

# **A Smart Home Networking Simulation for Energy Saving**

By

**Cheng Jin**

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs

in partial fulfillment of the requirements for the degree of

**Master of Applied Science in Electrical and Computer Engineering**

Ottawa-Carleton Institute for Electrical and Computer Engineering  
(OCIECE)

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

January 2011

©Copyright 2011, Cheng Jin

The undersigned recommend to the Faculty of Graduate and Postdoctoral  
Affairs acceptance of the thesis

**A Smart Home Networking Simulation Model for  
Energy Saving**

Submitted by  
**Cheng Jin**

In partial fulfillment of the requirements for the degree of  
Master of Applied Science in Electrical and Computer Engineering

---

Chair, Howard Schwartz, Department of Systems and Computer  
Engineering

---

Thesis Supervisor, Dr. Thomas Kunz

Carleton University

January 2011

## **Abstract**

To explore and evaluate the network performance of Demand-Response (DR) programs in smart homes, we designed and implemented a simplified networking simulation model characterized by a Radio Broadcast Data System (RBDS) network and a combination of ZigBee/IEEE 802.15.4 and HomePlug C&C in the Network Simulator Version-2 (NS-2) which supports multiple interfaces/channels. Simulation results show that a combined network generally outperforms a single wireless or wired network. Forwarding RBDS packets to all nodes, AODV and ZigBee routing perform worse than Flooding. Focusing on forwarding packets to individual nodes, for both AODV and ZigBee, a dual-path routing strategy and a backbone-based path routing strategy are superior to a joint-path strategy in terms of packet reception. Under such circumstances, the choice of protocols and routing strategies mainly depends upon various scenarios specific to a smart home as well as the constraints with respect to network energy consumption and the average network latency.

## **Acknowledgements**

First of all, I would like to sincerely thank Professor Thomas Kunz for his significant contribution that led to the ultimate achievement of my thesis. I was deeply impressed with his comprehensive knowledge, insightful guidance and extraordinary project management during the course of my thesis, which will be a great help to my career development in the near future.

Also, I would like to thank Monageng Kgwadi for providing the implementation package of the RBDS network and kindly support of how to execute the RBDS network simulations, Professor Mukul Goyal for sharing the source code of ZigBee routing protocol implementation and Professor Ramon Agüero Calvo for his valuable suggestion of the approach to multiple interfaces/channels intended for multiple networks.

Finally, I would like to thank my family, especially my wife, Li Zhu for her understanding, consistent encouragement and dedication to household chores, which offers mental and physical support to my academic exploration.

# Table of Contents

Abstract.....	i
Acknowledgements.....	ii
Table of Contents.....	iii
List of Figures.....	vi
List of Tables.....	ix
List of Acronyms.....	x
1 Introduction.....	1
1.1 Background and Motivation.....	1
1.2 Thesis Contributions.....	3
1.3 Thesis Outline.....	7
2 Appliance Control in Smart Homes.....	9
2.1 Energy Usage in Residences.....	9
2.2 Generation and Management of Renewable Energy Sources.....	9
2.3 Configuration of Components and Energy Control.....	11
2.4 Redefinition of the Operation Mode.....	13
2.5 Technology Independent Requirements of Utilities.....	14
2.6 Networking Pattern and Technologies.....	15
3 Enabling Network Technology in Smart Homes.....	18
3.1 PLC Technologies.....	18
3.1.1 X-10.....	18
3.1.2 INSTEON.....	19
3.1.3 PLC-BUS.....	21
3.1.4 LonWorks.....	22
3.1.5 HomePlug.....	24
3.1.6 Comparison of PLC Technologies.....	27
3.2 Low-Rate Wireless Network Technologies.....	28
3.2.1 Bluetooth.....	28
3.2.2 ZigBee/IEEE 802.15.4.....	30
3.2.3 Z-Wave.....	33
3.3 Conclusion.....	35
4 Implementation of Simulation Model Architecture.....	37
4.1 Existing Solutions to Multiple Interfaces/Channels.....	37
4.1.1 TENS.....	37
4.1.2 Hyacinth.....	39

4.1.3 Dynamic Interface Extension to NS-2.....	40
4.1.4 MW-Node.....	42
4.1.5 MIRACLE.....	43
4.1.6 Conclusion .....	45
4.2 Our Solution to the Networking Simulation Model .....	45
4.2.1 Architecture of Mobile Node with Multiple Interfaces .....	46
4.2.2 Parameter Binding of Energy Model to Multiple Interfaces .....	47
4.2.3 Object Binding of Error Model to Multiple Interfaces.....	48
4.2.4 Logic of Connection to Multiple Interfaces .....	49
4.3 Node Addressing Scheme in NS-2 .....	51
4.3.1 Data Transmission with Multiple Interfaces .....	51
4.3.2 United Addressing Solution to Multiple Interfaces/Channels .....	53
5 Modification to Network Objects.....	56
5.1 Communication Channel in NS-2 .....	56
5.1.1 Operational Mechanism of an NS-2 Channel.....	56
5.1.2 Decoupling of Configuration for Multiple Channels .....	57
5.1.3 Packet Delivery among Multiple Channels.....	59
5.2 MAC/PHY Layer .....	60
5.2.1 Interface Numbering and Packet Tagging .....	60
5.2.2 RBDS .....	62
5.2.3 ZigBee/IEEE 802.15.4 .....	62
5.2.4 HomePlug C&C .....	64
5.3 Routing Layer .....	65
5.3.1 Packet Transmission from RBDS to Smart Homes.....	65
5.3.2 Data Forwarding in a Smart Home .....	67
5.3.2.1 Flooding .....	68
5.3.2.2 Timer-Driven Sequential Packet Forwarding.....	69
5.3.3 Routing Strategies with Multiple Interfaces/Channels.....	74
5.3.3.1 Joint-Path Routing Strategy.....	75
5.3.3.2 Backbone-Based Routing Strategy.....	77
5.3.3.3 Dual-Path Routing Strategy.....	79
5.4 Application/Transport Layer .....	81
6 Networking Simulation and Result Analysis .....	83
6.1 Simulation Setting and Measurement .....	83
6.1.1 Node Deployment and Networking Parameters.....	83
6.1.2 Performance Metrics and Dynamic Factors .....	87

6.2 Simulation Results Analysis.....	91
6.2.1 Node Density and Percentage of PLC nodes.....	91
6.2.1.1 Network Energy Cost.....	91
6.2.1.2 Network Overhead.....	98
6.2.1.3 PDR/Average End-to-End Latency.....	102
6.2.2 RBDS Traffic Rate.....	113
6.2.3 RBDS Packet Size.....	118
6.2.4 Traffic Rate of Status Updates.....	124
6.2.5 Wireless Error Rate.....	127
6.3 Conclusions.....	132
7 Conclusions and Future Work.....	134
7.1 Conclusions.....	134
7.2 Future Work.....	135
References.....	137
Appendix A Summary of NS-2 Modifications.....	144
Appendix B Simulation Configuration and Execution.....	149
B.1 Basic Setting and Interface Allocation.....	149
B.2 Scenario and Location of Nodes.....	150
B.3 General Steps in Simulations.....	152
B.4 Parameter Configuration for Different Networks.....	165
B.4.1 RBDS.....	165
B.4.2 ZigBee/IEEE 802.15.4.....	168
B.4.3 HomePlug C&C.....	173
B.5 Configuration for Data Traffic among Networks.....	174
B.6 Configuration of Routing Strategies.....	176

## List of Figures

Figure 1	An ideal scenario of time-varying price through AMI to smart homes in smart grids .....	2
Figure 2	Simulation model of energy control network in smart homes .....	4
Figure 3	The household renewable energy management in the context of smart grid [4] .....	11
Figure 4	The concept of smart home[16] .....	15
Figure 5	Smart home based on LonWorks networking pattern [32] .....	23
Figure 6	Network topology of smart home via power line [38].....	26
Figure 7	The architecture of a Bluetooth-based smart home via remote control [42].....	29
Figure 8	The architecture of ZigBee/IEEE 802.15.4 protocol [44].....	30
Figure 9	Smart meter solution based on ZigBee/IEEE 802.15.4 technology [50].....	32
Figure 10	Protocol architecture of Z-Wave [53] .....	33
Figure 11	Setup of Z-Wave network [55].....	34
Figure 12	Architecture of mobile node in TENS .....	38
Figure 13	The Hyacinth prototype with multiple channels [61] .....	39
Figure 14	Dynamic interface extension intended for a mobile node [62].....	41
Figure 15	Schematic design of a MW-Node [63].....	42
Figure 16	The general modularized architecture within the MIRACLE framework [65].....	44
Figure 17	General architecture of mobile node with multiple interfaces/channels.....	46
Figure 18	Modification of parameter binding for the energy model.....	48
Figure 19	Modification of object binding for the error model.....	49
Figure 20	The flow chart of node construction in simulations.....	50
Figure 21	Object ID assignment for each layer in NS-2 environment.....	52
Figure 22	Issues of destination recognition in ZigBee routing .....	53
Figure 23	United addressing scheme in the simulation environment with multiple interfaces.....	54
Figure 24	Node ID/Address passing from node to each layer .....	54
Figure 25	Organization of nodes over a single channel .....	56
Figure 26	Array management of each node across multiple channels .....	57
Figure 27	Decoupling of parameter association among channels.....	58
Figure 28	Data transmission on the basis of object identification and packet scheduling .....	59
Figure 29	Node classification and packet tagging across multiple networks.....	61
Figure 30	The architecture of a Korea standard-based PLC-node in NS-2 [72] .....	64
Figure 31	A combined flowchart of RBDS packet forwarding through the central controller .....	66
Figure 32	A simplified flowchart of Flooding protocol .....	68
Figure 33	Diagram of route discovery originated from central controller .....	69



Figure 34	Packet queuing management of the ZigBee and AODV routing layer .....	72
Figure 35	Simplified implementation flowcharts of timer-driven sequential packet forwarding .....	73
Figure 36	The joint-path strategy based on interface tagging .....	75
Figure 37	A simplified flowchart of interface tagging intended for route establishment.....	76
Figure 38	Packet forwarding logic with backbone-based routing.....	78
Figure 39	Simplified diagram packet forwarding with dual routing.....	80
Figure 40	Data packing in RBDS message sender.....	82
Figure 41	Node density featured by various distance among nodes .....	83
Figure 42	The deployment of PLC nodes in a smart home.....	84
Figure 43	The path of RBDS packet transmission in simulation .....	87
Figure 44	The calculation of average end-to-end latency in a smart home.....	88
Figure 45	Network energy cost of Flooding with various node densities .....	92
Figure 46	The signal range with the transmission power equal to 2.0W (5m).....	94
Figure 47	Network energy cost of AODV (joint-path) .....	94
Figure 48	Network energy cost of AODV and ZigBee with various routing strategies (3m) .....	96
Figure 49	Simplified data transmission with the dual-path strategy .....	97
Figure 50	The network overhead of Flooding with CI (excluding the controller).....	99
Figure 51	Network overhead of AODV and ZigBee with CI (excluding the controller) .....	101
Figure 52	PDR and average end-to-end latency of Flooding with CI.....	103
Figure 53	PDR and average end-to-end latency of AODV with CI (joint-path).....	105
Figure 54	PDR and average end-to-end latency of Flooding with CI (backbone-based path).....	106
Figure 55	The PDR of AODV and ZigBee (CI tagged) .....	108
Figure 56	The average latency of AODV and ZigBee (CI tagged).....	110
Figure 57	The measurement of average latency based on the timer-driven packet forwarding.....	111
Figure 58	The average latency of a ZigBee network with 50% PLC nodes .....	113
Figure 59	The PDR and average latency of Flooding vs. varying RBDS traffic rates.....	114
Figure 60	The average latency of the RBDS network.....	115
Figure 61	The PDR of AODV and ZigBee vs. varying RBDS traffic rates .....	116
Figure 62	The average latency of AODV and ZigBee vs. varying RBDS traffic rates .....	117
Figure 63	The extended average latency in the RBDS network with large RBDS packets .....	118
Figure 64	The PDR and average latency of Flooding with the increase of RBDS packet size.....	119
Figure 65	The PDR of AODV and ZigBee with the increase of RBDS packet size .....	121
Figure 66	The average latency of AODV and ZigBee with the increase of RBDS packet size .....	123
Figure 67	The layout of nodes with capability of sending status messages.....	124
Figure 68	The PDR of AODV and ZigBee vs. varying status updating rates .....	125
Figure 69	The average latency of AODV and ZigBee vs. varying status updating rates .....	126

Figure 70	The PDR and average latency of Flooding vs. varying wireless error rates .....	128
Figure 71	The PDR of AODV and ZigBee vs. varying wireless error rates .....	130
Figure 72	The average latency of AODV and ZigBee vs. varying wireless error rates .....	131
Figure 73	Scenario of RBDS message delivery in smart homes.....	151

## List of Tables

Table 1	Comparison of PLC technologies.....	27
Table 2	Technical comparison between Bluetooth and ZigBee [49].....	31
Table 3	A summary of the network related parameters.....	85
Table 4	Energy cost of the central controller in data transmission over the RBDS network .....	93
Table 5	The network overhead of Flooding with CI (including the controller) .....	100
Table 6	Interface setting of Flooding/AODV/ZigBee routing for multiple networks .....	149
Table 7	Interface numbering for different scenarios in simulations.....	150
Table 8	PHY layer parameters based after calibration [67].....	165

## List of Acronyms

AC	Alternating Current
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AN	Ambient Network
AODV	Ad hoc On Demand Distance Vector
AP	Access Point
ARP	Address Resolution Protocol
ARQ	Automatic Repeat-reQuest
BPSK	Binary Phase-Shift Keying
BPL	Broadband over Powerline
C&C	Command and Control
CBR	Constant Bit Rate
CI	Confidence Interval
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DR	Demand Response
DCSK	Differential Code Shift Keying
DSL	Digital Subscriber Line
DSR	Dynamic Source Routing
DSSS	Direct-Sequence Spread Spectrum
EEPROM	Electrically Erasable Programmable Read-Only Memory
ESI	Energy Services Interface
FEC	Forward Error Correction
FFD	Full Function Device
FIFO	First-In-First-Out
FM	Frequency Modulation
FSK	Frequency-Shift Keying
GPS	Global Positioning System
HAN	Home Area Network
HCS	Home Control System
HEMS	Home Energy Management System
HPA	HomePlug Powerline Alliance
HVAC	Heating, Ventilating, and Air Conditioning
IFQ	InterFace priority Queue
IrDA	InfraRed Data Association
ISM	Industrial Scientific Medical

ISP	Internet Service Provider
LAN	Local Area Network
LL	Link Layer
LNS	LonWorks Network Services
MAC	Medium Access Control
MIMC	Multiple Interfaces and Multiple Channels
MIRACLE	Multi-InterfAce Cross Layer Extension
MMS	Multimedia Messaging Service
MW-Node	Module-based Wireless Node
NetIF	Network InterFace
NS-2	Network Simulator Version-2
OO	Object Oriented
OTcl	Object-oriented Tool Command Language
PAN	Personal Area Network
p-CSMA	p-persistent Carrier Sense Multiple Access
PCT	Programmable Communicating Thermostat
PDR	Packet Delivery Ratio
PEMS	Premise Energy Management System
PER	Packet Error Rate
PEV/PHEV	Plug-in Electric Vehicle/Plug-in Hybrid Electric Vehicle
PLC	Power Line Communication
PLC-BUS	Power Line Communication Bus
PPM	Pulse Position Modulation
PSK	Phase-Shift Keying
P2P	Peer-To-Peer
PV	PhotoVoltaic
QoS	Quality of Service
RBDS	Radio Broadcast Data System
RF	Radio Frequency
RFD	Reduced Function Device
RREP	Route REPLY
RREQ	Route REQuest
RSSI	Received Signal Strength Indication
SIG	Special Industrial Group
SINR	Signal to Interference plus Noise Ratio
Tcl	Tool Command Language
TCP	Transport Control Protocol
TDMA	Time Division Multiple Access

TENS	The Enhanced Network Simulator
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

# **1 Introduction**

## **1.1 Background and Motivation**

Intelligent management of the power grid, aiming at promoting more even utilization of electricity and minimizing energy loss during power transmission and consumption is currently highlighted at the global level by utilities, academic organizations as well as public administrations. To protect the interest of both utilities and customers to the full extent, the idea of a smart grid, with enabling technologies has been put forward over the recent years and attracts great attention from the power industry and academy engaged in such explorations.

One of the aspects with regard to power grid management that electricity utilities are confronted with is effective and smart approaches to cope with peak load as well as other emergencies regardless of their occurrences. Considering the infrequency and short periods under such circumstances, a DR program [1], as one of the most common services in smart grid technology, has been introduced into the power grid. In this way, utilities are capable of achieving load balance in the power grid through the DR procedure by encouraging customers to reduce their electricity consumption during peak load periods with special bonuses/incentives in return. Meanwhile, residents could benefit from the DR services in terms of the electricity bill reduction when adjusting their electricity usage of home appliances in houses in response to dynamic pricing and other events associated with the reliability of the power grid issued by utilities.

Serving as a key enabling technology in the context of smart grid management, the Advanced Metering Infrastructure (AMI) [2][3], has been widely deployed to facilitate DR programs between utilities and residences, as Figure 1 illustrates:

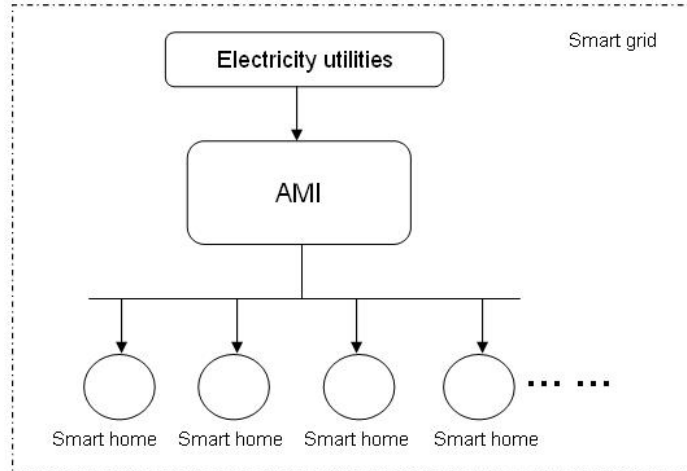


Figure 1 An ideal scenario of time-varying price through AMI to smart homes in smart grids

Generally, AMI covers smart meter units, device networking infrastructures, communication technologies, network management platforms as well as integration frameworks. Inside a smart home, a smart meter keeps track of message originated from utilities or third-party service providers through AMI and cooperates with the household central controller to schedule the usage of energy for home appliances based on the preference and pre-configuration of residents.

With the support of AMI, time-varying price messages are delivered to smart meters located in residents' houses. Based on these messages, smart meters issue instructions to smart appliances placed in houses by communicating with them in a wireless or wired way so as to accomplish end-to-end pricing transfer and power usage adjustment for the purpose of energy saving and improvement in power efficiency. Combining with the functionalities of a smart meter, a platform-centralized Home Energy Management System (HEMS) [4] plays a key role in automatic supervision of energy-aware smart appliances, small-scale renewable energy generation facilities around the houses as well as plug-in vehicles, and flexible cooperation with AMI in delivering resident-oriented messages.

To enable the HEMS in a smart home, both wired and wireless network technologies suitable for deployment in houses have to be evaluated and compared to meet the



requirements specific to residents. On the one hand, Power Line Communication (PLC) [5] has a long history of home appliance control due to the accessibility of power outlets in each room, which avoids the extra costs of wiring in most residences and thus promotes the convenience of promisingly seamless communication with utilities via underlying power line infrastructures. However, patent restrictions, unguaranteed reliability and lack of security, as well as high costs unaffordable to most residents inherent in some of these technologies restrict them in the advancement of smart home networking. On the other hand, short-distance wireless technologies emerging in recent years are featured with low speed, lower power consumption supported by battery supply, high cost-effectiveness and more flexibility in terms of networking and deployment in a house. Nevertheless, they also suffer from issues such as mutual interference with other technologies transmitting in a shared band, signal attenuation, shadowing and fading as well as multipath effects in the wireless environment that could deteriorate the quality of data transmission. In other words, there is no perfect solution to address every aspect in smart homes based on either PLC technologies or short-range wireless network technologies.

Only from the perspective of energy saving, it is interesting to explore what kind of networking solution suits well with smart homes and the efficiency of message transfer along with network performance in conjunction with the advancement of smart grid technology. For one thing, there are few publications and articles discussing such topics, particularly in terms of energy saving control due to the unavailability of realistic test-beds with a reasonable scale for independent experiments and lack of support in software simulation environments feasible to facilitate such evaluations; for another, lots of emphasis was placed on the energy management from the scope of the whole grid and corresponding underlying communication infrastructures on a large scale in the interest of utilities rather than residents.

## **1.2 Thesis Contributions**

In the thesis, we propose a networking solution to fill in the gap and boost research on energy management and networking technology involved in smart homes. It combines

ZigBee/IEEE 802.15.4 with HomePlug C&C that seems promising to smart homes in the sense that other factors are also taken into account in our proposal, such as openness of protocol stacks, layering-based interoperability and cost-effectiveness sensitive to customers, etc. Besides, the combined network could work with the support of renewable energy generation facilities available in the event of a power outage, whereas a HomePlug C&C network functions as an extensible and redundant medium necessary for data transmission in a house.

Given the idea of combined network, we designed and implemented an experimental model in the Network Simulator Version-2 (NS-2) software simulation environment along with resources publicly available to us in an effort to evaluate the network traffic and energy consumption on sensor-enabled nodes in smart homes. The complete simulation model includes a RBDS network and an indoor networking scheme of ZigBee/IEEE 802.15.4 plus HomePlug C&C in an environment of multiple interfaces and multiple channels. To simplify our model, we only focus on the connection of AMI (including a RBDS sender and a smart home controller in our model) with smart homes for the purpose of RBDS message delivery and device status updating in a smart home.

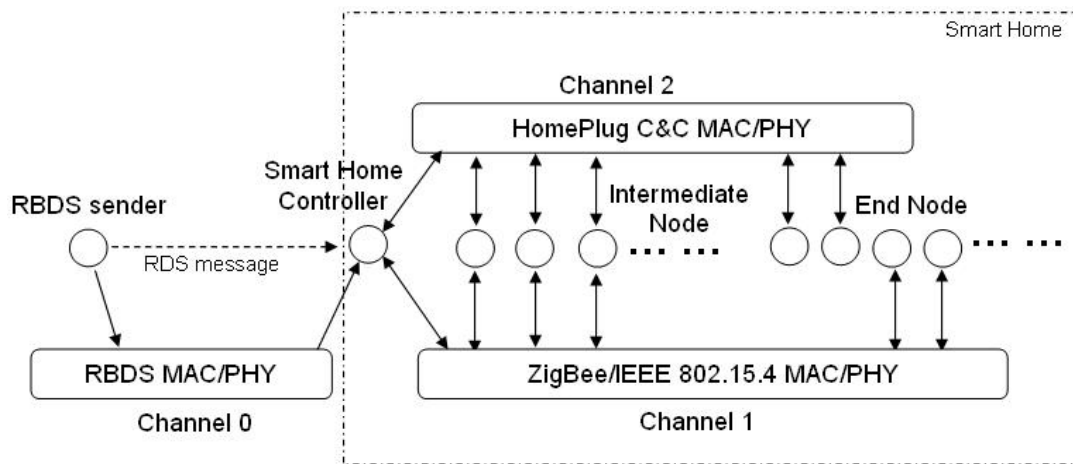


Figure 2 Simulation model of energy control network in smart homes

In the simulation model above, two nodes are involved in RBDS message transmission: the RBDS message sender at the electricity utilities (or third-party service providers) holds one interface to the RBDS network, and a smart home controller (an integration of

a smart meter and a centralized control platform in houses) holds three interfaces, one to the RBDS network, one to the ZigBee/IEEE 802.15.4 network and one the HomePlug C&C network irrespectively. Except the controller, all nodes in a house mimic the operation of home appliances in a smart home, such as refrigerator, water heater, dish washer, etc. A group of intermediate nodes are featured with interfaces to both the ZigBee/IEEE 802.15.4 network and the HomePlug C&C network in the house and function as both message recipients and forwarding nodes mainly targeted for RBDS packet transmission in the network based on the routes initially established to destinations. Also, this type of nodes could partially be configured as required to work through one interface to the HomePlug C&C network in order to mimic the behavior of smart home appliances that are only connected to the power line, with the wireless interface disabled in data transmission. The remaining nodes with one interface to the ZigBee/IEEE 802.15.4 network only act as generic smart home appliances located anywhere in a house, sporadically receiving RBDS messages through the central controller. Also, they are capable of forwarding these packets among other nodes that are connected to the ZigBee/IEEE 802.15.4 network.

Upon reception of a RBDS broadcast messages from the RBDS sender, the controller decides to send different messages reframed with new destination addresses that are pre-configured in the controller and the packet type indentified in a smart home to a range of devices in response to the new information gained about the power status/costs. All nodes in a house are configured in advance to receive these messages according to residents' preference. Meanwhile, any sensor-enabled node in the networking combination is capable of directly communicating with the smart home controller any time in terms of feedback of command execution, status report, etc.

Considering the sporadic nature of DR message delivery from utilities to residences, it is unnecessary to establish paths of packet transmission from the controller to destination nodes in a house in advance. Thus, three network layer protocols, including Flooding, AODV and ZigBee routing protocol, were adapted and integrated into our model to forward data packets from a RBDS network to a combined network in smart homes.

Flooding-based nodes forward data packets with the identical sequence number only once with the purpose of network performance, regardless of the number of interfaces and underlying links. With the support of the mechanism of timer-driven packet forwarding, AODV-based/ZigBee-based nodes in the network sequentially forward route request (RREQ) packets to destination nodes so as to avoid a broadcast-based storm caused by the simultaneous propagation of multiple RREQ packets from the central controller in the network. Meanwhile, four routing strategies are separately introduced in an AODV-based/ZigBee-based network. With the exception of the wireless link routing and the reliability-based routing directly configured in the scenario scripts, the remaining routing strategies are implemented individually in the AODV and ZigBee routing protocol to offer diverse routing alternatives to be exploited in the combined network. Besides, a united addressing scheme was proposed in the model framework to eliminate the issue of addressing collision accompanied by multiple interfaces/channels in the experimental model.

A group of metrics are adapted and combined with dynamic factors involved to evaluate the performance of the combined network from different aspects. Our research shows that a combined network generally outperforms a single wireless or wired network in the field of smart home networking from the perspective of energy saving. With a lower network overhead, a combined network can offer a PDR better to smart homes by offsetting the impact of dynamic factors with the aid of backbone. The simulation results indicates that the Flooding protocol shows a better performance than the AODV protocol and the ZigBee routing protocol when forwarding RBDS packets to all destination nodes in the network in terms of the network energy cost, the network overhead and the average latency. Concentrating on forwarding packets to individual nodes, a dual-path routing strategy and a backbone-based path routing strategy preset in an AODV-based/ZigBee-based network are superior to a joint-path routing strategy in terms of packet reception. Given a combined network, the choice of protocols and routing strategies depends to a great extent upon applications specific to smart homes and the demands of network energy cost and the average latency in a house in the interest of both utilities and residents.

To sum up, our contributions in the thesis are listed as follows:

- Comprehensively surveyed the features of home appliance control and the mainstream networking technologies applicable to smart homes for energy saving.
- Proposed a networking solution to smart homes that combines ZigBee/IEEE 802.15.4 with HomePlug C&C by establishing a simplified networking simulation model in NS-2 v2.33 with nodes equipped with multiple interfaces/channels and a unified address in the scope of the node architecture.
- Modified three network layer protocols (including Flooding, AODV and ZigBee), as well as the underlying links in order to handle and forwards packets over multiple networks.
- Integrated/configured four routing strategies into both the AODV and the ZigBee routing protocol intended for various simulation scenarios in a house.
- Evaluated the network performance as well as energy consumption of the simulation model by analyzing simulation results with different routing protocols/strategies.

### **1.3 Thesis Outline**

The remaining part of the thesis is organized as follows:

Chapter 2 briefly discusses the aspects of home appliances control in the context of the smart grid, ranging from electricity consumption and renewable energy generation and in smart homes, to the specific control scenarios along with the operation mode in the interest of both utilities and residents, presenting a group of benchmarks targeted for network technologies available in the areas of home appliance control.

Chapter 3 summarizes PLC technologies and low-rate wireless network technologies in terms of their technical characteristics, applications feasible to a smart home, as well as potential issues involved in home control networking, and proposes a competitive solution suited for a home control network for energy saving through a technical comparison between them.

Chapter 4 gives a brief review of the existing approaches to multiple interfaces/channels specific to networking scenarios and explains our solution that fits in our simulation model on the basis of the operational mechanism of NS-2, emphasizing the node

construction and interface connection of the simulation model. Also it discusses the addressing issues among nodes with multiple interfaces/channels in data transmission.

Chapter 5 presents a detailed modification to each type of network object from the bottom up in the framework of mobile nodes in NS-2, ranging from the node management of multiple channels/networks to the adjustment intended for RBDS packet transmission at the application/transport layer.

Chapter 6 describes the setup of simulation scenarios/parameters and the calculation of performance metrics and presents the corresponding simulation results.

Chapter 7 summarizes the main conclusions after simulations and suggests works to be explored in the future.

## **2 Appliance Control in Smart Homes**

To better understand the networking and control pattern in smart homes from the perspective of energy conservation, it is necessary to investigate the energy usage in most residences, the electric power sources that support the normal operation and management in a house, the configuration and control indispensable to build a smart home and the specific operation mode of home appliances and renewable energy sources and storage facilities. Also, architectural and functional requirements on behalf of utilities in the design of smart homes should be taken into consideration in that home energy control remains part of the overall smart grid infrastructures.

### **2.1 Energy Usage in Residences**

The main sources of energy consumption are the home appliances associated with heating and cooling, kitchen devices as well as lighting facilities. Among them, the operation of heating and cooling accounts for over 56% out of the total residential electricity consumption [6]. Even worse, a considerable amount of energy is not fully utilized by residents and energy waste occurs all day along. The author in [7] listed a group of factors that led to energy loss in a house as follows:

- 1) Endless working status of heating/cooling system in unoccupied houses and rooms
- 2) Overheating or overcooling to compensate for the temperature difference due to the constraints of a centralized thermostat.
- 3) Potential energy leakage due to appliances in a turned-off or standby mode (detailed data evidence was also found in [6]).

Inevitably, the improper applications of household appliances along with the lack of a smart energy infrastructure contributes to unnecessary energy consumption or waste in the majority of residences.

### **2.2 Generation and Management of Renewable Energy Sources**

Conceptually, a smart grid [8] integrates electronics and information technologies into the

massive electric systems in such a way as to strengthen reliability, flexibility, security, safety and efficiency as a whole. Put specifically, the implementation of smart grid technologies minimizes the electricity usage during costly peak hours by coordinating the load balance in the systems and leveraging demand-response mechanisms with time-based pricing notification oriented towards residents. As part of a smart grid, it makes great sense that a smart home includes parts of an AMI enabling the management of dynamic tariffs in homes, smart appliances intended for energy-awareness, renewable energy facilities and plug-in vehicles as well as the HEMS [4].

To some extent, distributed renewable energy sources installed in a house are here to mitigate the peak load in the power grid system in case of unexpected outages or blackouts. The majority of renewable energy sources are generated by solar or wind power (Geothermal heating generation systems are limited to geographic locations and climates). The PhotoVoltaic (PV) electric systems or solar panels [9] convert solar energy into electric power while wind turbines [10] utilize the kinetic energy in wind to produce electricity. The surplus electricity output generated by the PV system or the wind turbine could be fed back into the power grid system and in turn offset the residential energy consumption by the adjustment of AMI.

A Plug-in Electric Vehicle /Plug-in Hybrid Electric Vehicle (PEV/PHEV) [11] is a vehicle with a rechargeable battery that could be connected to an electric power source by a built-in plug. The PEV/PHEV could serve as a temporary energy storage bank intended for the power grid system and residential consumption [12], in which case the massive aggregation of PEVs/PHEVs plugged in the power grid substantially contributes to the peak demand and thus vehicle owners could get credit through the operation of AMI.

The deployment of HEMS integrated with renewable energy facilities owned by residents is illustrated as follows:



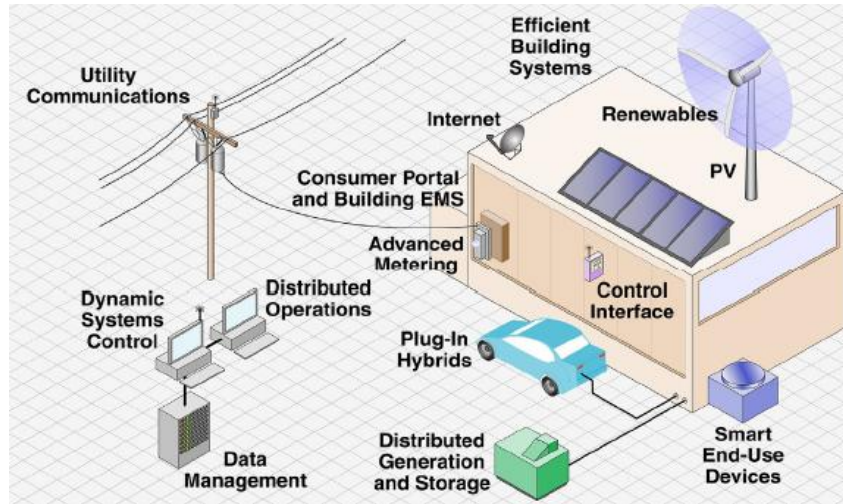


Figure 3 The household renewable energy management in the context of smart grid [4]

In addition to supervising the energy consumption by home appliances, the HEMS is also capable of managing the operations of solar panels and wind turbines, as well as the charging of PEV/PHEV as the back-up energy source, where the control interface functions as the central controller/residential gateway intended for home energy management and coordination. To be specific, the central controller cooperates with a smart meter deployed by utilities to schedule the usage of energy for home appliances according to the resident's preferences. In such case, the dynamic pricing notifications are issued by utilities or third-party service providers via power line or through other communication mediums to the smart meter. Following that, the central controller determines whether to introduce other energy sources available in the house, including PV system (solar panels), wind turbine and PEV/PHEV. If necessary, the central controller directly cuts off the power supply for a group of home appliances and postpones their execution to off-peak periods (at night) for cost saving. In addition, the central controller could be connected to the Internet for remote monitoring.

## 2.3 Configuration of Components and Energy Control

As suggested in [7][13], the standard components for energy conservation in a smart home are summarized as follows:

- Home appliance control platform or gateway intended for the control and management of the control network
- An intelligent utility electrical meter that keeps track of the power usage and serves as a portal of electricity information between utilities and household owner
- Renewable generation sources (solar panels/wind turbine) and energy storage facilities (PEV/PHEV)
- Wired (through power line) and wireless networking protocols and smart devices
- Networked programmable thermostats intended for cooperation with Heating, Ventilating, and Air Conditioning (HVAC)/refrigerator/water heater/lighting system to adjust and schedule tasks based on parameters sampled from target sensors [14]
- Sensors intended for strength of light, temperature, humidity and motion of objects
- Networked power boards over power lines connected to home appliances

With the support of a smart energy infrastructure, the control of home appliances combines the contextual adjustment with flexible strategies of power usage intended for home appliances with high or low power consumption respectively. Specifically, the smart control mainly consists of three types of scenarios:

- 1) When the residents stay at home, only appliances currently necessary for the residents are working, whereas others are cut off entirely from the power board to avoid standby mode. Meanwhile, the thermostat of controlled appliances (HVAC/refrigerator/water heater) cooperates with sensors/actuators to maintain a certain temperature suitable for residents.
- 2) When there is nobody at home, all unused appliances are cut off from the power board except the refrigerator; when the residents return home, the motion sensors may notify the control platform to guide all home appliances with thermostats into normal operation mode (i.e. a timed mode that lasts for a preset time range)
- 3) When the meter receives the notification of demand-response from utilities, it cooperates with the control platform to temporarily switch off all high-power appliances in use or to postpone their scheduled tasks to off-peak hours at night when renewable energy facilities are unavailable for power supply.

