the described scenario (see Chapter 5.4 and 6.1) are presented in the following steps:

- Network inventor: 3 sinks, 25 nodes (all mobile), 1 analyzer.
- Simulation area: 100x100 m.
- TX power (node/sink comm. range):
  1E-08 W (14.038 m radius at -143 dBW),

4E-08 W (28.076 m radius at -143 dBW),
7E-08 W (37.141 m radius at -143 dBW).

- Sink beacon TX power:
  7E-08 W (37.141 m radius at -143 dBW),
  2.8E-07 W (74.281 m radius at -143 dBW),
  4.9E-07 W (98.265 m radius at -143 dBW).
- Mobility model: random direction, speed 1-5 m/s, pause at the borders 5-10 s.
- Beacon period (BP) 1s, packet size 0 bits, start time 1005 s.
- Inter-beacon arrival time: 0.05 s.
- Random Beacon Forwarding:
  Random delay: 0 - 0.1 s,
  Beacon waiting time: 0.05 s.
- Node *n_0* generates data traffic.
- Data packet inter-arrival time 5 s, packet size 256 bits, start time 1011.2 s.
- MAC address: manually assigned, 8 bit.
- No. of retransmissions N = 2, min. back-off exponent 3, max. back-off number 4.
- RSSI threshold: -143 dBW.
- Expiration timers:
  Sink entry expiration time: 1.2 s,
  Neighbor entry expiration time: 1.2s.
- Packet TTL: 35 hops.
- Simulation runtime: 3000 s (including mobility initialization of 1000 s).

6.3 Simulation Results

This subchapter provides the simulation results of the decribed scenario with the given setup parameters (see Chapter 6.2).

Mobile nodes move inside the bounded simulation area. The random direction mobility model enables the homogenous distribution of nodes as shown in Figure 6.2. Nodes visit each location with equal probability (uniform distribution of direction angle). After the initialization period of 1000 s, the number of nodes which are crossing the area becomes constant. Beacon and data generation start after the initialization period.

6.3.1 Network Global Statistic Results

This subchapter presents global statistic results of the simulated WSN network scenario:

- radio receiver business and collision status,
- network power consumption,
- dropped acknowledgment requiring packets during the simulation,
- total number of transmitted and received data packets,

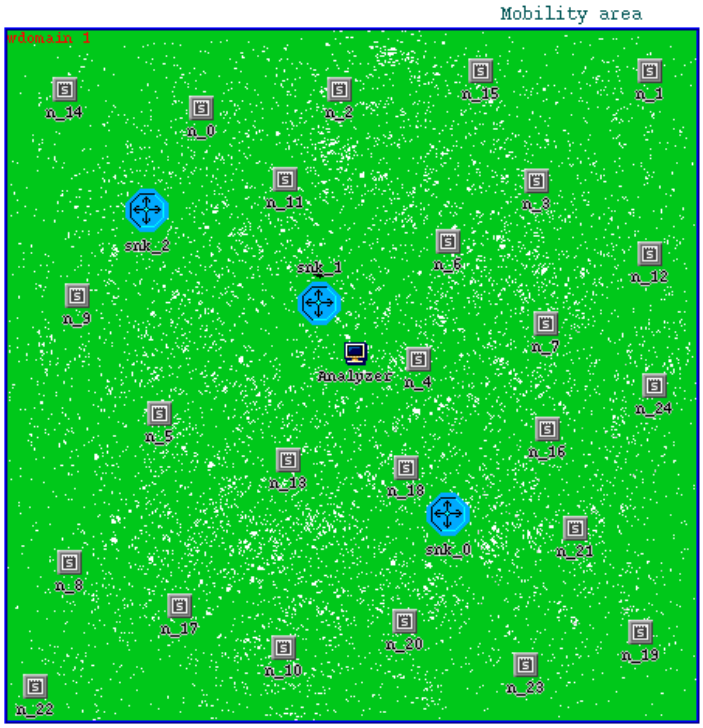

Figure 6.2: Node distribution density during the simulation

- throughput,
- end-to-end delay,
- network output load,
- routing length.

The random beacon forwarding technique helps to decrease the number of collisions. The global collision status is shown in Figure 6.3. The achieved collision ratio is 0.068%. The small value is possible in this case, because only one node is generating

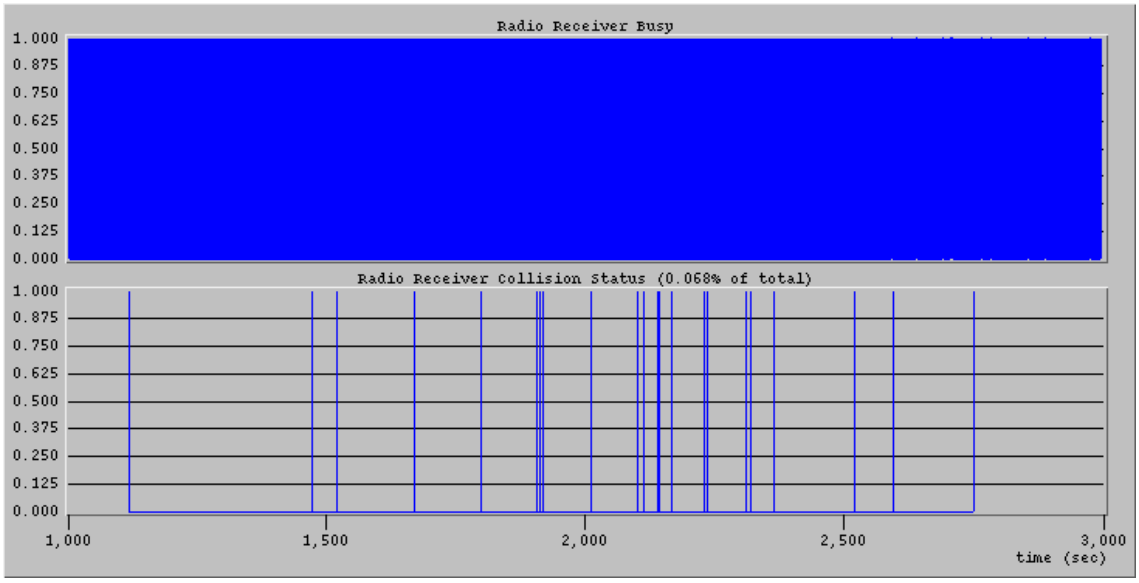

Figure 6.3: Global collision status

data packets. If all nodes would generate data packets simultaneously, the probability of collision would be larger.

The global power consumption by all nodes in the network is shown in Figure 6.4. The total amount of consumed energy is equal to 13.926 J. The proposed total amount of required energy for one year is 15768 J, including the calculation of radio transmission costs only, not the rest of the hardware power consumption, etc. An amount of 1.5507 J is consumed by 3 sink nodes. It takes 11.1% of total energy. In average, 3.55% of the energy is spent per sensor node. Nodes that participate in routing process consume more energy.

Even if a low collision ratio is possible, the loss of acknowledgment requiring transmission packets still can occur. The number of dropped acknowledged transmission packets during the simulation is shown in Figure 6.5. The dropping of packets occurs due to a low RSSI (SNR). It is the result of signal to noise and interference, also the hardware thermal noise which is enabled in the OPNET radio model. An amount of 3.45% of the total acknowledgment requiring transmission packets are lost due to transmission or ACK reception failures. In the network layer, no packet loss can occur. All packets are retransmitted until a successful transmission is reached. In order to avoid packet loops in the network, the TTL parameter is used. When the TTL is exceeded, the packet is dropped at the network level.

The total number of received packets during the simulation is shown in Figure 6.6. All packets reach one of the destination sink nodes with some delay. The generated traffic of data packets is constant.

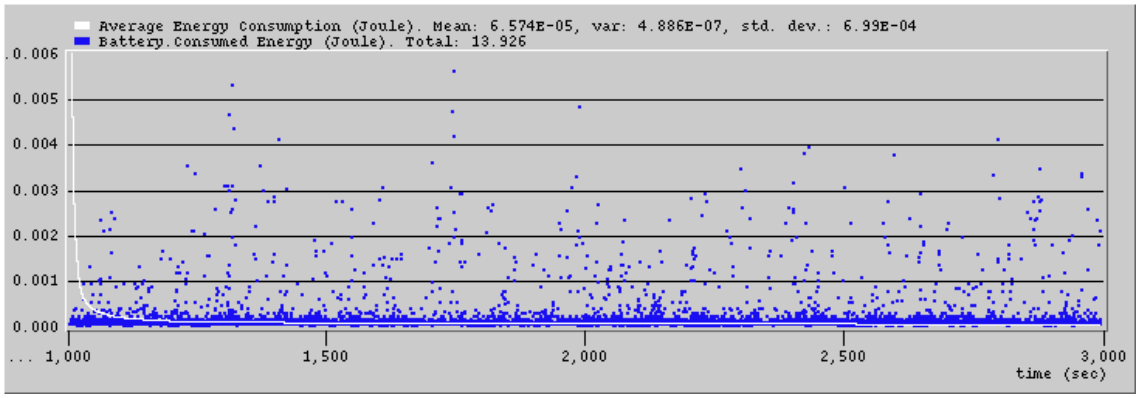

Figure 6.4: Global network power consumption

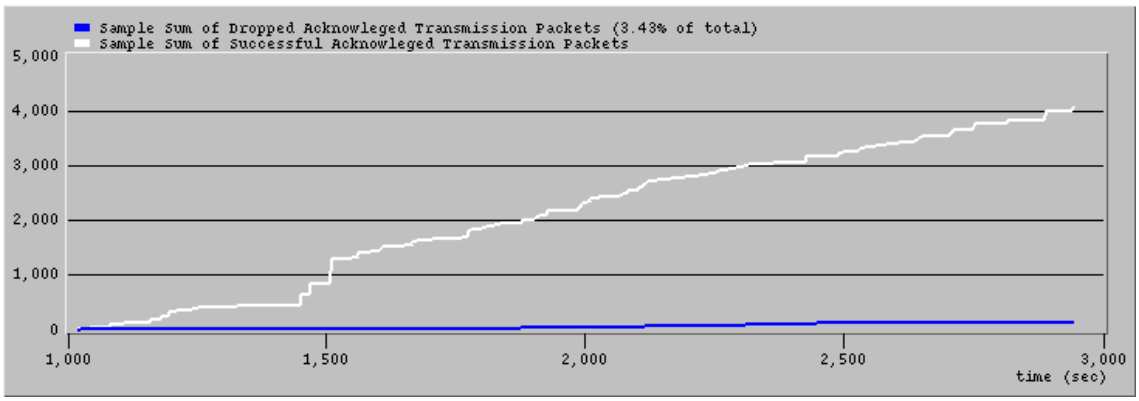

Figure 6.5: Dropped Acknowledged transmission packets

The goodput of acknowledged data transmission packets is shown in Figure 6.7. After a transient phase, the goodput reaches a constant level. The mean rate of the received traffic and the generated traffic rate (256 bit/s) must coincide. Due to the intermittent connectivity between nodes, data packets are routed to the destination nodes in compound amounts. This can be identified as fluctuations of the received rate.

When a generated data packet is transmitted, it starts travelling to the nearest destination node via multiple hops of intermittently connected nodes. Higher delays are expected in networks with lower mobility, longer pause times or short communication ranges. In Figure 6.8, the global end-to-end delay is shown. In this case, it is a node-to-sink end-

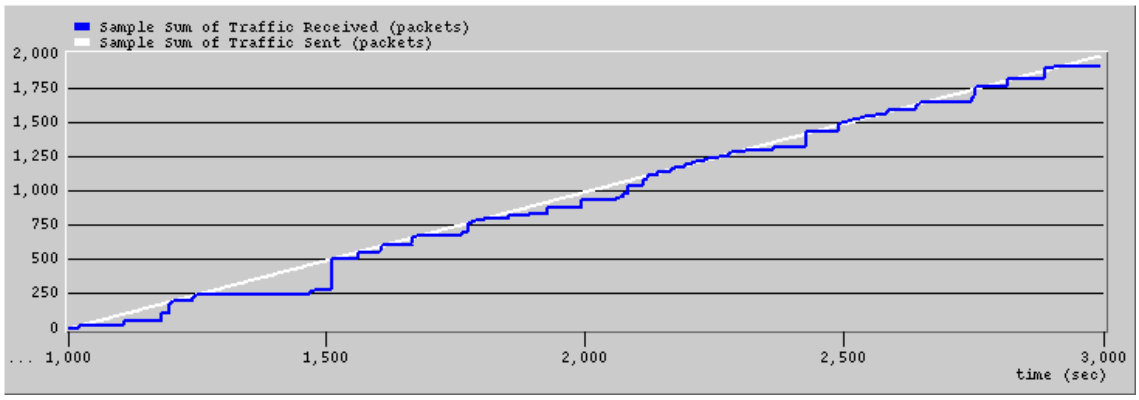

Figure 6.6: Total number of received packets

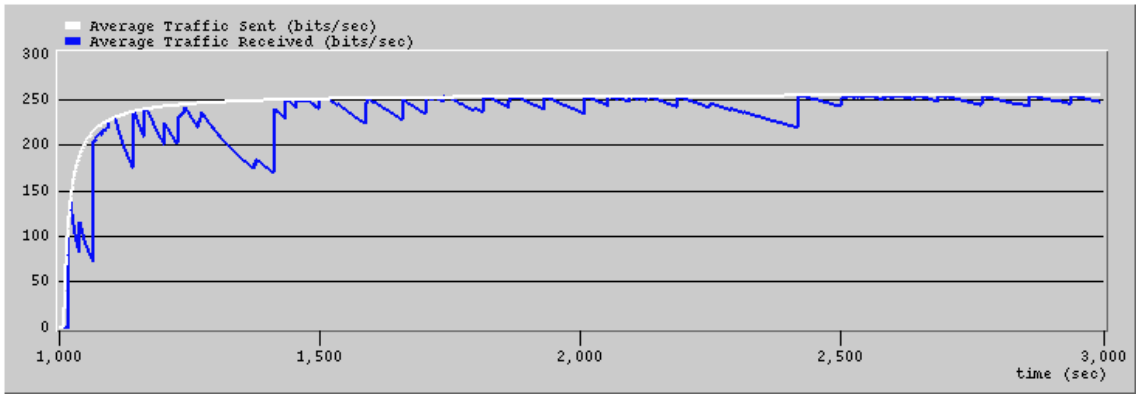

Figure 6.7: Goodput of ACKed pacets

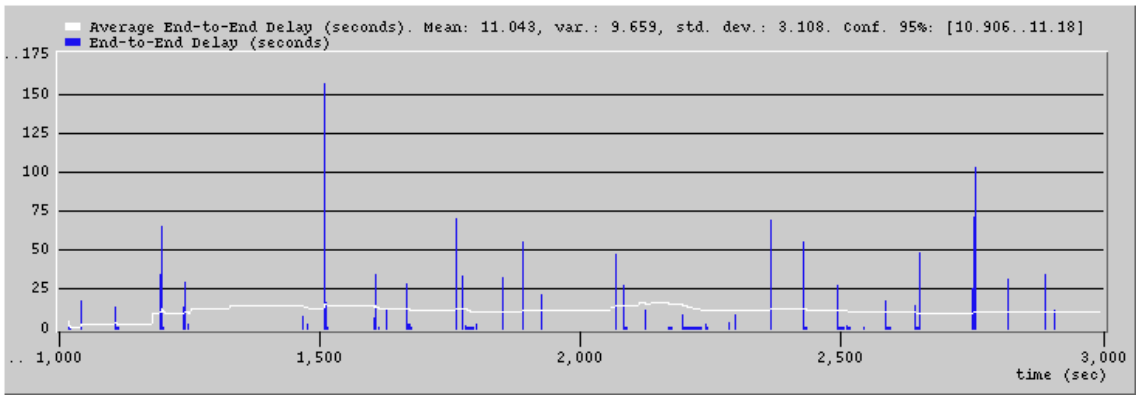

Figure 6.8: End-to-end delay

to-end delay, because only one node generates traffic. It can be noticed, that delays are relatively high. Comparing Figures 6.7 and 6.8 at 1500 s point, it can be seen that large delays decrease the thoughput. The average end-to-end delay is in the range of 11 s.

The total network output load is shown in Figure 6.9. Besides the data packets, the beacon packets are transmitted in the network. In average, 3.45 kbps of the total network traffic load is necessary to transmit the 256 bps of data traffic rate according to the network conditions, provided by the first scenario. For low throughput, a relatively large overhead network load can be identified from the obtained results.

An acknowledged transmission packet is sent in multiple hops until it reaches the destination node or the TTL number of hops is exceeded. The length which is travelled to the destination is called the routing length. The simulation results of the routing length of the given scenario are shown in Figure 6.10. Data packets travel from 1 to 7 hops. The routing length depends on the average nodes mobility between source and sink. The average route length is 2.207 hops. This length can be shortened by increasing the transmission range (TX power).

6.3.2 Node Statistic Results

The operation of a sensor or sink node can be analyzed with a help of node statistics. The following local statistic results are collected about the mobile node:

– RSSI,

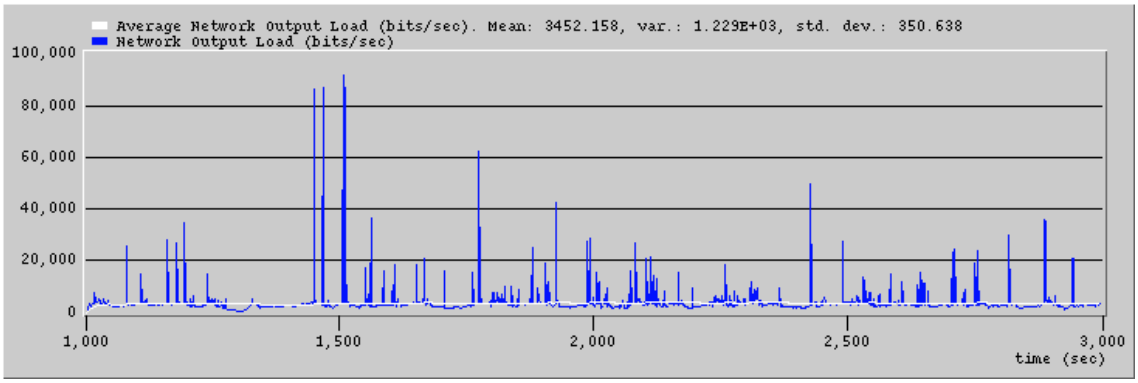

Figure 6.9: Network output load

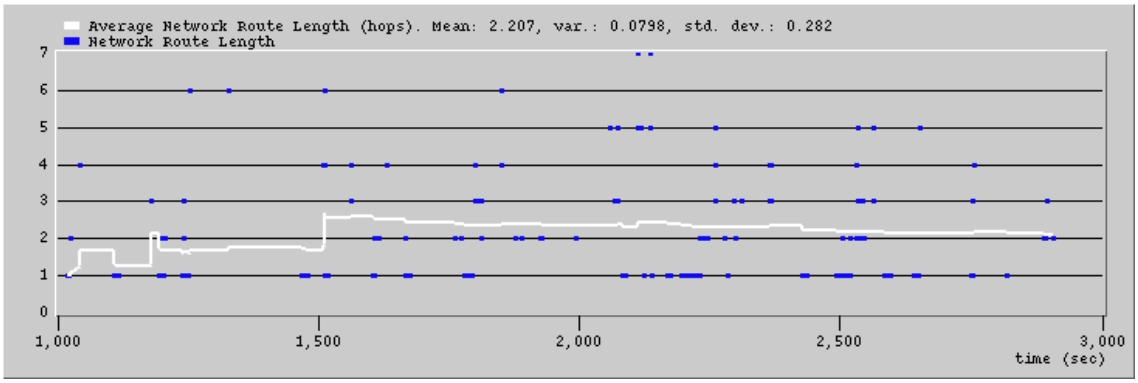

Figure 6.10: Routing length

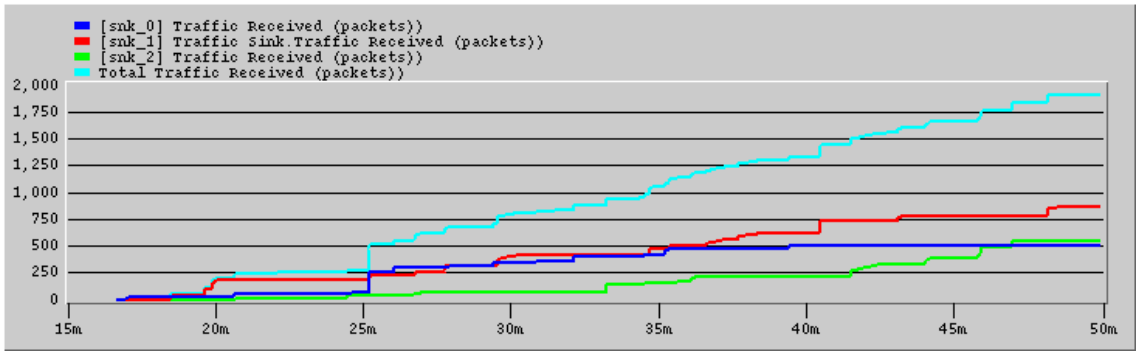

Figure 6.11: Received traffic by sink nodes

- mobility gradient,
- CSMA/CA statistics,
- best neighbor availability,
- routing queue size,
- consumed and remaining energy levels.