To sum up, smart control can be distributed where the thermostat helps to adjust the operation mode of controlled appliances or be centralized from the control platform to all appliances when a demand-response event or other emergency cases occurs in the house.

## **2.4 Redefinition of the Operation Mode**

In terms of energy management, the operation mode is categorized into two parts: home appliances, and renewable energy sources covering PV systems (solar panels), wind turbines and PEV/PHEV.

Given the practical demand of electricity, the major operation modes of home appliances and renewable energy facilities are redefined in terms of the schedule for execution or closure:

- Device registration when plugged in initially
- Request for power supply both in a house and in the power grid
- Switched on partially for the room when the room is occupied
- Switched off totally when nobody is at home
- Switched off according to the demand-response notification during peak hours
- Postpone normal tasks to off-peak hours (i.e. at night)
- Cut off from the power board (namely the distributed power board with multiple outlets that allows a couple of devices to be plugged in simultaneously) when the house is unoccupied in case of electricity leakage
- Adjust the temperature/humidity/the strength of light in the room for occupants (i.e. at night) with the support of thermostats/ dimmers/temperature sensors

From the perspective of energy utilization, what mostly happens in a smart home due to the dynamics of electricity prices is that the control platform chooses to adjust power supply and energy consumption in the house upon reception of this information from a smart meter. Firstly, it checks with the energy generation and storage facilities one by one by issuing a power supply request. If power is available, the facilities automatically switch their output towards the whole residence, with the power grid as a supplement; otherwise, the control platform sends a postponement message to all devices (including

PEV/PHEV) featured with high power consumption regardless of their current operation status and simply cut off power for a couple of devices in case of emergency. If some devices run at task mode (such as automatic defrosting of the refrigerator, heating of the water heater, temperature/humidity adjustment of the HAVC facilities, working mode of the dish washer, the washing machine, as well as the clothes dryer, etc.), they suspend their task immediately and return back to a low power consumption mode with an acknowledgement to the control platform, waiting for the next control message for task resumption.

## **2.5 Technology Independent Requirements of Utilities**

To provide a guideline of serviceability, security and interoperability intended for Home Area Network (HAN) device manufacturing and home network management in terms of electricity control, technical frameworks and functional considerations have been established and discussed in favor of utilities in [15]. The key devices in this framework are the Energy Services Interface (ESI) and the Premise Energy Management System EMS (PEMS). ESI is an independent device mostly provided by utilities and serves as a gateway between the AMI infrastructure and the HAN, whereas PEMS resides in a computer as an independent gateway with centralized control. Based on similarities in their functionality, the two entities could be integrated into one physical device. To establish a secure communication connection between utilities and HAN, all HAN customer devices associated with energy management must register themselves via ESI with the utility network. In this way, confidential control data or information sensitive to customer could be delivered through the secure channel from utilities to target devices in the home network. Also, device status information or operation result could be transferred conversely in the same channel to utilities for data recording. PEMS actually works as an application gateway to other functional components. It controls renewable energy generation, consumption and storage in the network, shares the functions with ESI to delivery control commands or events from utilities to smart appliances, and gathers all types of information from HAN devices.

Functionally, residents have the right to choose whether to accept the remote control from

utilities. To be specific, residents who own the HAN could grant the privilege of control to utilities by registering their own smart devices via ESI on the utility networks after applying for automatic energy management services. As another alternative, residents could also pre-program smart devices not to respond to the control command or load event from utilities for their own preference, regardless of electricity price dynamics.

## 2.6 Networking Pattern and Technologies

The author in [16] depicted the basic framework in a smart home setup as illustrated in Figure 4.

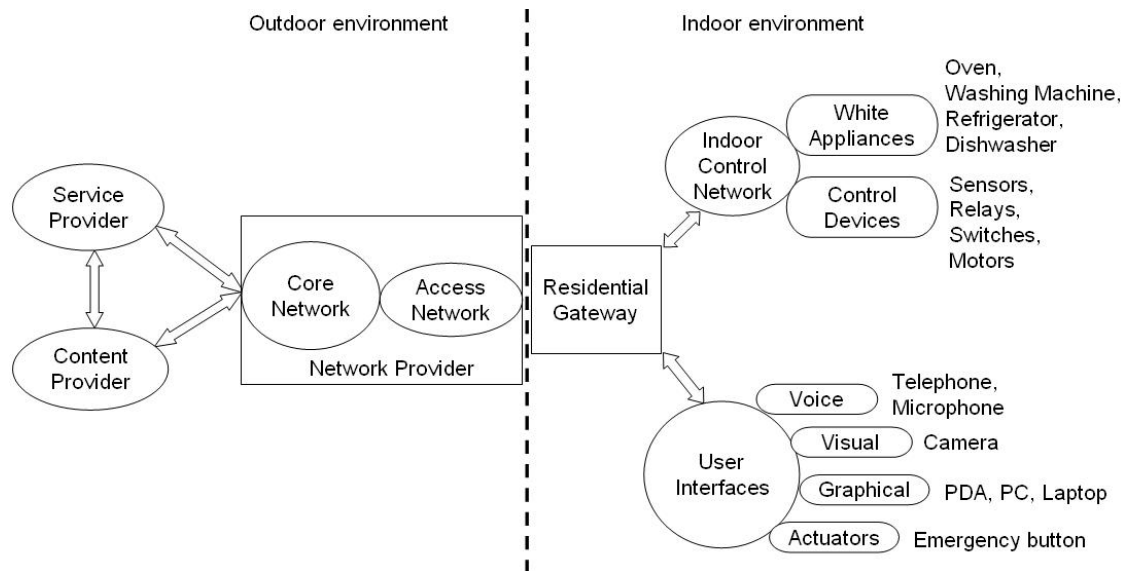


Figure 4 The concept of smart home[16]

The smart home is functionally categorized into two main networks: the broadband communication network mainly for things associated with personal needs such as entertainment, study or home office etc., whereas the control network is intended for the control and management of controlled appliances.

Both the broadband communication network and the control network converge at the household service gateway, which bridges the single home network to the outside network in a wired or wireless way. The gateway can be equipped with a normal interface for Internet access for indoor web surfing and e-mail retrieval, or with a wireless modem

directly attached to it for data exchange through long-distance mobile/wireless networks.

The control network in the smart home mainly supervises the regular operation for all kinds of home devices such as the switching-on/off for lamps and curtains, the start-up and stop of the air-conditioner along with the adjustment of temperature and velocity of wind, the signal collection and execution in security & surveillance system, indoor data measurement through wired or wireless sensors located at different places of the house as well as the adjustment of power usage based on the data indication on electrical meters. Under such circumstances, the control network is loaded with relatively small data packets required for control and sampling which are featured with relatively low signal frequency and accordingly low transmission rate in order to meet their requirements. Besides, the expectation of reliability is higher than in the network for entertainment in that excessive error or loss of control information happening in the network highly likely leads to the malfunction or even breakdown of target devices or will result in use discomfort, such as dishes not yet cleaned up, rooms with an extremely low temperate, and so forth.

According to [6][17], home devices used for heating and cooling are main sources of energy consumption in a house. Thus, we only focus on how to set up the control network for the purpose of energy saving on the background of smart grid infrastructures, in which case utilities notify residents of the incoming change of the electricity price via the intelligent meter in a wired or wireless fashion and enable them to adjust manually or automatically the schedule of operation for the home electrical equipments to avoid the demand of electricity during the peak hours in a demand-response manner.

There are several basic elements that matter in terms of electricity management:

- Relatively low transmission rate
- Lower power consumption
- Relatively high reliability and security in data transmission
- As little physical deployment as possible
- Low cost as a whole

- The coverage of the network
- Mainly for short control message in size periodically or in the case of emergency
- Seamless communication between the internal control network and utilities

The wiring layouts existing in most of residences are listed as follows:

- One socket for telephone line
- One cable jack for TV or cable modem for Internet access,
- At least one electrical outlet installed in each room of the house.

Telephone networking such as HomePNA and cable networking are undoubtedly taken out of consideration due to the cost of extra wiring for each room due to a shortage of outlets which make them less attractive in terms of home appliance control. The same is true of Local Area Network (LAN). For the control network, higher speed or bandwidth in data transmission is unnecessary in that each instruction or parameter for monitoring and adjustment on the network is short in size and such instructions are issued sporadically. Meanwhile, the cost of deployment mounts with the number of home appliances. Even for IEEE802.11 Wireless LAN (WLAN), the Access Points (APs) have to be connected to each other in such a way to construct a network, which also leads to extra cost and inconvenience to residents.

Technically, two types of networking techniques are widely adopted in the field of home appliance control. One is to directly transmit data over power lines, benefiting from the availability and the quantity of electrical outlets in a house. The mainstream protocols in Power Line Communication (PLC) technology are X-10, INSTEON, PLC-BUS, LonWorks and HomePlug. The other networking alternative is to exchange data between sender and receiver in a wireless way with a much lower speed than LAN/WLAN. The representative protocols in that case are Bluetooth, ZigBee/IEEE 802.15.4 and Z-wave.

## **3 Enabling Network Technology in Smart Homes**

### **3.1 PLC Technologies**

PLC technology [18] makes use of the distributed power line infrastructure to transmit data and control signals, in which case the high frequency coded with data is coupled onto the power line intended for decoupling by a modem on the receiver end so as to realize the information transmission and exchange. Originally, the application of PLC was chiefly to secure the normal operation of the electric power supply system in case of malfunctions or faults through the instant exchange of information between power plant, substation and distribution center, thereby making this approach a competitive alternative to smart home networking, considering the benefit of its robustness, ready connectivity as well as availability. In principle, the prerequisite of massive adoption of PLC technology is based on the fact that power lines have extended to every residence with multiple outlets installed in each room, which means that device control information and power supply are integrated as a whole through one outlet. As a consequence, there is no extra wiring indoors for the economy and convenience to residents.

#### **3.1.1 X-10**

As an international general-purpose protocol and a de facto open standard for Power Line Communication, X-10 [19] is applied to all aspects of home automation including house security and surveillance, home appliance control, indoor lighting control, household meter access, etc. It exploits the existing household electrical wiring to transmit digital data between X-10 enabled devices by encoding data onto a 120 KHz power carrier during the zero crossing (a time when the electrical current flows in a reverse direction and thus the unidentified noise diminishes to the minimal level) of the 50 or 60 Hz Alternating Current (AC) power wave, in which case one bit is transmitted at each point of zero crossing.

The system equipped with X-10 protocol normally consists of a controller module with a transmitter and multiple controlled components with a receiver, each of which is



distinguished by its own address code, configured by a combination of 16 house codes and 16 unit codes. For each X-10 data packet, it contains an identifier (a start code) followed by a house code and a function code. During the indoor deployment, the controller is plugged into one power socket, while the controlled components with house appliances attached to them are plugged into other power sockets, in which case the customer is able to input commands and component address code in a programmable way for the purpose of remote control of household appliances.

The main advantages of X-10 protocol over other similar technologies are listed as follows:

- Low cost for the overall deployment
- No requirement of extra wiring indoors
- Ease of installation for the convenience of household owners
- Interoperability and compatibility among commercial products

Admittedly, there are some issues that may delay its sustainable expansion in the field of home control network. A detailed performance evaluation of X-10 used for Home Control System (HCS) based on the on-site experiment in [20] indicated that its time to response is in inverse proportion to average distance for data transmission (the longer the distance is, the slower the response). As a matter of fact, there is no way to confirm whether or not the target device has executed the incoming instruction due to the one-way communication in X-10. Beyond that, a bandwidth issue associated with overhead occurs when multiple nodes compete simultaneously to communicate over the power line without effective support of medium access mechanism. The authors in [21] also suggested through experiments that X-10 transmission is susceptible to noises stemming from other appliances plugged into the shared electrical wiring. Meanwhile, other X-10 signals also disturb the normal operation of data transmission over power line [22].

### **3.1.2 INSTEON**

Introduced by SmartLabs, Inc. in 2001, INSTEON [23][24] is an X-10 model-based, dual-band mesh technology in home automation that is low in complexity, power

consumption, data rate and cost. The main goal of INSTEON is to serve as a replacement of X-10 in the mass market place in the sense that it tries to achieve fast response-time, reliability and robustness in data transmission through the combination of power line and Radio Frequency (RF) channels with a specially designed protocol.

INSTEON is much faster than X-10 on the basis of the fundamental discrepancies in carrier frequency and the transmission method from the perspective of mathematical analysis. An INSTEON-based device works at a frequency of 131.65 KHz over power line with Binary Phase-Shift Keying (BPSK) modulation and on a frequency of 904 MHz over RF physical channel with Frequency-Shift Keying (FSK) modulation at the same time. Like X-10, zero crossing is also adopted in the INSTEON technology to transmit data packets over power line during the time with the least noise disturbance. With 240 cycles of a 131.65 KHz carrier for one INSTEON packet, each INSTEON packet starts 0.8 milliseconds before a zero crossing and lasts 1.823 milliseconds to finish, whereas the X-10 signal adopts a burst of approximately 120 cycles of a 120 KHz carrier starting at the zero crossing and lasts about 1 millisecond to the end [25].

INSTEON establishes a Peer-To-Peer (P2P) mesh network with redundant capability, in which all INSTEON-enabled devices equipped with a transceiver and a repeater are equal to each other in functionalities and act as controllers (or command senders), repeaters intended for message retransmissions as well as responders (command receivers). The message is normally issued by a controller to responders via multiple repeaters without the need of a central controller and complex routing strategies. Each message must be responded to with an acknowledgement message except those intended for broadcasting. With the support of the simulcasting mechanism, the same message from the original controller is retransmitted simultaneously by multiple repeaters in the network at the same time within a given timeslot for the purpose of enhancing the signal strength.

Admittedly, INSTEON technology demonstrates its reliability and robustness only in terms of a theoretical model. Nevertheless, the lack of public academic literatures and substantial evidences from on-site experiments on a large scale due to its proprietary

nature prohibit people from being engaged in further research on it and possibly in turn limit the growth of INSTEON in the marketplace.

### **3.1.3 PLC-BUS**

Power Line Communication Bus (PLC-BUS) [26] was introduced by ATS Ltd located in Amsterdam, Holland in 2002 to provide a high-stability and low-cost solution to power line communication as compared to other contemporary power line technologies. PLC-BUS technology covers every aspect in home automations, ranging from lighting/home appliance/HVAC control to inter-communication between the appliances via the power line.

Similar to X-10, PLC-BUS utilizes the alternate current on power lines to transmit control signals to household electrical devices. Meanwhile, PLC-BUS is capable of checking the ON/OFF status of lights and home appliances via two-way communication as compared to X-10. What is more significant is that PLC-BUS employs a proprietary Pulse Position Modulation(PPM) [27] technology to encode data based on the location of the modulated pulses determined by the time intervals between pulses, which enables data transmission at a rate of 200bps at the frequency of 50Hz on power line. Specifically, the data-encoded frame corresponds to every half cycle of the sinus wave on alternate current close to the zero-crossing, in which case the frame is divided into four parts and the location of the pulse in each part denotes two bit. As a result, one byte-length data is encoded in every two cycles of the sinus wave.

PLC-BUS is mainly composed of three units: transmitter, receiver and equipment associated with system configuration. The controller, with a built-in transmitter, receives commands wired or wirelessly from a variety of communication terminals and converts these commands into PCL-BUS control signals that are transmitted via power line to a receiver to be executed for indirect manipulation of household electrical devices.

Due to the fact that there is actually no literature evaluating its performance either through simulations or via test-beds, researchers have reason to be skeptical of the

alleged features in PLC-BUS technology.

### **3.1.4 LonWorks**

LonWorks[28], introduced by Echelon Co. in the mid-nineties, is a general-purpose and peer-to-peer control network that is widely deployed in intelligent building and industrial supervision, mainly supporting a range of communication media including twisted pair, coaxial cable, fiber, Infrared/RF and power line, mostly due to its robustness, openness and interoperability. However, the overall price remains the main obstacle to the field of home automation in the sense that the LonWorks hardware components (including three microcontrollers per chip) attached to each home appliance for data transmission are more expensive as compared to other prevailing PLC technologies such as X-10.

The core technology of LonWorks is the Neuron chip that encapsulates three microcontrollers dealing with the embedded LonTalk protocol that refers to the seven-layer ISO-Model Protocol Stack and standardized in EIA-709.1[29]. Each of the three microcontrollers takes responsibility for functionalities corresponding to specific layers: the first one implements the control and processing at the physical (PHY) layer and the Medium Access Control (MAC) layer; the second one is in charge of management dealing with network routing and addressing from Layer 3 to Layer 6; the last one executes the services of the operation system and user applications [30]. Additionally, predictive p-persistent Carrier Sense Multiple Access (p-CSMA) algorithm [29] with a random time-slot based on priority level is adopted at the MAC layer of the LonTalk protocol, where it adjusts the probability of access to channel based on the estimation of network traffic load in such a way as to minimize the delay for shared medium access in lightly loaded networks and the probability of collisions in heavily loaded networks.

Normally, each control point called node in LonWorks-based networks consists of a sensor/actuator, Neuron chip with a unique 48-bit ID as well as a transceiver attached to the physical medium [31]. With a 3-layer addressing pattern (domain, subnet and node) and programmable nodes, LonWorks is capable of providing support for a variety of topologies including bus, star, ring, tree or hybrid on a large scale.

A possible networking pattern based on LonWorks technology via power line for smart homes was presented in [32], as illustrated as follows:

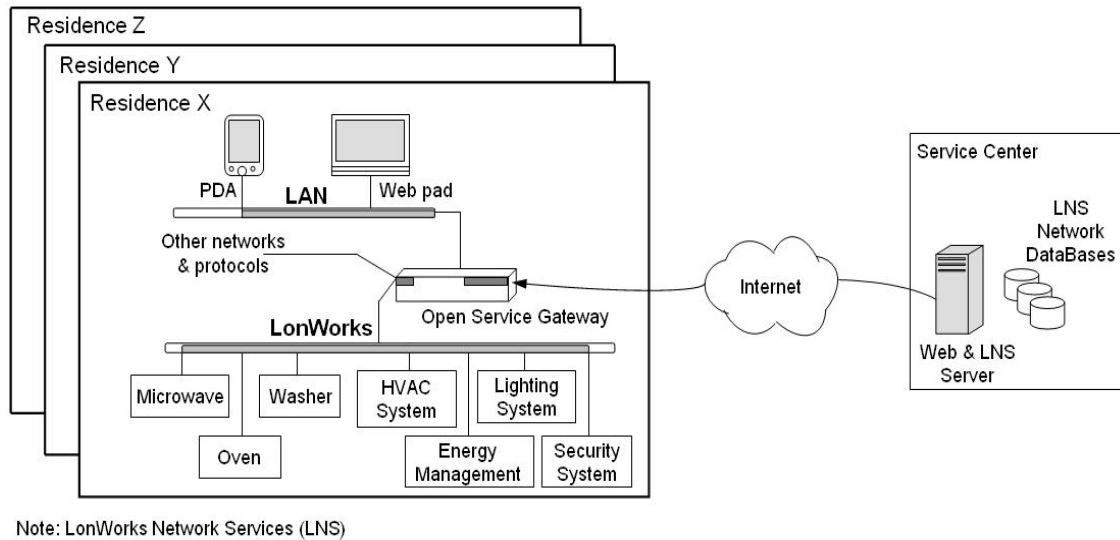


Figure 5 Smart home based on LonWorks networking pattern [32]

The solution can be seen as a typical application in smart homes in the sense that it explicitly divides the entire home network into two subnets, one of which is mainly control-centric for the majority of home appliances. The two subnets communicate with each other through a residential gateway that links the home network to the Internet. Besides, a LonWorks-equipped electrical meter can be installed on the power line and seamlessly interact with an energy management unit on the LonWorks network so as to dynamically adjust the electricity consumption in a house for the benefits of both utilities and residents.

The performance evaluation of LonWorks technology mainly covers two aspects: application-specific and p-CSMA algorithm specific. The authors in [33] built a simulation model by using a commercial simulation language (SIMAN v7.0) to explore the transmission delay of a network intended for various scenarios, indicating that the LonWorks protocol achieves a high performance in processing urgent asynchronous messages as long as such messages are transmitted within a maximum allowable delay from the perspective of customers, while it performs badly in the case of urgent

asynchronous messages with a minimal delay. The cross-validation of the p-CSMA algorithm at the MAC layer through a mathematical analytical model, an OPNET-based simulation model as well as a physical test-bed (a six-node network operating under a saturated condition where each node in the network always has a packet to send) was carried out by the authors in [34]. Through theoretical calculations and experimental results, they demonstrated that the channel access is treated as the decisive factor in a network with a large number of participating nodes, in which case the end-to-end delay increases due to a longer contention window. Apart from that, a similar approach found in [35] also suggested that the rate of the average channel access delay becomes lower once packets are transmitted in an acknowledged fashion.

### **3.1.5 HomePlug**

Since June 2001, a series of HomePlug specifications with different PHY modulation techniques were released by the HomePlug Powerline Alliance (HPA) [36] in efforts to boost the creation of standards or specifications for in-home power line networking products and services in a cost-effective, interoperable way, which includes HomePlug 1.0 with a rate of 14 Mbps for connecting household devices via power lines, HomePlug AV with a rate of theoretically 200 Mbps targeted for the transmission of multimedia data in residences, HomePlug Broadband over Powerline (BPL) for high-speed Internet access to residences and HomePlug Command and Control (C&C) that provides a low-speed solution with extremely low cost for home automation.

All specifications of HomePlug include a robust PHY layer and an effective MAC layer in order to guarantee reliable communication through power line mediums. The MAC layer in HomePlug is a variant of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, serving as the contention scheme for the channel access medium, including the mechanism of carrier sensing to detect the channel availability for priority-based assignment, as well as a backoff algorithm to increase network utilization based on different priority levels even in heavily loaded networks in the interest of Quality of Service (QoS). With CSMA/CA, the PHY can support data transmission and reception in a bursty mode, in which case each connected device starts

up the transmitter only when it has data to send. The transmitter is switched off and returns back to the reception mode once the delivery of data is over.

In the catalogue of HomePlug specifications, HomePlug C&C was developed and standardized in recent years to meet the basic consideration of cost and convenience in home control networking, ranging from home appliance monitoring, security, to Automatic Meter Reading and electricity conservation based on the Demand-Response mechanism as a feasible extension of the smart grid management technology [37]. Moreover, it specifies the bridge link to other RF networks such as ZigBee and Z-wave, etc.

In addition to the commonalities consistent with the HomePlug standards, HomePlug C&C also provides other features specific to the environment of home control. The maximal data rate of the PHY layer is 7.5Kbps with a patented Differential Code Shift Keying (DCSK) spread spectrum technology to secure robust transmission. Meanwhile, the MAC layer is based on Advanced Encryption Standard (AES) 128-bit encryption with authentication for security, providing support for up to 1,023 logical networks with 2,047 nodes per each network. In addition, the interoperability among household electrical devices configured with the HomePlug C&C protocol stack is specified on the host layer through a common description language that defines the services and actions of devices.

To evaluate the performance of HomePlug 1.0, the authors in [38] presented a HomePlug 1.0 based networking solution appropriate for a smart home as follows:

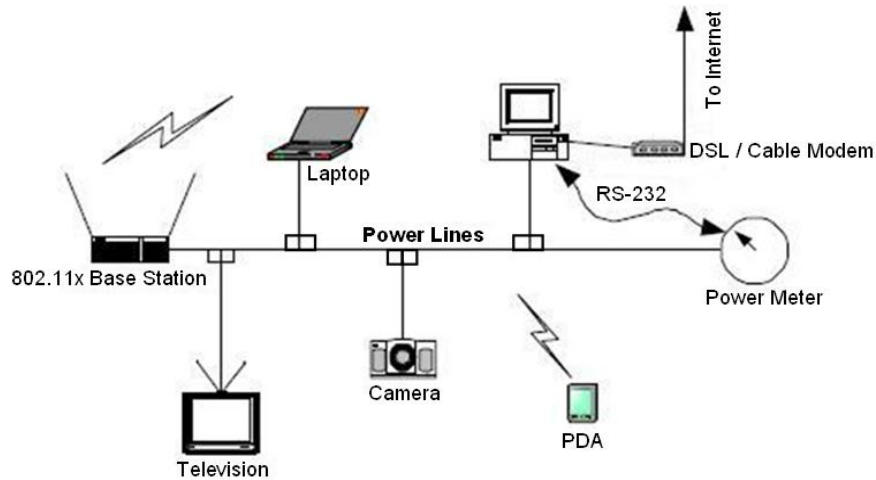


Figure 6 Network topology of smart home via power line [38]

The tree-line networking illustrated above is based on the common power line topology in a North American home. In this case, two power line trunks with different voltage (110V and 220V) are divided into several branches on which data can be transmitted. In Figure 6, home appliances along with multiple computers are connected onto the power line branch for data exchange at high speed. Meanwhile, there is one computer attached to a Digital Subscriber Line (DSL)/cable modem serving as the residential gateway to the Internet. Nevertheless, the solution does not include any device associated with energy conservation or demand-response control. In other words, the solution should address how to deal with multimedia data streams and control messages respectively with preset priorities over the same physical medium within a home if it is required to incorporate entertainment devices and household appliances into a single network for the convenience of management and supervision from the perspective for residents. On the basis of the existing power line network, the authors also demonstrated the performance of HomePlug 1.0 for multimedia data traffic in terms of TCP/UDP/MAC throughput and delay with an event-based simulation environment and a real HomePlug 1.0 power line network linked with multiple computers respectively.

Meanwhile, more researchers concentrated on the performance improvement of the existing MAC layer in the HomePlug family. A new analytical model to evaluate the MAC throughput and delay under both normal traffic and saturation was proposed in [39].



Another modification of the MAC sub-layer by defining a fast collision-avoidance mechanism to increase the throughput regardless of network traffic was simulated and discussed in [40]. For the moment, there is no literature exclusively for HomePlug C&C available to explore the specific applications or to evaluate its performance accordingly, partially due to the considerable annual membership fee demanded by the alliance.

### 3.1.6 Comparison of PLC Technologies

A summary comparison of chief features of these PLC technologies is shown as follows:

Table 1 Comparison of PLC technologies

TYPE	X-10	INSTEON	PLC-BUS	LonWorks	HomePlug C&C
PHY(Power line)	60Hz Carrier Frequency/ Zero-Crossing	131.65KHz Carrier Frequency/ BPSK modulation	Pulse Position Modulation	Carrier Frequency dependent	DCSK spread spectrum
MAC	N/A	N/A	N/A	predictive p-CSMA	CSMA/CA with adaptive back-off algorithm
Layering	N/A	N/A	N/A	OSI 7-Layer Model	PHY/MAC/Network/ Host
RATE(bps)	60	180 to 1698	200	3.6K or 5.4K	1.25K to 7.5K
COMMUNICATION	One-way without ACK	Two-way with ACK/P2P	Two-way	Two-way with ACK/P2P	Two-way with ACK
RELIABILITY	Low	High with simulcasting	High	High	High
ADDRESS SPACE	256	16,777,216	64,000	32,385 nodes per domain	2,047 nodes per network
STANDARD	Open	Proprietary	Proprietary	Open	Open
COST	Low	Low	Low	Expensive	Low
DEPLOYMENT	Simple	Simple	Simple	Complex	Simple

Obviously, one-way communication with low reliability remains the main issues in X-10. For one thing, all control messages are issued by senders without any feedback from receivers, in which case the final status of the target device is unknown to senders; for another, normal signals without any protection or recovery mechanism are susceptible to electrical noise from other home devices and even falsely recognized as different commands. INSTEON and PLC-BUS hold the same issues including the proprietary nature patented by a single private company and the lack of compelling support by independent experiments and simulations. LonWorks enjoys widespread acceptance in intelligent building and monitoring in manufacturing industries, but the cost of the

sophisticated protocol stack chips makes it unaffordable to most house owners. In addition to the reliability and robustness guaranteed by the technology itself, the openness of the protocol stack, interoperability of devices, as well as further extension for advanced applications are also key factors to be addressed for network deployment. Hence, the protocol standard specified in HomePlug C&C seems to be a reasonable candidate for the backbone of home appliance control in terms of PLC technologies.

## **3.2 Low-Rate Wireless Network Technologies**

Due to the complexity and cost of re-wiring and potential retrofit in a house, a variety of short-distance wireless technologies are emerging to provide flexible networking patterns convenient to residents without the considerations of physical wiring and deployment. These technologies, including WLAN, Bluetooth, ZigBee, Z-Wave etc., mostly work in the Industrial Scientific Medical (ISM) bands, especially the 2.4GHz frequency range. In terms of the control network in a smart home, they are characterized with low speed, low power consumption, high cost-effectiveness, flexibility in networking and deployment as well as the coverage of a house. Despite the fact that the InfraRed Data Association (IrDA) [41] technology remains one of the most popular wireless technologies globally, the main issue is that communication only happens directly between two devices within an extremely short distance with no physical barriers located between them. Hence, such drawback inherent in IrDA leaves it out of consideration for indoor wireless networking.

### **3.2.1 Bluetooth**

Bluetooth [41], promoted by the Bluetooth Special Interest Group (SIG), provides a comparably low-cost solution wireless communication among portable or handheld devices at a maximum data rate of 1Mbps within up to 10 meters. It operates in the 2.4GHz ISM band with as low as 0dBm transmission power and employs frequency-hopping spread-spectrum techniques to overcome interference and multi-path fading in the wireless channel. Meanwhile, Bluetooth adopts Forward Error Correction (FEC) and Automatic Repeat-reQuest (ARQ) to improve reliability by reducing errors in data transmission.

A standard Bluetooth network called piconet consists of a group of Bluetooth enabled devices sharing the same communication channel. In the piconet, only one device serves as the master unit that actively synchronizes with other devices, whereas the rest of devices serve as slave units that passively establish the communication with the master unit. Technically, a master unit is able to interact with up to seven slave units at the same time and synchronizes with more than 200 slave units without communication. In order to avoid interference from the same frequency, Bluetooth adopts Time Division Multiple Access (TDMA) technique to separate the communication between master unit and any slave unit in a piconet, which enables the master unit to communicate with other slave units in a peer-to-peer fashion by scanning.

Given the features of the Bluetooth technology, an End-to-End wireless solution for remote control in a smart home was established by the authors in [42], as illustrated in Figure 7:

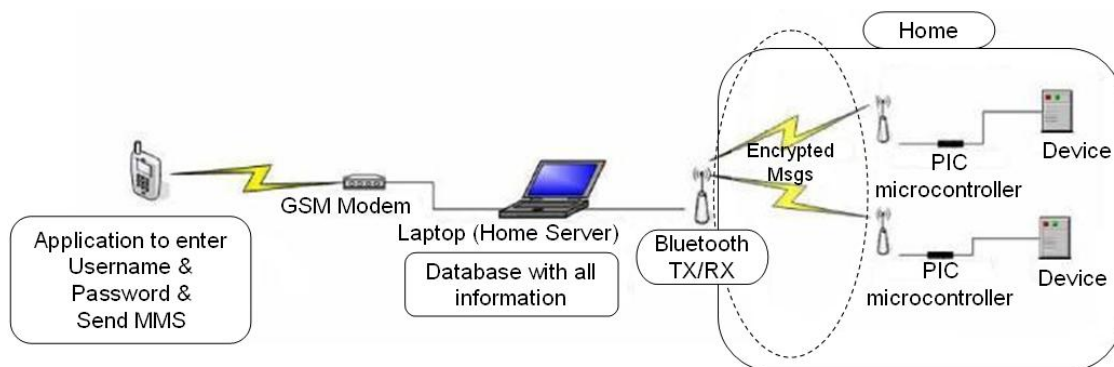


Figure 7 The architecture of a Bluetooth-based smart home via remote control [42]

The core of the smart home here is the home server, which is connected to the mobile network via a wireless modem to interact with the mobile phone via Multimedia Messaging Service (MMS) messages and which communicates with home devices via the Bluetooth connection. In addition, the responsibility of the PIC microcontroller is to supervise and control the household devices at the hardware level by executing a C application program, in which case the microcontroller receives and interprets commands from the mobile phone via the home server and sends operation instructions to target

devices. Another Bluetooth-based simplified solution to home control that is fundamentally similar to [42] was also implemented in [43]. The only difference between them was that the PDA/mobile phone took control of the home facilities via direct Bluetooth connection in the house.

### 3.2.2 ZigBee/IEEE 802.15.4

ZigBee/IEEE 802.15.4 [44][45] is a bidirectional wireless technology featured with short-range, low cost, low power consumption, low data rate as well as small size, which makes it more suitable for any domains associated with monitoring and remote control that is integrated with functional sensors and actuators. Normally, ZigBee/IEEE 802.15.4 works in the license-free 2.4GHz ISM band with a data rate of up to 250Kbps and the transmission distance ranges from 10 to 75 meters, depending on the power output and environmental dynamics [46].

In terms of the protocol stack, ZigBee/IEEE 802.15.4 entirely adopts the IEEE 802.15.4 PHY and MAC as the underlying layers to support reliable data transmission in a harsh environment with noise and signal disturbances as illustrated in Figure 8:

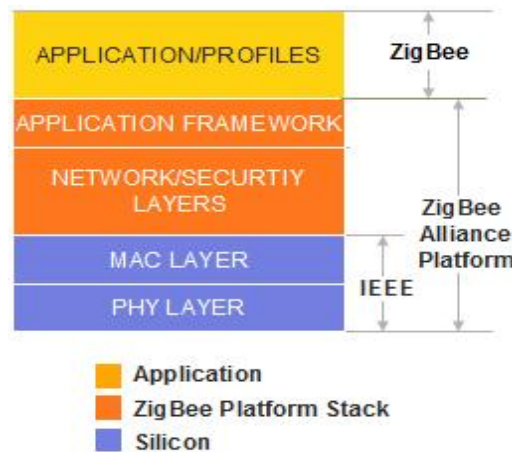


Figure 8 The architecture of ZigBee/IEEE 802.15.4 protocol [44]

At the PHY layer, ZigBee/IEEE 802.15.4 uses Direct-Sequence Spread Spectrum (DSSS) with two different Phase-Shift Keying (PSK) modulations to minimize interference. At the MAC layer, ZigBee adopts the CSMA/CA channel access mechanism to improve

network throughput and minimize transmission delay [46][47].

The main advantages of the ZigBee/IEEE 802.15.4 technology are summarized as follows [47][48]:

- 1) Low power consumption in terms of the battery life cycle installed in ZigBee devices.
- 2) Low data rate (250Kbps)
- 3) Short distance in terms of coverage in a house
- 4) Low cost, resulting from the low-rate and the simplicity of the protocol stack.
- 5) Supports as many as 65535 devices per network.
- 6) Robust and self-formed mesh networking allows for reliable data transfer.
- 7) Flexibility in networking with multiple topologies
- 8) Data integrity verification and authentication by adopting the 128-bits AES encryption algorithm at the MAC layer.