Energy consumption statistics of separate mobile nodes are listed in Table 6.1 (p. 69). The source node *n_0* generates packets and attempts to transmit the data. This node consumes the most energy. The sink node *snk_1* is the next most active node. This sink node receives the most of the data packets (see Figure 6.11).

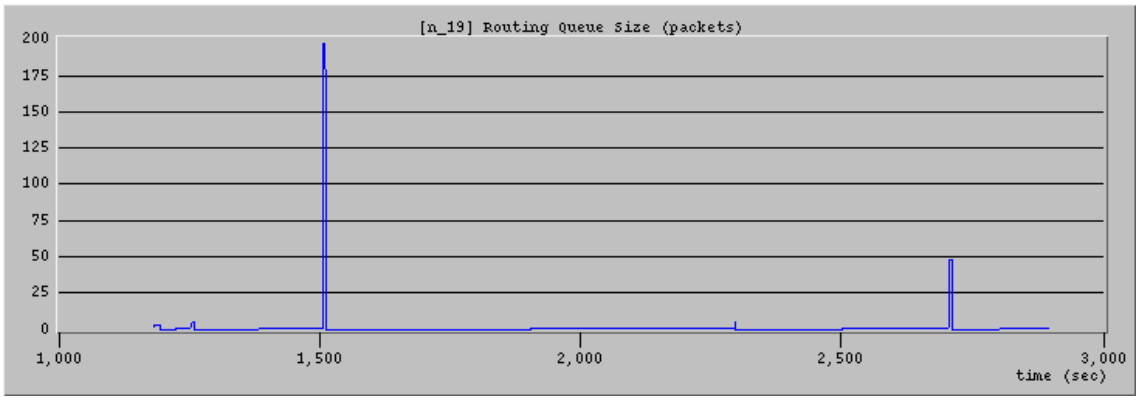

Figure 6.12: Routing queue size of node *n_19*

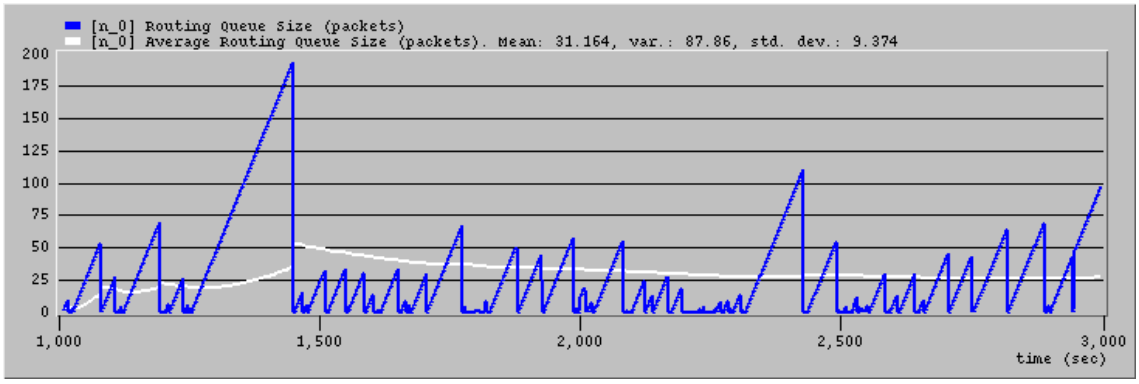

Figure 6.13: Routing queue size of node *n_0*

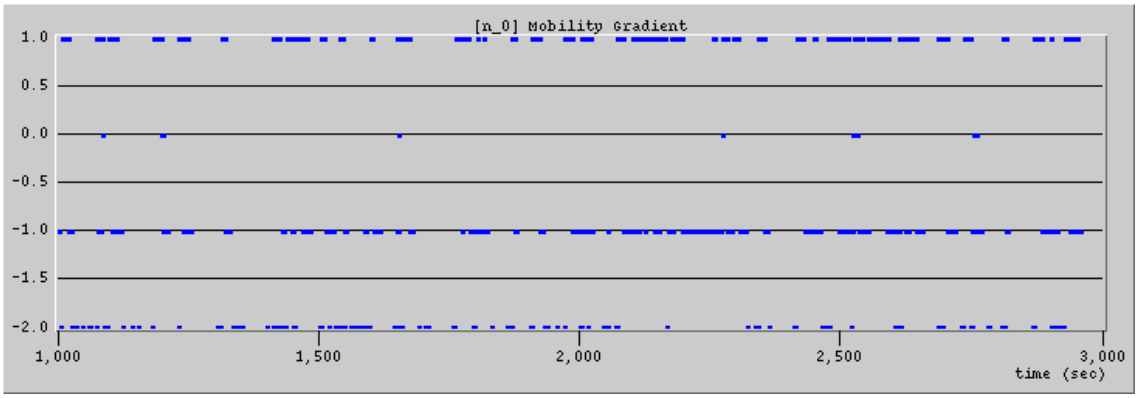

Figure 6.14: Mobility gradient of node *n_0*

Node *n_19* participates in the routing of data packets from node *n_0*. the routing queue size of node *n_19* is shown in Figure 6.12. This node routes almost 200 packets at 1500 s model time and 50 packets at 2700 s model time. The routing queue of source node *n_0* is shown in Figure 6.13. The queue is filled with the rate of 1 packet/s. There is a limited availability of neighbor nodes, hence the queue is increased periodically. The average routing queue size is 31.64 packets.

A node obtains information about its mobility from the sink beacon packets. The mobility gradient is calculated from the obtained RSSI information. The simulation result for the mobility gradient of node *n_0* is shown in Figure 6.14. Different levels indicate the mobility direction. When the direction is unknown, a data point at level of -2 is specified. The beacon range of the sink nodes is not covering the whole area, hence there is frequent loss of mobility information (dots at -2). Constant phases when sensor and sink nodes are stopped, appear rarely (level 0).

Table 6.1: Power consumption of mobile nodes (in Joules)

Rank	Node Name	Min.	Average	Max.	Std. Dev.
1	n_0	0.060341	0.46149	0.89518	0.24018
2	snk_1	0.060340	0.30736	0.55358	0.14222
3	n_19	0.060642	0.32207	0.55208	0.14336
4	n_8	0.060400	0.29773	0.54378	0.13951
5	n_12	0.060341	0.28896	0.53681	0.13719
6	n_11	0.060341	0.28363	0.52859	0.13598
7	n_4	0.060340	0.29097	0.50770	0.12697
8	snk_0	0.060340	0.29142	0.50341	0.12624
9	n_24	0.060341	0.29286	0.50007	0.12873
10	n_15	0.060341	0.28512	0.49967	0.12344
11	snk_2	0.060341	0.27072	0.49371	0.12476
12	n_2	0.060340	0.27178	0.47726	0.11975

13	n_9	0.060341	0.26676	0.47607	0.12288
14	n_13	0.060340	0.25190	0.47571	0.12016
15	n_23	0.060340	0.26559	0.47284	0.12153
16	n_17	0.060340	0.27542	0.47283	0.11946
17	n_16	0.060341	0.26967	0.47272	0.12104
18	n_5	0.060341	0.26590	0.47010	0.11720
19	n_22	0.060341	0.25602	0.46907	0.11879
20	n_7	0.060763	0.28322	0.46873	0.11694
21	n_3	0.060340	0.26979	0.45933	0.11379
22	n_10	0.060341	0.25292	0.45800	0.11302
23	n_18	0.060341	0.25637	0.45746	0.11385
24	n_21	0.060340	0.26593	0.44689	0.11005
25	n_20	0.060883	0.23575	0.43983	0.10829
26	n_14	0.060581	0.25436	0.43413	0.10690
27	n_6	0.060340	0.23716	0.43227	0.10923
28	n_1	0.060469	0.25254	0.42790	0.10695

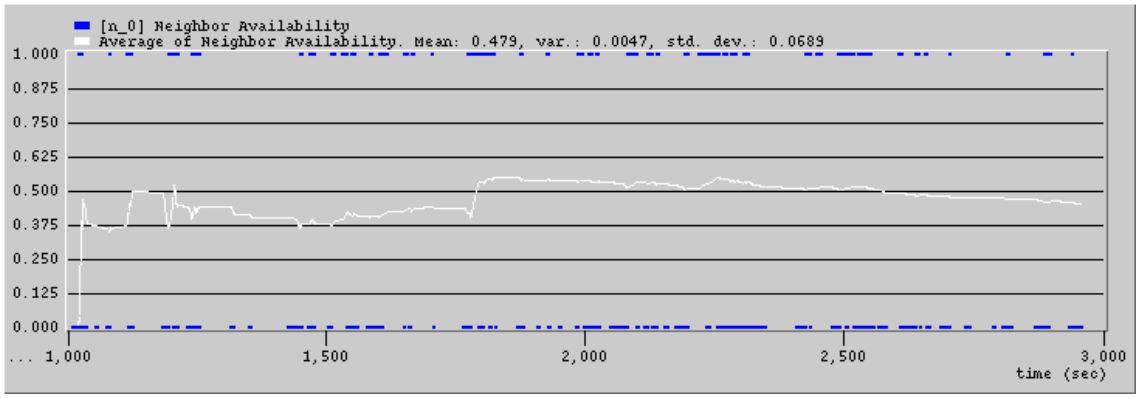

Figure 6.15: Neighborhood availability of node *n_0*

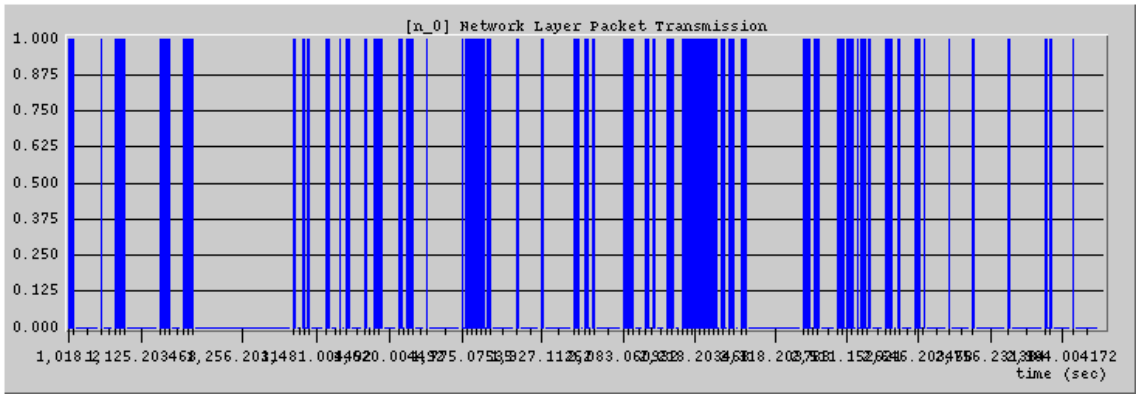

Figure 6.16: NET layer packet transmission initiation of node *n_0*

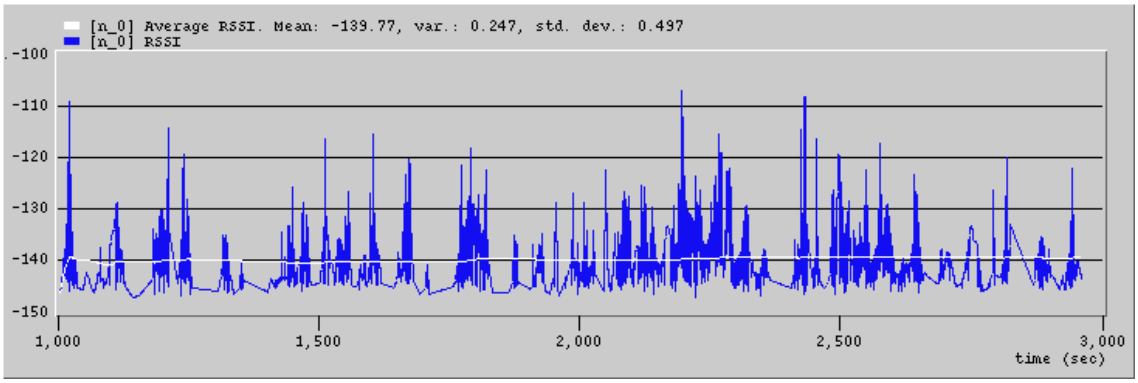

Figure 6.17: Received packet RSSI indication of node *n_0*

Neighborhood information results for node *n_0* are shown in Figure 6.15. When a sensor node receives a forwarded beacon from a neighbor node, it builds the neighborhood availability information. If a neighbor is known, level 1 is occoupied (level 0 otherwise). In this figure, the average neighborhood availability indicates that the node *n_0* knows its neighbor for less than the half of the total time (47.9%). This causes the longer delays.

When neighbors are available in the neighborhood, the BNN is elected. When the BNN is valid (not equal -1), the NET layer can start the packet transmission to the BNN. The result of the NET layer packet transmission initiation of node *n_0* is shown in Figure 6.16. Comparing this result with the previous one, it is noticeable that the NET layer delivers packets when a BNN is available. The initiation also depends on the waiting ACK flag. When an ACK is returned from the MAC layer, a new packet from the network routing queue is started.

Received packets are evaluated in the MAC layer by the RSSI parameter, which is provided by the PHY layer. RSSI statistic results of node *n_0* are shown in Figure 6.17. The minimum received levels start from -147 dBW. The average RSSI is near -140 dBW. The best RSSI is around -109 dBW when the TX power is -80 dBW.

6.4 Evaluation of Simulation Results

In the previous subchapter, the results of ORMMA-WSN simulation present the functionality of the implemented ORMMA-WSN protocol. These results are not reliable as they are shown over time regarding only one simulation run. Using a different random seed value for each simulation run, mobility paths change. Different mobility paths cause random changes of the network node density. It is necessary to evaluate the the measured parameters by presenting the mean parameter values with confidence intervals.

In the scenario with multiple sinks, several mobile sink nodes are implied in the WSN. The network size is changed in steps. Starting from 5 nodes and 3 sinks, 5 additional nodes are added in every step. The TX power is adjusted in three levels. Five independent simulations are performed for each parameter. The evaluation parameters are related to the network size value and to the TX Power.

For comparison with AODV, only a single sink is enabled in the simulation scenario.

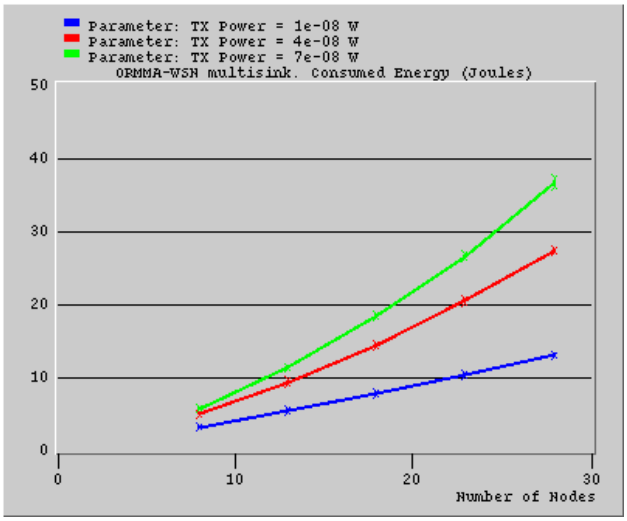

Figure 6.18: Consumed energy of ORMMA-WSN in the multi-sink scenario

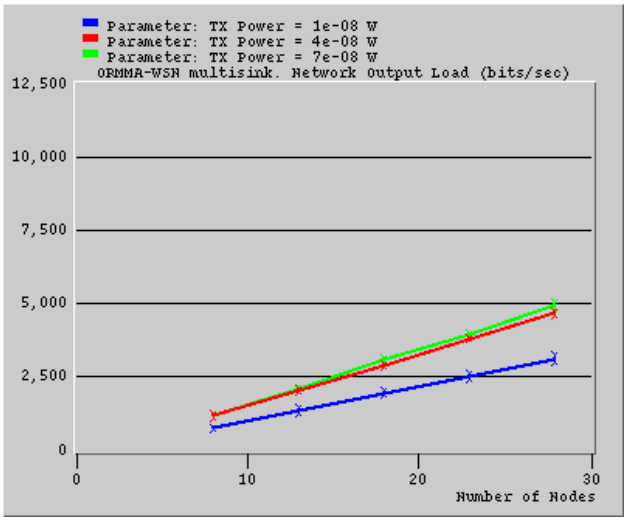

Figure 6.19: Throughput of ORMMA-WSN in the multi-sink scenario

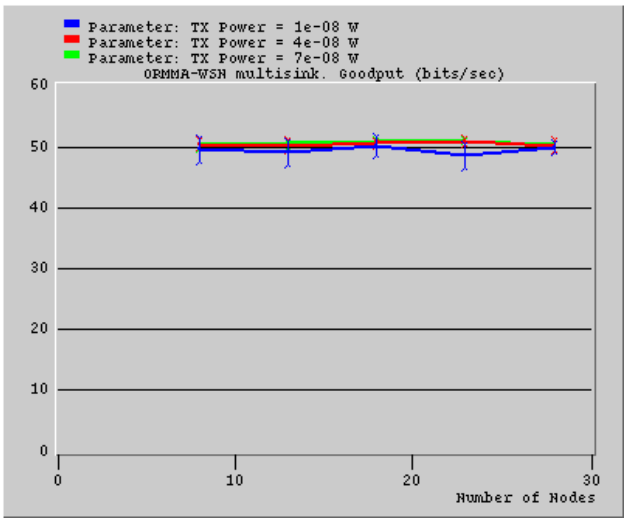

Figure 6.20: Goodput of ORMMA-WSN in the multi-sink scenario

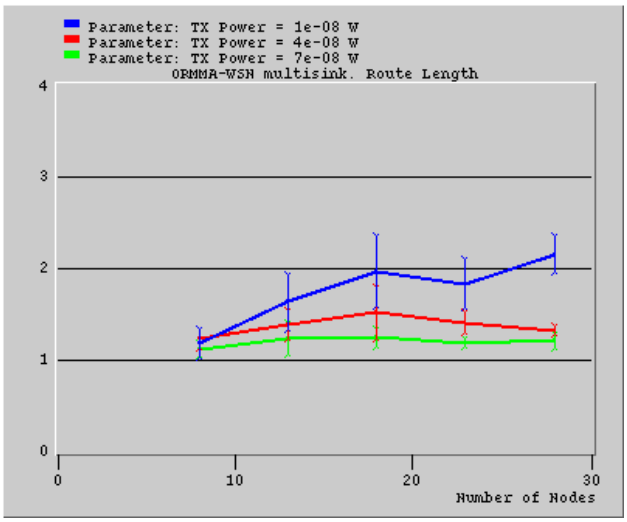

Figure 6.21: Routing length of ORMMA-WSN in the multi-sink scenario

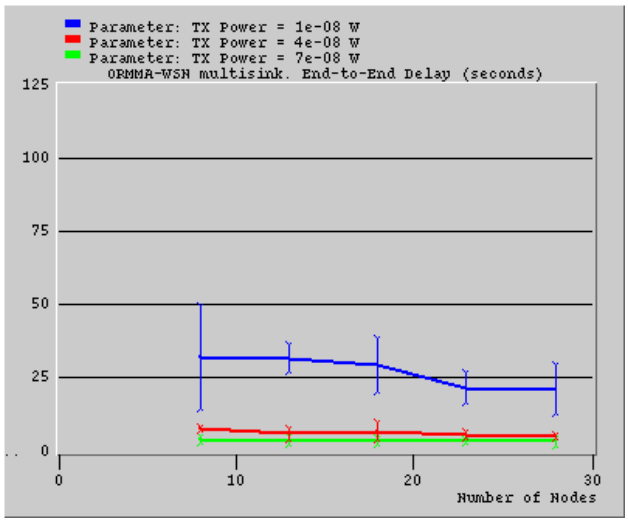

Figure 6.22: End-to-end delay of ORMMA-WSN in the multi-sink scenario

Evaluation of the simulation is done by the analysis of collected statistics about energy consumption, end-to-end delay, throughput, goodput and routing length.