In comparison with ZigBee/IEEE 802.15.4, the main disadvantages of Bluetooth technology are the price of purchase, the number of network nodes, the limited distance along with the corresponding power consumption in terms of the coverage of home control network as Table 2 shows:

Table 2 Technical comparison between Bluetooth and ZigBee [49]

Comparing Wireless Technologies		
Feature(s)	IEEE 802.15.3 Bluetooth	IEEE 802.15.4/ZigBee
Battery Life	Days	Years
Complexity	Complex	Simple
Nodes/Master	7	65540
Latency	Enumeration up to 10 seconds	Enumeration 30 ms
Range	10 m	70 m–300 m
Extendability	No	Yes
Base Data Rate	1 Mbps	250 Kbps
Effective Throughput	700 Kbps	100 Kbps
Security	64-bit, 128-bit	128-bit AES and Application Layer
Application	File Transfer	Monitoring and Control

Given the characteristics of ZigBee/IEEE 802.15.4, the authors in [45] built an experimental environment for smart home solutions including energy consumption management, entrance guards, indoor security, home automation and real-time message

delivery. What is important here is that the home appliances are specially equipped with a microcontroller and sensors in such a way as to exchange appliance status information and instructions for control between appliances and ZigBee/IEEE 802.15.4 nodes. Another similar but simplified solution with sensors and actuator specially intended for environment dynamics was built in [48], featuring with more detailed control messages to the control actuator in XML format including node ID, device ID, category, control level, current status, action (on/off), the length of time, etc. In addition, the authors in [50] developed a ZigBee-based smart meter solution for the purpose of power management as illustrated in Figure 9:

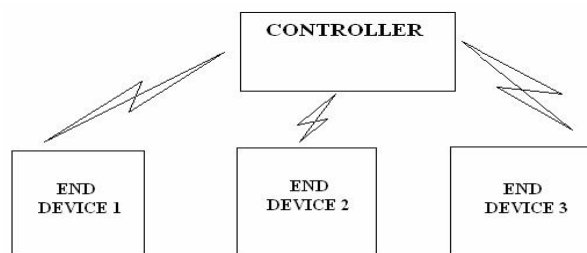


Figure 9 Smart meter solution based on ZigBee/IEEE 802.15.4 technology [50]

In this solution, the ZigBee/IEEE 802.15.4-based controller is equipped with a GSM modem which receives messages from utilities, whereas the ZigBee/IEEE 802.15.4-based end-devices are connected to a power factor measurement IC that calculates the power factor from the total power and the threshold stored on the Electrically Erasable Programmable Read-Only Memory (EEPROM). Specifically, the utilities notify the controller via the GSM network of power adjustments with a new power value. Subsequently, the controller first compares the value with the total power threshold and sends a message of adjustment to all end-devices. Upon reception of the message, the microcontroller in the end-devices recalculates the power value with the power factor and compares it with the stored threshold before taking actions, such as whether to keep the device operating or to switch it off.

Admittedly, harsh environmental conditions may deteriorate the quality of communication, as explored by the authors in [51]. They established a ZigBee/IEEE 802.15.4-based star network topology in their living laboratory home environment, where all electrical devices including home appliances and lamps were tagged with RFID in

order to identify themselves to the mobile receiver node carrier by a person. While the authors demonstrated an overall promising result of over 90% in terms of precision value and the acceptability of the signal strength measurement, the experiment indicated that the physical obstructions and disturbances are the key factors that influence data transmission in a ZigBee/IEEE 802.15.4 network.

### 3.2.3 Z-Wave

Z-Wave [52] is a proprietary wireless technology that was originally introduced by Zensys, a Danish-American Company and later advocated by the Z-Wave Alliance formed by manufacturers who build products based on Z-Wave technology. Specifically, Z-Wave is oriented towards residential control and home automation with a concise protocol stack appropriate to home facilities in order to reliably transfer the messages in a house. The protocol stack of Z-Wave is shown in Figure 10:

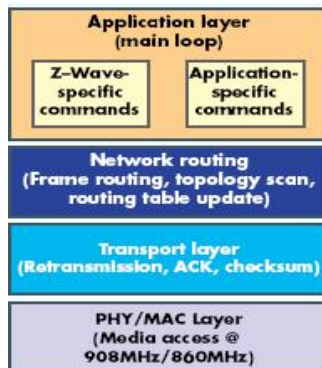


Figure 10 Protocol architecture of Z-Wave [53]

As illustrated above [53], Z-Wave works in the ISM band of both 860MHz (for Europe) and 908MHz (for U.S.A). It adopts FSK modulation with Manchester channel encoding at the PHY layer at a data rate of up to 40Kbps within 100 meters. At the MAC layer, Z-Wave uses standard CSMA/CA mechanism that manages access to the radio frequency medium when it is in a busy mode.

Similar to ZigBee, Z-Wave also defines two sets of nodes to support a self-healing mesh networking pattern: a controller that is in charge of configuring a series of parameters for the establishment of the network and slave devices that server as either end-nodes or

repeaters with routing capability for data forwarding. With the support of a dynamic routing selection mechanism in Z-Wave, routes at most 4 hops long are enough to entirely cover every spot for most residences [53].

The main features of Z-Wave are summarized as follows [54]:

- 1) Simplicity of installation and deployment with automatic address assignment for the convenience of network management.
- 2) Lower cost based on the integration technology on chip.
- 3) Ultra low power consumption with the help of the lightweight protocol stack and compressed frame format.
- 4) Very small in size in terms of the hardware module for the benefit of integration with other devices.
- 5) Excellent in anti-disturbance with the support of two-way acknowledgement, random back-off algorithm and collision-avoidance [52].
- 6) No support for data security in communication.

To evaluate the performance of a wireless sensor network in a real environment, the authors in [55] established two groups of experimental deployments based on different scenarios for both ZigBee and Z-Wave respectively. The location of the Z-Wave based nodes in the network is illustrated in Figure 11, similar to the topology of ZigBee.

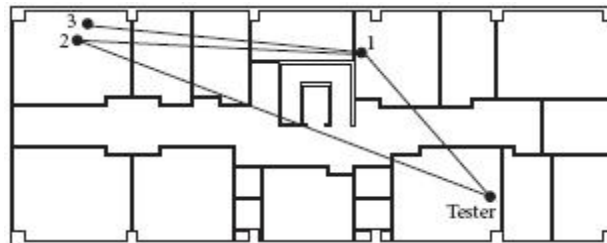


Figure 11 Setup of Z-Wave network [55]

Besides physical deployment of the ZigBee network, the author also built an OPNET simulation environment to analyze the performance based on the measurement of Received Signal Strength Indication (RSSI), throughput, delay and Packet Error Rate (PER). It is indicated that the experimental findings are consistent with the simulation



data and theoretical deductions.

With respect to the Z-Wave, the authors only examined the PER in the preset environment without the support of simulation and theoretical performance analysis due to the proprietary nature of the Z-Wave protocol stack. Despite these restrictions, the experimental results demonstrated that Z-Wave performs well over one-hop links with a distance longer than 20 meters under attenuation, reflection as well as the link breakages that are caused by the movement of passers-by.

Based on the experiment, the authors suggested that the external factors including signal attenuation, reflection, multipath-effect, man-made interference as well as the location of the deployed node negatively influence the network performance.

### **3.3 Conclusion**

The main advantages of the PLC technologies superior to other alternatives is the availability of power line outlets in each room for a house, which avoids the costs of additional wiring in most residences and the convenience of the promisingly seamless communication with utilities via power line. However, issues still exist in these protocols. The drawbacks of X-10 are the unguaranteed reliability in data transmission (i.e. data signal via power line is treated as noise and filtered out afterwards) and the lack of security mechanism due to the limitation of frame length. While INSTEON and PLC-BUS allegedly outperform other PLC technologies from all aspects and pose a serious challenge to X-10, it is difficult to evaluate them without extensive experiments on a large scale and the overall evaluation of performance based on both simulation and on-site data due to the proprietary nature of this technology, which in turn delays their adoption to some extent. The comparably high price of LonWorks overshadows its excellent performance in the sense that the technology is initially oriented towards building automation.

Despite the fact that the short-range low-rate wireless technologies have features in common with the PLC technologies in terms of installation and cost, there are also other

issues to be taken into consideration and to be addressed. First of all, they possibly operate on the same ISM frequency band which gives rise to the overload resulting from a high-degree of mutual interference with each other [56], especially in the case that a WLAN is deployed in house. Secondly, signal attenuation, shadowing as well as multipath effect in the wireless environment deteriorate the quality of data transmission. In addition, those technologies also show vulnerability to malicious wireless attacks such as jamming, forging of random collision frame, etc. [57]. For Bluetooth, the main obstacle to the field of home control network is the total cost. As a proprietary protocol, Z-Wave suffers from the same problem as INSTEON and PLC-BUS, lacking substantial analysis of its performance based on massive on-site experiments and simulations.

In short, there is no solution that addresses all aspects in smart homes based on either PLC technologies or short-range wireless network technologies. Hence, it is more desirable to combine PLC technologies with wireless network technologies in some way to meet the practical requirements in smart homes in terms of energy saving. To be specific, a backbone network of HomePlug C&C plus ZigBee/IEEE 802.15.4 seems more promising for home appliance control in a smart home in the sense that the suggestion also takes other factors into account, such as openness of the protocol stack, interoperability based on layering and cost-effectiveness, etc.

## **4 Implementation of Simulation Model Architecture**

A networking simulation model combining ZigBee/IEEE 802.15.4 with HomePlug C&C was implemented in NS-2 v2.33. Given the existing mechanism of NS-2, nodes in a smart home are reconstructed on the basis of the architecture of the simulation model so as to produce and forward data traffic in multiple networks. Besides, the node addressing scheme was proposed to avoid the address discrepancy of nodes featured with multiple interfaces/channels during simulations.

### **4.1 Existing Solutions to Multiple Interfaces/Channels**

The architecture of a mobile node and the operational mechanism of network objects within a mobile node inherent in NS-2 are only suitable for the creation of nodes with a single channel over a single network [58][59]. To meet our requirements of multiple channels over multiple networks in smart home networking simulations, the connection between network objects, the organization of connecting nodes as well as part of the implementation logic within network objects needs to be adjusted on the basis of the principle of node construction.

Multiple Interfaces and Multiple Channels (MIMC) has already been attracting attention in the academic community for its improvement of the overall performance and throughput in wireless networks. From the perspective of software modeling and simulation, the major efforts are placed upon the creation of mobile nodes equipped with MIMC and the optimization of MAC and routing options aiming at promoting the utilization of multiple channels (summarized in Section 5.3) within a mobile node during data transmission. Served as a range of constructional comparisons with our networking simulation model, these solutions to MIMC adopted in NS-2 are briefly summarized below in the context of their own applications.

#### **4.1.1 TENS**

The Enhanced Network Simulator (TENS) project [60] was built in an attempt to address

the omissions encountered in modeling the IEEE 802.11 WLAN. To make it more realistic in simulations of long distance links, the TENS project also supports multiple interfaces for mobile nodes, a static routing protocol as well as a simplified directional antenna model, as partially illustrated in Figure 12:

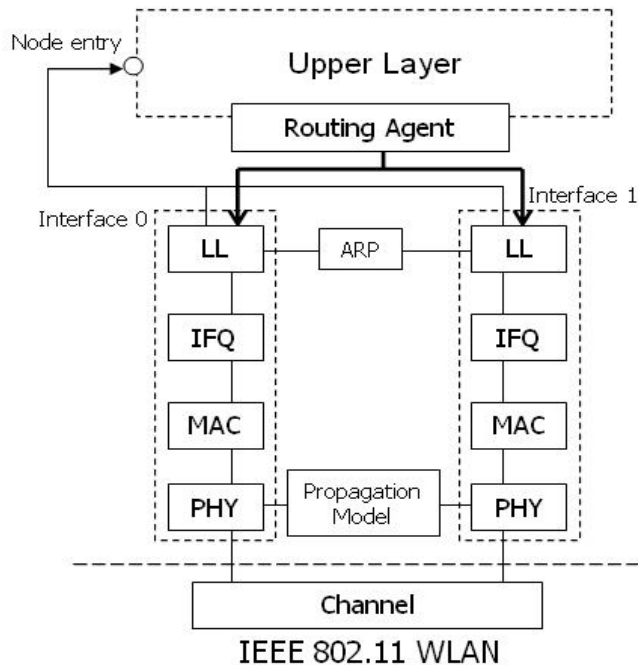


Figure 12 Architecture of mobile node in TENS

Specifically, it is assumed in this solution that all nodes co-exist in only one network regardless of the number of their interfaces. As a consequence, a table for MAC address resolution as well as a radio propagation model is implemented in a shared way among interfaces within a mobile node. Apart from that, a single channel object is multiplexed in the architecture to mimic the packet delivery behavior over multiple channels by indexing each pseudo-channel explicitly in scenario scripts. With the shared channel object, the metrics associated with co-channel interference can be calculated for each PHY layer object when transmitting packets in the same network.

In terms of the construction of a mobile node, this solution does not differentiate which interface at a receiver side is eligible to handle incoming packets. Hence, the PHY layer object bound with one pseudo-channel within a mobile node could receive packets originated from other pseudo-channels with high probability. In addition, the mechanism

of simplified channel multiplexing downgrades the realistic behavior occurring in multiple channels to some extent and further impacts the network traffic with the increase of mobile nodes in that all packets to be transmitted in the network are scheduled simultaneously over the same channel object.

### 4.1.2 Hyacinth

A multi-channel Wireless Mesh Network (WMN) architecture called Hyacinth was proposed by the authors in [61] so as to address the issue of constrained bandwidth by fully utilizing existing non-overlapped radio channels available in the IEEE 802.11 specifications. The Hyacinth prototype was evaluated in NS-2 simulation and a test bed experiment environment was also established to demonstrate its feasibility in improving the network throughput as compared to a single channel ad hoc network when the prototype was deployed in an wireless network owned by an Internet Service Provider (ISP) or a wireless enterprise backbone network, as illustrated in Figure 13.

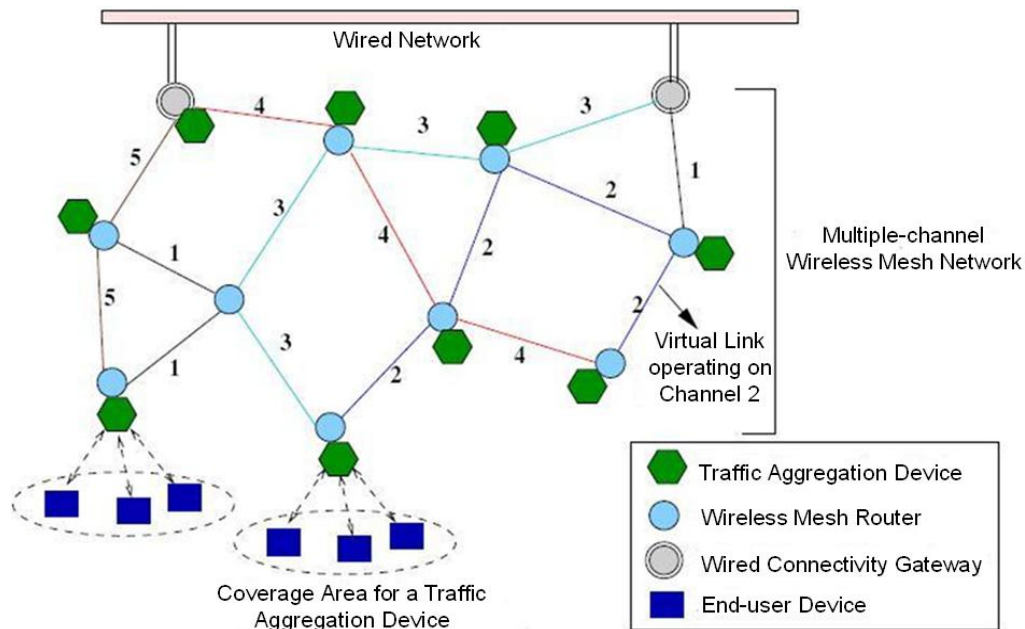


Figure 13 The Hyacinth prototype with multiple channels [61]

The main goal of the prototype is to enable end-user devices to access the Internet or an enterprise internal network via the multi-channel WSN core which is composed of a group of wireless mesh router nodes and traffic aggregation devices. Each router node in

the core is equipped with only two interfaces and each interface within a router node is bound to a distinct radio channel, considering the neighboring nodes within the signal interference range and the total number of channels initially allocated in the core. Any two router nodes within communication range should share at least one channel intended for direct communication with each other in an attempt to forward the data traffic originated from end-user devices to the wired network through the router gateway nodes. To achieve this goal, a fully distributed channel assignment algorithm along with a multiple spanning tree-based routing algorithm was adopted in the prototype to support dynamic traffic adjustment for the purpose of load balance.

It is evident that the prototype is partially scenario-specific with the algorithm employed above in terms of the direction of the data flows in the network, which prevents it from being extended to more general cases. Besides, the prototype only supports a static routing configuration in simulation scripts and forces all nodes involved to be generated with the same number of interfaces, irrespective of whether they are used in execution.

### **4.1.3 Dynamic Interface Extension to NS-2**

The approach implemented in [62] to a great extent refers to the idea of interface construction within a mobile node proposed in [61], as illustrated in Figure 14.

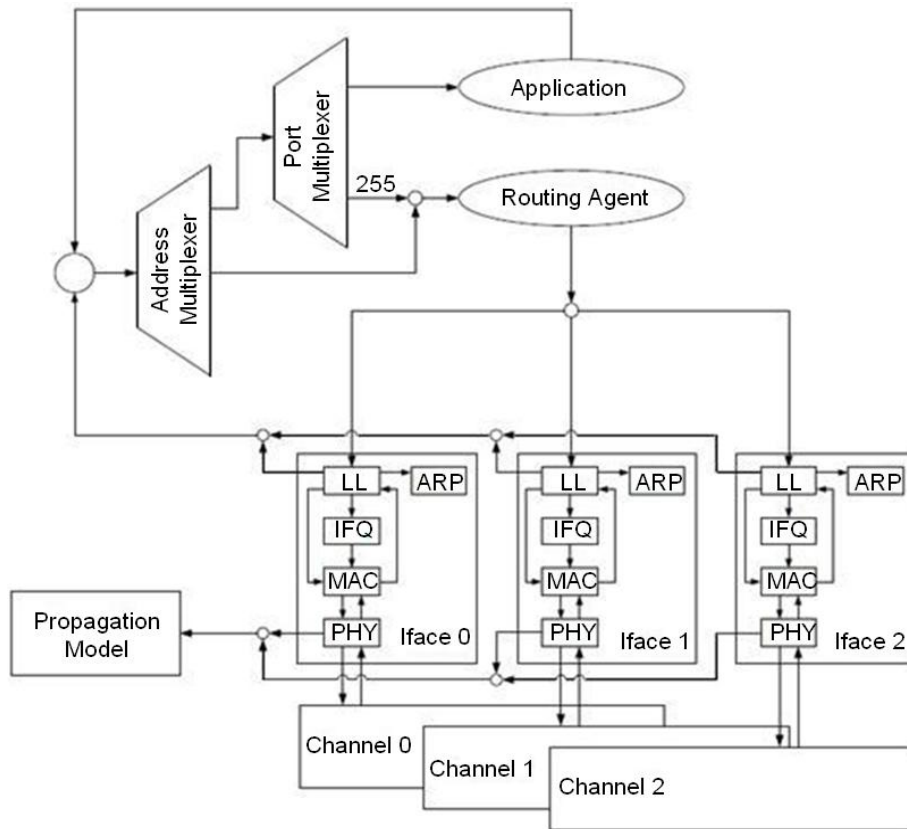


Figure 14 Dynamic interface extension intended for a mobile node [62]

Specifically, the authors designed and implemented an architecture for mobile nodes that is featured with a comparatively flexible configuration through simulation scripts, as compared to the approach in [61]. Nodes with a different amount of interfaces could co-exist in the same scenarios for communication. Meanwhile, each interface of a mobile node is assigned a single channel object, in which case packets passed down from the upper layer could be transferred respectively over multiple shared channels among nodes. In addition, all interfaces within a mobile node are attached to a dynamic routing protocol for the purpose of united packet forwarding with the support of the underlying interface index calculated from the corresponding MAC address.

To sum up, the approach only focuses on the scenario of multiple channels within an IEEE 802.11 network in the sense that a common radio propagation model is shared among all PHY layer objects when transmitting packets. Beyond that, it does not address the issue of address mapping from a node to multiple MAC objects attached to the node

intended for the identification of packet addresses, since packets are transferred at the lower layer with the source and destination address distinct from the upper layer.

#### 4.1.4 MW-Node

A Module-based Wireless Node (MW-Node) is an innovative layout of a mobile node implemented by the authors in [63][64] to support multiple interfaces through reorganizing the existing components responsible for the functionalities of mobile node, as shown in Figure 15.

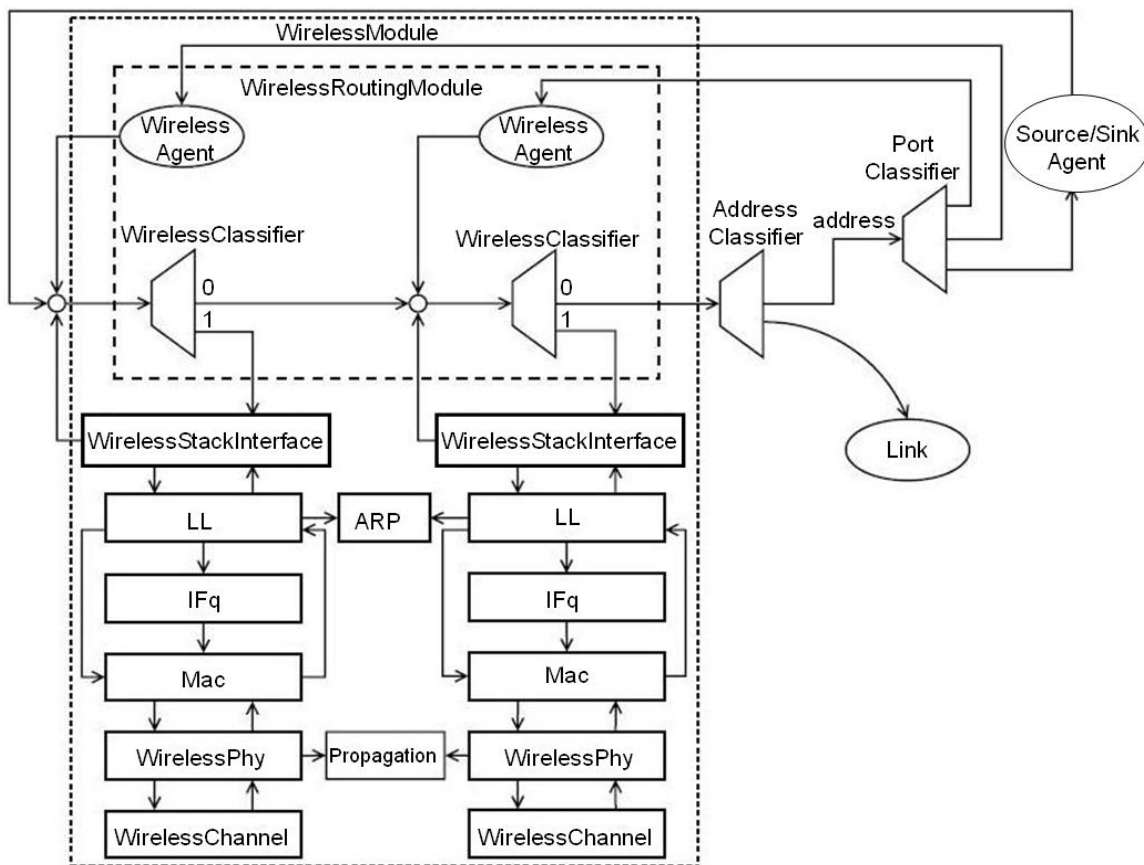


Figure 15 Schematic design of a MW-Node [63]

One of the major features in a MW-Node is that a routing protocol object originally linked to mobile nodes is replaced with a wireless routing module that functionally subdivides the routing protocol into two separate modules: a wireless agent and a wireless classifier. The wireless agent takes responsibility for generating packets associated with data routing and tagging them with the corresponding interfaces connected to it, whereas



the wireless classifier is primarily used for forwarding the packet from the wireless agent or a source agent within mobile nodes to destination nodes. In addition to that, it is the wireless stack interface that tags incoming packets with the current interface identifier before handing them over to the wireless routing module.

Meanwhile, the author assumed that some of mobile nodes might play multiple roles at the same time in a wireless network. Therefore, a wireless agent along with a wireless classifier is created and interconnected in the wireless routing module so as to support multiple routing protocols within a mobile node when another interface is attached to the mobile node. As a consequence, a routing information base is shared among multiple routing protocols, which enables the wireless routing module to determinate over which interface to send packets originated from the upper layer or received from one of the underlying interfaces.

The main drawback of the architecture is that it is mostly oriented towards emerging routing protocols which could be built upon the subdivision mechanism at the sacrifice of backward compatibility with existing routing protocols in NS-2. In addition, interfaces of a mobile node fail to remain entirely independent from each other since they still share an Address Resolution Protocol (ARP) object as well as a radio propagation model at the lower level.

#### **4.1.5 MIRACLE**

The authors in [65][66] presented a Multi-InterRfAce Cross Layer Extension (MIRACLE) to NS-2, which serves as a generalized modular framework aiming at providing well-defined software interfaces for new features in NS-2 so as to facilitate simulations in the environment of multiple radio technologies. To be specific, the whole architecture is featured with modularization at each layer and cross-layer communication due to constructional design and functionalities involved, as shown in Figure 16.

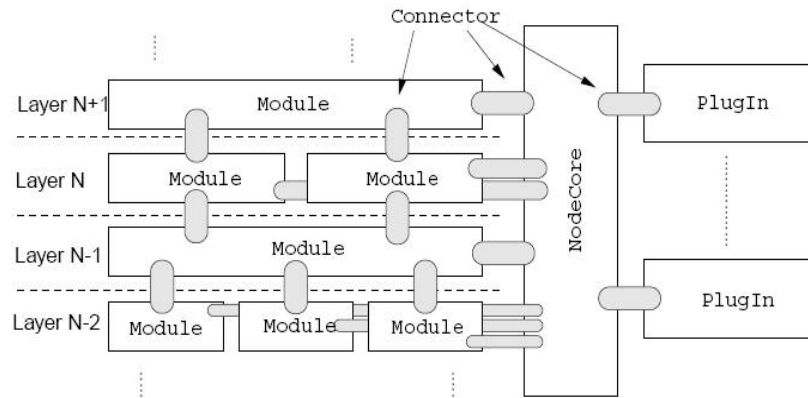


Figure 16 The general modularized architecture within the MIRACLE framework [65]

Each module in the architecture is an independent software container encapsulating a functional entity or a protocol object that includes application, transport layer, routing layer, MAC, PHY, and so forth. Multiple modules with identical functionalities can share the same protocol layer and establish multiple protocol stacks independent from one another by linking to their upstream and downstream modules with Connector objects. Meanwhile, a unique structure called NodeCore placed at multiple layers acts as a coordinator and a manager that enables inter-module communication and provides common functionalities for all modules, whereas each PlugIn object, attaching to the NodeCore holds cross-layer algorithms that are employed in message exchanges among modules. Consequently, a module is capable of communicating with any other module by sending messages through a Connector object with the support of the NodeCore and the PlugIn objects.

To reuse the existing protocol implementations in NS-2, the parameter interfaces of each protocol class and the mechanism of packet transfer within the protocol class have to be fundamentally adjusted to suit the demands of modules specified in MIRACLE, which seems to be a burdensome and time-consuming tasks to researchers from the perspective of backward compatibility. Moreover, the authors failed to cover the issue of whether or not the cross-layer object communication has a negative impact upon the normal packet delivery in terms of delay. In addition, the whole architecture and the corresponding architecture is scenario-specific to some degree in dealing with the issues of routing among multiple interfaces as well as how to utilize the underlying channel objects in a

detached way, since the whole architecture was well-tuned by the authors to support their own Ambient Network (AN), combining it with Universal Mobile Telecommunications System (UMTS) and IEEE 802.11 in the context of beyond 3G networks.

#### **4.1.6 Conclusion**

Undoubtedly, there is no alternative that is appropriate to address generic issues that arises in the context of MIMC among multiple networks. Existing solutions to the issues of MIMC are project-specific in the sense that the architectural design of nodes and the majority of procedures in handling packets are mostly tailored to a special scenario such as multiple interfaces with a single radio technology, a mixture of wireless and wired network, etc. In terms of software implementation, technical tradeoffs always exist between the architecture of mobile node and the internal mechanism of protocol objects during data transmission. Even so, a wide range of methodologies with regard to the node construction as well as packet forwarding were explored in these solutions which lay the foundation for the implementation of our simulation model.

### **4.2 Our Solution to the Networking Simulation Model**

The solution to our project is partially inspired from the idea of dynamic configuration in [62] and the modularity of node construction in [65]. Unlike these solutions mentioned above, we focus on the scenario of multiple channels, each of which belongs to a single network. Meanwhile, packets issued by one mobile node in one of these networks are required to be transmitted to any destination node over other networks based on the scenarios specific to our implementation. Thus, the construction of a mobile node is the first step to be taken to deal with the issues of MIMC in our project. The implementation mechanism of protocol layer objects should be modified according to the established framework so as to meet our demands in smart home networking simulations (discussed in Chapter 5).

## 4.2.1 Architecture of Mobile Node with Multiple Interfaces

To clarify the layering and modularized structure of mobile nodes in our solution, a general architecture of a mobile node is shown as follows:

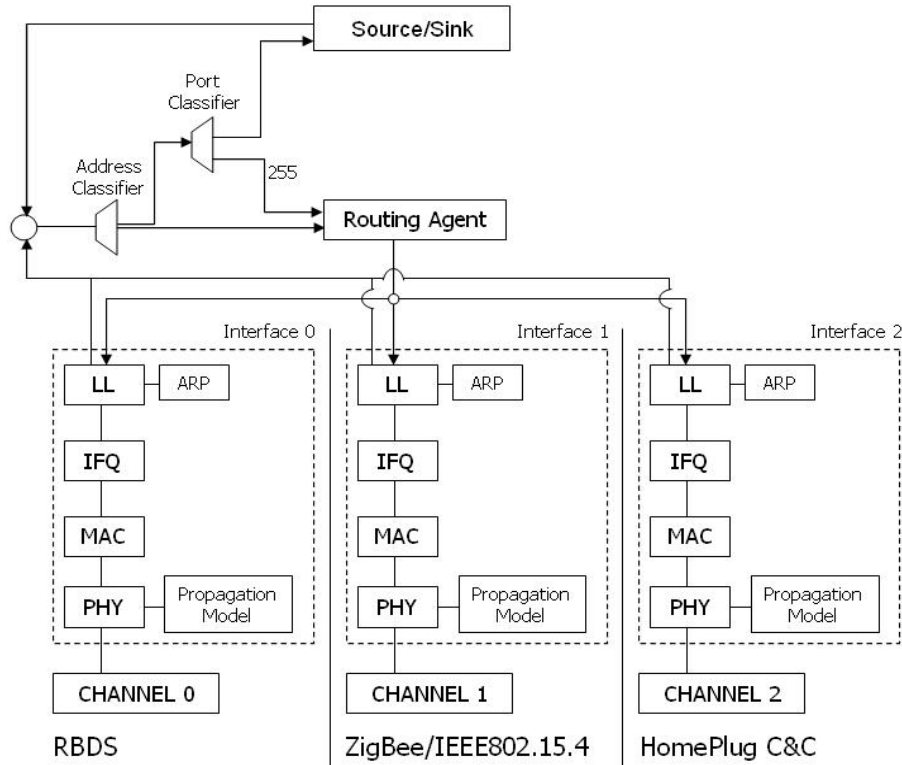


Figure 17 General architecture of mobile node with multiple interfaces/channels

In terms of the functionalities of each object in the architecture, there is no difference between our solution and the original framework of a mobile node existing in NS-2. However, the number of supported protocol stacks below the routing agent dynamically increases. Equipped with a unique index, each set of protocol stacks within a mobile node serves as an independent interface linked to an underlying wireless network for the purpose of data transmission. In order to do so, each physical layer object holds a single radio propagation model object configured in advance for its own use. Meanwhile, each channel object oriented towards one network in our simulation is independent from others with respect to communication-related parameters that were originally shared in NS-2 (discussed in Section 5.1). In addition, the static numbering allocation for channels used in NS-2 is also kept so as to enable each channel object to distinguish itself from others,

which entirely identifies each wireless network in simulations.

Currently, there are four types of mobile nodes involved in our project: one node with one interface used for RBDS message broadcasting (the RBDS message originator), one node with three interfaces (the smart home central controller) mainly responsible for RBDS message forwarding from the RBDS network to the other two networks in the smart home, a group of intermediate nodes with two interfaces acting as both routers with multiple paths and RBDS message recipients, and the remaining nodes with one interface active for data transmission, functioning as ordinary nodes in the ZigBee/IEEE 802.15.4 network or the HomePlug C&C network. To handle packets received from different networks for all types of nodes, the node entry point is concurrently linked to multiple interfaces available in the node so as to pass incoming packets up to the corresponding layer object. Besides, the routing agent has to make decision of which interface to employ for outgoing packets, depending upon the routing strategy as well as the mechanism of packet tagging (discussed in Section 5.2).

#### **4.2.2 Parameter Binding of Energy Model to Multiple Interfaces**

One of the properties of mobile nodes is the energy model that represents the energy level for the node. At the beginning of simulations, the mobile nodes in a network can be configured with an initial energy value and preset power levels for each packet to be received and transmitted. Therefore, the data transmission in different networks will decrease the energy level of mobile nodes, which in turn prevents nodes from handling any incoming or outgoing packets when their energy capacity is reduced to zero.

Originally, the calculation of power consumed for packet reception and transmission are conducted by only one PHY object with the energy level passed down from the given node object in NS-2, since it is assumed that only one network exists, as illustrated on the left side in Figure 18:

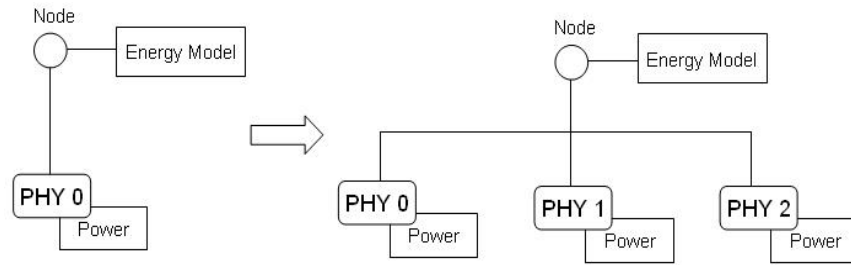


Figure 18 Modification of parameter binding for the energy model

Considering the fact that the setting of power levels at the physical object indexed 0 has already been done in NS-2, all the PHY layer objects within a mobile nodes are configured with the power levels respectively specified in scenario scripts through a group of united parameter setting methods in our implementation in such a way as to maintain backwards compatibility with the existing mechanism in NS-2. In this case, the energy level of a mobile node could be passed down to each PHY layer object for the calculation of power consumption when receiving or transmitting packets upon request.

### 4.2.3 Object Binding of Error Model to Multiple Interfaces

The error model supported by NS-2 is considered an independent object that simulates packet errors or loss over communication links that are produced by various methods of error calculation. After determining an incoming packet to be a corrupted one, the error object either sets the error flag of the packet or directly dumps it to a drop target according to the configuration in the scenario scripts. Given the direction of data transmission, an error-tagged packet is forwarded to the corresponding protocol layer object pointed to by the error object for the purpose of further handling, whereas a corrupted packet is simply discarded by the drop target. Also, the error object enables error-free packets to go through without any intervention to the next protocol layer. Hence, we chose to discard the corrupted packets generated by a random variable at the receiver side so as to satisfy the requirement of reliability in simulation scenarios.

For a mobile node over wireless networks, an error model is inserted between the MAC layer and the PHY layer, as illustrated on the left side in Figure 19.

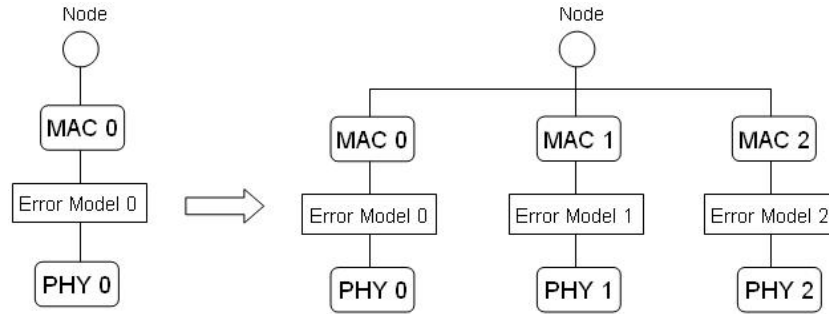


Figure 19 Modification of object binding for the error model

Similar to the energy model, the existing NS-2 simulation environment only provides support for one mobile node bound with one error model. To simulate the packet loss oriented towards each interface attached to one mobile node over multiple networks, each interface is equipped with one error object preset with an individual packet error rate in our implementation. As a consequence, each error object is capable of handling incoming packets from the corresponding interfaces connected to it separately, which enables mobile nodes to forward packets via multiple networks, depending upon their reliability during data transmission.