The results of the simulation of the multi-sink scenario are shown in Figures 6.19 to 6.22. Confidence intervals and other statistical data are described in Table 6.2 (p. 73).

The power consumption of the ORMMA-WSN protocol in the scenario with multiple sinks is shown in Figure 6.18. As expected, the increasing number of mobile sensor nodes causes higher power consumption. When the communication range and also the beacon range increases, the probability of a higher collision ratio also increases. The total number of retransmission attempts becomes higher.

The network output load is called the throughput of the network. The throughput shows the rate of all transmissions in the network. It constantly increases with growing network size. As shown in Figure 6.19, while increasing the communication range, the throughput increases but becomes saturated when the communication coverage becomes close to the network area size.

The total network output load contains the traffic of data packets. The rate of data packets reaching the destination is called the goodput. Results of the goodput in the ORMMA-WSN multi-sink scenario are shown in Figure 6.20. The expected value of goodput must converge to the data packet rate, which is 51.2 bits/s (256 bits/5s). It is noticeable that when the TX power is low, a larger variation of goodput occurs. This is caused by long end-to-end delays (see Figure 6.22). The low communication range is the reason of intermittent connectivity between nodes. When the TX power is increased, the goodput increases and the end-to-end delay decreases. When the network size is bigger (more sensor nodes), the end-to-end delay is more influenced at the low TX power level. The end-to-end delay depends not only on the availability of neighbor nodes and node mobility. The ORMMA-WSN does not exploit the adaptivity of mobility gradient and RSSI thresholding. The RSSI threshold is fixed to a constant value. In a future extension, it could be related with the speed of change of the mobility gradient.

Results of the routing length of data packets in the multi-sink scenario are shown in Figure 6.22. The number of hops is increased in denser network at low TX power. When the communication range is larger, this value decreases because there are less hops between source and destination nodes. When communication range is large, the number of hops and hence the end-to-end delay becomes constant (like in a static network).

Table 6.2: Statistical results of ORMMA-WSN scenario with multiple sinks

Energy Consumption (Joules)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	7.913	15.335	19.729
Variance	11.987	63.403	121.076
Std. Dev.	3.462	7.963	11.003
No. of nodes	Conf. Inteval (95%)		
8	3.179 (+/- 0.041)	4.976 (+/- 0.114)	5.691 (+/- 0.122)
13	5.431 (+/- 0.21)	9.334 (+/- 0.243)	11.278 (+/- 0.139)

18	7.705 (+/- 0.197)	14.433 (+/- 0.205)	18.418 (+/- 0.276)
23	10.269 (+/- 0.243)	20.513 (+/- 0.336)	26.547 (+/- 0.286)
28	12.979 (+/- 0.184)	27.416 (+/- 0.194)	36.71 (+/- 0.67)
Throughput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	1,944.6	2,926.74	3,048.38
Variance	698,237.9	1,544,486.43	1,770,998.45
Std. Dev.	835.61	1,242.77	1,330.79
No. of nodes	Conf. Inteval (95%)		
8	746.87 (+/- 33.51)	1,175.28 (+/- 71.73)	1,172.92 (+/- 63.96)
13	1,376.9 (+/- 109.35)	2,048.79 (+/- 68.67)	2,093.83 (+/- 83.99)
18	1,962.17 (+/- 85.32)	2,912.06 (+/- 43.68)	3,088.4 (+/- 70.81)
23	2,518.6 (+/- 109.58)	3,813.56 (+/- 29.99)	3,937.42 (+/- 60.64)
28	3,118.4 (+/- 137.28)	4,684.02 (+/- 71.91)	4,949.32 (+/- 142.0)
Goodput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	49.464	50.514	50.71
Variance	1.787	0.3196	0.2512
Std. Dev.	1.337	0.5654	0.5012
No. of nodes	Conf. Inteval (95%)		
8	49.54 (+/- 1.923)	50.46 (+/- 0.6661)	50.53 (+/- 0.7869)
13	49.02 (+/- 1.981)	50.28 (+/- 0.8181)	50.64 (+/- 0.5987)
18	50.18 (+/- 1.425)	50.61 (+/- 0.3469)	50.99 (+/- 0.1805)
23	48.59 (+/- 1.872)	50.99 (+/- 0.5553)	51.02 (+/- 0.0867)
28	49.997 (+/- 0.756)	50.23 (+/- 0.8859)	50.36 (+/- 0.8571)
Routing Length (hops)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	1.757	1.376	1.1998
Variance	0.1501	0.0217	0.0072
Std. Dev.	0.3875	0.1472	0.0846
No. of nodes	Conf. Inteval (95%)		
8	1.187 (+/- 0.1541)	1.237 (+/- 0.1066)	1.122 (+/- 0.0685)
13	1.634 (+/- 0.3013)	1.387 (+/- 0.1483)	1.229 (+/- 0.1727)
18	1.969 (+/- 0.3845)	1.518 (+/- 0.2773)	1.249 (+/- 0.093)
23	1.836 (+/- 0.2681)	1.412 (+/- 0.1122)	1.189 (+/- 0.0456)
28	2.161 (+/- 0.2021)	1.327 (+/- 0.0386)	1.21 (+/- 0.0701)
End-to-End Delay (seconds)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	27.29	6.223	3.499

Variance	76.31	2.299	0.642
Std. Dev.	8.74	1.516	0.801
No. of nodes	Conf. Inteval (95%)		
8	32.07 (+/- 17.66)	7.903 (+/- 0.581)	3.996 (+/- 1.089)
13	31.84 (+/- 4.690)	5.876 (+/- 1.653)	3.633 (+/- 1.336)
18	29.55 (+/- 9.169)	6.759 (+/- 2.819)	3.371 (+/- 0.925)
23	21.75 (+/- 4.956)	5.533 (+/- 0.973)	3.275 (+/- 0.5439)
28	21.24 (+/- 8.093)	5.043 (+/- 0.5253)	3.219 (+/- 1.112)

6.4.1 Comparison Scenario Parameters

ORMMA-WSN Network and IEEE 802.15.4:

- 1 sink, 25 nodes (all mobile), 1 analyzer.
- The number of nodes is changed in steps (5, 10, 15, 20, 25). Total number of nodes (6, 10, 16, 21, 26).
- All other simulation parameters are the same as described in the first scenario (see Chapter 6.2).
- PHY layer parameters:
  Data rate: 250 kbps,
  Bandwidth: 2 MHz,
  Base frequency of a channel: 2.401 GHz.

Most of the AODV MANET station parameters are set to default values:

- Route discovery parameters:
  Route Request Retries: 5,
  Route Request Rate Limit (packets/s): 10.
- Active route expiration interval (seconds): 1.2.
- Hello message interval (seconds): uniformly distributed in [1, 1.1].
- Allowed hello loss: 1.
- Net diameter: 35.
- Node Traversal Time (seconds) : 0.04.
- Route Error Rate Limit (packets/s): 10.
- Timeout Buffer: 2.
- TTL Parameters:
  TTL Start: 1,
  TTL Increment: 2,
  TTL Threshold: 7,
  Local Add TTL: 2.
- Packet queue size: infinite.
- Local repair is enabled.
- Addressing mode - Ipv4.

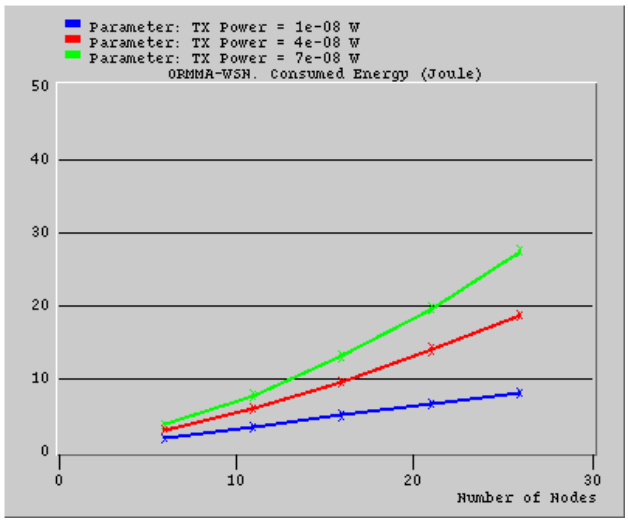

Figure 6.23: Energy consumption of ORMMA-WSN in the single sink scenario

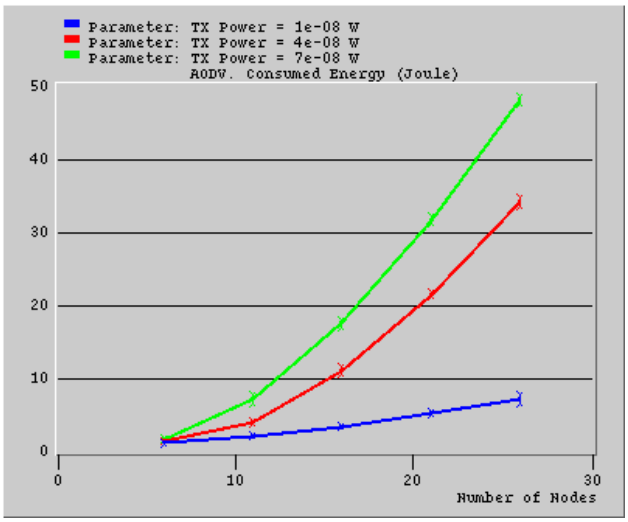

Figure 6.24: Energy consumption of AODV in the single sink scenario

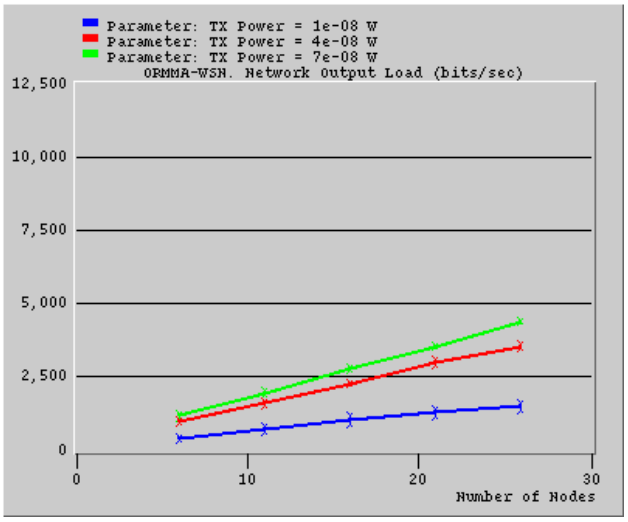

Figure 6.26: Throughput of ORMMA-WSN in the single sink scenario

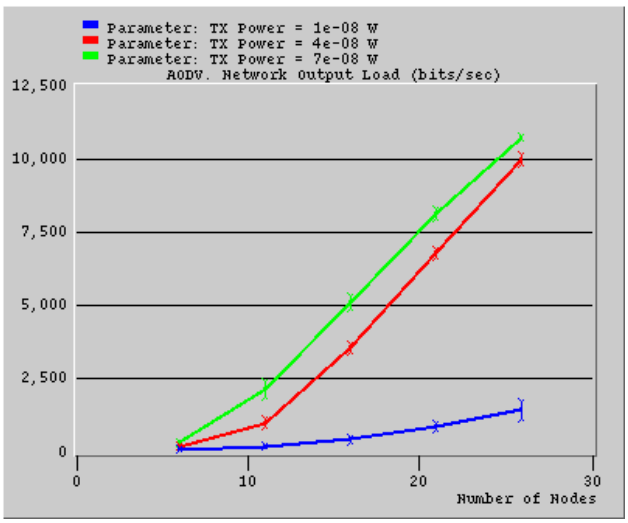

Figure 6.25: Throughput of AODV in the single sink scenario

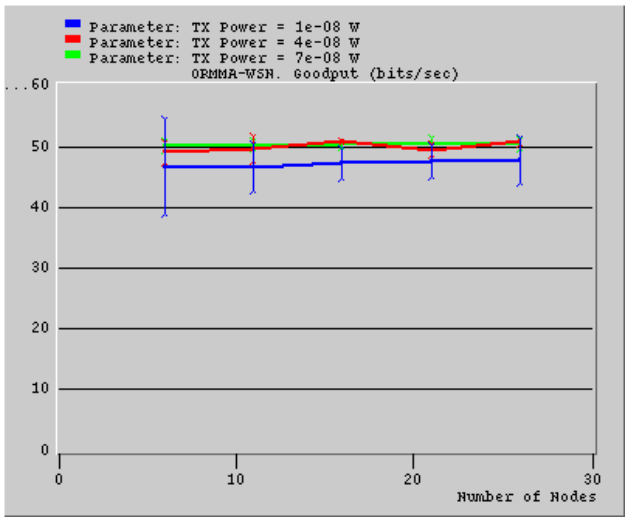

Figure 6.27: Goodput of ORMMA-WSN in the single sink scenario

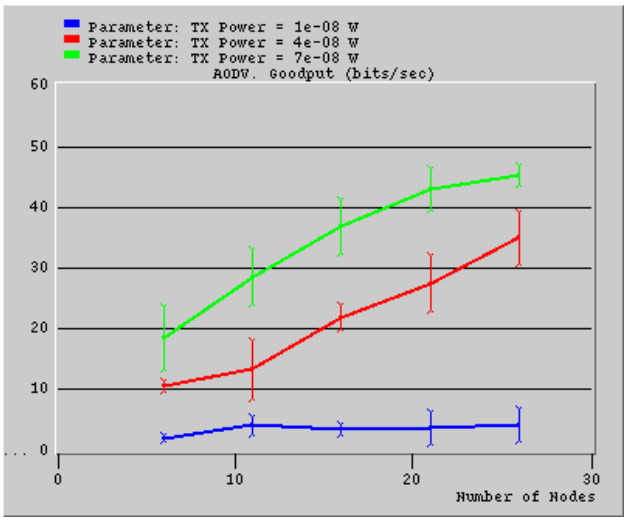

Figure 6.28: Goodput of AODV in the single sink scenario

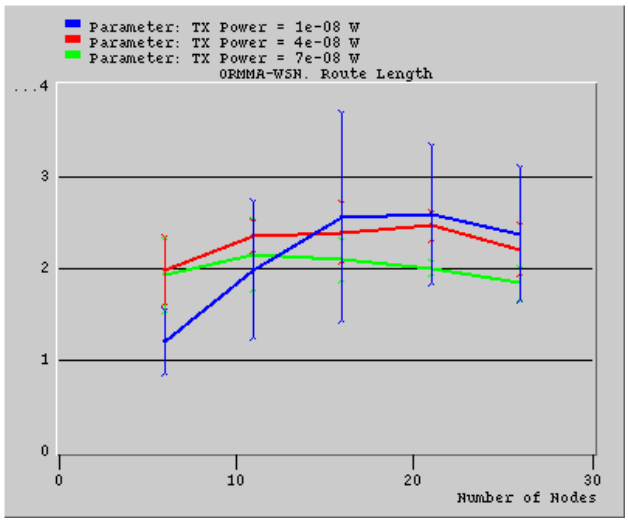

Figure 6.29: Routing length of ORMMA-WSN in the single sink scenario

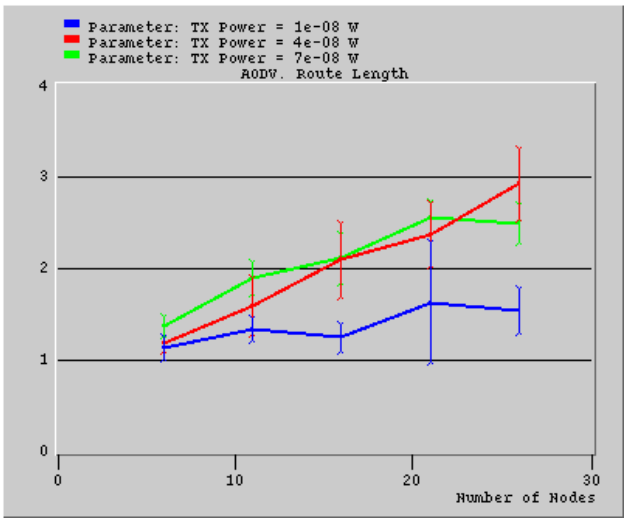

Figure 6.30: Routing length of AODV in the single sink scenario

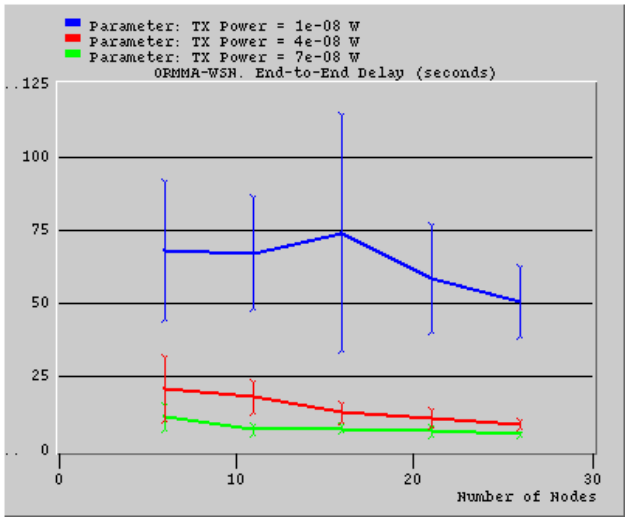

Figure 6.31: End-to-end delay of ORMMA-WSN in the single sink scenario

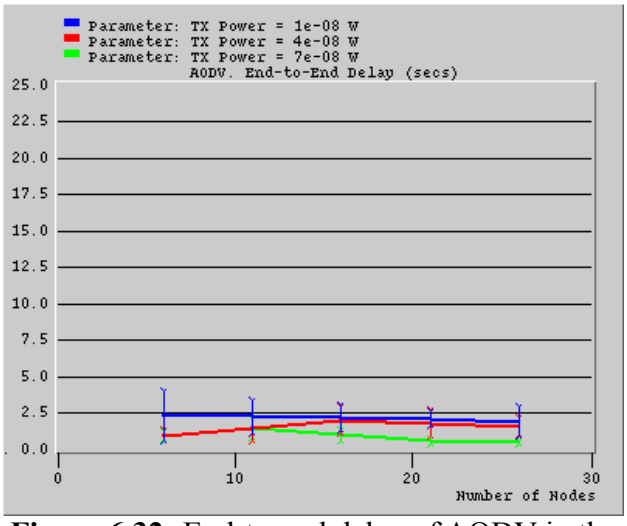

Figure 6.32: End-to-end delay of AODV in the single sink scenario

6.4.2 Simulation Results of the Comparison Scenario

This subchapter provides the evaluation of the obtained simulation results from the comparison scenario with a single sink. The ORMMA-WSN and AODV routing protocols are configured to have the same scenario parameter and environmental conditions according to the simulation parameter setup described in the previous subchapter. All steps are repeated with the same random seeds and exact deployment of sensor nodes. A controllable random number generator allows to produce the same mobility patterns for both cases.