#### 4.2.4 Logic of Connection to Multiple Interfaces

In NS-2 simulations, interpretation-based Object-oriented Tool Command Language (OTcl) objects are generated step by step based on the scenario script, whereas compilation-based C++ objects are generated afterwards through the mechanism of static shadow mapping from the OTcl space to that of C++. To guarantee correct connections among layering objects in both interpreted and compiled hierarchies, the construction of a mobile node should strictly follow the order of creating network layering objects for each interface within the node, as shown as follows:

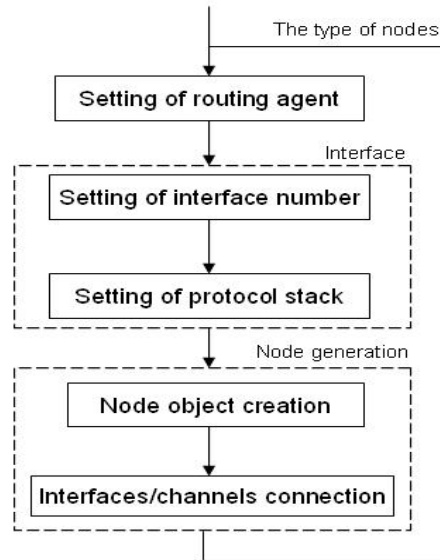


Figure 20 The flow chart of node construction in simulations

The figure above illustrates the general procedure of how to establish valid connections for each interface within a node for each type of nodes in our project. Meanwhile, the procedures are set once for each type of nodes in multiple networks before the nodes are generated. To be specific, the procedures are subdivided into three parts that cover the setting of the routing protocol type, the configuration of multiple interfaces, and the node generation.

First of all, only the routing protocol type is configured for the first node to be created in the scenario. In terms of multiple networks, the type of routing protocol varies with the functionality of nodes as configured in advance. Secondly, the number of interfaces needs to be initialized by a default value without specifying any layering object along with it, which allows the NS-2 simulator to generate a group of object arrays rather than individual objects, given the mechanism of dynamic type binding inherent in OTcl (the type of a variable is not determined until the variable is assigned a value with a type automatically recognized in OTcl). Each object array stores the same type of layering objects involved in multiple networks prior to node construction.

Subsequently, the number of interfaces and the type of underlying protocol objects in each interface are specified for the current type of nodes. Unlike the layering objects,



each propagation model object belonging to one PHY layer object within a node must be generated in advance to avoid collision with the existing procedures of node construction in NS-2.

The last part for node construction is to instantiate node objects and to establish the connections among layering objects within the nodes from top to bottom with all configurations prepared in the previous steps. Underlying network objects within a node are created for each interface after the generation of the node object. Besides, all interfaces along with the corresponding communication channel object (generated before any node is created) are linked to the node one by one through a loop. Additionally, the order of different types of interfaces for each type of node is statically assigned specific to our design in later cooperation with the complied objects in transferring packets among multiple interfaces.

On the basis of the node framework, the newly established logical correlation among these objects is used to transfer parameters of interface creation from interpreted network objects to complied network objects. Besides, the compiled network objects must adhere to the new correlation in packet handling and packet forwarding across multiple networks during simulations. Hence, we discuss the modifications to each network object involved from the perspective of operational mechanism and implementation logic in the following chapter.

## **4.3 Node Addressing Scheme in NS-2**

### **4.3.1 Data Transmission with Multiple Interfaces**

NS-2 is considered an Object Oriented (OO) simulation environment in the sense that any entity including a node, layers and channels is treated as an object independent from each other. To identify them in terms of routing or packet forwarding in simulations, each entity involved must be assigned a unique ID as its address in steps of node configuration before the simulation is executed, as illustrated in Figure 21:

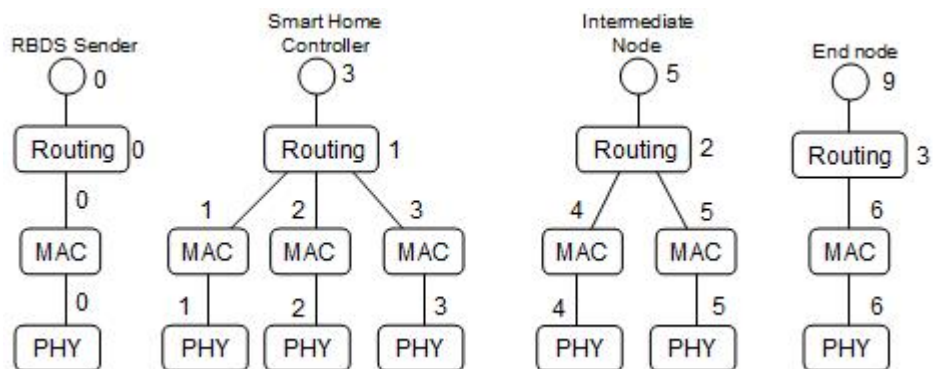


Figure 21 Object ID assignment for each layer in NS-2 environment

For each node, its ID and corresponding address could be assigned automatically from a static integer variable defined in its OTel class if there is no direct assignment to them or manually if a number is attached to them in simulation scripts (the Node ID and its address are identical in NS-2). Following that, the ID/address is passed through the OTel object of a node to the corresponding C++ object of the node based on the variable binding mechanism in the split model in NS-2.

The ID of Layers covering routing layer, MAC layer and PHY layer are generated automatically from a static integer variable only shared in their peer objects. The static variable for each layer increases by one each time when a value is assigned as a new ID to a layer object. In this case, the ID assignment of nodes and layers originate from different places only for their own use. In other words, there is no direct or indirect connection between a node ID/address and layers' IDs.

However, the identification of a source address and a destination address intended for data transmission is only set through script files. It is obvious that a random choice of node IDs will cause trouble in traces or log analysis in terms of addresses of nodes, since each layer object only recognizes their own peers when in execution. More than that, it ultimately results in address mismatch and packet loss under the circumstance of multiple interfaces/channels. To be specific, an example of data transmission in the ZigBee/IEEE 802.15.4 network is illustrated in Figure 22:

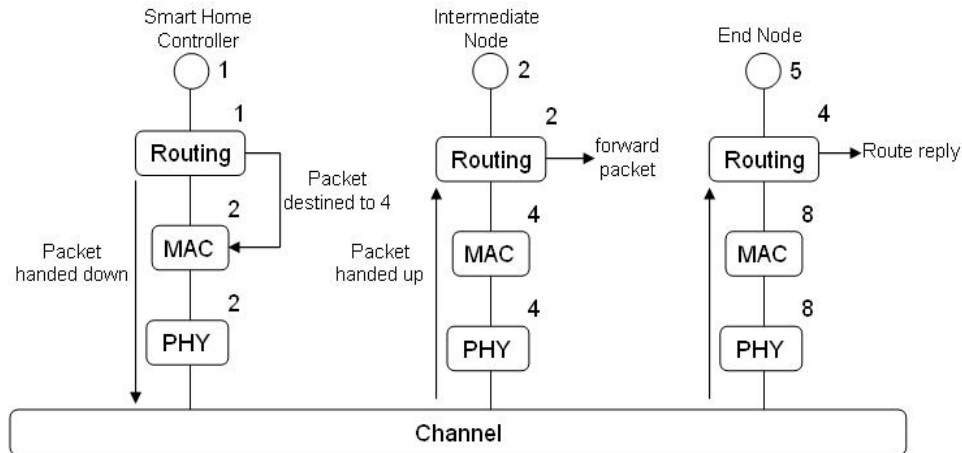


Figure 22 Issues of destination recognition in ZigBee routing

According to the figure, the ID of end node numbered 5 is chosen randomly without consideration of automatic increment of the static integer variable for ID assignment for nodes and layers. When controller node numbered 1 tries to forward a RBDS message destined to node 4 (only known in the script file but unclear about the corresponding ID at the routing layer), it directly sends a broadcast request down to the MAC layer with the routing layer ID as its source. As a matter of fact, only node 5 with routing layer numbered 4 successfully recognizes the destination in the packet transmitted in the network and accepts it while the remaining nodes only take responsibility of relaying the request along the way. Even so, it is technically impossible that node 5 sends the RREP packet to the controller numbered 1 as the MAC/PHY layer numbered 1 held by the controller belongs to the RBDS network rather than the ZigBee/IEEE 802.15.4 network. Ultimately, all packets destined to node 4 are dropped by the central controller at expiration due to a failure in delivering the packet, which in turn deteriorates data delivery of any kind in the whole network.

### 4.3.2 United Addressing Solution to Multiple Interfaces/Channels

To avoid such problems caused by mismatch and misuse of the ID/address in the environment of multiple interfaces/channels, a united ID/address assignment scheme is introduced as illustrated in Figure 23:

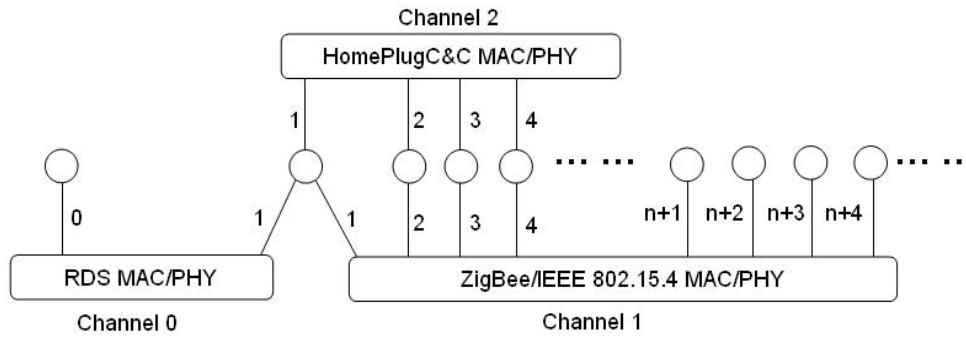


Figure 23 United addressing scheme in the simulation environment with multiple interfaces

In this scheme, any node in multiple networks is manually assigned a unique ID around the simulation environment from the node object, routing layer to MAC/PHY layer regardless of which network it belongs to. The idea behind it is based on the fact that the node ID/address, routing layer ID as well as MAC/PHY layer ID is considered unique within each one of these networks. In doing so, collisions associated with node addressing among multiple networks are eliminated through the multiplexing of ID/address.

In order to keep consist with existing implementations in NS-2 without any impact in terms of address transferring, three steps have been involved to achieve the scheme as Figure 24 shows:

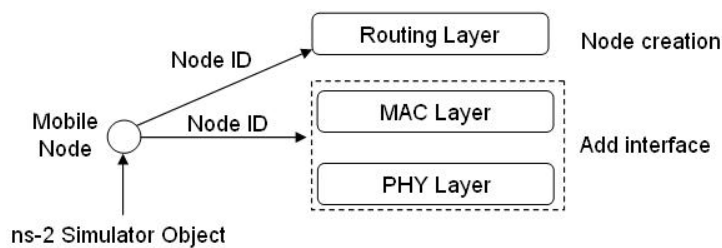


Figure 24 Node ID/Address passing from node to each layer

First of all, node ID is manually assigned to each node involved in the replacement of static assignment before execution. After the node is created, the node ID is passed to its routing layer object through an OTcl method existing in NS-2 that connects the routing layer object to the node object. Following that, the node ID is passed down to the MAC/PHY layer objects after the MAC/PHY layer objects are generated by adding

multiple interfaces to the node object. In such way, those IDs that statically increase in each layer object could be overridden with new IDs passed through from the corresponding node.

## 5 Modification to Network Objects

In addition to the architecture of the networking simulation model, each type of network object involved in the architecture in NS-2 was modified from the bottom up in order to address various issues relevant to the execution of the model in simulations, including the node management of multiple channels, the interface numbering and packet tagging mechanism at the MAC/PHY layer, the packet forwarding mechanism over multiple network and the corresponding routing strategy at the routing layer, as well as the identification of RBDS packets at the application/transport layer.

### 5.1 Communication Channel in NS-2

#### 5.1.1 Operational Mechanism of an NS-2 Channel

A Channel object acts as a logic abstract in NS-2 to simulate the realistic transmission of packets over the shared physical medium. To achieve it, the Channel object must calculate the total number of neighbor nodes within the reach of the transmission signal as well as the communication delay involved in the propagation model before scheduling the packets to destination nodes with the help of the scheduler. Thus, the primary function of the Channel object is to manage all nodes attached to the same channel, as illustrated in Figure 25:

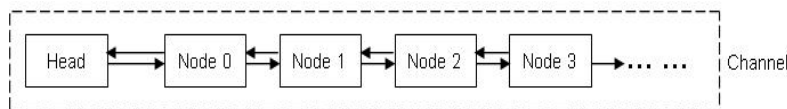


Figure 25 Organization of nodes over a single channel

Each node object within a shared channel is connected the others through a bi-direction linked list held by the Channel object when it is generated with the same channel in the program space of an NS-2 simulation. In this way, the Channel object is capable of pinpointing any destination node in its list that is eligible to receive packets as long as these nodes are kept unchanged in the list (nodes could be added and removed in special cases).

NS-2 was originally not designed to support multiple networks coexisting in the same scenario for simulations. As a consequence, the relationship between nodes and a linked list has to be redefined for the purpose of the situation of multiple interfaces/channels. Considering the fact that each channel in the scenario is used to support a single network, a matrix of linked lists is constructed for nodes and multiple networks as illustrated in Figure 26.

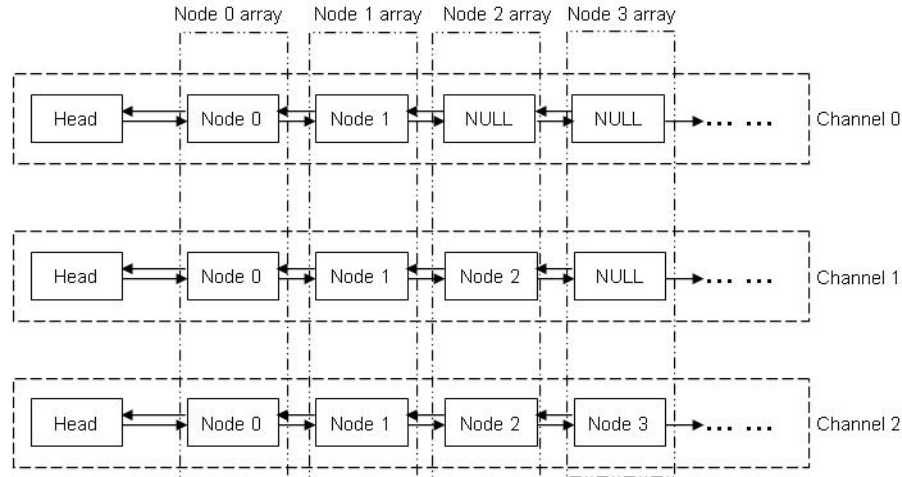


Figure 26 Array management of each node across multiple channels

The figure above gives an example of nodes with three interfaces/channels. In our implementation, channel 0 is assigned to the RBDS network, whereas channel 1 and channel 2 are assigned to the ZigBee/IEEE 802.15.4 network and the HomePlug C&C network respectively. Moreover, a bi-directional pointer array intended for multiple channels is created for each node so as to connect to other nodes over the same channel in a horizontal manner. In such way, each node is only located over the same channel when transmitting packets in the same network without any impact upon data communication over other channels in the sense that nodes are vertically attached to linked lists that belong to distinct channels.

### 5.1.2 Decoupling of Configuration for Multiple Channels

The authors of the NS-2 implementation assumed that all nodes in simulations should share the same parameters for data transmission associated with the physical layer and the corresponding propagation model in that they communicate with each other within a

single network. Under this assumption, all variables related to the range of the transmission signal are statically declared in the Channel class so as to be employed among all nodes in the network (calculation is executed only once during the whole simulation by the very first node that transmits packets), as illustrated on the left side in Figure 27.

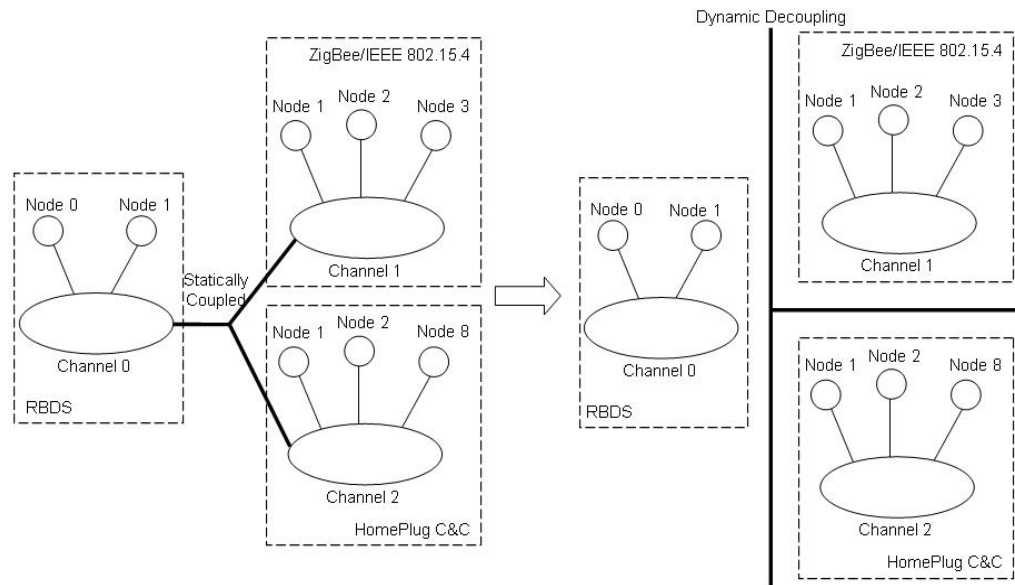


Figure 27 Decoupling of parameter association among channels

Nevertheless, this is not the case in our simulation model, in which different networks hold a stand-alone channel with a physical layer different from other networks and the corresponding propagation model configured. Besides, the propagation model intended for each network distinguishes itself from others in terms of parameter configuration even though these networks are configured with the same propagation model. To address this issue, the static property of those variables and the static assignment to them have to be replaced with dynamic declarations and initializations in the Channel class for each channel object generated in the NS-2 environment (on the right side in Figure 27). Each channel object holds its own parameters relevant to data transmission that has no connection to other networks in such a way as to avoid issues of packet loss and abnormal transmission in each network during simulations.



### 5.1.3 Packet Delivery among Multiple Channels

Originally, all nodes share the same channel for data transmission in the case of one network with a single channel in the NS-2 environment. Packets could be delivered to destination nodes by default after the calculation of transmission range and propagation delay. For the situation of multiple channels occupied by multiple networks, there are two steps to be taken so as to enable the PHY layer of destination nodes to identify the right packet when transmitting a packet. First of all, all neighboring nodes affected by the transmission are filtered out, since all nodes are organized in each channel respectively. Secondly, an address pointer to the right PHY layer object of each node that is directly connected to the current channel object and the value of propagation delay are placed as key fields in the packet header before it is inserted as an event into the scheduling queue exclusively manipulated by the scheduler object, as shown as follows:

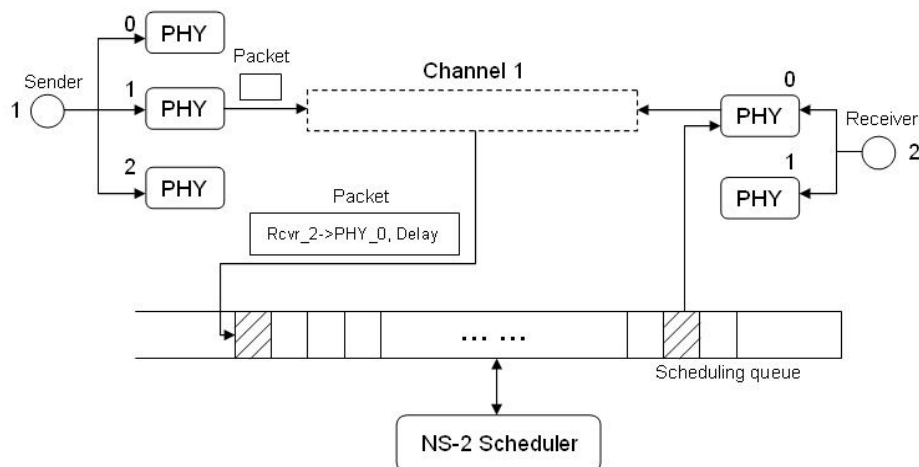


Figure 28 Data transmission on the basis of object identification and packet scheduling

After the interval specified by the propagation delay, the packet is picked up from the queue and dispatched by the scheduler object to the PHY layer of the destination node through the callback mechanism of C++ objects in that the address of any PHY layer object is unique in the execution space of a NS-2 program. Besides, it is the routing layer object that takes responsibility for forwarding packets among multiple networks, since each PHY layer object passes packets up to upper layers for further handling.

Normally, mutual interference of signals among channels exists in on-site experiments

executed in a realistic environment when more than one channel of a node is simultaneously involved in data transmission. To take that factor into account in NS-2, a mechanism of inter-object message communication is supposed to be implemented in all PHY layer objects within one mobile node in the sense that each PHY layer object is capable of measuring and calculating the influence of interference by communicating with other PHY layer objects when transmitting or receiving packets. However, such an approach is technically sophisticated in terms of the existing mechanism and the architecture of software inherent in NS-2 since it deals with the construction of nodes and the reestablishment of the existing procedures of packet scheduling. Moreover, it could also fundamentally alter generic behaviors in simulations, which is far beyond our focus in this project.

Therefore, we exclude this factor from our implementation so as to simplify the networking model. In other words, there is no way for data transmission of any kind in one network to disturb other networks in our solution on the basis of the underlying packet delivery mechanism, the uniqueness of the address of each PHY layer object as well as the independence of each channel object (simulations of multiple networks with a Flooding protocol configured are adopted to demonstrate the mechanism).

## **5.2 MAC/PHY Layer**

### **5.2.1 Interface Numbering and Packet Tagging**

Nodes are categorized into four types intended for multiple networks in our model that includes a RBDS message sender with one interface, a central controller with three interfaces, intermediate nodes with two interfaces, and the remaining nodes with one interface active in use. Each kind of interface within a node is attached to one channel object, as illustrated in Figure 29.

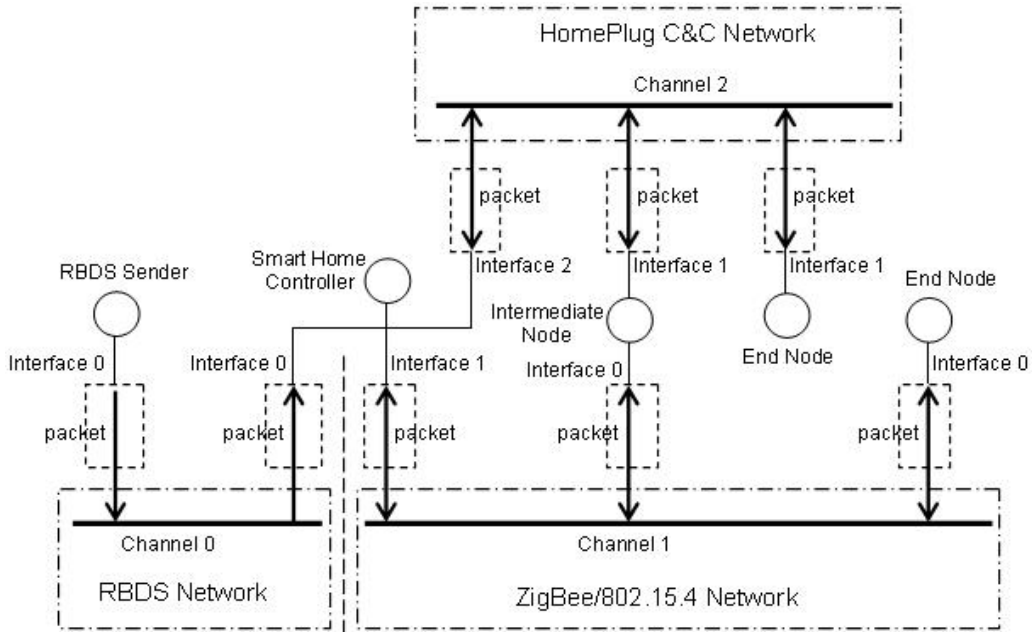


Figure 29 Node classification and packet tagging across multiple networks

In NS-2, a protocol object within a node has little knowledge of the operational status of other protocol objects due to the independence of objects at each layer, which seems quite common in ordinary simulations. Nevertheless, this is not the case in the scenario with multiple networks involved. For one thing, any node engaged must be notified in advance of the total number of interfaces currently connected to it for the purpose of proper execution; for another, the routing layer object of nodes has to make routing decision for outgoing packets on the basis of packet type as well as the identifier of interfaces corresponding to a specific network.

Therefore, there are two steps that are taken to guarantee that packets are transferred from the RBDS network to the mixture of networks in a smart home rather than to be delivered in the reverse direction. In the first place, each interface configured in a node is explicitly specified with an integer identifier starting from zero in the scenario scripts at the beginning of simulation. In the second place, all incoming packets passed through the current interface are tagged with the corresponding interface identifier before handed over to the upper layer. In such way, packets could be forwarded through the right interfaces to destination nodes.

## 5.2.2 RBDS

To model packet transmission in the RBDS network, we adopt the RBDS MAC/PHY protocol stack implemented in [67]. The radio propagation model at the RBDS PHY layer is a combination of the Shadowing model and the Ricean/Rayleigh fading model, which concurrently simulates the large scale fading effect of a wireless channel and burst errors on the basis of the time correlation of the received signal in packets. The RBDS MAC layer employs the TDMA-based scheme modified in the existing NS-2 implementation to allot all the time slots to a RBDS message originator in our multi-interface model for data broadcasting in such a way as to mimic the operation of Frequency Modulation (FM) radios. Another node acting as a central controller in a smart home is configured to stay tuned to the broadcast from the RBDS message originator in each time slot. Meanwhile, the destination address of each packet issued by the RBDS message originator is set to be the broadcasting address before transmission.

By default, the RBDS message originator, indexed 0, mainly takes responsibility for transmitting broadcast packets through the underlying interface 0 connected to the node in our simulation model. Without sending time slots allocated, the central controller, indexed 1, simply receives all packets over the RBDS network through the interface with the same index and routes them to destination nodes in a smart home through the remaining interfaces attached to the same node.

## 5.2.3 ZigBee/IEEE 802.15.4

The IEEE 802.15.4 MAC/PHY protocol stack already included in the core release of NS-2 implementation is adopted in our project to fit in the corresponding part of underlying interfaces attached to a mobile node. Considering the fact that the IEEE 802.15.4 MAC/PHY protocol implementation serves as an ideal model intended for software simulation, part of its operational mechanisms remains distinct from that of off-the-shelf ZigBee/IEEE 802.15.4-based devices in realistic environments due to the intrinsic characteristics of NS-2 (issues over the organization of participating nodes as well as the packet transmission mode of our simulation model are detailed in Sections 6.3.2 and 6.3.3

in [68]).

First of all, the node type and the corresponding functionalities partially conform to the ZigBee/IEEE 802.15.4 technical specifications. To be specific, a Reduced Function Device (RFD) is capable of transmitting or routing packets to any node within its signal range instead of transferring them to the sub-root coordinator regardless of its type. Therefore, the data communication among nodes is executed in a peer-to-peer way in our implementation.

Secondly, there is no direct support for sleep mode in the activities of nodes during simulations. The ZigBee/IEEE 802.15.4 specification has been originally designed to minimize the active energy usage of standard-compliant devices. To keep nodes at the lower level of power consumption during a long-term operation, each node in a network should remain dormant during the majority of operational time, except that it is re-triggered from dormancy to respond to periodical events [69]. To idealize the execution, the NS-2 simulator treats the power consumption in idle mode the same as in sleep mode on the basis of the energy model configured to nodes. Therefore, the power levels of both idle mode and sleep mode that are assumed to be extremely low in simulations are set to identical values for simplicity.

Thirdly, the choice of the logic number of a communication channel is entirely unrelated to the static identifier assigned to the underlying channel object. According to the specification, a total of 27 channels starting from 0 to 26 are available across three frequency bands in which the ZigBee/IEEE 802.15.4 protocol stack can operate (250 kbps in the 2.4 GHz band, 40 kbps in the 915 MHz band, and 20 kbps in the 868 MHz band) [70]. Given the predetermined frequency band, the PHY layer is capable of tuning its transceiver to a certain channel within the numbering scope upon receipt of packets from the upper layer. In terms of simulation implementation, the logic number of a channel is calculated by the PHY layer object with a preconfigured frequency band in an attempt to tag the wireless link among nodes in data communication, whereas the channel identifier, statically assigned to the channel object in our implementation, is uniquely

recognized and handled by the simulator during the run-time scheduling of NS-2. Hence, there is no mapping between the two types of identifier for the same channel object in that they apply to different scopes.

### 5.2.4 HomePlug C&C

Initially, a power line was designed to transmit 50 or 60Hz signals instead of high frequency signals. Similar to a wireless channel, a power line channel suffers from a range of signal attenuations, including noise originated by the operation of neighboring electrical devices, fading, multi-path effect and interference caused by the limitation inherent in channels [71]. Based on the commonality between two types of communication medium, the authors in [72] demonstrated the feasibility to model the power line communication in the NS-2 simulation by attaching a Korea standard-based PLC-MAC protocol component to the built-in architecture of a mobile node, as illustrated in Figure 30.

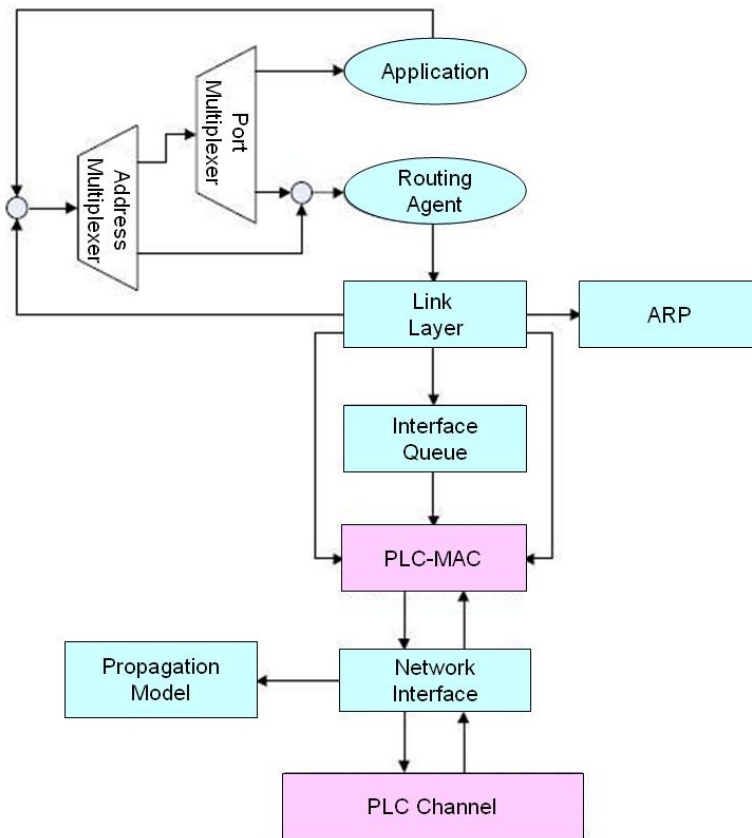


Figure 30 The architecture of a Korea standard-based PLC-node in NS-2 [72]

In this architecture, the PLC-MAC layer object mostly takes control of the access to the shared medium with the channel contention mechanism in addition to such basic functionalities as transmission and reception, segmentation and reassembly, error control, etc. To accomplish the goal, the channel estimation module in the PLC-MAC layer object independently collects the current status of the channel so as to calculate an adaptive contention window.

Inspired by the characteristics of a power line channel as well as the approach to construct a PLC node in NS-2, we chose to clone the IEEE 802.11 WLAN protocol stack along with the corresponding communication channel from the existing NS-2 implementation with a data rate reduced to a low value (25Kbps), relative to that of ZigBee/IEEE 802.15.4 (250Kbps at 2.4GHz). This creates a technical approximation of the HomePlug C&C MAC/PHY (with a data rate of 7.5Kbps) since there is no detailed technical specification and software implementation publicly available for reference and adoption. Further bandwidth reduction is restricted mainly by the operational mechanism of NS-2 simulation environment as well as the complexity of event scheduling in the cloned implementation. Meanwhile, the newly cloned channel class and the existing radio propagation models are tailored to this substitution in terms of the computation of propagation delay in packet transmission.

## **5.3 Routing Layer**

The routing layer in our simulation model mainly deals with packet identification and data forwarding from the RBDS network to the combination of wired and wireless networks in a smart home, the routing of data to all nodes configured to receive RBDS messages, and the establishment of routes for nodes across multiple networks in a house. The following sections in this chapter are organized to discuss the corresponding operational mechanism of each issue from the perspective of our model implementation.

### **5.3.1 Packet Transmission from RBDS to Smart Homes**

The simulation model in our project consists of two types of networks: an outdoor

network intended for long distance wireless transmission and multiple indoor networks interconnected through intermediate nodes in a smart home to enable short range packet forwarding. Normally, only the RBDS message sender preset in our model periodically broadcasts packets over a RBDS network to a smart home central controller within its signal range. Outgoing RBDS packets are initialized with the corresponding packet type at the RBDS originator side and tagged with the RBDS interface identifier at the recipient side during transmission. Upon reception of incoming RBDS packets at the routing layer, the routing object of the central controller takes responsibility for forwarding packets to destinations based upon a given routing strategy, as illustrated in Figure 31.

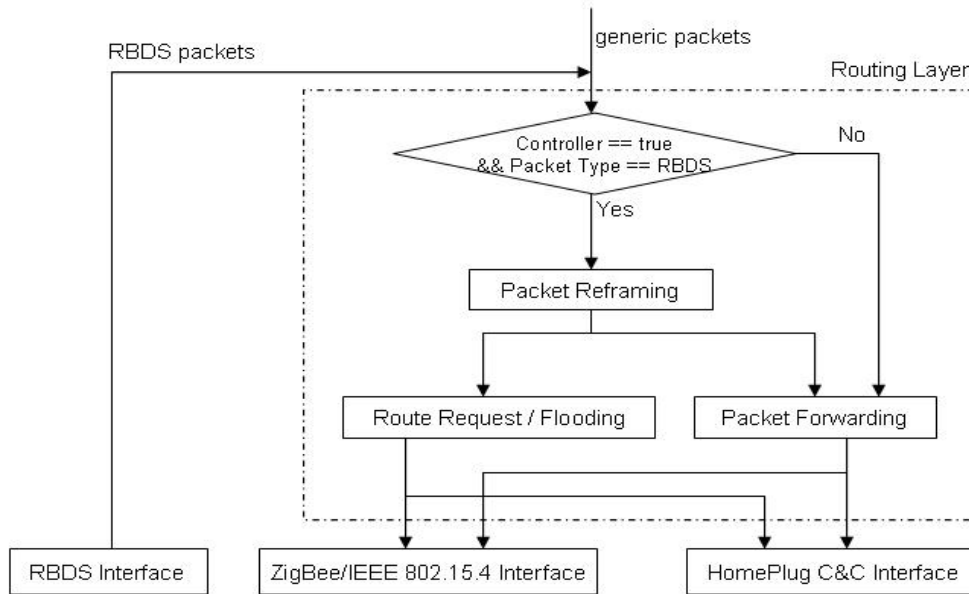


Figure 31 A combined flowchart of RBDS packet forwarding through the central controller

In the first place, the routing object of the central controller distinguishes different packets to be transmitted according to the current node type and the packet type along with a tagged interface identifier in that all nodes in a smart home are configured with a common routing protocol intended for packet forwarding over multiple networks. Incoming packets from the RBDS interface are intercepted by the routing object for further handling, whereas generic packets from the upper layer or other networks are directly passed down to the corresponding interface with the established route entry to destinations in the routing table.



In the second place, the routing object addresses issues in packet re-encapsulation and packet forwarding for incoming RBDS packets based on the chosen routing protocol (Flooding, AODV and ZigBee routing protocol are employed in our simulation model for the purpose of performance comparison). To be specific, outgoing RBDS packets are reframed with distinct source and destination addresses as well as other route-related parameters specific to the configured routing protocol, as compared to the original ones. In other words, the source address of packets is set to the address of the central controller while the destination address of packets is set with each node configured to receive RBDS packets in scenario scripts. Subsequently, the reframed RBDS packets are delivered to destinations by the routing object with the support of the routing protocol configured in simulations. Flooding-based packets could be directly handed over to all other interfaces except the RBDS interface. For AODV and ZigBee routing protocol, the routing object must determine whether to issue RREQ packets to destination nodes by examining whether a route entry with outgoing interface identifier exists in the routing table.

To sum up, all nodes configured in a smart home, including the central controller, intermediate nodes and generic nodes, are implemented to follow the same logic of handling outgoing packets. In terms of functionalities for AODV and ZigBee routing based nodes, it is evident that only the central controller is in charge of forwarding RBDS packets from the RBDS network to home networks, while the remaining nodes in a house handle incoming RBDS packets or issue status updates to the central controller through registered interface indices that identify the corresponding networks in their own routing entries.

### **5.3.2 Data Forwarding in a Smart Home**

According to the ZigBee specification [73], a ZigBee/IEEE 802.15.4-based device should be equipped with a ZigBee routing protocol when transmitting packets after device association. As a variation of the AODV routing protocol, the current implementation of the ZigBee routing protocol enables ZigBee/IEEE 802.15.4-based devices to deliver packets to destinations with minimal link cost calculated from the corresponding packet

delivery probability over the underlying communication link, whereas an AODV-based device employs the shortest hop count in packet forwarding. Therefore, both ZigBee and AODV routing protocol are modified to accommodate themselves to the simulation environment of multiple networks for the purpose of a close comparison between them. Also, an improved Flooding protocol is adopted in our project as another alternative to a redundant and robust data transmission among multiple networks.

### 5.3.2.1 Flooding

The improved Flooding protocol in our simulation model is implemented differently from the traditional flooding approach. In the first place, it is the central controller that serves as the source node delivering flooding packets to all other nodes in a smart home. To do so, the RBDS packets broadcasted by the RBDS originator to smart homes are reframed by the central controller with a new source address (the address of the central controller) and the corresponding packet type (the Flooding type) applicable to data transmission in a house. In the second place, the implementation of the Flooding protocol is inspired by the approach proposed in [74] to mitigate the network traffic in a smart home. The simplified flowchart of the Flooding protocol is shown as follows:

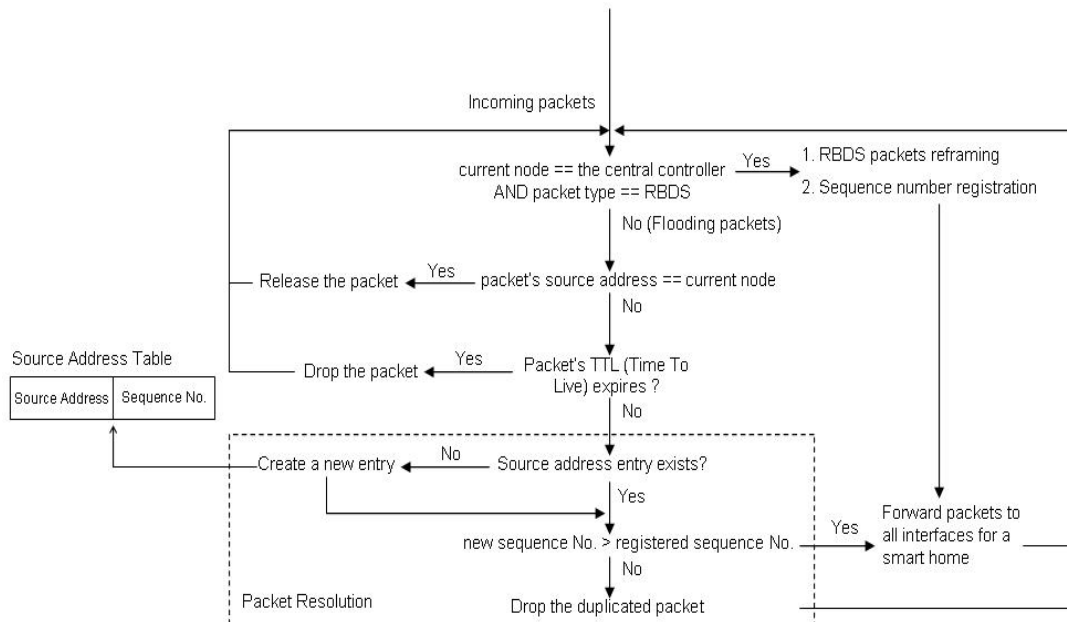


Figure 32 A simplified flowchart of Flooding protocol

The normal operation of the Flooding protocol is achieved mainly by a source address table maintained by each node in a house. Unlike generic routing tables, the source address table only consists of two fields: the address of a source node (namely the central controller) that issues flooding packets, and the sequence number of the latest flooding packet. Initially, the central controller transforms incoming RBDS packets into outgoing flooding packets and transmits them to all other nodes in a house after increasing their sequence number by 1. Upon reception of the first flooding packet, a node establishes an entry in its source address table with the source address and the sequence number specified in the header of the packet. Otherwise, the node compares the sequence number in the newly received packet with the registered one in the entry to identify if it received an entirely new flooding packet originated from the central controller. To be specific, a flooding packet with a sequence number greater than the registered one is considered a new one. It is used to update the entry and transmitted through all interfaces equipped in the node to other nodes afterwards. A flooding packet with a sequence number less than or equal to the registered one is directly dropped by nodes as a duplicated packet, which reduces the network overhead to some extent.

### 5.3.2.2 Timer-Driven Sequential Packet Forwarding

To forward incoming RBDS packets via the ZigBee or AODV routing protocol, routes from the central controller to destination nodes should be established in advance for long-term RBDS packets transmission by disseminating RREQ packets to neighboring nodes so as to calculate the minimal route cost along the way to destination nodes, as illustrated in Figure 33.

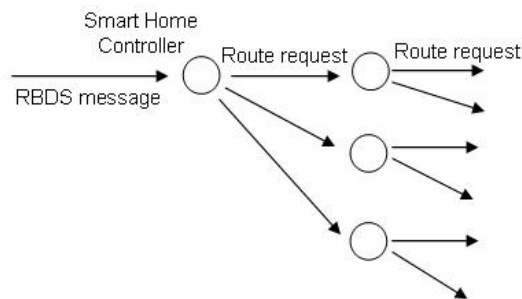


Figure 33 Diagram of route discovery originated from central controller

With the increase of nodes preconfigured to receive RBDS messages, a broadcast storm [75] caused by RREQ packets oriented towards distinct nodes could deteriorate the entire network traffic, given that all RREQ packets originated by the central controller are propagated simultaneously to nodes within its signal range, which is not supported in the existing implementation of NS-2. Meanwhile, nodes in a network are most likely to be overwhelmed by consecutive rebroadcasted route quests to different destination nodes and ultimately may fail to transmit route reply (RREP) packets destined to the central controller, which in turn severely compromises the data communication between the central controller and the recipients of RBDS messages.

A variety of schemes were proposed by the authors in [76] to address the issue of broadcast-based storm, including a probabilistic scheme, a distance-based scheme, a location-based scheme, a cluster-based scheme, and a counter-based scheme. These schemes are distinguished by their approaches to the estimation of broadcast redundancy as well as the corresponding decision-making. Meanwhile, the authors argued that a stand-alone counter-based scheme is capable of eliminating most of the redundant rebroadcasts in a densely distributed network as compared to the simple flooding approach.

Technically, these schemes accompanied by additional methods are susceptible to special conditions or complicated in terms of software simulations. To be specific, the probability of rebroadcasting statistically varies with a preset random value and the network size in the probabilistic scheme; the distance-based scheme resorts to the signal strength of received packets to approximately estimate the distance of nodes for the decision of rebroadcasting, while the location-based scheme requires the geometric location of nodes in order to minimize rebroadcasting with the help of positioning equipment, such as Global Positioning System (GPS) receivers; the cluster-based scheme forces all nodes engaged in a network to be interconnected so as to form a cluster composed of a head and a group of members by periodically advertizing their presence to neighbors, in which case the role of each node determines whether the node is qualified to rebroadcast packets along the cluster; the counter-based schemes suggested by the authors assumes that all

broadcasting packets are tagged with the same broadcast identifier and destined to only one node when comparing the times of received packets with a preset counter threshold, which is infeasible in the case of multiple RREQ packets concurrently issued to various nodes in a network, given the complexity of tracking packets in implementation.

To optimize the processing of RREQ packets and alleviate the issue of broadcast-based storm in our simulation model without fundamentally affecting the nature of route discovery of the ZigBee and AODV protocol, we implemented an approach of timer-driven sequential packet forwarding to the RBDS packet transmission by exploiting the relationship of precedence between RREP packets to originators and data packets to recipients at the routing layer. According to the mechanism of both the ZigBee and AODV routing protocols, an originator has to accept a RREP packet from a recipient for the creation of a route in its routing table before delivering any data packet to the recipient. Considering that all nodes preset to receive RBDS packets are stored in the transaction list of the central controller, a RREQ packet destined to the next node held in the list is normally postponed till a RBDS packet with an established route to the target node is successfully sent out by the central controller, or is triggered by a timer indicating that the central controller fails to receive the RREP packet from the target node for a preset interval, depending on the numerical order of nodes configured through scenario scripts.

The operational mechanism of sequential packet forwarding is designed on the basis of the packet queuing management in the implementation of the ZigBee and AODV protocols, as illustrated in Figure 34.

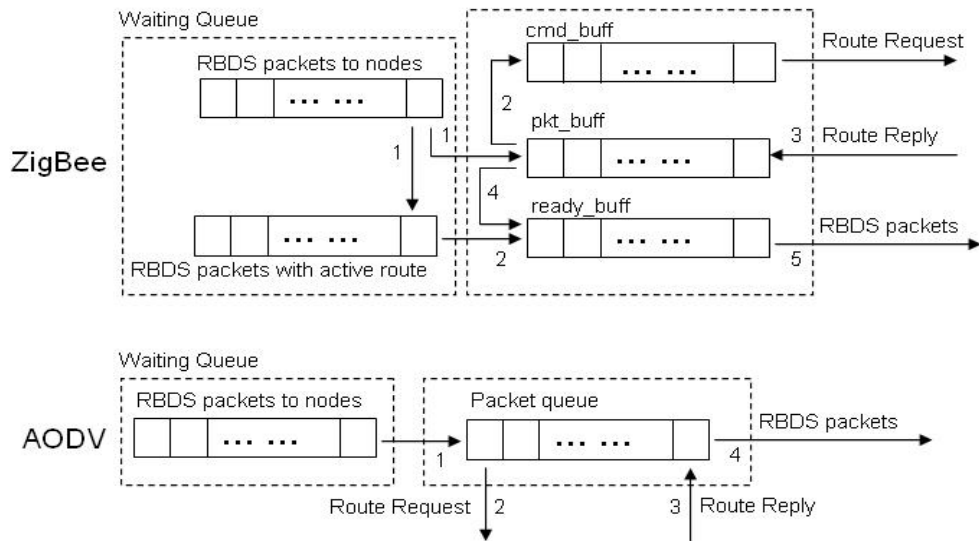


Figure 34 Packet queuing management of the ZigBee and AODV routing layer

Originally, the ZigBee routing object holds three kinds of queues (pkt\_buff, ready\_buffer and cmd\_buff) which are used for data packets without a route to their destinations, data packets ready to be transmitted and routing command packets respectively, while the AODV routing object holds only one queue intended for data packets. For both of them, routing requests are generated by the routing object for outgoing data packets. The only difference between them is that the ZigBee routing object supplies more than one queue for packets with different status or type in coordinating their transmission triggered by the notification of active status from the MAC layer, as compared to the AODV protocol. Meanwhile, the ZigBee routing object moves data packets destined to a recipient from the pkt\_buff to the ready\_buff pending for transmission after receiving the RREP packet from the recipient, whereas the AODV routing object directly delivers the data packets extracted from its pending queue. Based on the internal queuing mechanism of packet delivery, queues equivalent to the existing ones are implemented for data packets so as to minimize RREQ packets destined to distinct nodes that occur simultaneously in a network. The corresponding modification to the existing mechanism is shown as follows.

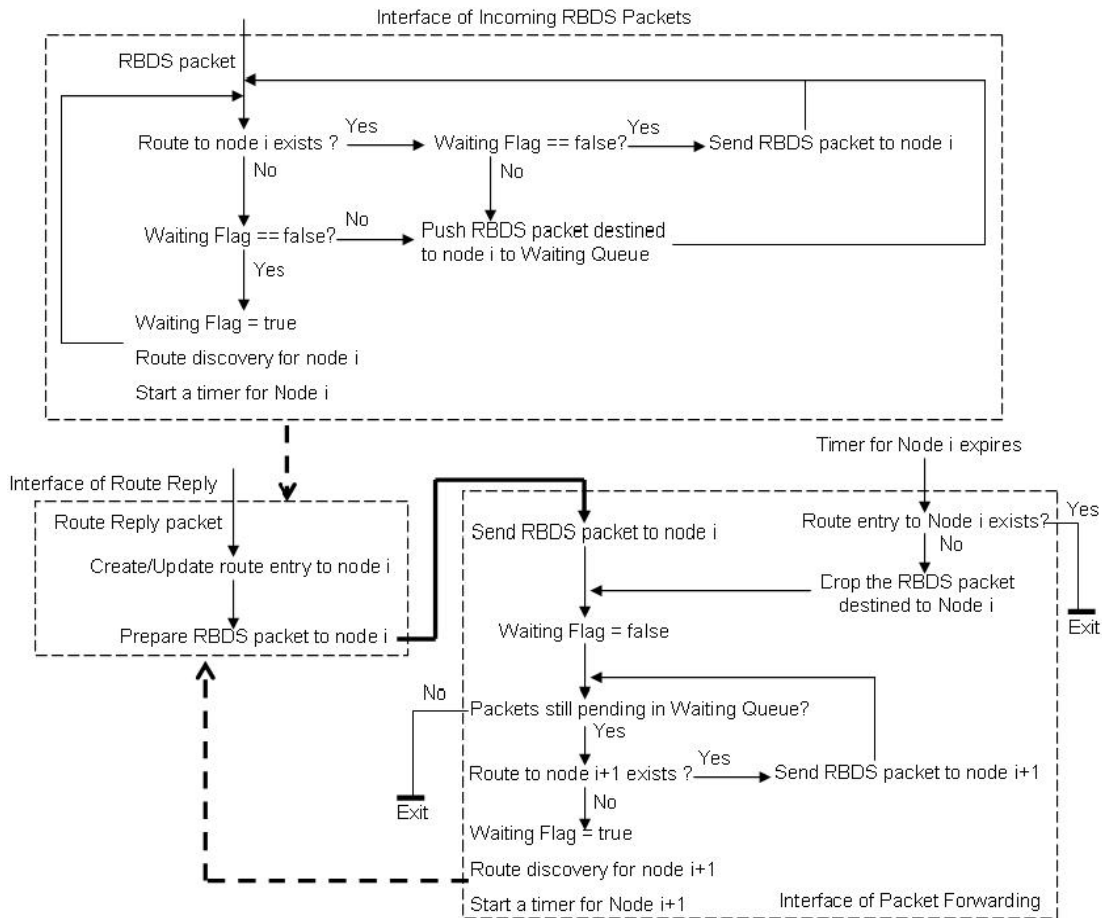


Figure 35 Simplified implementation flowcharts of timer-driven sequential packet forwarding

With support of the extra waiting queue extended for the routing object, the sequential packet forwarding is implemented in three interfaces: the interface of incoming RBDS packets from the RBDS network, the interface of RREP packets, and the interface of packet forwarding. At the beginning of the transmission, all reframed RBDS packets to destination nodes are inserted into a waiting queue. Only one RBDS packet is extracted each time by the routing object from the head of the waiting queue till it is successfully sent out to a recipient or is dropped immediately at the expiration of a timer preset for it in that the requested route to the destination remains inactive. As a consequence, the routing object repeatedly executes the same process as the previous one by relocating a RBDS packet for the successive node from the waiting queue to the existing queue.

Technically, the routing object determines whether to send the outgoing RBDS packet by

querying the routing table about an active route entry to the corresponding destination address. In such case, the waiting queue is sequentially retrieved in order to get the target RBDS packet through to the existing queue held by the routing object as long as a switching flag is set to be active. In addition, all types of queues at the routing layer are emptied upon expiration of a route counter intended for pending packets in the sense that the remaining RBDS packets queuing up for transmission are considered useless once the routing object receives a new one from the RBDS network from the perspective of the response-demand program.

### **5.3.3 Routing Strategies with Multiple Interfaces/Channels**

In principle, the existing approaches to MIMC and ours differ with respect to experiential scenarios as well as the objective of implementation. To be specific, the majority of existing approaches place emphasis upon the enhancement of throughput in a heavily loaded wireless network so as to achieve higher performance by fully exploiting the remaining non-overlapped channels available for use in the network. As a consequence, one of the main responsibilities of the routing protocol in these approaches is to strategically choose one from the existing interfaces with support of a certain switching mechanism to minimize the probability of access contention for one channel. One typical example is [77], in which the authors adopted a heuristic routing algorithm in the Dynamic Source Routing (DSR) protocol by computing the cost in interface switching, choice of different channel and the global resource usage at the expense of network delay.

In contrast to them, our solution is implemented as a combination of wireless and wired networks with comparatively low traffic, since short-sized packets are transferred to smart homes from the RBDS network at long intervals due to the characteristics of demand-response programs as well as sporadic activities of nodes associated with control-based operations in smart homes. Furthermore, it is unnecessary for power-restrained devices to increase extra channels in one network from the perspective of the utilization of channels in data transmission.

Given the AODV and ZigBee routing protocols tailored to our requirements, a range of



routing strategies are separately introduced so as to measure the performance of the combination of multiple networks from different aspects. With the exception of the wireless link routing and the reliability-based routing that could be directly configured in the scenario scripts, the remaining routing strategies are implemented in particular to address different types of routing alternatives in simulations.

As described in Section 7.4 in [68], the issues associated with the ZigBee/IEEE 802.15.4 MAC/PHY Layer and the synchronization mode of the existing implementation of ZigBee routing protocol have been resolved to meet our requirements of multiple networks.

### 5.3.3.1 Joint-Path Routing Strategy

The ZigBee and the AODV routing object employs a routing table to keep track of the optimal paths destined to recipients in data transmission. The routing table is composed of a group of active route entries, each of which includes such route-related information as a destination address, a sequence number of route packets, the minimal route cost to the destination node, etc. Given the routing tracking pattern, we take advantage of route entries to establish joint routes that may traverse multiple networks to destination nodes without influencing the existing routing functionalities in the ZigBee and AODV protocol, as illustrated as follows:

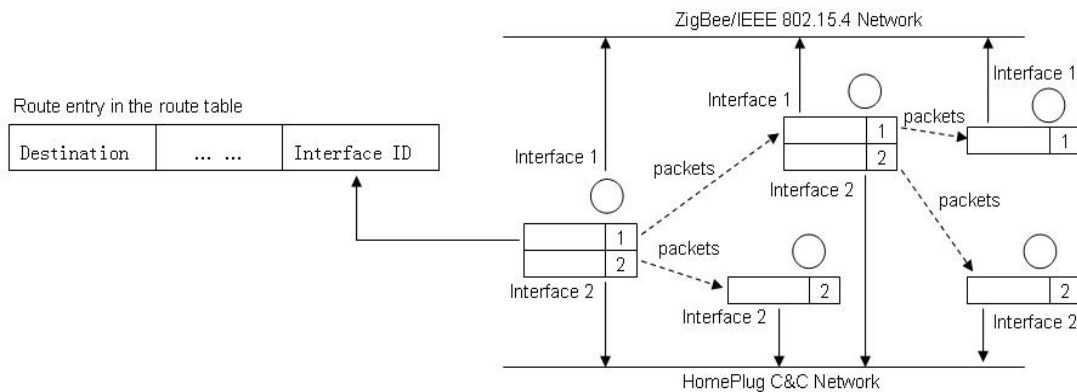


Figure 36 The joint-path strategy based on interface tagging

In our implementation, the combination of wireless and wired networks in a smart home

is treated as a single network from the perspective of the routing layer which operates as usual with no knowledge of the actual deployment of underlying networks. Each link of the combined network could be chosen by nodes with an identical probability to forward data packets. Hence, it is essential that the routing object of each node registers the corresponding interface ID in an active route entry for a route with the minimal route cost to a destination node by investigating incoming route packets tagged with the underlying interface ID at the MAC layer. To do so, an extra field is extended in the route entry so as to record interface IDs required in packet forwarding across multiple networks. The key steps of how to deal with incoming route packets prior to data packet transmission are illustrated in Figure 37.

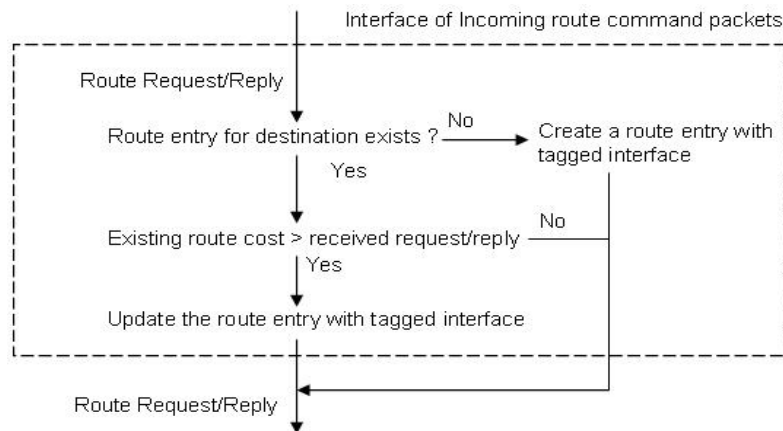


Figure 37 A simplified flowchart of interface tagging intended for route establishment

RREQ and RREP are two route commands exclusively used for route establishment in the ZigBee or AODV routing protocols. Upon reception of either of the two types of packet, the routing object of any node in a smart home extracts the interface ID identified in the packet header and decides whether to create a new route entry with the interface ID by examining the availability of a route entry destined to the recipient in the routing table. Besides, an active route entry could be updated with a new path along with the extracted interface ID attached to a different network as long as the new path is better than existing path in terms of path cost. Consequently, optimal routes to destination nodes in the combined network are tagged with the registered interface IDs in the route entries within each node involved after route establishment.

Additionally, the modes of packet forwarding in the combined network are closely associated with the underlying interfaces attached to nodes. Broadcast-based RREQ packets are relayed through the ZigBee/IEEE 802.15.4 interface and the HomePlug C&C interface that belong to the central controller and intermediate nodes, and through the ZigBee/IEEE 802.15.4 interface or the HomePlug C&C interface connected to generic nodes, in which case RREQ packets are propagated via the combined networks in a redundant way; Unicast-based RREP packets as well as generic data packets are guided to travel along a single route, with only one interface ID bound with the optimal route cost registered in the routing table of each node. Hence, the classification of packet forwarding mode separately manipulated in the routing object within nodes enables originators to transfer packets along unique interface-registered routes to recipients, which applies to both the central controller and the remaining nodes in a smart home.

### **5.3.3.2 Backbone-Based Routing Strategy**

In addition to the data transmission to destinations only through the wireless link, our simulation model offers the HomePlug C&C network as a wired backbone accessible to all end nodes for packet forwarding, since it is convenient for intermediate nodes with both wireless and wired interfaces to be deployed nearly anywhere power outlets are available in a house. For one thing, nodes are enabled to transmit packets over the wired network as much as possible if it is reachable within the range of nodes, which alleviates the potential disturbance produced by nodes through the wireless interface; for another, such routing mechanism could effectively reduce the overall power usage consumed by all indoor nodes during data transmission, given that the central controller and intermediate nodes equipped with multiple interfaces always treats the power line as their own energy source. Hence, we designed such a routing strategy based on the HomePlug C&C backbone for the purpose of performance measurement in simulations, as illustrated below.

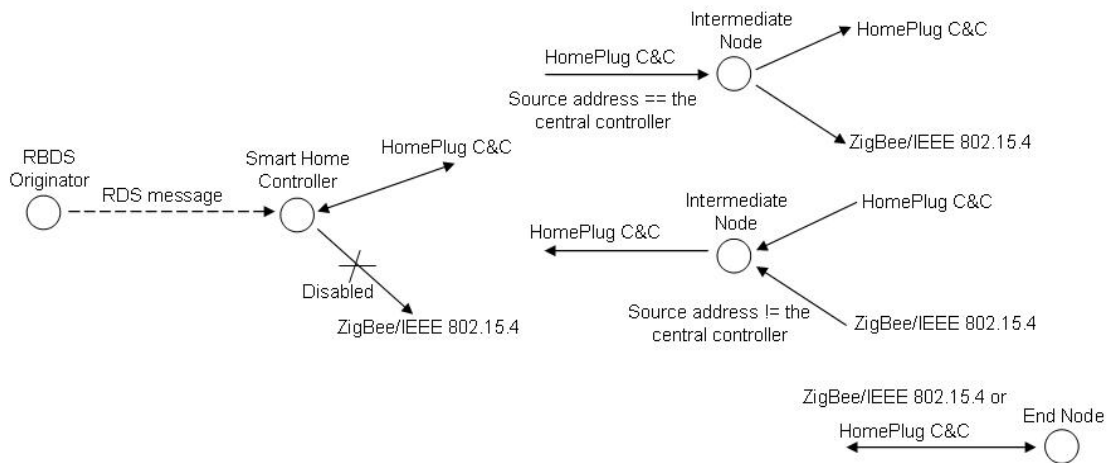


Figure 38 Packet forwarding logic with backbone-based routing

Following the principle of timer-driven sequential packet forwarding intended for RBDS packets, the backbone-based routing strategy is essentially built up on the basis of the joint-path routing mechanism with particular constraints on the wireless interface, in the sense that packets are possibly forwarded by generic nodes equipped with only one wireless interface connected to the ZigBee/IEEE 802.15.4 network. To establish a route to a destination node through the backbone, a RREQ packet is extended with a source interface field in their header that records the count of interfaces hold by the source node when being transmitted. Under such circumstances, intermediate nodes are able to identify the type of source node by examining the source interface field in each RREP packet header (the central controller holds three interfaces; intermediate nodes normally hold both two interfaces; the remaining nodes in a house only hold one wireless interfaces) and determine through which interface to transmit the RREP packet afterwards.

Meanwhile, there are two rules implemented in both the AODV and ZigBee routing protocols: firstly, the central controller with the wireless interface disabled in the routing object is only allowed to transmit packets through the HomePlug C&C network; secondly, RREQ packets originated from the central controller are transmitted by local intermediate nodes through both two interfaces, which enable intermediate nodes and end nodes to receive the packets in a wired or wireless way from nodes within their range, whereas

RREQ packets issued by intermediate nodes or end nodes will be forwarded by intermediate nodes only through the wired interface to the backbone upon reception. In other words, RBDS packets destined to end nodes are forced to traverse the backbone to the wireless network in which an end node receives RBDS packets directly from a intermediate node reachable to it or indirectly from neighboring end nodes according to their location in the multiple networks; on the contrary, the transmission of status update message destined to the central controller are restricted to the backbone as long as they are intercepted by any intermediate node without regard to the network property of incoming interface. In addition, any incoming RREQ packets issued by nodes with more than one interface will be discarded by local intermediate nodes as long as these packets are received through the wireless interface, which guarantees that routes are always established through the backbone.

### **5.3.3.3 Dual-Path Routing Strategy**

Both the wireless and the PLC network potentially suffer from noise and interference problems, leading to packet losses. To achieve a higher possibility of packet reception at destinations with the increase of nodes deployed in multiple networks, it is feasible that the routing object within nodes is specially adjusted so as to allow nodes to take advantage of two entirely distinct routes through both the wireless network and the backbone simultaneously for data transmission. In contrast to the routing strategies characterized with a single path to destination nodes, the dual-path routing strategy provides nodes with another alternative to robust and redundant data delivery, in which case a packet accidentally dropped for some reason along one route has no impact upon its duplicate forwarded along the other route in that the two routes are established independently from each other within each node. Eventually, a destination node receives up to two identical data packets issued from a source node. Hence, we designed and implemented the mechanism of dual-path routing in both AODV and ZigBee routing protocols as illustrated in Figure 39.

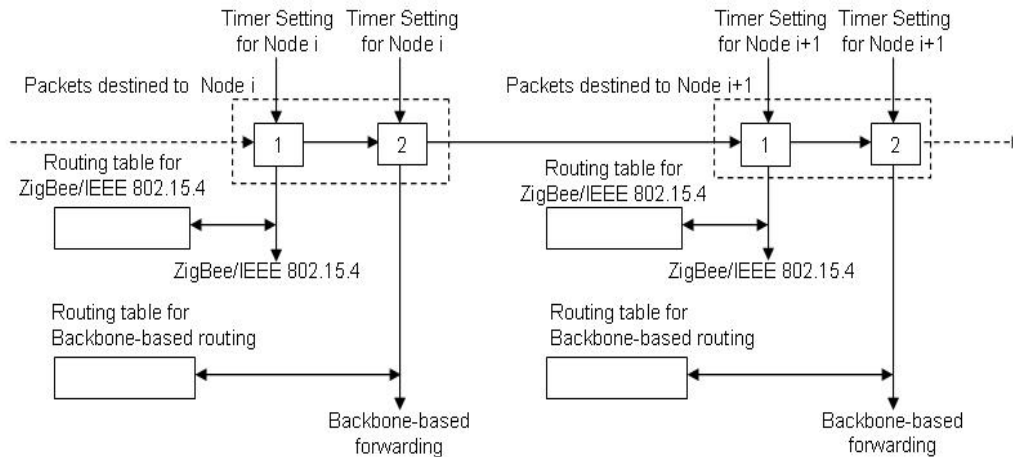


Figure 39 Simplified diagram packet forwarding with dual routing

Technically speaking, the dual-path routing strategy is considered an integration of the wireless link routing strategy and the backbone-based routing strategy, in the sense that the transmission of each data packet and its duplicate originated from source nodes are determined by the two routing strategies respectively. To achieve so, we created two routing tables within the routing object for each node preconfigured with the dual-path routing strategy in a house, each routing table corresponding to one of the two base routing strategies. With the support of the wireless link routing strategy, nodes equipped with multiple interfaces in a smart home transmit packets through the wireless interface to ensure that packets are disseminated only in the ZigBee/IEEE 802.15.4 network. Also, the backbone-based routing strategy preset in the routing object is performed individually to force nodes to forward packet through the wired interface as much as possible. In this way, two routes to each destination node are generated independently in the two routing tables within all nodes involved in the networks.

Besides the integration of the two routing strategies, the existing mechanisms are slightly adapted to the situation of dual-path packet forwarding. First of all, each of two RREQ packets featured with different routing strategies intended for the same data packet are configured with one timer when being sent. Under such circumstances, the timer tied to the first route will trigger the other RREQ packet transmission in an attempt to establish the second route upon expiration, which indicates failure to receive the RREP packet relevant to the first route. Given the packet queuing management, the routing object

within the central controller will repeat the same procedure for the next destination by moving another RBDS packet to the pending queue after completing the transmission of the previous data packet or automatically triggered by the timer of the previous one tied to its second route. In contrast, the routing object within generic nodes could remain idle till it receives the next status update message passed down from the application layer at regular intervals if configured in the scenario scripts. Secondly, a new field labeling the type of routing strategy is inserted in the header of each packet by source nodes before transmission, which contributes to the identification of the routing strategy made by forwarding nodes along the path to destinations. With the mechanism of field tagging, the wireless link routing strategy and the backbone-based routing strategy can coexist and be performed separately in the multiple networks.

## **5.4 Application/Transport Layer**

NS-2 offers the combination of Constant Bit Rate (CBR) traffic for an application-layer object and a User Datagram Protocol (UDP) agent intended for connectionless short-size data communications. In our simulation scenarios, a CBR application over UDP tagged with a normal type flag is employed to simulate the nodes in a house periodically transmitting data to the central controller when RBDS messages are being sporadically forwarded by the central controller to preconfigured destination nodes.

The transmission of RBDS messages is illustrated below:

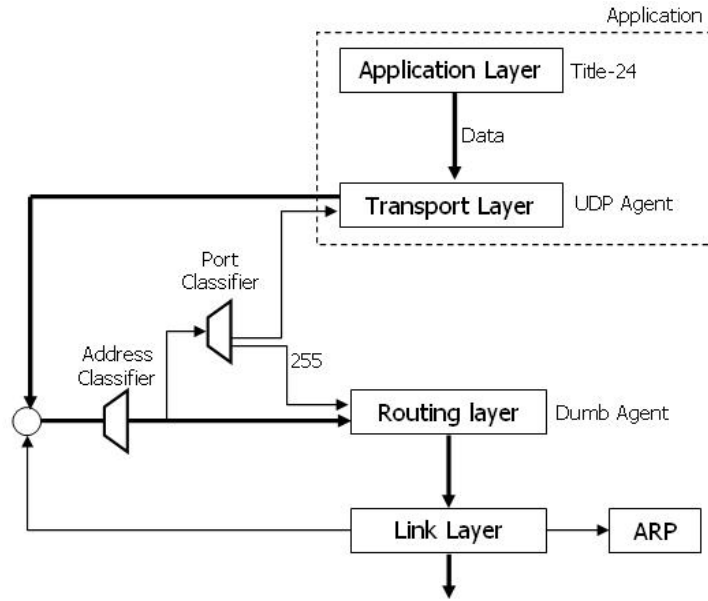


Figure 40 Data packing in RBDS message sender

To simulate messages issued by utilities to smart homes over the RBDS network, a Title-24 specification [67] based application class that extends the Application class in NS-2 is employed to generate Programmable Communicating Thermostat (PCT) application data at fixed intervals specified in scenario scripts with a timer mechanism. In addition to encapsulating the application data from the Title-24 object with addresses and the port number, the UDP agent attached to the RBDS message sender also initializes the packet type as well as the corresponding type flag. In this way, RBDS packets could be distinguished from other type of packets by the routing object and properly handled upon reception in simulations.



## 6 Networking Simulation and Result Analysis

In this chapter, we mainly concentrate on the analysis of simulation results in an effort to evaluate whether and how dynamic factors influence the networking model in terms of performance metrics oriented towards various protocols/routing strategies in our implementation. Prior to that, the setting of simulation environment with regard to the organization of nodes in the combined network and network related parameters are briefly summarized as below (refer to Appendix B for detailed discussion of the simulation layout, configuration steps and other parameter settings intended for various scenarios). Besides, the calculations of performance metrics slightly different from the conventional equations as well as dynamic factors to be adopted during simulations are also explained in the following section for the purpose of result analysis.

### 6.1 Simulation Setting and Measurement

#### 6.1.1 Node Deployment and Networking Parameters

Given that a smart home is occupied by two individual networks with distinct propagation models, nodes in the house are placed in a grid fashion to guarantee that each node engaged in the combined network is capable of receiving packets via the wireless link or the wired link. Following the pattern of grid deployment, three node densities (the distance among nodes: 3 meters with 48 nodes, 4 meters with 30 nodes and 5 meters with 20 nodes) featured with various amount of nodes are adopted so as to mimic the data transmission in flat houses of different size, as shown in Figure 41. The central controller is located at the left bottom of each grid in a house.