The comparison is performed by collecting simulation statistics about energy consumption, throughput, goodput, routing length and data propagation delays in the same way as described earlier in this chapter.

Figures 6.23 through 6.32 present simulation results with calculated confidence intervals. Detailed statistical results for ORMMA-WSN are given in Table 6.3 (p. 78) and for AODV, in Table 6.4 (p. 79).

Routing of data packets in the AODV routing protocol is performed when the active routing path is known. In the mobile network when all nodes are mobile, this active routing path changes frequently. The rate of change depends on the time of neighborhood availability and communication range. When the TX power and the network size (5 sensor nodes + 1 sink) are low, the AODV performance is very low. Most of the data packets have a short routing length of 1.135 hops (see Figure 6.30). This causes a low thoughput (Figure 6.25) and a low goodput (Figure 6.28). Only a fraction of the total data packets reaches the destination sink *snk_0*. ORMMA-WSN in this case presents better performance (see Figure 6.27). The goodput of 46.72 bit/s of a total data packet rate of 52.1 bit/s is reached. ORMMA-WSN shows a large performance advantage over AODV in an intermittently connected network. The goodput of AODV is only 1.92 bits/s in the 6 node netwrok. However, intermittent connectivity requires long delays. The end-to-end delay results of ORMMA-WSN are shown in Figure 6.31. When the TX power is low and network consists of only 5 sensor nodes and 1 sink, the delay reaches in average 61.56 s. This value decreases in the larger networks. Comparing to AODV (see Figure 6.32), the end-to-end delays of this routing protocol are low. That is because AODV data packets are sent when route is available. Small goodput indicates that only a small part of the total data packets can reach the destination. The energy consumption of both routing algorithms is similar when TX power and network size are low (see Figures 6.23 and 6.24).

Table 6.3: Statistical results of ORMMA-WSN in the single sink scenario

Energy Consumption (Joules)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	4.9	10.15	14.24
Variance	4.94	31.38	71.77
Std. Dev.	2.22	5.6	8.47
No. of nodes	Conf. Inteval (95%)		
6	1.774 (+/- 0.1116)	2.917 (+/- 0.0696)	3.618 (+/- 0.1813)
11	3.301 (+/- 0.1713)	5.849 (+/- 0.2177)	7.643 (+/- 0.2654)
16	4.92 (+/- 0.3213)	9.482 (+/- 0.1431)	13.03 (+/- 0.3607)
21	6.489 (+/- 0.3062)	13.93 (+/- 0.3513)	19.5 (+/- 0.3031)
26	8.015 (+/- 0.2818)	18.589 (+/- 0.2164)	27.4 (+/- 0.3122)
Throughput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	982.9	2,277	2,778.3
Variance	167,003.4	866,720.2	1,290,232.5
Std. Dev.	408.7	930.98	1,135.9
No. of nodes	Conf. Inteval (95%)		
6	386.5 (+/- 61.34)	958.5 (+/- 53.32)	1,193.4 (+/- 76.57)
11	708.1 (+/- 103.2)	1,607.7 (+/- 82.2)	1,958.5 (+/- 86.5)
16	1,032.1 (+/- 168.5)	2,280.1 (+/- 33.39)	2,773.1 (+/- 52.52)
21	1,287.1 (+/- 136.8)	2,982.9 (+/- 104.9)	3,563.1 (+/- 38.89)

26	1,500.7 (+/- 128.4)	3,555.9 (+/- 61.51)	4,403.6 (+/- 33.22)
Goodput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	47.21	49.96	50.39
Variance	10.9965	1.352	0.2908
Std. Dev.	3.316	1.163	0.5393
No. of nodes	Conf. Inteval (95%)		
6	46.72 (+/- 7.896)	49.05 (+/- 1.612)	50.25 (+/- 0.7885)
11	46.67 (+/- 3.863)	49.61 (+/- 2.011)	50.22 (+/- 0.6193)
16	47.31 (+/- 2.382)	50.82 (+/- 0.112)	50.38 (+/- 0.5665)
21	47.54 (+/- 2.581)	49.46 (+/- 0.8716)	50.69 (+/- 0.7169)
26	47.82 (+/- 3.687)	50.87 (+/- 0.4957)	50.38 (+/- 0.8273)
Routing Length (hops)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	2.146	2.285	2.003
Variance	0.5892	0.0661	0.0503
Std. Dev.	0.7676	0.2571	0.2243
No. of nodes	Conf. Inteval (95%)		
6	1.196 (+/- 0.3428)	1.985 (+/- 0.3604)	1.928 (+/- 0.38)
11	1.99 (+/- 0.737)	2.361 (+/- 0.154)	2.146 (+/- 0.3754)
16	2.567 (+/- 1.13)	2.398 (+/- 0.3157)	2.097 (+/- 0.2122)
21	2.593 (+/- 0.7526)	2.469 (+/- 0.1507)	2.006 (+/- 0.0642)
26	2.382 (+/- 0.7291)	2.212 (+/- 0.2713)	1.839 (+/- 0.169)
End-to-End Delay (seconds)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	64.055	14.38	7.454
Variance	380.005	37.32	6.15
Std. Dev.	19.49	6.11	2.48
No. of nodes	Conf. Inteval (95%)		
6	68.51 (+/- 23.43)	21.23 (+/- 10.65)	11.23 (+/- 3.961)
11	67.54 (+/- 18.8)	18.09 (+/- 5.1)	6.987 (+/- 1.417)
16	74.44 (+/- 40.26)	12.84 (+/- 2.782)	7.268 (+/- 0.7549)
21	58.8 (+/- 18.06)	10.81 (+/- 2.687)	6.466 (+/- 1.473)
26	50.99 (+/- 11.76)	8.949 (+/- 1.056)	5.322 (+/- 0.3504)

Table 6.4: Statistical results of AODV in the single sink scenario

Energy Consumption (Joules)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	3.782	14.38	21.19

Variance	4.724	146.19	285.9
Std. Dev.	2.173	12.09	16.91
No. of nodes	Conf. Inteval (95%)		
6	1.113 (+/- 0.0639)	1.37 (+/- 0.051)	1.657 (+/- 0.0807)
11	2.105 (+/- 0.1606)	3.916 (+/- 0.2784)	7.06 (+/- 0.6161)
16	3.37 (+/- 0.1652)	11.03 (+/- 0.5168)	17.46 (+/- 0.6025)
21	5.175 (+/- 0.2227)	21.44 (+/- 0.3166)	31.64 (+/- 0.529)
26	7.147 (+/- 0.6096)	34.15 (+/- 0.6997)	48.11 (+/- 0.526)
Throughput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	612.45	4,321.01812	5,306.5
Variance	258,082.7	13,441,361.01	14,567,620.3
Std. Dev.	508.02	3,666.25	3,816.8
No. of nodes	Conf. Inteval (95%)		
6	102.5 (+/- 9.631)	207.2 (+/- 11.33)	327.73 (+/- 36.17)
11	201.02 (+/- 29.9)	990.6 (+/- 128.4)	2,142.4 (+/- 256.7)
16	425.6 (+/- 74.8)	3,578.75 (+/- 140.45)	5,133.5 (+/- 225.6)
21	888.05 (+/- 99.8)	6,819.3 (+/- 138.7)	8,168.98 (+/- 152.59)
26	1,445.1 (+/- 304.0)	10,009.3 (+/- 160.45)	10,759.9 (+/- 41.75)
Goodput (bit/s)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	3.5	21.7	34.4
Variance	2.409	87.74	105.69
Std. Dev.	1.552	9.367	10.28
No. of nodes	Conf. Inteval (95%)		
6	1.92 (+/- 0.388)	10.62 (+/- 0.768)	18.46 (+/- 5.118)
11	4.122 (+/- 1.491)	13.34 (+/- 4.731)	28.54 (+/- 4.505)
16	3.405 (+/- 0.842)	21.94 (+/- 2.02)	36.89 (+/- 4.43)
21	3.789 (+/- 2.515)	27.55 (+/- 4.442)	43.01 (+/- 3.372)
26	4.275 (+/- 2.606)	35.05 (+/- 4.211)	45.26 (+/- 1.533)
Routing Length (hops)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	1.377	2.034	2.088
Variance	0.0892	0.426	0.206
Std. Dev.	0.2987	0.6528	0.454
No. of nodes	Conf. Inteval (95%)		
6	1.135 (+/- 0.1156)	1.178 (+/- 0.077)	1.373 (+/- 0.1024)
11	1.339 (+/- 0.1233)	1.587 (+/- 0.3096)	1.9017 (+/- 0.1701)
16	1.243 (+/- 0.1385)	2.1 (+/- 0.4006)	2.112 (+/- 0.2612)

21	1.632 (+/- 0.6511)	2.376 (+/- 0.33412)	2.563 (+/- 0.1731)
26	1.538 (+/- 0.2418)	2.931 (+/- 0.3807)	2.493 (+/- 0.1999)
End-to-End Delay (seconds)			
TX Power	1E-08 W	4E-08 W	7E-08 W
Sample Mean	2.149	1.55	0.8817
Variance	0.653	0.4076	0.189
Std. Dev.	0.8079	0.6385	0.4348
No. of nodes	Conf. Inteval (95%)		
6	2.286 (+/- 1.671)	0.9443 (+/- 0.3344)	0.9465 (+/- 0.2728)
11	2.279 (+/- 1.112)	1.419 (+/- 0.8078)	1.4571 (+/- 0.6147)
16	2.168 (+/- 0.8631)	2.013 (+/- 0.8662)	0.9587 (+/- 0.4028)
21	2.1 (+/- 0.4856)	1.777 (+/- 0.9162)	0.5758 (+/- 0.1655)
26	1.914 (+/- 1.026)	1.594 (+/- 0.5453)	0.4705 (+/- 0.1038)

The TX power is increased in order to increase the neighborhood of the nodes. With a high TX power (7E-08 W), AODV gains more performance of goodput and delays than in the low power case. The end-to-end delay of AODV is always lower than that of ORMMA-WSN. However, AODV performs well only in the case of available routing paths. The goodput of ORMMA-WSN reaches the maximum data packet rate with relatively small end-to-end delay compared to the low TX power case. These delays are expected to be even lower if the ORMMA-WSN protocol would include the adaptation of mobility parameters to a changing environment.