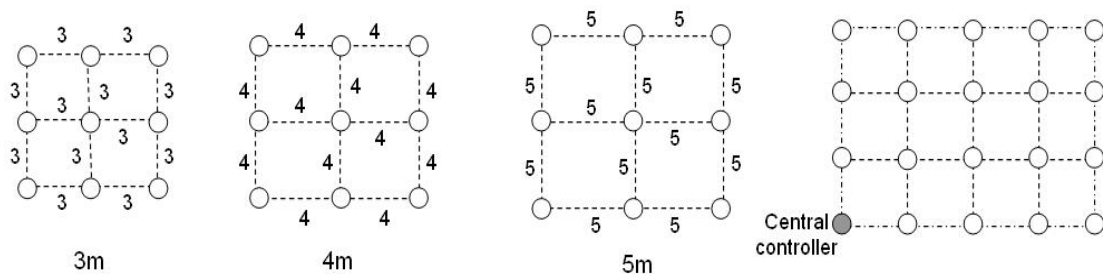


Figure 41 Node density featured by various distance among nodes

Given the fixed transmission power pre-configured for each node at the wireless interface in the house, the grid deployment enables nodes to forward packets to neighboring nodes along the path of grid via the wireless link.

With the default setting of HomePlug C&C network, outgoing data packets from the central controller could reach forwarding PLC nodes/destination PLC nodes configured in the house via the wired link at a comparatively lower data rate by one hop, regardless of the node density. In this case, packets through the backbone could reach wireless nodes away from PLC nodes by multiple hops via the wireless link. Hence, the deployment of PLC nodes makes trivial difference to data transmission through the backbone from the perspective of the central controller. For simplicity, we increase PLC nodes (including the central controller) in order from bottom to top and from the left to the right, depending upon the specific demands of the sum of PLC nodes in the simulation scenarios, as illustrated in Figure 42.

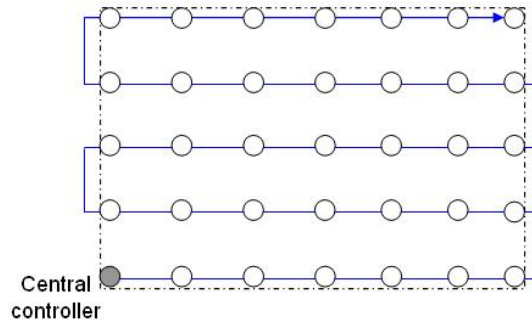


Figure 42 The deployment of PLC nodes in a smart home

The network parameters are summarized in Table 3 to reflect the configuration of simulation environment intended for various networking protocols in a smart home (other parameters settings in the RBDS network are detailed in Section B.4.1 in Appendix B).

Considering the complexity in setting up simulation environments, there are a couple of parameters in the table above that need to be explained as follows:

- (1) It is demonstrated in [67] that devices up to 140 km from the RBDS transmitter are capable of receiving RBDS message 30 bytes long in size with a high reception probability of 99.5%. Based on the conclusion, the RBDS transmitter is located at (0m,0m,210m) and the central controller is located at (100km,5m,1.5m) in our

simulations, considering that the RBDS transmitter should be placed high enough to successfully send RBDS packets over FM broadcast channels to all kinds of smart homes located at different heights. The distance from the RBDS transmitter to the central controller is less than 140km to guarantee that the central controller receives each RBDS packet issued from the RBDS transmitter without error. Meanwhile, a simulation area with 120km  $\times$  120 km is laid out to cover the distance from the RBDS transmitter to the central controller and a smart home with 16m  $\times$  21m in size (discussed in Section B.2 in Appendix B).

Table 3 A summary of the network related parameters

General Setting	Simulation Area (X $\times$ Y)	120km $\times$ 120km
	Size of House	16m $\times$ 21m
	Coordinate of RBDS Sender (X,Y,Z)	(0m,0m,210m)
	Coordinate of Central Controller (X,Y,Z)	(100km,5m,1.5m)
	Application Type of RBDS packet	Title-24
	Transport Layer	UDP
	Sum of RBDS packets transmitted in the RBDS network	$\leq 51$
	RBDS Packet Size	30 bytes
	Count of Interfaces	$\leq 3$
	Count of in-house Nodes	48(3m)/30(4m)/20(5m)
	Network Layer Protocol	Flooding/AODV/ZigBee
ZigBee/IEEE 802.15.4	Channel Type	WirelessChannel
	Propagation Model	TwoRayGround
	Antenna Model	OmniAntenna
	PHY Layer	Phy/WirelessPhy/802_15_4
	MAC Layer	Mac/802_15_4
	Interface Queue Type	Queue/DropTail/PriQueue
	Maximal Packets in IFQ	50
	Link Layer Type	LL
	Frequency(Hz)	2.4GHz
	Carrier Sense Threshold	0.00000769113W
	Reception Power Threshold	0.00000769113W
	Transmission Power	0.7W(3m)/1.244W(4m)/2.0W(5m)
	Initial Energy	13000Joules
	Power Consumption (Transmission)	0.0744Joules
	Power Consumption (Reception)	0.0648Joules
Power Consumption (Idle)	0.00000552Joules	
Power Consumption (Sleep)	0.00000552Joules	
HomePlug C&C	Channel Type	PowerChannel
	Propagation Model	Shadowing
	Antenna Model	OmniAntenna
	PHY Layer	Phy/HomeplugCCPhy
	MAC Layer	Mac/HomeplugCC
	Interface Queue Type	Queue/DropTail/PriQueue
	Maximal Packets in IFQ	50
	Link Layer Type	LL
	Data Rate	25Kbps

- (2) For each simulation, the total number of RBDS packets issued from the RBDS transmitter to the central controller is set to 51. Given the number, the time interval of RBDS traffic should be adjusted accordingly for various protocols and routing strategies in such a way as to enable destination nodes in the house to have enough time to receive data packets in normal cases.
- (3) Based on [67], the typical RBDS packet size in the RBDS network is set to 30 bytes. The adjustment of RBDS packet size is part of our simulations which are discussed in Section 6.2.3.
- (4) The maximal number of interfaces in a combined network is 3, in which case the central controller is equipped with 3 interfaces (RBDS, ZigBee/IEEE 802.15.4, and HomePlug C&C), whereas the remaining nodes are equipped with at most 2 interfaces (PLC nodes with 2 interfaces, and wireless nodes with only 1 interfaces).
- (5) The parameter settings related to the power consumption at the ZigBee/IEEE 802.15.4 interface of nodes refers to the device data of ZMD44101 transceiver offered in [78]. Reception power threshold and carrier sense threshold are offered by the authors of implementing the ZigBee/IEEE 802.15.4 protocol stacks (including MAC/PHY) at /ns2-allinone-2.33/NS-2.33/ex/wpan.
- (6) Based on the reception power threshold, the transmission power is calculated individually for each node density to enable nodes involved to receive packets along the fixed grid during simulations. The transmission power of a certain node density is adjusted only to the measurement of network energy cost. To be specific, the transmission power is promoted to 2.0W for all three node densities (with a grid size of 3 meters, 4 meters and 5 meters) in order to compare the energy cost among different node densities in a house. Given a combined network with a grid size of 3 meters, the transmission power is set back to 0.7W so as to compare the energy cost among various routing strategies in an AODV-based/ZigBee-based network. There is no need to further reduce the corresponding parameters of power consumption since all routing strategies share the identical network parameters in the same network with a grid size of 3 meter, covering the transmission power and parameters of power consumption. For the measurement of the remaining performance metrics, the transmission power for each node density is set back to its original value (0.7W with

3 meters, 1.244W with 4 meters, 2.0W with 5 meters).

(7) Since the HomePlug C&C protocol stacks is cloned from the IEEE 802.11 wireless LAN MAC/PHY stack included in NS-2 v2.33, all network parameters involved maintain the default values except that the data rate of the cloned implementation is reduced to 25Kbps (detailed in Section B.4.3 in Appendix B).

## 6.1.2 Performance Metrics and Dynamic Factors

A group of metrics used in analyzing data produced in simulations are chosen in our project to evaluate the performance of the combined network. Moreover, part of them should be adapted to meet our demands of simulation scenarios.

(1) Packet Delivery Ratio (PDR)

PDR is considered as a basic indicator that presents the percentage of data packets successfully received by destination nodes. It is produced by the sum of received data packets divided by the sum of data packets sent by all source nodes. In our project, only one source node (the RBDS originator in the RBDS network) exists during simulations. The central controller keeps forwarding RBDS packets from the source node to all destination nodes preset to receive packets in a house after packet reframing, as illustrated as follows (“N” is the total number of nodes in a house, including the central controller):

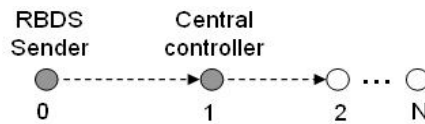


Figure 43 The path of RBDS packet transmission in simulation

Hence, the equation of PDR is readjusted as:

$$PDR = \frac{\text{Sum of RBDS packets received}}{M*n}, \quad n \leq N - 1$$

where “Sum of RBDS packets received” excludes the RBDS packets received by the central controller since it only acts as a forwarding node instead of the destination node, and “M” represents the sum of RBDS packets issued by the RBDS originator during a

simulation. In the equation, “ $n$ ” is the total number of destination nodes preset to receive RBDS packets. In other words, one incoming RBDS packet is duplicated by the central controller by “ $n$ ” times to deliver it to “ $n$ ” destination nodes.

In terms of the routing strategies implemented in our project, PDR of the dual-path is also adjusted based on the previous equation, as presented as follows:

$$PDR_{dl} = \frac{\text{Sum of RBDS packets firstly received}}{M*n}, \quad n \leq N - 1$$

“Sum of RBDS packets firstly received” indicates that we only count in RBDS packets firstly arriving at the destination nodes each time when these packets are transmitted by the central controller, since these packets are routed to the destinations through the wireless link and the backbone separately.

## (2) Average End-to-End Latency (AL)

Originally, the average end-to-end latency is measured by the time taken for a data packet from the source node to the destination node. However, the time taken for each data packet in a house is only taken into consideration for performance evaluation rather than the time span between the RBDS originator and the destination nodes. As a consequence, the time spent on the data transmission over the RBDS network should be excluded in calculation, as illustrated in Figure 44.

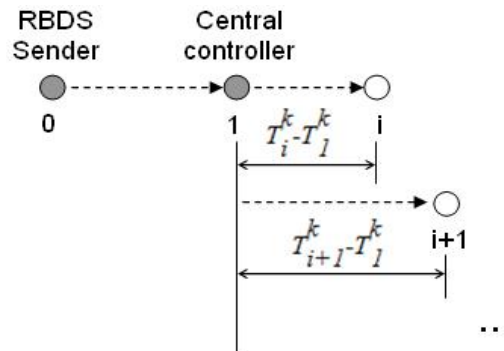


Figure 44 The calculation of average end-to-end latency in a smart home

In this diagram, “ $T_l^k$ ” is the transmission time at the central controller while “ $T_i^k$ ” is the reception time at the destination node. Following the way of calculating the latency, the

average end-to-end latency is generated as:

$$AL = \frac{\sum_{k=0}^M \left( \sum_{i \geq 2}^N (T_i^k - T_1^k) \right)}{\text{Sum of RBDS packets received}}$$

Similar to the calculation of PDR intended for the dual-path, the average end-to-end latency of the dual-path is also modified as:

$$AL_{dl} = \frac{\sum_{k=0}^M \left( \sum_{i \geq 2}^N (T_i^k - T_1^k) \right)}{\text{Sum of RBDS packets firstly received}}$$

where “ $T_i^k$ ” represents the reception time for a RBDS packet firstly received by the destination node each time (nodes selectively receive data packets by identifying their sequence number as well as the packet type extracted from the packet header).

### (3) Energy Cost (EC)

It is worth noting that nodes equipped with a wired interface are supposed to obtain power entirely from the power line for data transmission. The calculation of energy cost only involves battery-powered nodes with only a wireless interface in the sense that these nodes, acting as energy-constraint devices, are the main factor to the energy consumption of participating nodes in a house. The equation of network energy cost is presented as:

$$EC = \sum_{i=1}^m (E - E_i) , m \leq N$$

where “ $E$ ” is the initial value of battery energy, and “ $E_i$ ” is the remaining energy of the “ $i$ ”th wireless node by the end of simulation. Thus, “ $E - E_i$ ” means the total energy cost of the “ $i$ ”th wireless node, whereas “ $m$ ” represents the sum of wireless nodes configured in a house.

#### (4) Network Overhead (OVH)

To measure the number of MAC packet delivered per a single data packet received at destinations, the network overhead is used to evaluate the wireless network and the wired network individually. The equation of the network overhead is presented as:

$$OVH = \frac{\textit{Sum of packets transmitted at the MAC layer}}{\textit{Sum of RBDS packets received}}$$

It is to be noted that RBDS packets received by the central controller are entirely excluded in the calculation of overhead since the central controller is only treated as a forwarding node rather than a destination node in our project.

In addition to the performance metrics, several dynamic factors involved in setting up simulation scenarios are listed as follows:

- (1) Node Density (a grid size of 3 meters, 4 meters, and 5 meters are chosen individually for nodes deployed in a house)
- (2) The percentage of PLC nodes (determines the number of node equipped with the wired interface)
- (3) RBDS Traffic Rate (time interval of RBDS packet issued by the RBDS originator)
- (4) RBDS Packet Size
- (5) Interval of status update message (5 nodes in a house are selected to periodically send status packets to the central controller)
- (6) Wireless Error Rate (nodes randomly reject incoming packets from their wireless interface based on the packet error rate bound to the wireless interface)

The performance metrics combined with dynamic factors to be configured in simulations contribute to an overall understanding of the performance of the combined network from different perspectives, which also helps us to determine which protocol or routing strategy should be chosen under what circumstances.

Additionally, a desired 95% Confidence Interval (CI) (“t” value for 95% confidence interval is 2.262, according the t-table) helps to explore the statistical significance of simulation results produced with different dynamic factors, considering that 10 independent simulation data for each sampling point follow a t-distribution with 9 degrees



of freedom, as the sample set size is less than 30. The equation of calculating the confidence interval used in our project is presented as:

$$CI = \bar{X} \pm 2.262 \times \frac{S}{\sqrt{10}}$$

where “ $\bar{X}$ ” is the mean of 10 independent simulation data of a single sampling point, and “ $S$ ” is the corresponding standard deviation.

## **6.2 Simulation Results Analysis**

This section discusses the impact of dynamic factors upon performance metrics by investigating data results collected from various simulation scenarios, and figures out how these network layer protocols and the corresponding routing strategies operate under such circumstances.

### **6.2.1 Node Density and Percentage of PLC nodes**

Typically, nodes in a smart home are classified into the central controller with at most 3 interfaces (RBDS, ZigBee/IEEE 802.15.4 and HomePlug C&C), intermediate nodes with 2 interfaces (ZigBee/IEEE 802.15.4 and HomePlug C&C) and generic nodes with only 1 interface (ZigBee/IEEE 802.15.4). Given different node densities in a house, the dynamic of a certain performance metric could be observed by adjusting the percentage of intermediate nodes in an effort to learn whether such node layout matters to different protocols/routing strategies.

#### **6.2.1.1 Network Energy Cost**

The main goal of energy cost is to explore the situation of energy consumption for all battery-powered nodes with a wireless interface and how the increase in number of PLC nodes influences the energy cost of the whole network by replacing wireless nodes preconfigured in place with PLC nodes. To evaluate the energy cost of the combined network with different densities, the transmission power of node is set to be identical to

all three node densities (the transmission power equal to 2.0W could reach nodes within a radius of 5 meters).

The energy cost of the network configured with the Flooding protocol in a smart home is illustrated as follows (all diagrams involved in simulations are CI-tagged for all sampling points with error bars):

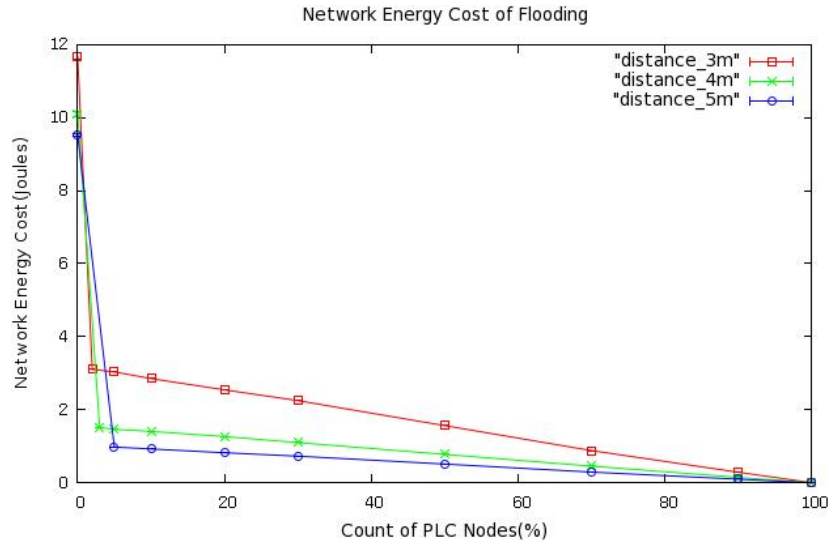


Figure 45 Network energy cost of Flooding with various node densities

In the diagram above, the first sampling point (from left to right) of each curve with a fixed node density indicates that there is no node connected to the power line, in which case all nodes in the house are supplied by battery during data transmission. The second sampling point means that only the central controller equipped with the wired interface obtains power from the power line. The vertical gap between the first point and the second point represents the energy consumed by the central controller mostly when receiving incoming RBDS packets and transmitting these reframed packets to other in-house nodes, and when establishing the wireless network for the purpose of node association, as listed in Table 4.

The table below indicates that the energy gap among distinct density is statistically identical for all three node densities mainly due to the identical frequencies of RBDS packet sent from the RBDS originator to the central controller. In terms of the central controller, energy used in network establishment and neighboring node association only

accounts for a very small proportion of the total energy gap.

Table 4 Energy cost of the central controller in data transmission over the RBDS network

Node Density	First Point (Y)	Second Point (Y)	Vertical Gap (Y)
3m	11.681 [11.598,11.764]	3.103 [3.103,3.103]	8.578 [8.495,8.661]
4m	10.092 [10.032,10.152]	1.515 [1.515,1.515]	8.577 [8.517,8.637]
5m	9.526 [9.485,9.566]	0.979 [0.979,0.979]	8.547 [8.506,8.588]

Given the combined network with a fixed node density in a smart home, the diagram shows that the percentage of PLC nodes keeps in inverse proportion to the network energy cost, indicating that increasing PLC nodes statistically impacts the energy consumption of the network. The more PLC nodes are installed in a network, the more wireless nodes are replaced with PLC nodes, and the less energy is consumed by the network. Besides, the node density indirectly influences the network energy cost in that the node density solely determines the total number of node in the house. Under such circumstance, the increase of node density undoubtedly augments the network energy cost, depending upon the total number of wireless nodes placed in simulations.

It is to be noted in the diagram that the energy cost of a 3m-gridded network remains remarkably higher than that of the other two node densities under the same conditions. The reason mainly comes from two aspects: the difference in the total number of nodes among different node densities as well as the identical setting of transmission power in simulation scenarios. Given the percentage of PLC nodes in a smart home, a higher node density means more wireless nodes are powered by battery, which substantially increases the network energy cost (i.e.  $\text{PLC node}(\%) = 20\%$ ,  $\text{wireless nodes}(3\text{m}) = 48 * 80\% \approx 38$ ,  $\text{wireless node}(4\text{m}) = 30 * 80\% = 24$ ,  $\text{wireless node}(5\text{m}) = 20 * 80\% = 16$ ). On the other hand, the identical setting of transmission power forces the 3m-gridded network to consume more power from batteries than the other two, as shown as follows:

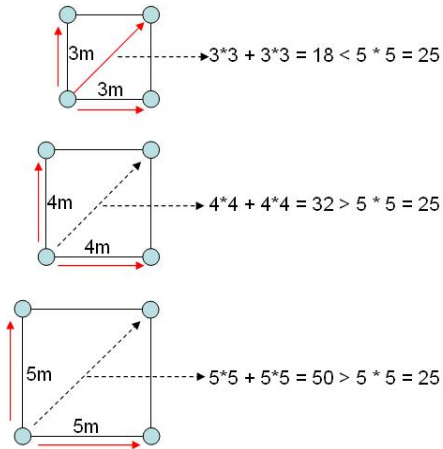


Figure 46 The signal range with the transmission power equal to 2.0W (5m)

For the transmission power equal to 2.0W, the signal could reach neighboring nodes within a radius of 5 meters from the sender. Based on the results of calculation illustrated above, only nodes in a grid of 3m × 3m in size are able to receive packets in a diagonal directional direction, which also contributes to the increase of total energy cost, in the sense that nodes in that direction still consume power when receiving packets.

Likewise, similar simulation results are observed in the AODV-based network and the ZigBee-based network featured with various routing strategies, including the joint path, the backbone-based path and the dual path, one of which, based on the AODV routing protocol, is illustrated as follows:

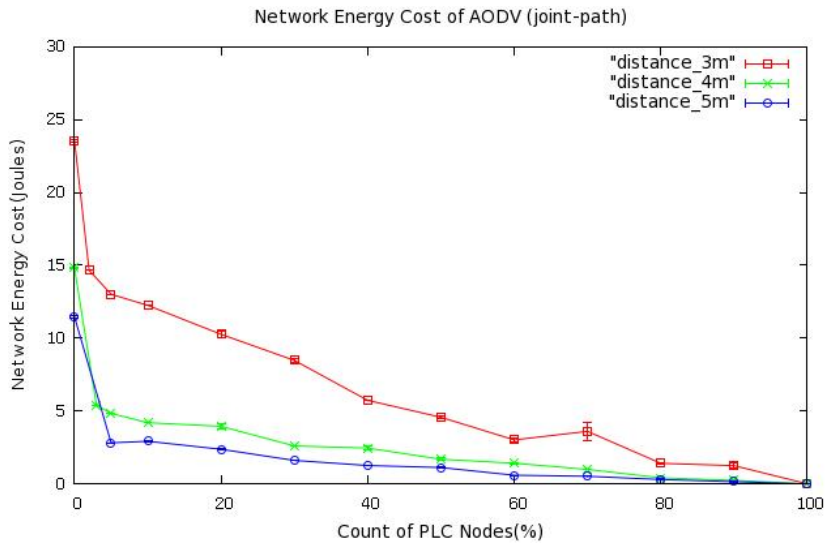


Figure 47 Network energy cost of AODV (joint-path)

The diagram above shows that the routing protocol-based network experienced a relatively high energy cost in contrast with the Flooding-based network shown in Figure 45. In the Flooding-based network, the energy cost only occurs when wireless nodes are involved in broadcasts and receive data packets along the grid. In the AODV-based or ZigBee-based network, wireless nodes also need energy to forward control packets for the purpose of route establishment to destinations, and to retransmit packets due to collision or packet loss, apart from the data packet transmission after route establishment.

Given the 3m-gridded network with the transmission power equal to 0.7W(signal from the sender only reaches nodes within a radius of 3 meters), the network energy cost of the AODV protocol and the ZigBee protocol configured with various routing strategies individually in simulations are illustrated as follows:

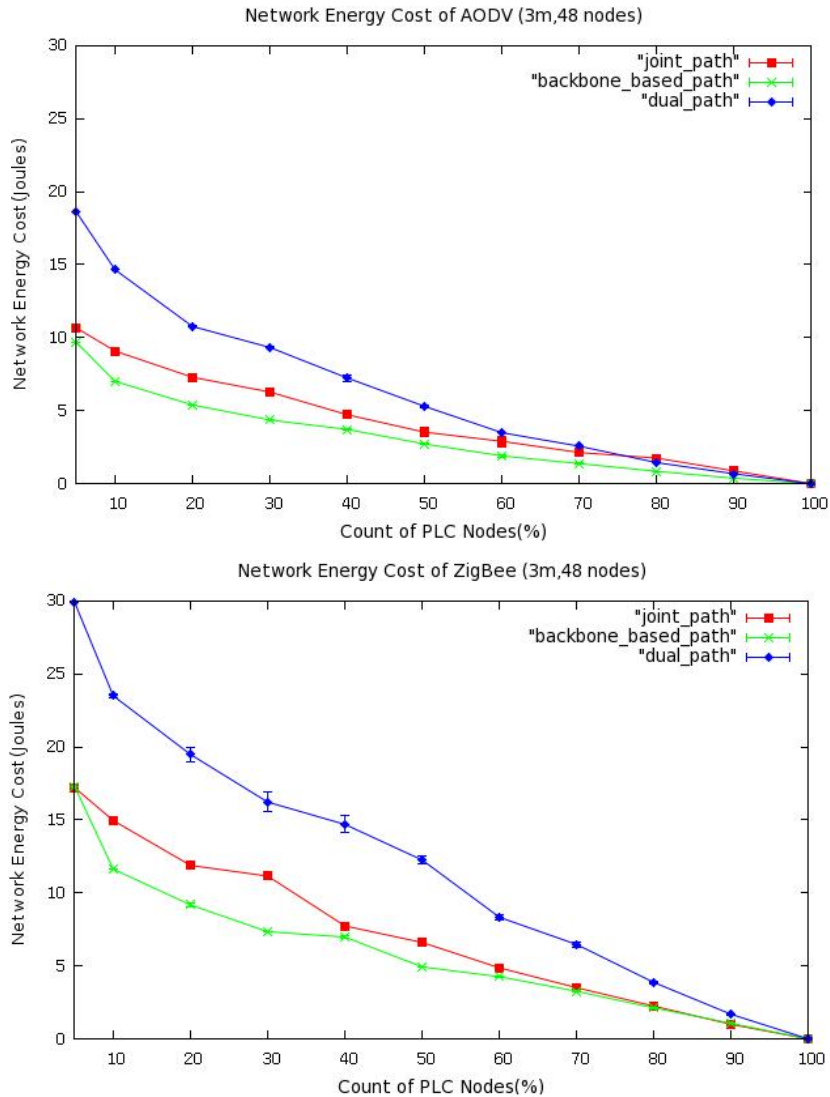


Figure 48 Network energy cost of AODV and ZigBee with various routing strategies (3m)

Theoretically, a combined network (at least two nodes including the central controller are attached to the power line) with the dual-path strategy is supposed to consume at most twice as much energy as with the backbone-based strategy, since a dual-path route destined to a wireless node consists of a wireless path and a backbone-based path, as demonstrated in Figure 49.

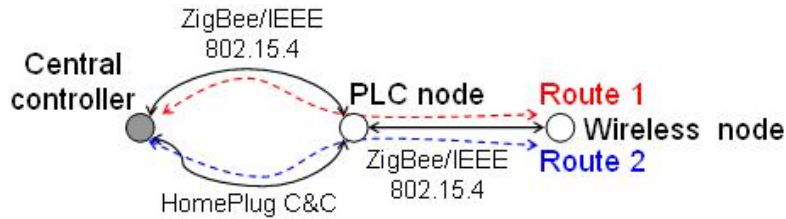


Figure 49 Simplified data transmission with the dual-path strategy

In such case, the energy cost mostly depends upon the total number of wireless nodes with two established routes (wireless and wired) in the network, since the central controller and all other PLC nodes are directly powered by the backbone. Hence, the simulation results above statistically meet our anticipation.

In comparison with the dual-path strategy, the energy cost of the joint-path strategy remains considerably lower and stays close to that of the backbone-based path strategy, for both the joint path and the backbone-based path consist of only one route from the central controller to destination nodes. From the perspective of strategy implementation, the backbone-based path strategy forces packets to travel through the power line before arriving at destinations, while the joint-path strategy guides packets based on the principle of optimal path/cost, which is not necessarily through the backbone due to its lower data rate in most cases. Nevertheless, data transmission via the wireless network inevitably experiences packet retransmission or packet loss due to signal interference or transmission collision with a higher possibility, which in turn result in a higher energy cost as a whole in the network with the joint-path strategy, as shown in the simulation results above.

Additionally, the gap of the network energy cost between AODV and ZigBee with identical strategy is mainly determined by their differences with regard to the mechanism of route establishment as well as the packet transmission mode (AODV with the asynchronous mode, and ZigBee with the synchronous mode specified in ZigBee protocol standard, as detailed in Section 7.4.2 in [68]).

### 6.2.1.2 Network Overhead

To explore the overhead of the ZigBee/IEEE 802.15.4 network and the HomePlug C&C network individually, nodes are specially constructed according to the modified mechanism of node configuration in our project. Simply put, nodes in the wireless network only equipped with the wireless interface forward packets via the wireless link, while nodes in the wired network with both the wireless interface and the wired interface could transmit packets only through the wired interface by disabling the wireless interface in simulation scripts.

According to our Flooding implementation, each in-house node has only one chance to broadcast a packet regardless of the network type, as long as the packet is identified as a new one by distinguishing the sequence number in the packet header. In terms of the Flooding protocol, there are no control-related packets existing in the network except RBDS data packets. Hence, the network overhead for the Flooding protocol could be measured as:

$$OVH = \frac{n * P}{(n-1)*P} = \frac{n}{n-1} > 1 ,$$

where “ $n$ ” represents the number of nodes in a smart home (including the central controller), and “ $P$ ” is the number of times a RBDS packets is received by the central controller from the RBDS network.

Theoretically, all destination nodes (excluding the controller) are able to receive a RBDS packet every time when the packet is broadcasted by the central controller. For the node placement with a grid size of 3 meters (48 nodes involved in the network),

$$OVH_{(3m)} = \frac{48}{48-1} = \frac{48}{47} = 1.0213 ,$$

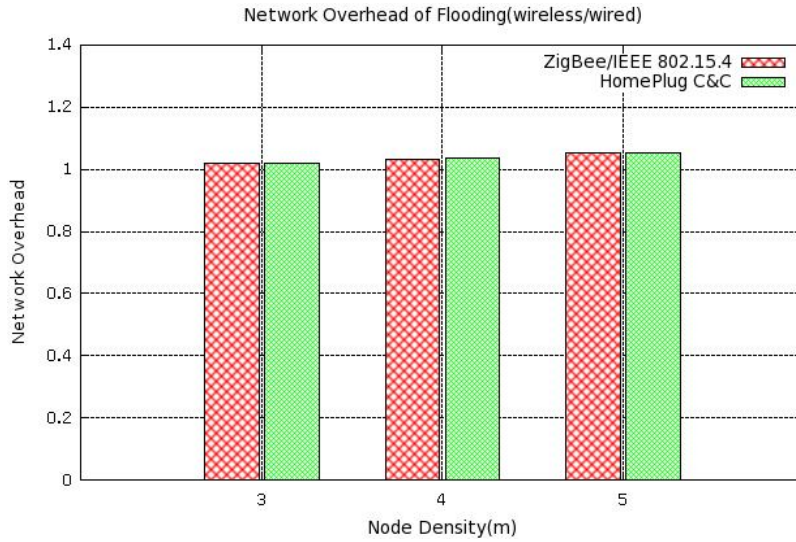
while

$$OVH_{(4m)} = \frac{30}{30-1} = \frac{30}{29} = 1.0345 , \text{ and}$$

$$OVH_{(5m)} = \frac{20}{20-1} = \frac{20}{19} = 1.0526$$



The network overhead of the Flooding protocol along with the CI range is illustrated as follows:



Node Density \ Network Type	3m	4m	5m
Wireless (0% PCL nodes)	1.005 [1.005,1.005]	1.033 [1.033,1.033]	1.052 [1.052,1.052]
Wired (100% PCL nodes)	1.021 [1.021,1.021]	1.034 [1.034,1.034]	1.053 [1.053,1.053]

Figure 50 The network overhead of Flooding with CI (excluding the controller)

It is demonstrated in the diagram and table above that the simulation results are statistically identical to our previous theoretical calculation. If we count RBDS packets received by the central controller, the results of theoretical calculation will be adjusted as follows:

$$OVH_{(3m)} = \frac{48}{47+1} = \frac{48}{48} = 1 ,$$

while

$$OVH_{(4m)} = \frac{30}{29+1} = \frac{30}{30} = 1 , \text{ and}$$

$$OVH_{(5m)} = \frac{20}{19+1} = \frac{20}{20} = 1$$

Based on the approach, the simulation results are recalculated as follows:

Table 5 The network overhead of Flooding with CI (including the controller)

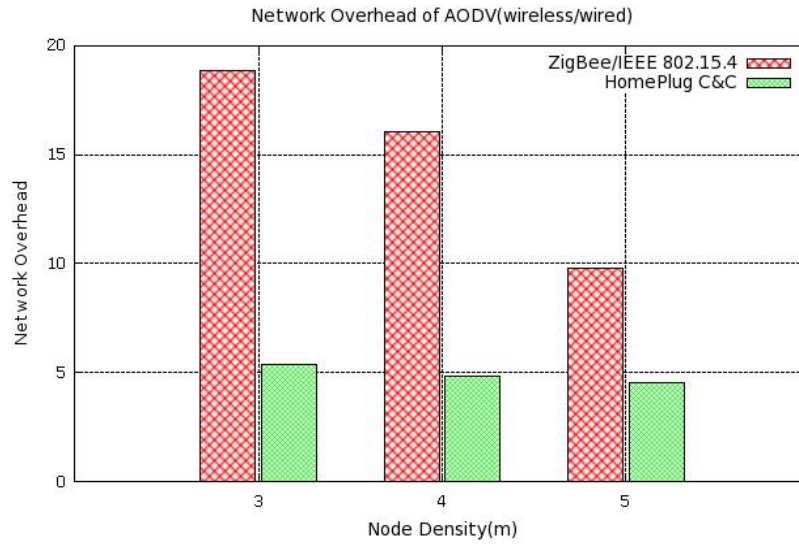
Node Density Network Type	3m	4m	5m
Wireless (0% PCL nodes)	0.984 [0.984,0.984]	0.999 [0.999,0.999]	0.999 [0.999,0.999]
Wired (100% PCL nodes)	1 [1,1]	1 [1,1]	1 [1,1]

As listed in Table 5, the difference of overhead among various node densities is caused by the way of calculation rather than the node density itself. Give an identical node density, the trivial gap between the wireless network and the wired network suggests that packets are more likely to be dropped due to signal interference/collision in the wireless network than in the wired link. Thus, the node density statistically has little impact upon the overhead of a network configured with the Flooding protocol, regardless of the underlying link (wired or wireless).

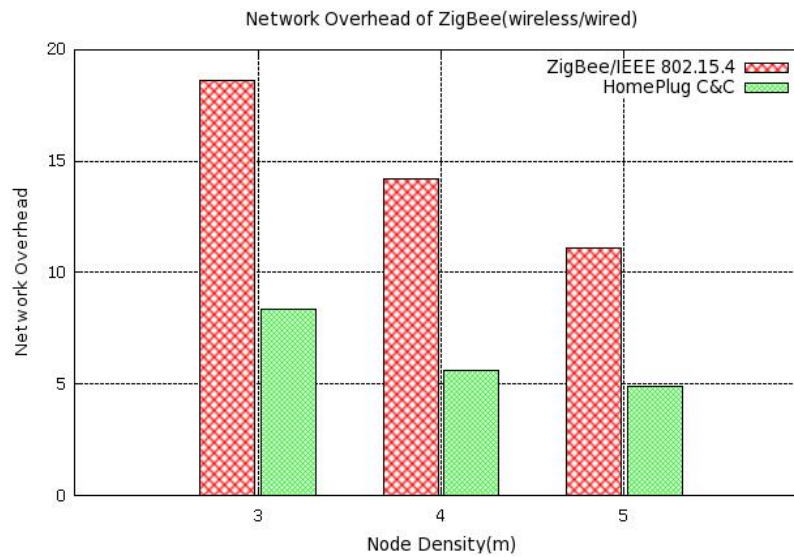
With respect to the AODV-based or ZigBee-based network, the equation of overhead should be modified as:

$$OVH = \frac{P_d + P_c}{(n-1)*P} ,$$

where “ $P_d$ ” represents the total number of RBDS data packets are sent through the MAC layer to destination nodes, and “ $P_c$ ” represents the total number of control packets are transmitted at the MAC layer for the purpose of route establishment and potentially maintenance. The value of “ $P_d$ ” and “ $P_c$ ” mainly depend upon the network type as well as the sum of destination nodes engaged in the network which are solely determined by the node density, as illustrated as follows.



Node Density \ Network Type	3m	4m	5m
Wireless (0% PCL nodes)	18.877 [18.877,18.877]	16.03 [16.03,16.03]	9.781 [9.781,9.781]
Wired (100% PCL nodes)	5.348 [5.314,5.382]	4.844 [4.829,4.859]	4.559 [4.557,4.562]



Node Density \ Network Type	3m	4m	5m
Wireless (0% PCL nodes)	18.645 [18.645,18.645]	14.201 [14.2,14.203]	11.134 [11.134,11.134]
Wired (100% PCL nodes)	8.768 [8.417,9.119]	5.647 [5.646,5.648]	4.913 [4.894,4.931]

Figure 51 Network overhead of AODV and ZigBee with CI (excluding the controller)

The simulation results above show that an increase in node density leads to the increase

of the network overhead, independent of the network type. Given a fixed node density in the house, the overhead of the wireless network remains significantly higher than that of the wired network. The reason for this can be explained as follows:

- (1) Considering that the node density determines the sum of nodes in the house, the network overhead is positively affected by the total number of nodes.
- (2) In terms of the underlying network, packets in the wireless network travels through multiple hops/relays to reach destinations nodes with the wireless interface, while packets in the wired network could reach destination nodes with the wired interface by one hop according to the setting of network parameters, which in turn results in a significantly lower overhead spent on control packets.
- (3) Packet loss and retransmission due to the signal interference/collision occur with a higher possibility in the wireless network than in the wired network.

Therefore, the impact of the node density upon the overhead of the wireless network is statistically significant as compared to the impact upon the wired network, given a routing-based network (AODV/ZigBee).

In terms of the dynamic of network overhead, ZigBee routing shows a performance comparable to AODV in a wireless network due to the similarity in their protocol. Limited to the synchronous transmission mode as well as the mechanism of underlying link quality detection inherent in the ZigBee specification [68], ZigBee routing was not designed to support a wired network in an asynchronous manner. In such case, our tradeoffs of implementation in forcing ZigBee routing to forward packets in the asynchronous mode through the backbone inevitably increase the possibility of packet loss and retransmission, which in turn results in a noticeably higher network overhead than AODV with the increase of PLC nodes (for a wired network, PLC nodes (3m) = 48 \* 100% = 48, PLC nodes (4m) = 30, PLC nodes (5m) = 20).

### **6.2.1.3 PDR/Average End-to-End Latency**

The PDR as well as the average end-to-end latency of a Flooding-based network are illustrated as follows:

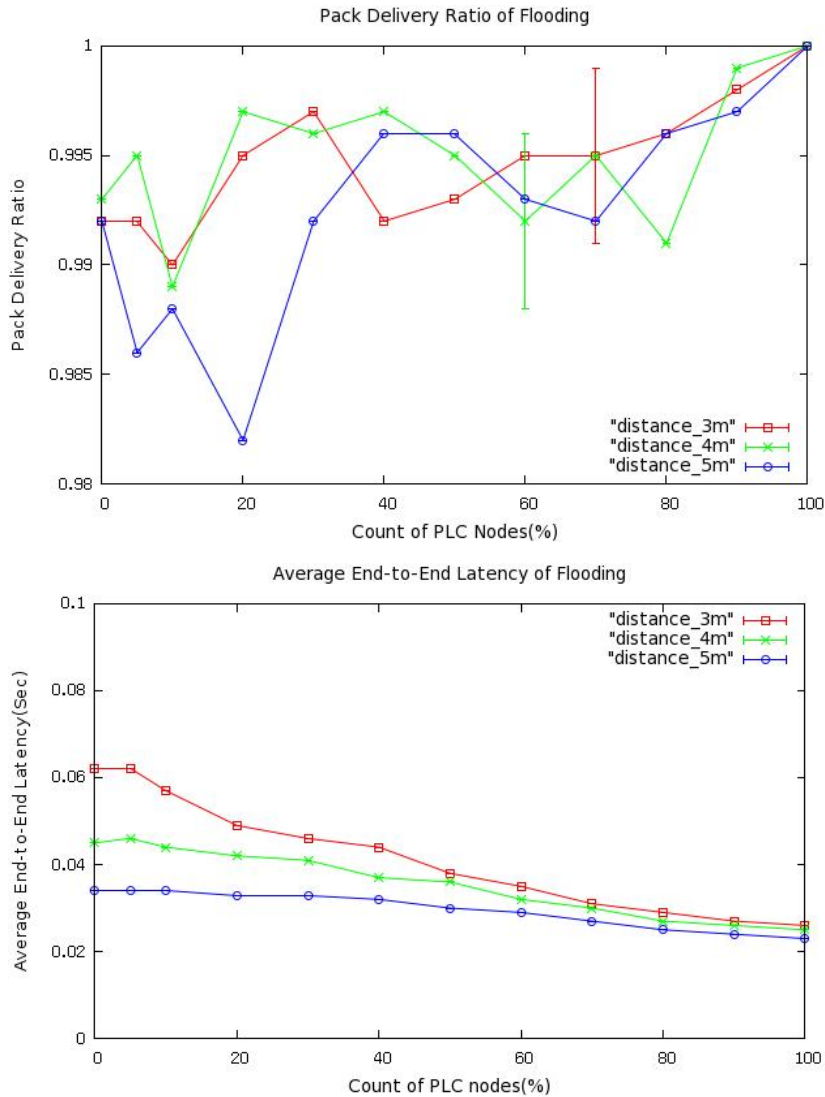


Figure 52 PDR and average end-to-end latency of Flooding with CI

It is obvious that the node density and the count of PLC nodes statistically has little impact upon the PDR of a Flooding-based network in that the PDR of network remains nearly 100% (less than one node failing to receive packets due to signal interference/collision via the wireless link) with various node densities or the percentage of PLC nodes. Besides, the PDR of a wireless network (PLC nodes = 0%) is statistically identical to that of the combined network, demonstrating that the underlying channels in our project are independent from each other when transmitting packets according to the mechanism of channel management, as explained in Section 5.1.3.

In terms of the average latency, the simulation results above indicates that a higher node density gives rise to a higher average latency when the total number of PLC nodes is maintained on a lower level, which means that RBDS data packets delivered by the central controller travel through more hops via the wireless link to the majority of destination nodes only equipped with the wireless interface. In this case, the increase in number of PLC nodes effectively reduces the average latency of the combined network, for destination nodes far away from the central controller are able to receive data packets firstly through the wired interface with a higher possibility. In terms of flooding transmission without acknowledgement involved, the time spent upon the multiple hops via the wireless link which covers the transmission delay, the corresponding scheduling delay among layers and queuing delay within each forwarding node remains slightly longer than the time spent upon one hop via the wired link, in spite of the high data rate of the wireless link. Additionally, the influence of node density as well as the percentage of PLC nodes becomes statistically trivial once the percentage of PLC node goes beyond 70%, suggesting that the average latency is mostly determined by the latency of packets received via the wired link in such case.

Likewise, the diagrams of an AODV-based network featured with the joint-path strategy are illustrated as follows:

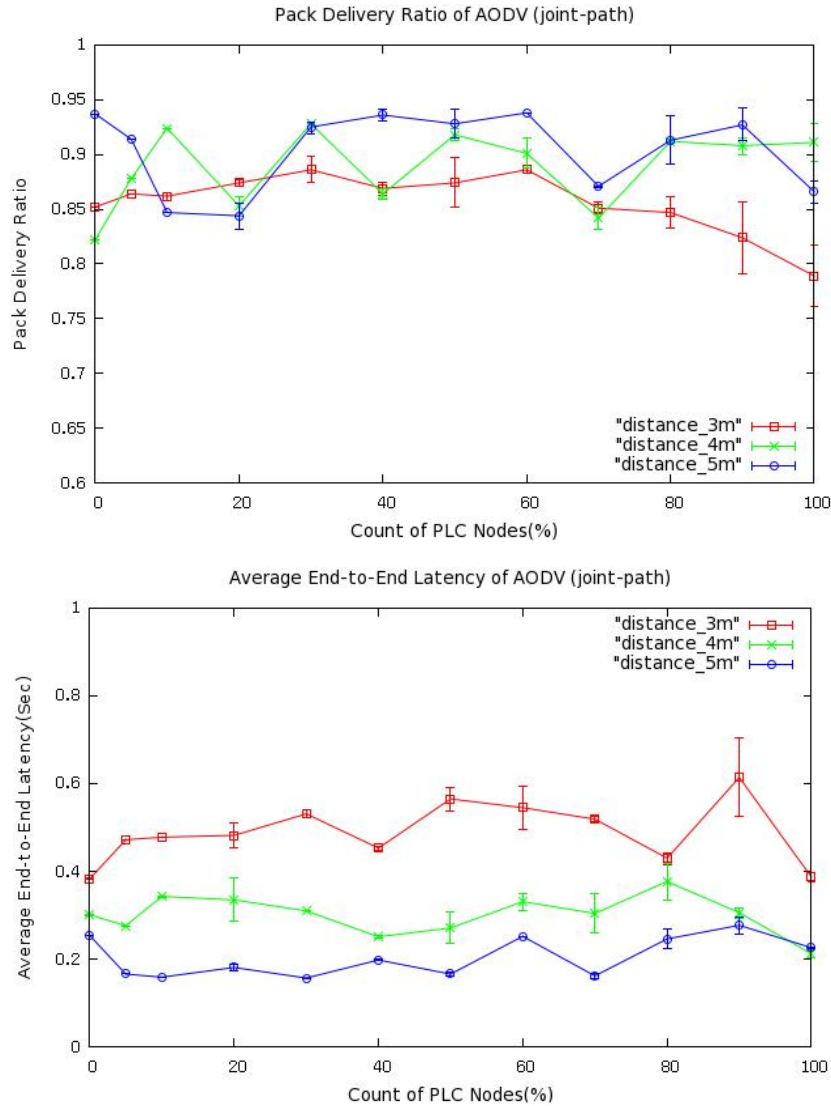


Figure 53 PDR and average end-to-end latency of AODV with CI (joint-path)

In terms of node density, the simulation results above indicate that a comparatively lower network density enables nodes to receive data packets with a higher possibility, which in turn results in a comparatively higher PDR together with a lower latency, regardless of the node type (wireless node or PCL nodes). In other words, the node density statistically impacts the average latency, depending upon the total number of nodes involved in the combined network. Given a fixed node density, there is no significant change of the PDR and the average latency with the increase of PLC nodes (i.e. noticeably ascending tendency or descending tendency), suggesting that PLC nodes statistically contribute little to the improvement of performance of the network. The reason is that AODV-based

nodes with joint-path strategy prefer the wireless link to transmit packets rather than the wired link in most cases. Nevertheless, the wireless link suffers from packet loss and retransmission with a higher possibility due to signal interference and collisions as compared to the wired link, which negatively impacts the packet reception at destination nodes as a whole.

With regard to an AODV-based network with the backbone-based strategy, the node density and the percentage of PLC nodes statistically makes little difference to the PDR of the combined network, since the PDR remains nearly 100% in such case, as illustrated as follows:

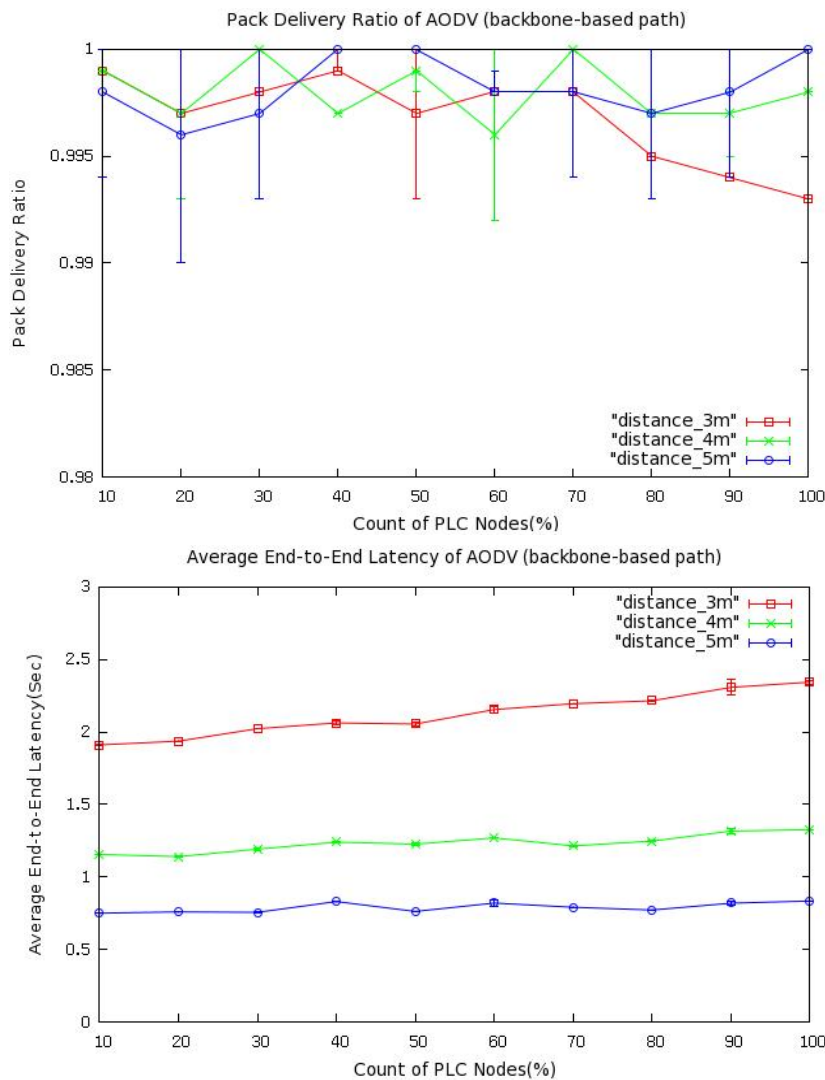


Figure 54 PDR and average end-to-end latency of Flooding with CI (backbone-based path)



Also, the simulation results show that a higher network density leads to a higher average latency during data transmission, which is directly associated with two aspects as follows:

- (1) The total number of nodes involved in data transmission in the combined network, which is mostly determined by the node density, as we discussed before.
- (2) The total number of PLC nodes involved in packet forwarding via the wired link since the wired link experience a comparatively higher latency as compared to the wireless link (i.e. if PLC node(%) = 20%, then PLC nodes (3m) =  $48 * 20\% \approx 10$ , PLC nodes (4m) =  $30 * 20\% = 6$ , PLC nodes (5m) =  $20 * 20\% = 4$ ).

On the basis of the mechanism of timer-driven packet forwarding, a higher network density will increase the waiting time for route establishment as well as the transmission time. Moreover, an increase of PLC nodes allows destination nodes currently equipped with a wired interface to receive packets by one hop through the backbone on the basis of timer-driven packet forwarding rather than through the wireless link in the progress of route establishment, which contributes to a higher average latency in the combined network according to the implementation of backbone-based path strategy.

As observed in the case of the backbone-path strategy, the same conclusion is applicable to the dual-path strategy according to the simulation results, which means that the node density combined with the count of PLC nodes statistically extends the average latency of the combined network. Additionally, similar results with regard to the impact of node density are also observed in a ZigBee-based network featured with various routing strategies during simulations (the impact of PLC nodes upon the ZigBee-based network is discussed later in the following paragraphs).

The PDR of AODV and ZigBee featured with various routing strategies are shown as follows:

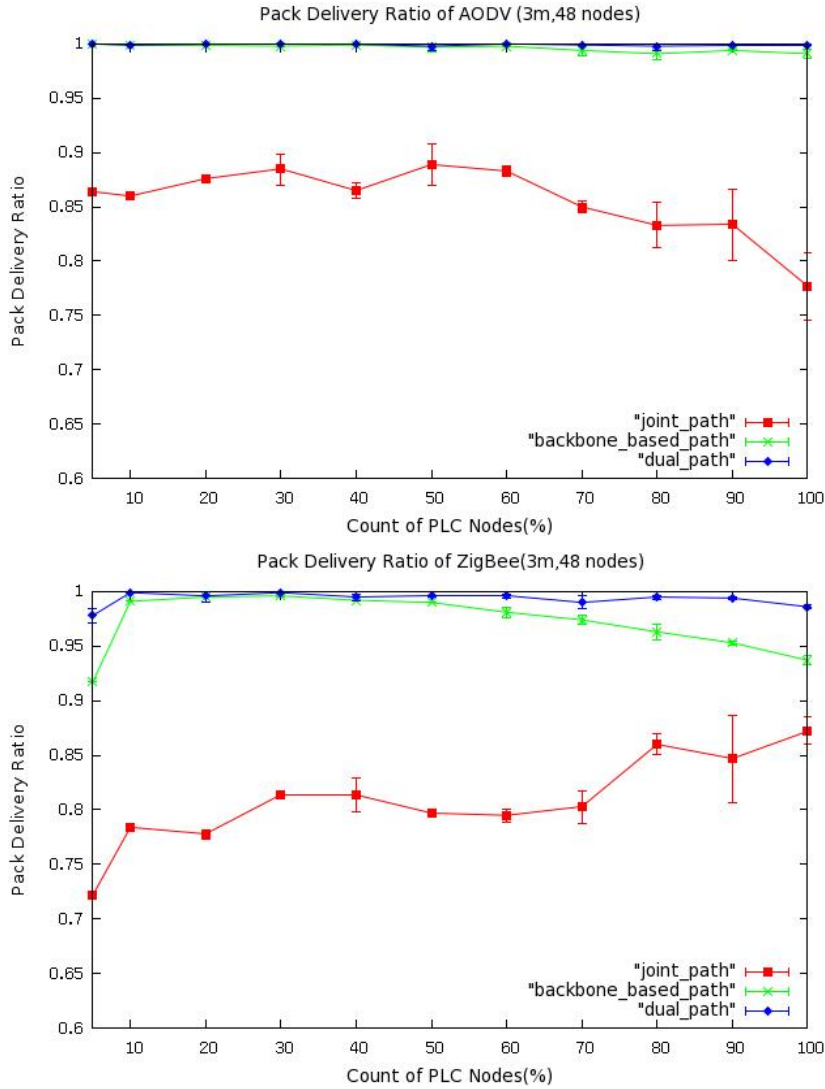


Figure 55 The PDR of AODV and ZigBee (CI tagged)

As we explained previously, the PDR of the combined network using the backbone-based path strategy remains remarkably higher than that of the joint-path strategy in that packets issued from the central controller are forced to travel through the wired link to destination nodes. Similar results also apply to the combined network using the dual-path strategy since its PDR is the result of the wireless-path strategy plus the backbone-based path strategy during data transmission.

It is worth noting that an increase of PLC nodes slightly influences the PDR of the ZigBee-based network using the backbone-based path strategy due to the synchronous

mode inherent in the routing layer [68]. Given a density of 3 meters, approximately 2 to 3 out of 47 destination nodes fail to receive data packets in the worst case that the percentage of PLC nodes is equal to 100%. Based on the ZigBee routing protocol standard and the corresponding implementation, the routing layer is closed tied with the underlying link. To be fair to both the wireless interface and the wired interface, outgoing RREQ packets to be transmitted through both two interfaces should be broadcasted at the same time for both the AODV protocol and the ZigBee protocol. In the case of a ZigBee-based network, outgoing RREQ packets within PLC nodes have to be queued as long as the wireless link is busy in our implementation. The underlying link does not indicate the idle status to the routing object until it receives an acknowledgement packet from the receiver or ends up with a failure to access the channel, which inevitably disturbs the processing of packets and in turn impacts the PDR. On the contrary, an AODV-based network follows the standard asynchronous mode in NS-2 where each network object keeps independent from each other, avoiding this issue.

In addition to that, the simulation results also indicate that an increase in number of PLC nodes statistically enhances the PDR of the ZigBee-based network featured with the joint-path strategy, as compared to that of the AODV-based network. According to the ZigBee routing protocol standard, the mechanism of link quality detection was introduced in the ZigBee protocol so as to dynamically detect the reliability and availability of underlying links, which helps to establish optimal routes to destination nodes. Considering the highly frequent occurrences of signal interference and collisions in the wireless network, an increase in number of PLC nodes promotes the possibility that nodes failing to receive packets entirely via the wireless network receive packets forwarded through the wired network. Nevertheless, such possibility is also subject to the limitation of the synchronous mode. As shown in the simulation results, it occurs in the case of a considerably high percentage of PLC nodes occupying the combined network (i.e. beyond 70% for a grid size of 3 meters). Generally, the PDR of the ZigBee-based work is the result of the mechanism of link quality detection and the synchronous mode.

The average latency of AODV and ZigBee featured with various routing strategies are

shown as follows:

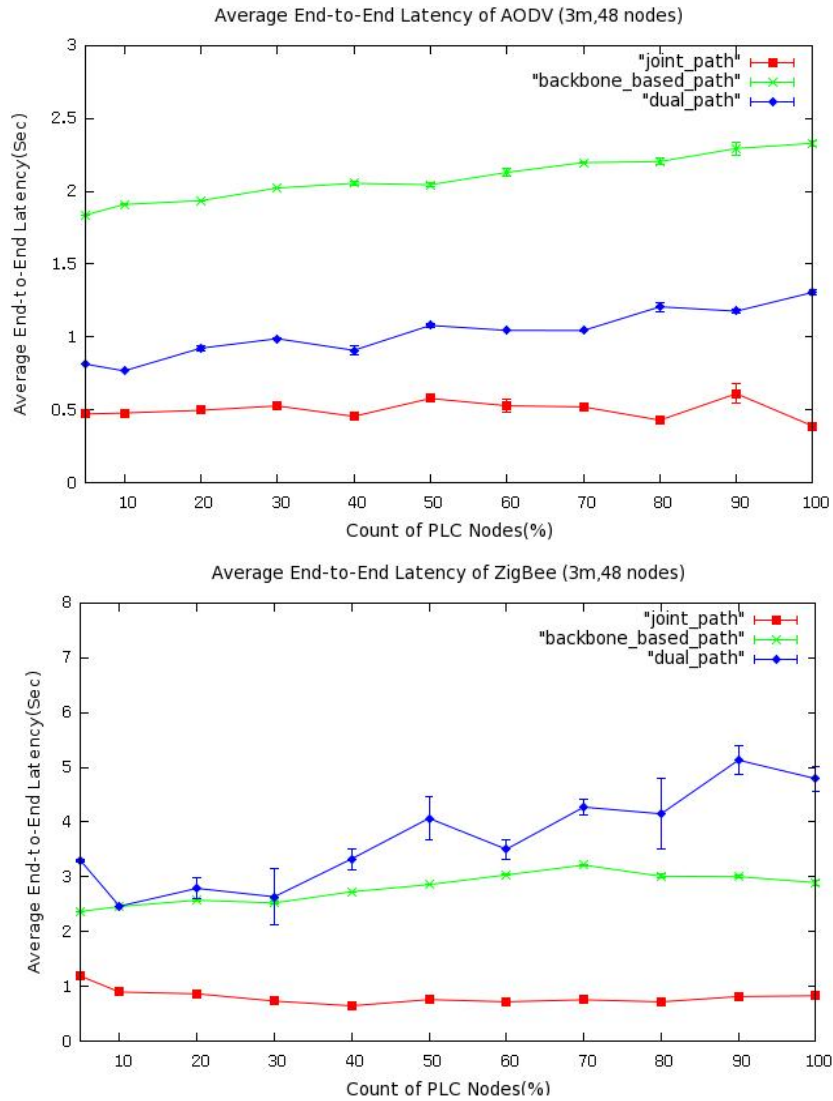


Figure 56 The average latency of AODV and ZigBee (CI tagged)

The simulation results above shows the similarity between AODV and ZigBee with respect to the impact of PLC nodes upon the network featured with various routing strategies mainly due to the similarity in their implementation. To accommodate the synchronous mode inherent in the ZigBee protocol for the purpose of the stability and reliability of data transmission, the timer used in the mechanism of timer-driven packet forwarding is set to a longer value than that in the AODV protocol, which leads to a generally higher latency of the ZigBee-based network as compared to that of the AODV-based network.

Also, the simulation results meet our anticipation that the average latency of the backbone-based path strategy or the dual-path strategy is higher than that of the joint-path strategy, which is mainly determined by two aspects as follows:

- (1) The delay spent upon the route establishment for each destination node based on the mechanism of the timer-driven packet forwarding, including the delay of route packet transmission as well as the waiting time in a queue of the central controller, as illustrated in Figure 57.
- (2) The delay in data transmission via the wired link or the wireless link after route establishment.

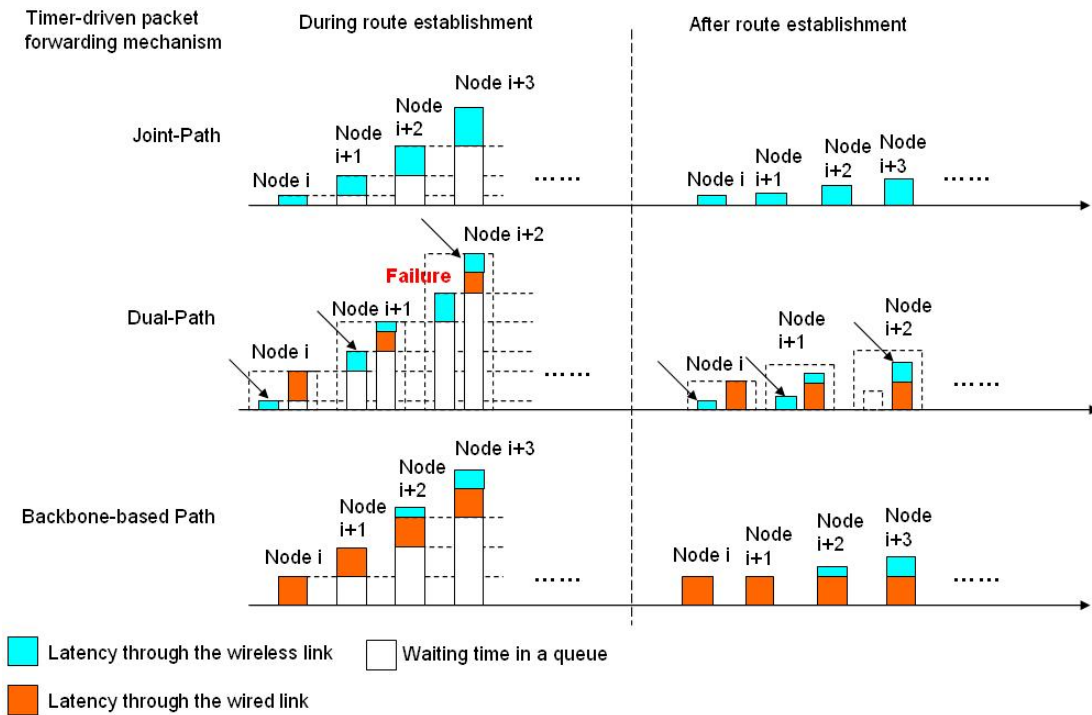


Figure 57 The measurement of average latency based on the timer-driven packet forwarding

Considering that packets through the wired link experience a higher delay as compared to through the wireless link during data transmission under the same conditions, the average latency of the backbone-based path strategy should be longer than that of the joint-path strategy since packets are firstly forwarded through the backbone to destination nodes in a combined network featured with the backbone-based path strategy, while nodes with joint-path strategy prefer the wireless link to forward packets.

In a wireless network (PLC nodes = 0%), there exist some nodes that fail to receive packets due to the signal interference as well as collisions in data transmission. The dual-path strategy ensures that each destination node in the combined network receives packets from the wireless link or the wired link in the sense that nodes failing to receive packets via the wireless link are capable of receiving packets forwarded through the wired link. In our project, the calculation of the average latency for the dual-path strategy only counts the first data packet received at the destinations through the wireless interface or the wired interface. In other words, it is the result of the delay in data packet transmission via both the wireless link and the wired link as well as the delay during route establishment.

In terms of the dual-path strategy, the majority of destination nodes receive data packets entirely via the wireless network while the remaining nodes receive data packets forwarded through the backbone. Thus, the average latency of the dual-path strategy should be slightly higher than that of the joint-path strategy and remarkably lower than that of the backbone-based path strategy, as typically shown in Figure 56 with respect to the AODV protocol.

In contrast with the AODV protocol, the average latency of the dual-path strategy in the ZigBee-based network remains even higher than that of the backbone-based path strategy. The reason is that the time spent upon the route establishment is noticeably longer due to the limitation of the synchronous mode in data transmission and the preset timer for packet forwarding. An example of a 3m-gridded network with 50% PLC node configured is illustrated as follows (the sequence number of RBDS packets transmitted in the network starts from 0):

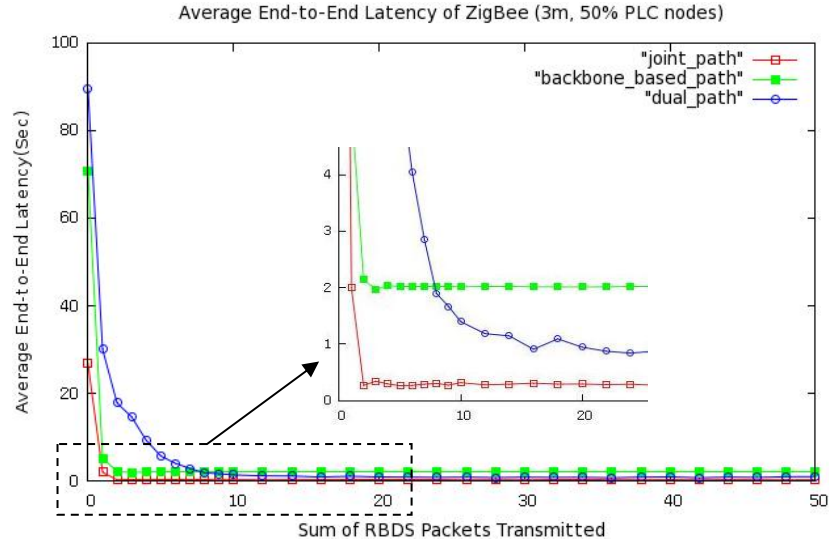


Figure 58 The average latency of a ZigBee network with 50% PLC nodes

Even though the average latency of the dual-path strategy is considerably higher than that of the backbone-based path strategy in the initial stage during route establishment, it tends to be stable and remains significantly below that of the backbone-based path strategy after a couple of times of RBDS packet transmission for the purpose of route establishment. Under such circumstances, routes from the central controller to each destination node have been established, whether through the wireless link or through the wired link. In other words, the average latency of the dual-path strategy keeps significantly lower than that of the backbone-based path strategy after route establishment, which meets our demand of implementing the dual-path strategy in the ZigBee protocol.

### 6.2.2 RBDS Traffic Rate

Given a 3m-gridded network with 48 nodes(including the central controller), we explore how the RBDS traffic affects the combined network featured with various protocols or routing strategies by adjusting the time interval of RBDS packet transmission with RBDS packet size equal to 30 bytes (typical for the RBDS network) in simulation scripts, as illustrated as follows:

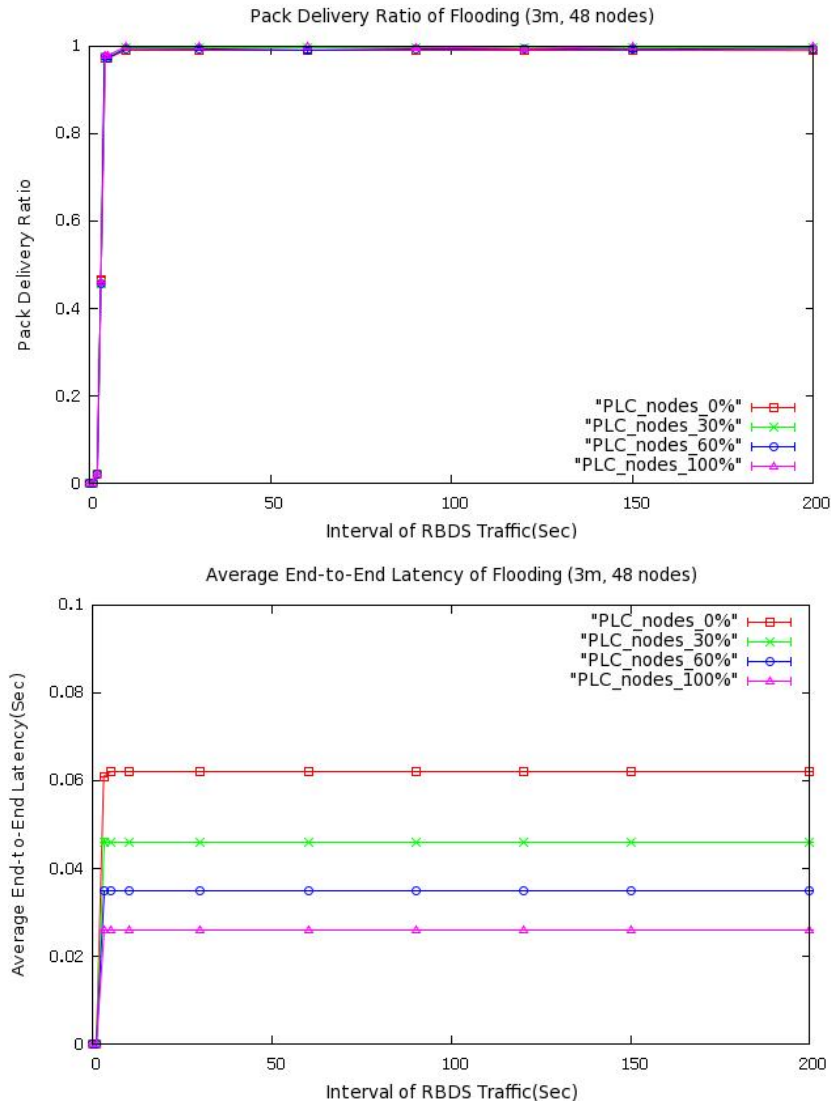


Figure 59 The PDR and average latency of Flooding vs. varying RBDS traffic rates

The simulation results above indicate that the PDR and the average latency of Flooding are significantly influenced by the RBDS traffic rate greater than one round of data transmission every 3.5 seconds in the RBDS network. The impact of the RBDS traffic rate upon the Flooding-based network is caused by two factors as follows:

- (1) The transmission delay of the RBDS network
- (2) The time spent upon the packet broadcasting in the Flooding-based network

To be specific, a complete data transmission from the RBDS network to the Flooding-based network consists of the sum of both delays that should be taken into consideration when setting the time interval of RBDS traffic. For one thing, the transmission delay of



the RBDS network is mainly determined by the RBDS packet size, as illustrated as follows:

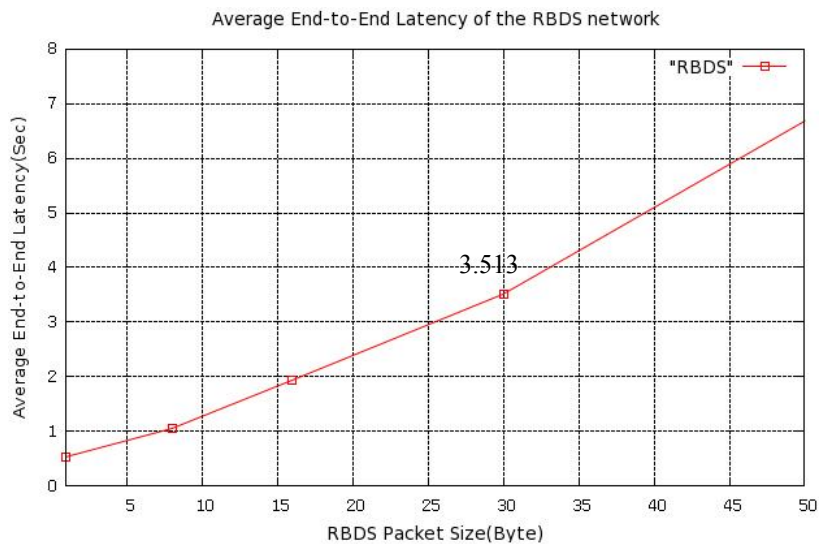


Figure 60 The average latency of the RBDS network

Based on the implementation of the RBDS network, the increase of the RBDS packet size leads to a higher reception delay at the side of central controller. In our case, the average latency of the RBDS network with the RBDS packet size equal to 30 bytes is approximately 3.513. At the same time, the average latency of the Flooding-based network is far less than 0.1 second as illustrated above, considering that all destination nodes in the network have enough time to receive RBDS packets forwarded by the central controller. Given the fixed delay in the RBDS network, the time interval of RBDS traffic close to or lower than this delay value will squeeze the transmission time in the Flooding-based network and cause two results as follows:

- (1) The central controller receives nothing from the RBDS network.
- (2) The majority of nodes fail to receive RBDS packets in such a short delay, considering the reception time as well as packet loss/retransmission due to signal interference/collision at the underlying link.