When network size is larger, energy consumption increases. The energy consumed by the ORMMA-WSN protocol is always lower than AODV energy consumption. AODV wastes energy for finding the routing path. With the increased TX power, AODV finds more routes and performs more route requests when a link failure occurs. This phenomenon is indicated by the network output load of AODV transmissions (see Figure 6.25) by a steeper increase for a larger network size. The required throughput for ORMMA-WSN is much lower than for AODV (Figure 6.26).

The routing length of ORMMA-WSN decreases when the TX power is larger for a larger network size (from 10 sensor nodes upwards). When the network size is low (5 sensor nodes), a smaller route length occurs (see Figure 6.29). When number of nodes is larger, this helps to increase the routing length and to decrease the delay as data packets can be routed in multiple hops instead of waiting for the meeting with the sink node. The routing length reaches a saturation value and decreases for denser networks with larger TX power, because more nodes are available for routing between source and sink.

6.5 Conclusions

The obtained simulation results show the behaviour of ORMMA-WSN in different scenarios. Comparing the results in multi-sink and single sink scenarios, it can be noticed that end-to-end delays are decreased in the multi-sink network. This is because data packets are routed to the nearest available sink. Goodput has better performance in

a multi-sink enabled network at the cost of slightly increased power consumption and similar network output load.

Comparison results of AODV and ORMMA-WSN in the single-sink scenario indicate that AODV performs better in high transmit power and denser networks. AODV gains performance when intermittent connectivity occurs rare and the mobility is low. ORMMA-WSN has an advantage in low TX power, intermittently connected mobile networks. However, a low network density causes longer end-to-end delays.

CHAPTER 7

7. Conclusions and Outlook

In this work, the Opportunistic Routing protocol in Mobile Multi-Sink Ad Hoc Wireless Sensor Networks (ORMMA-WSN) is presented. The simulation model is implemented in the OPNET simulator. Simulation results describe the principles and performance of the ORMMA-WSN model. An evaluation is done by the comparison of ORMMA-WSN with the AODV routing protocol.

The obtained results show that ORMMA-WSN is suitable for low rate, low power mobile wireless sensor networks with intermittent connectivity. The AODV protocol is outperformed in all specified scopes except the end-to-end delay. The adaptivity to the context information about mobility and radio channel conditions is necessary to be implemented in order to reduce end-to-end delays in ORMMA-WSN.

In ORMMA-WSN, the non-beacon IEEE 802.15.4 MAC is exploited. The standard model of this MAC is not adaptive to the radio channel conditions, decisions are made only in the Network layer. Constant RSSI thresholding is used in order to decrease the packet loss ratio. This induces a long end-to-end delay even in the case of high TX power. The separating distance between two nodes must exceed the specified RSSI threshold value in order to communicate. Adaptive RSSI thresholding can be done by implementing an adaptive TX power control mechanism. The MAC layer should collect connectivity information to make a final decision. For this reason, the NET and MAC layers must be integrated as it is done in some available opportunistic routing protocols which have been presented in this work.

The ORMMA-WSN model exploits a one directional source-to-sink data packet flow. End-to-end ACKs from sink nodes and queries of information are not covered by this work. A distributed configuration and data extraction from specified locations provided from the sinks to the mobile nodes can be considered as future work.

The mobility gradient only shows the relative movement between sensor and sink nodes. The maximum route length for nodes that appear outside a sink beacon coverage is two hops. Neighbor nodes can only forward their mobility information. Advanced localization algorithms which are aware of contextual information are required to overcome this disadvantage.

Context aware routing is an adaptive routing technique. The adaptivity to the context of the routing environment is performed by a synthesis of contextual parameters, such as

energy consumption, mobility, information, privacy, quality of service, etc. A performance gain can be expected in mobile wireless sensor networks consisting of wireless sensor nodes running the opportunistic routing protocol with the enabled features of context aware routing.

ILLUSTRATION INDEX

TABLE INDEX

LIST OF ABBREVIATIONS

ACK	Acknowledgment
AES	Advanced Encryption Standard
AODV	Ad-hoc On-demand Distance Vector
APP	Application
BC	Beacon Count
BE	Backoff Exponent
BER	Bit Error Rate
BFI	Beacon Forwarding Interval
BI	Beacon Interval
BIFS	Beacon Inter Frame Spacing
BNN	Best Neighbor Node
BP	Beacon Period
BPSK	Binary Phase Shift Keying
BS	Base Station
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CID	Cluster Identifier
CLH	Cluster Head
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
CW	Contention Window
ED	Energy Detection
ExOR	Extremely Opportunistic Routing
FFD	Full Function Device
FIFO	First In First Out
GAF	Geographical Adaptive Fidelity
GBR	Gradient Based Routing
GEAR	Geographic and Energy Aware Routing
GeRaF	Geographic Random Forwarding
GPRS	General Packet Radio Service
GPSR	Greedy Perimeter Stateless Routing
GTS	Guaranteed Time Slot
HSR	Hierarchical State Routing
ICI	Inter-Control Interface

IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter Frame Spacing
IP	Internet Protocol
LEACH	Low Energy Adaptive Clustering Hierarchy
LLC	Logical Link Control
LQI	Link Quality Indication
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MCU	Micro Controller Unit
MG	Mobility Gradient
MOR	Multipath On-demand Routing Protocol
NAK	Not Acknowledgment
NAV	Network Allocation Vector
NB	Number of Backoffs
NET	Network
NN	Neighbor Node
NNET	Node Neighbor Expiration Time
O-QPSK	Offset-Quadrature Phase Shift Keying
OLSR	Optimized Link State Routing Protocol
OPRAH	Opportunistic Routing in Ad Hoc Networks
OR	Opportunistic Routing
ORMMA-WSN	Opportunistic Routing in Multi-Sink Mobile Ad Hoc Wireless Sensor Networks
PAN	Personal Area Network
PC	Personal Computer
PHY	Physical
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFD	Reduced Function Device
RSSI	Received Signal Strength Indicator
RTS	Ready To Send
RX	Receive
SCAR	Sensor Context Aware Routing
SEQ	Sequence Number
SIFS	Short Inter Frame Sequence
SNET	Sink Neighbor Expiration Time
SNR	Signal To Noise Ratio
SPI	Serial Peripheral Interface
SPIN	Sensor Protocol for Information via Negotiation
SRAM	Static Random Access Memory
SSCS	Service Specific Convergence Sublayer

STEM	Sparse Topology and Energy Management
TCP	Transmission Control Protocol
TICER	Transceiver Initiated Cycled Receiver
TORA	Temporally-Ordered Routing Algorithm
TTDD	Two-Tier Data Dissemination
TX	Transmission
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WRAN	Wireless Regional Area Network
WSN	Wireless Sensor Network

BIBLIOGRAPHY

---

k[1] K. Römer and M. Friedemann, "The Design Space of Wireless Sensor Networks," *IEEE Wireless Communications*, vol. 11, pp. 54-61, 2004.

[2] J. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, pp. 6- 28, 2004.

[3] "ZigBee Alliance," *http://www.zigbee.org/*, June 2007.

[4] "TinyOS," *http://www.tinyos.net*, August 2007.

[5] K. Akkaya and M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks," *Elsevier Ad Hoc Network Journal*, vol. 3, pp. 325-349, 2004.

[6] L. Wang, "A survey on sensor networks," *http://web.cs.msu.edu/~wanglim1/research/survey.pdf*, 2004.

[7] Archana Bharathidasan, Vijay Anand Sai Ponduru, *Sensor Networks: An Overview*. Technical report,
University of California: IEEE Potentials, 2003.

[8] C. Mascolo and M. Musolesi, "SCAR: context aware adaptive routing in delay tolerant mobile sensor networks," *Proceedings of the 2006 international conference on Communications and mobile computing*, pp. 533 - 538, July 2006.

[9] IEEE, *IEEE Standard 802.15.4, http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf*. 2003.

[10] R.C. Shah et al., "Modeling and Analysis of Opportunistic Routing in Low Traffic Scenarios," *WIOPT '05: Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 294-304, 2005.

[11] S. Biswas and R. Morris, "Opportunistic Routing in Multi-Hop Wireless Networks," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 69-74, 2004.

[12] C. Westphal, "Opportunistic Routing in Dynamic Ad Hoc Networks: the OPRAH protocol," *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference*, pp. 570-573, 2006.

[13] R.C. Shah et al., "Joint optimization of a protocol stack for sensor networks," *Military Communications Conference, 2004. MILCOM 2004. IEEE*, vol. 1, pp. 480-486, 2004.

[14] B. Chen et al., "SPAN: An energy-efficient coordination algorithm for topology maintenance," *IEEE/ACM MobiCom2001*, July 2001.

[15] C. Schurgers et al., "Optimizing sensor networks in the energy-latency-density design space," *IEEE Transactions on Mobile Computing* , vol. 1, pp. 70-80, 2002.

[16] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for Ad Hoc routing," *MobiCom '01: Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 70-84, 2001.

[17] B. Karp and H.T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 243-254, 2000.

[18] M. Zorzi and R.R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," *IEEE Transactions on Mobile Computing*, vol. 2, pp. 349-365, 2003.

[19] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, pp. 483-502, 2002.

[20] "OPNET Simulator," *http://www.opnet.com*, June 2007.

[21] A. Koubâa and M. Alves, "OPNET simulator for IEEE 802.15.4 protocol, release 1.0, http://www.open-zb.net/download," 2006.

[22] D. Curren, *A Survey of Simulation in Sensor Networks*. University of Binghamton project report for subject CS580: 2005.

[23] "Open-ZB," *http://www.open-zb.net*, May 2007.

[24] A. Klein and P. Tran-Gia, "Energy Consumption Framework for Wireless Sensor Networks," 2007.

[25] C. E. Perkins, E. M. Belding-Royer, and I. Chakeres, *Ad Hoc On Demand Distance Vector (AODV) Routing. RFC 3561*. 2003.