Consequently, only a couple of destination nodes close to the central controller in distance successfully receive broadcasted packets from the central controller or even no node at all receive any packet in the worst case when the interval is nearly zero, which inevitably leads to a considerably lower PDR and lower average latency accordingly,

which is measured based on successfully received packets only.

On the contrary, a RBDS traffic rate below the maximal threshold statistically makes no difference to the data transmission in the Flooding-based network as suggested in the simulation results. Literally, it guarantees that all destination nodes in the Flooding-based network have enough time to receive RBDS packets in terms of transmission delay.

Likewise, similar results are also observed in the case of AODV and ZigBee with various routing strategy, as illustrated in Figure 61 and Figure 62.

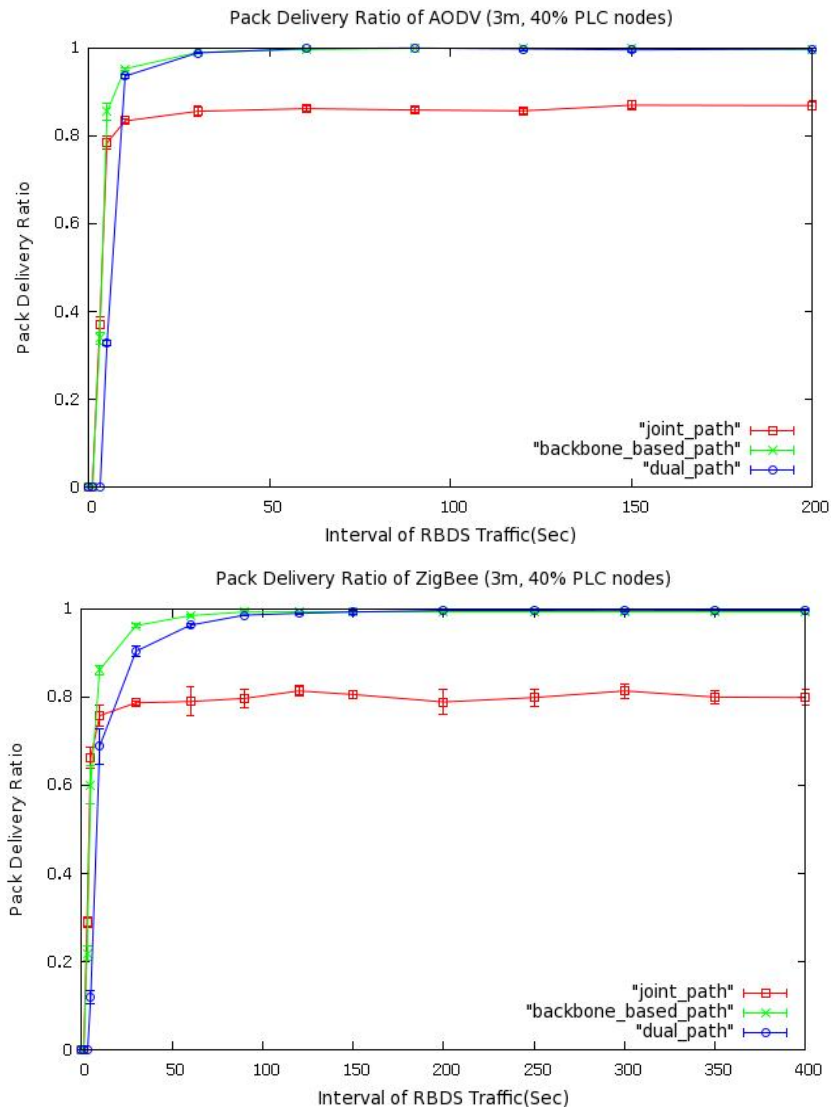


Figure 61 The PDR of AODV and ZigBee vs. varying RBDS traffic rates

The only discrepancy between the Flooding-based network and these routing-based

networks is that the maximal threshold of RBDS traffic rate set in the AODV protocol and the ZigBee protocol keeps considerably lower than that set in the Flooding protocol. As explained in Section 6.2.1, the average latency of these routing-based networks includes the time of route establishment on the basis of timer-driven packet forwarding, in addition to the transmission delay in data transmission after route establishment. Except for the delay in the RBDS network, the time interval of RBDS traffic lower than the average latency of the combined network will generate the same results as in the Flooding-based network, due to the fact that the majority of destination nodes fail to establish routes or fail to receive RBDS packets from the central controller under the same circumstances.

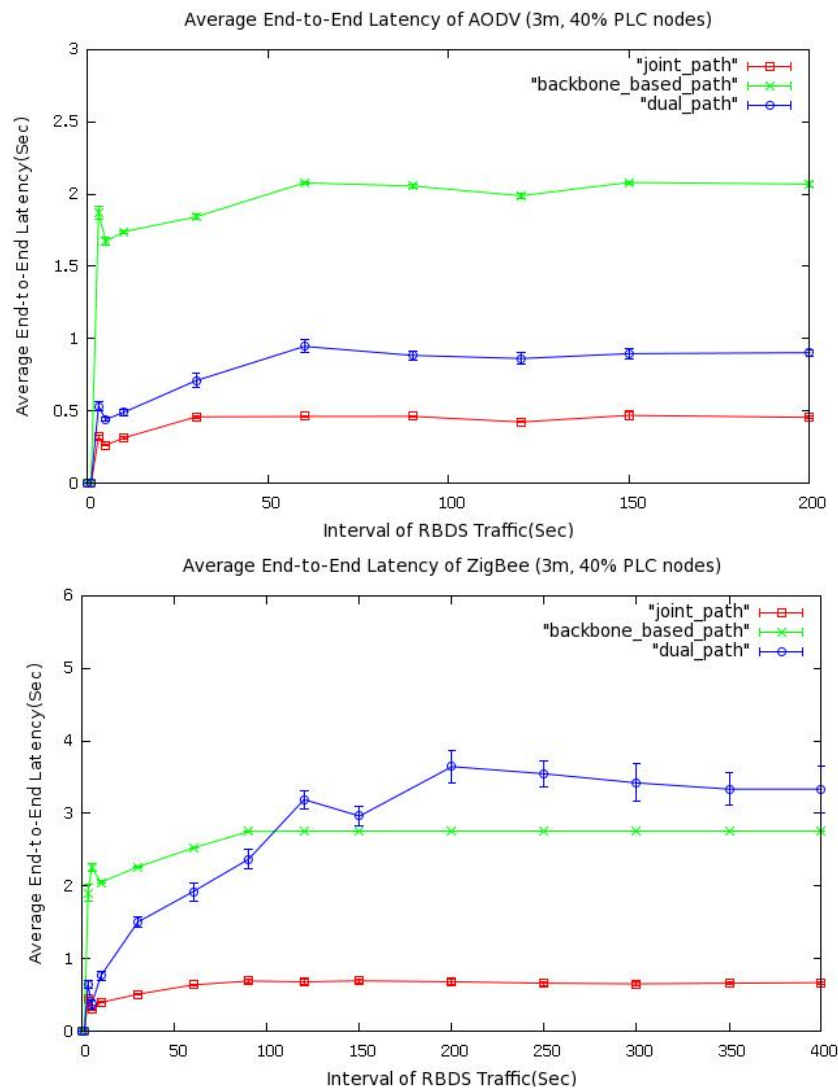


Figure 62 The average latency of AODV and ZigBee vs. varying RBDS traffic rates

As compared to the AODV-based network with the dual-path strategy, the maximal interval of RBDS traffic in the ZigBee-based network with the dual-path strategy remains longer than the ZigBee-based network with the other two routing strategies. In the ZigBee-based network with the dual-path strategy, the time of route establishment for all destination nodes is noticeably longer than in the network with the other two routing strategies due to the timer setting as well as the limitation of the synchronous mode in data transmission, as already discussed previously in Section 6.2.1. Thus, the ZigBee-based network with the dual-path strategy takes even more time than the other two routing strategies to complete the RBDS packet transmission at the initial stage, which in turn prolongs the maximal interval of RBDS traffic and reduces the threshold of RBDS traffic rate accordingly.

### 6.2.3 RBDS Packet Size

As discussed in the previous section, a large RBDS packet results in a high reception delay at the central controller side in the RBDS network, as illustrated in Figure 63.

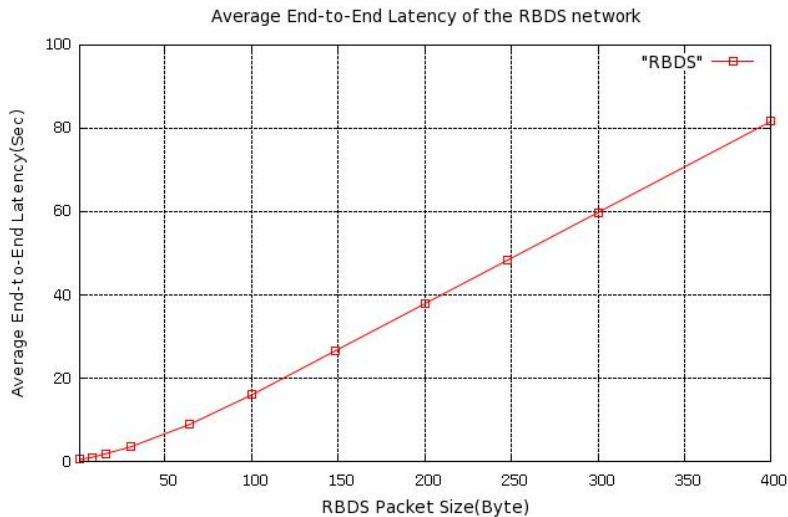


Figure 63 The extended average latency in the RBDS network with large RBDS packets

Given the fixed number of times RBDS packets are transmitted in the RBDS network, the time interval of RBDS traffic is large enough to so that the central controller is able to receive all incoming RBDS packets delivered from the RBDS network and forward them to all destination nodes in the combined network. Thus, the setting of time interval is

based on the transmission delay in the RBDS network and the average delay in combined network with Flooding, AODV or ZigBee routing individually.

The impact of RBDS packet size upon the combined networks featured with various protocols/routing strategies is illustrated as follows.

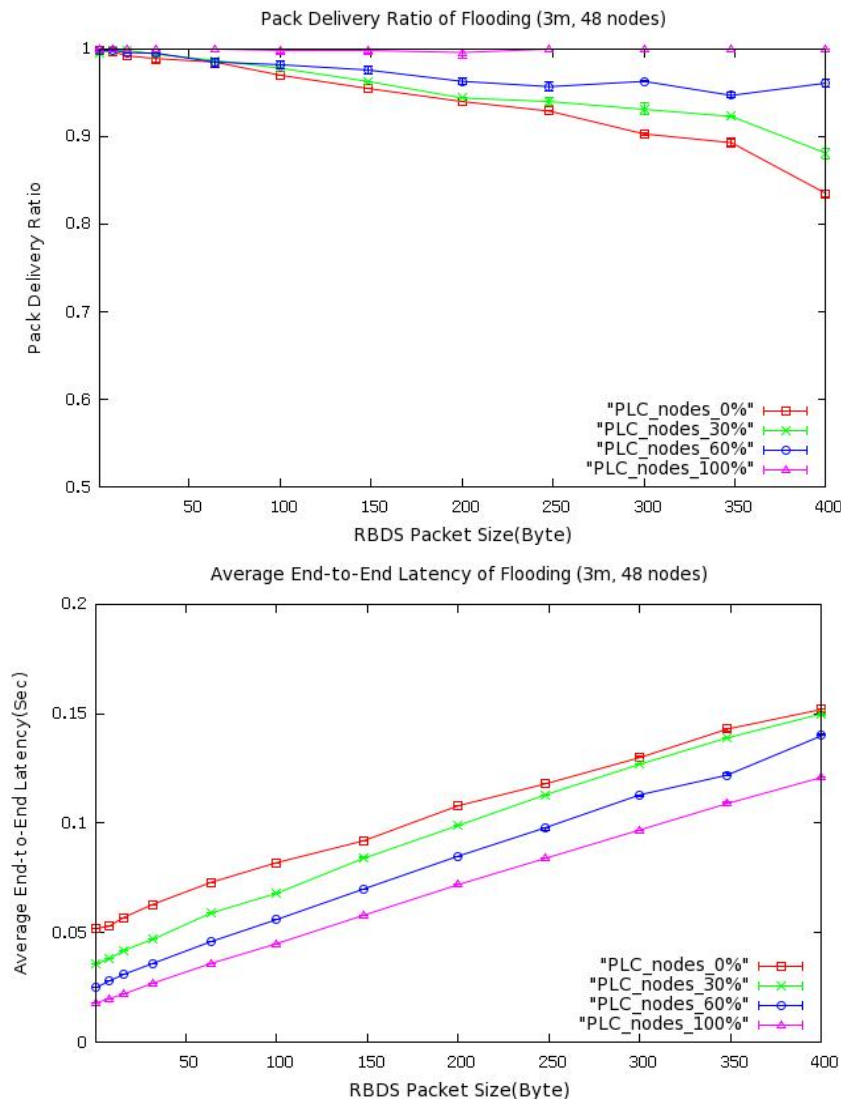


Figure 64 The PDR and average latency of Flooding with the increase of RBDS packet size

The simulation results above indicate that the increase of RBDS packet size significantly reduces the PDR and extends the average latency of the network. The situation is directly associated with two factors as follows:

- (1) The processing time of network objects within a node during data transmission that is

subject to the simulation environment of NS-2 itself.

(2) Packet loss and retransmission due to signal interference and collisions existing in the wireless link.

As shown previously in Figure 63, the increase of RBDS packet size extends the transmission delay in the RBDS network. The same conclusion applies as well to the data transmission in a smart home. To be specific, a large RBDS packet will extend the processing time from the upper layer to the underlying link, independent of the network type. On one hand, the extension of transmission time reinforces the possibility of failure to send data packets through the busy shared channel based on CSMA, which inevitably deteriorates the network performance. On the other hand, the extension of processing time upon reception of packets also aggravates the packet loss and retransmission caused by signal interference and collisions especially in the wireless link, which in turn enables packets to be forwarded via the wired link with a higher possibility. Hence, a high percentage of PLC nodes in the network could effectively offset the impact caused by a longer RBDS packet size in terms of PDR, even though the combined network experiences a higher average latency.

Given a fixed percentage of PLC nodes, results similar to the Flooding protocol are observed in the case of an AODV-based network or a ZigBee-based network with various routing strategies, as illustrated as follows.

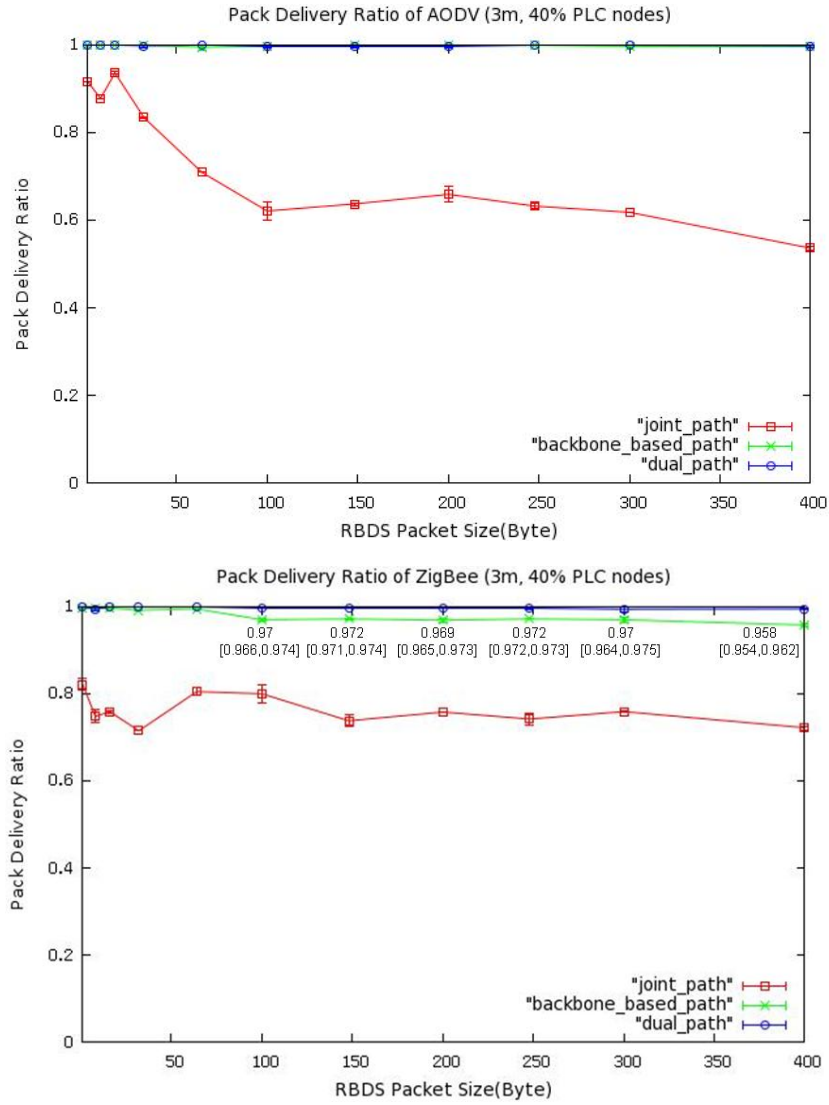


Figure 65 The PDR of AODV and ZigBee with the increase of RBDS packet size

Apart from the factors that affect the Flooding protocol, the extension of RBDS packet size also compromises the normal process of route establishment in the combined network, especially with the joint-path strategy. Based on the mechanism of timer-driven packet forwarding in our project, a new RREQ packet is sent by the central controller to the next destination node as soon as a RBDS data packet is sent out to the previous destination node after its route establishment. After that, incoming or outgoing route packets to be forwarded nodes along the established route have to wait till these nodes finish handling RBDS data packets. Under such circumstances, a large RBDS data packet inevitably prolongs the processing time ranging from the central controller, forwarding

nodes to destination nodes involved in route establishment and RBDS data packet forwarding, which further promotes the possibility of packet loss and retransmission (including route packets and RBDS data packets) via the wireless link. As a consequence, the combined network with the backbone-based path strategy or with the dual-path strategy is far less susceptible to variations of the RBDS packet size than the joint-path strategy in terms of PDR (the size of RBDS packet has a trivial impact upon to the PDR of the ZigBee-based network with backbone-based path strategy due to the limitation of synchronous mode, considering that less than two nodes fails to receive RBDS packets during data transmission).

In contrast with the descending PDR of the joint-path strategy in the AODV-based network, the mechanism of link quality detection in the ZigBee-based network helps nodes to chose the underlying links with better quality under the same conditions as much as possible, whether the wired link or the wireless link, which to some extent offsets the negative influence of increasing RBDS packet size upon the combined network as illustrated above.



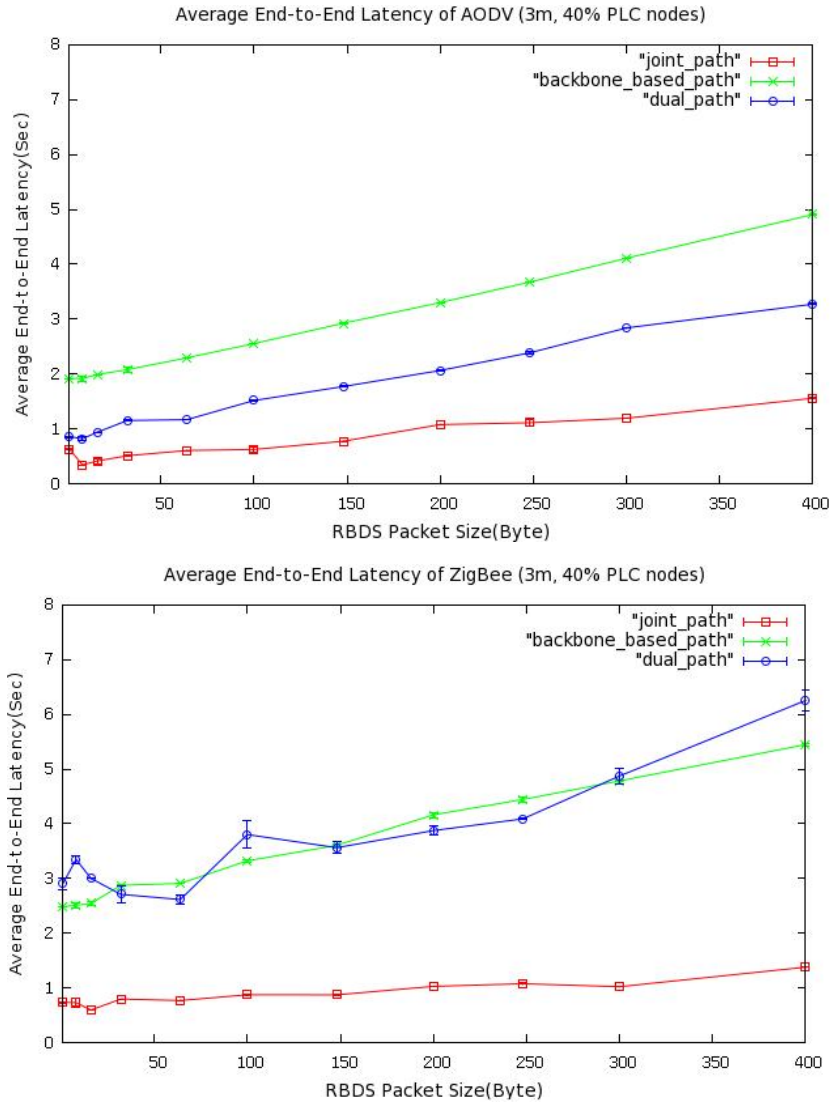


Figure 66 The average latency of AODV and ZigBee with the increase of RBDS packet size

Similar to the Flooding protocol, an AODV-based network or an ZigBee-based network also experiences a longer average latency due to the extended delay during timer-based route establishment and large RBDS packet transmission, as illustrated in Figure 66 (As discussed in Section 6.2.1.3, the average latency of a ZigBee-based network with the dual-path strategy keeps close to or higher than that with backbone-based strategy due to timer setting as well as the corresponding delay for route establishment intended for two routes individually).

## 6.2.4 Traffic Rate of Status Updates

In smart homes, a limited amount of large-scale home appliances are capable of periodically informing the central control platform of their updated status, such as the refrigerator, the water heater, the HVAC system, as so forth. To model such a scenario in our project, 5 nodes along the corners of a house with a fixed node density are chosen to send short-sized packets (CBR over UDP) to the central controller at identical time intervals, as shown as follows:

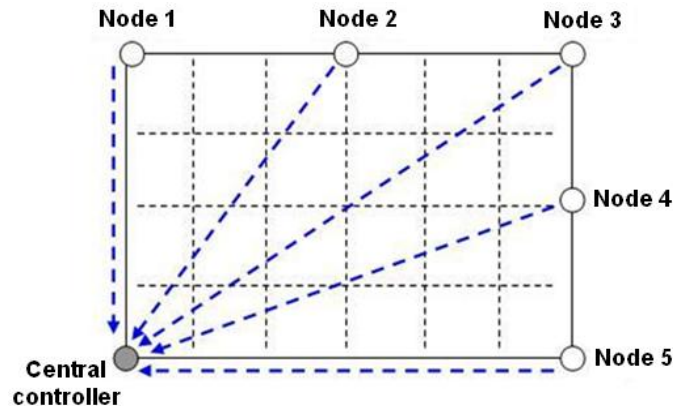


Figure 67 The layout of nodes with capability of sending status messages

By adjusting the time interval of status packet transmission, we investigate how the intensity of status update traffic influences the performance of an AODV-based network or a ZigBee-based network, as illustrated in Figure 68 and Figure 69.

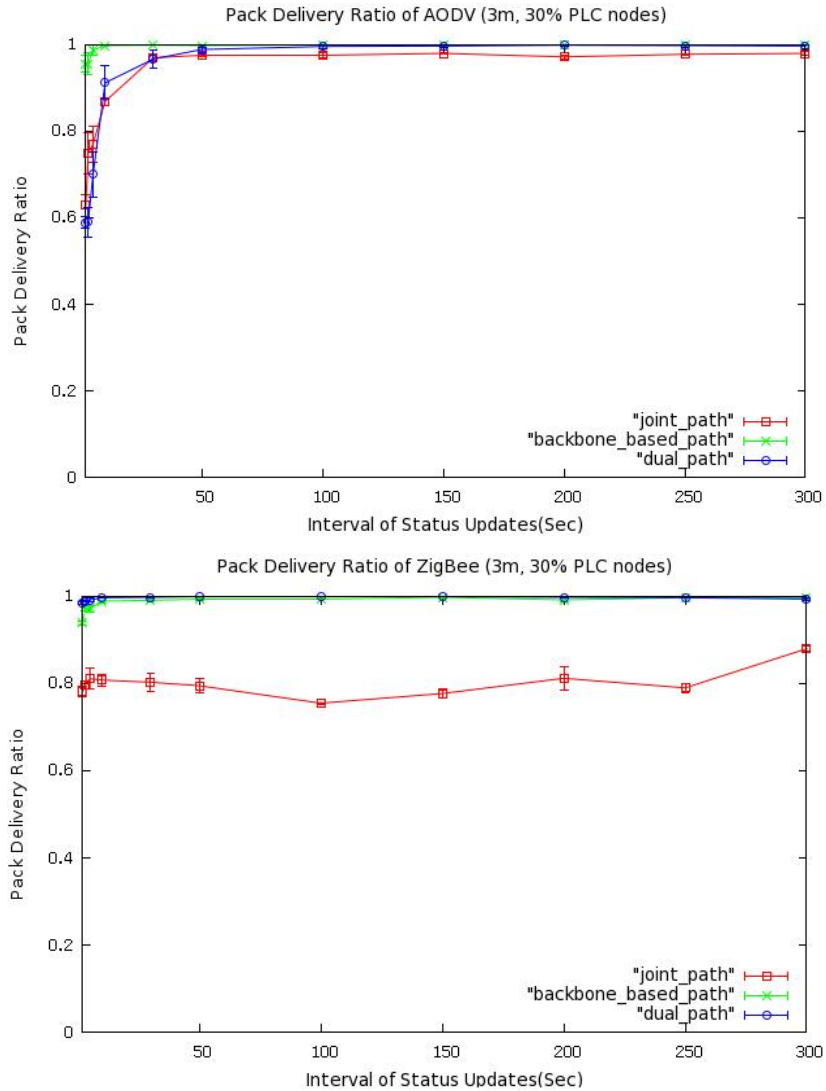


Figure 68 The PDR of AODV and ZigBee vs. varying status updating rates

In our project, status updating transmission follows various routing strategies preset in the combined network. Considering that status update messages are sent in a direction opposite to the RBDS traffic, nodes with the capability of status feedback could be treated as the disturbance source as long as they transmit status messages in an extremely intensive way. To be specific, these messages overwhelming the combined network will cause two problems as follows:

- (1) A higher delay of route packet forwarding during route establishment and RBDS data packet transmission after route establishment.
- (2) Packet loss and retransmission with a higher possibility due to signal interface/

collision on the shared wireless channel.

As a consequence, the status update traffic with an extremely short interval statistically reduces the PDR and prolongs the average latency in the combined network, especially for an AODV-based network. As compared to the AODV-based network, the ZigBee-based network featured with various routing strategies is less subject to the intensity of status update traffic since the mechanism of link quality detection partially offsets the impact of status update traffic in data transmission.

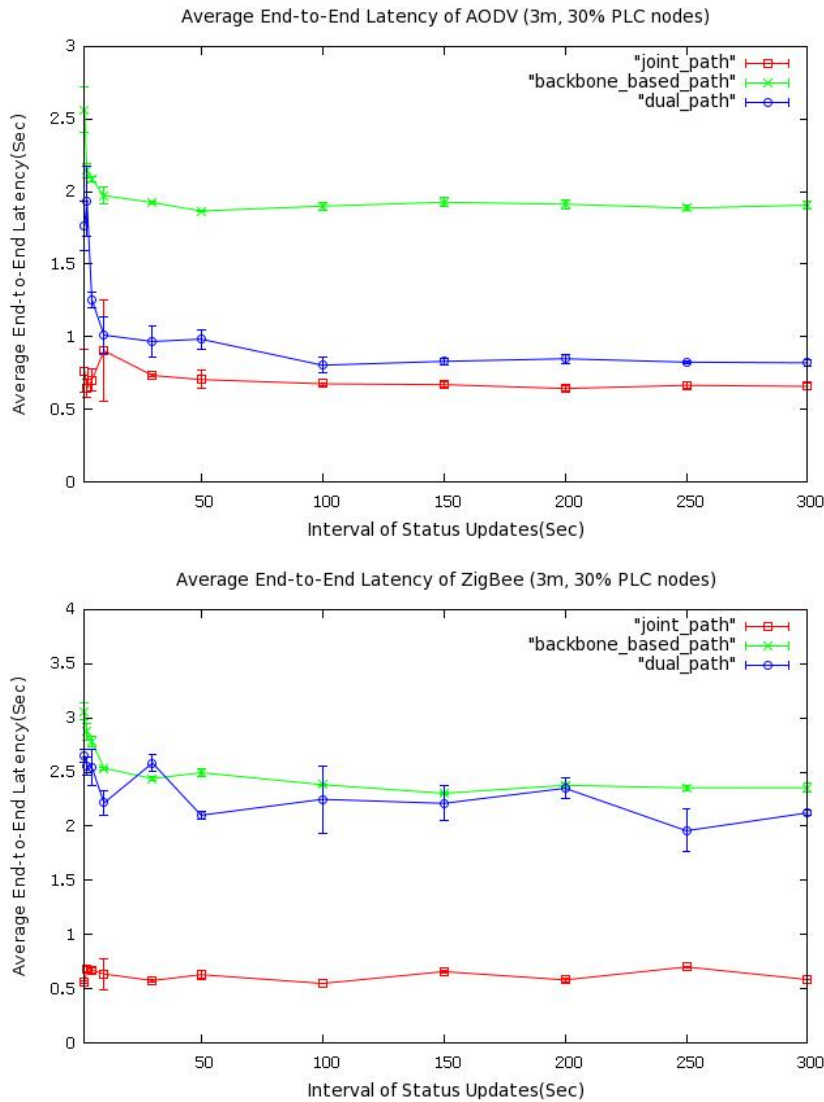


Figure 69 The average latency of AODV and ZigBee vs. varying status updating rates

On the other hand, increasing the time interval of status update traffic minimizes such disturbance during the RBDS packet transmission, regardless of protocols and route

strategies, which allows the combined network to behave as usual, as shown in the simulation results. Besides, the status update traffic with a reasonable interval contributes to increment of PDR of the joint-path strategy in the sense that routes to destination node are partially created during the status packet transmission. In contrast with an AODV-based network, a ZigBee-based network with the joint-path strategy remains less susceptible to status update traffic mainly due to the limitation of synchronous mode inherent in the ZigBee implementation. In addition, the dynamic of status update traffic rate statistically makes no difference to the combined network with the joint-path strategy since the majority of routes are established via the wireless link.

### **6.2.5 Wireless Error Rate**

To explore the reliability and robustness of a combined network, we adjust the packet error rate at the wireless interface of nodes and observe how the occurrence impacts the combined network configured with various protocols or routing strategies, as illustrated as follows:

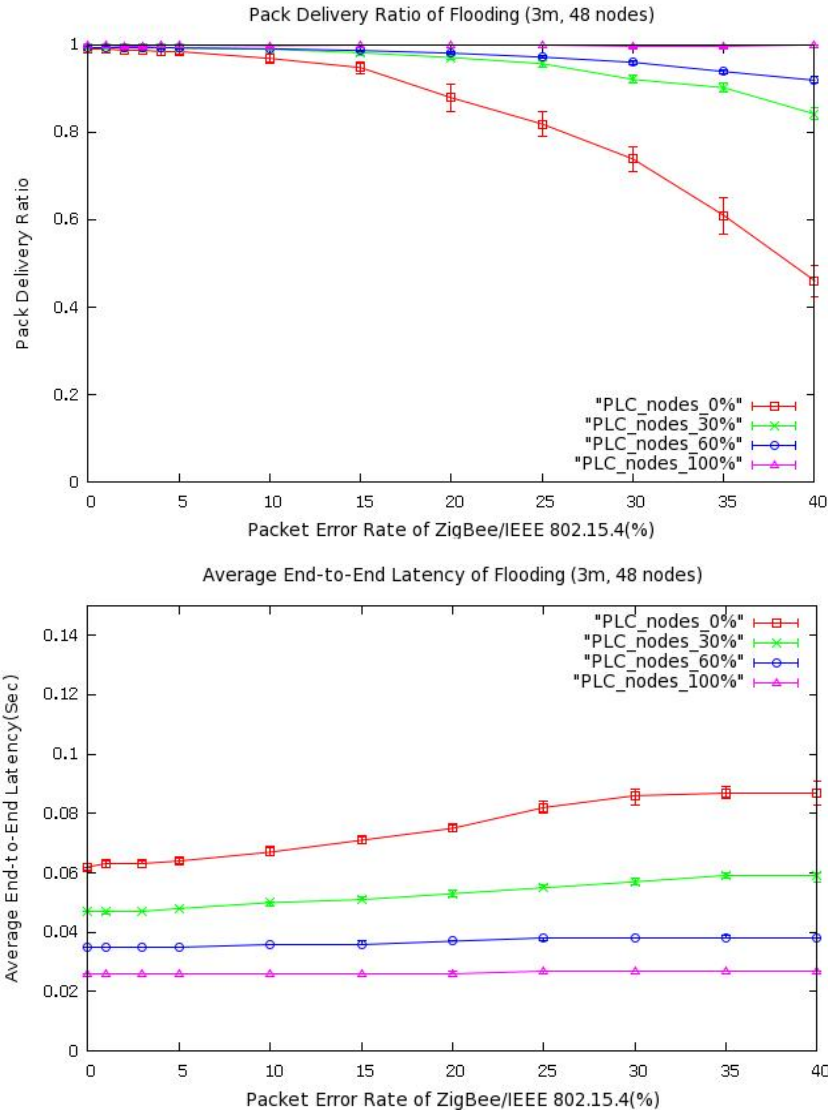


Figure 70 The PDR and average latency of Flooding vs. varying wireless error rates

The simulation results above indicate that a wireless network (PLC nodes = 0%) is inevitably influenced by an increased wireless error rate without support of the backbone. Specifically, the increase of wireless error rate statistically reduces the PDR and extends the average latency accordingly due to the fact that incoming broadcast packet through the wireless interface are randomly discarded with a higher possibility based on the setting of packet error rate. Under such circumstances, a combined network could effectively reduce the impact of wireless errors in the sense that identical packets rejected at the wireless interface are more likely to be forwarded through the backbone to destination nodes. As discussed in Section 6.2.1.3 with regard to the Flooding

transmission, the more PLC nodes deployed in the network, the more RBDS broadcast packets received at destinations are successfully forwarded by the backbone due to the processing delay of multiple hops via the wireless link. In this case, the average latency of a combined network with a higher percentage of PLC nodes is mostly determined by the transmission delay of the wired link rather than the wireless link. In other words, an increase in number of PLC nodes substantially diminishes the impact of wireless errors upon the combined network, as shown in the simulation results above.

Similar to the case of a Flooding-based network, a high percentage of wireless error rate in an AODV-based wireless network or an ZigBee-based wireless network (PLC nodes = 0%) statistically reduces the PDR and prolongs the average latency mainly caused by packet loss and retransmission of route packets during route establishment and of RBDS packets after route establishment, as illustrated in Figure 71 and Figure 72.

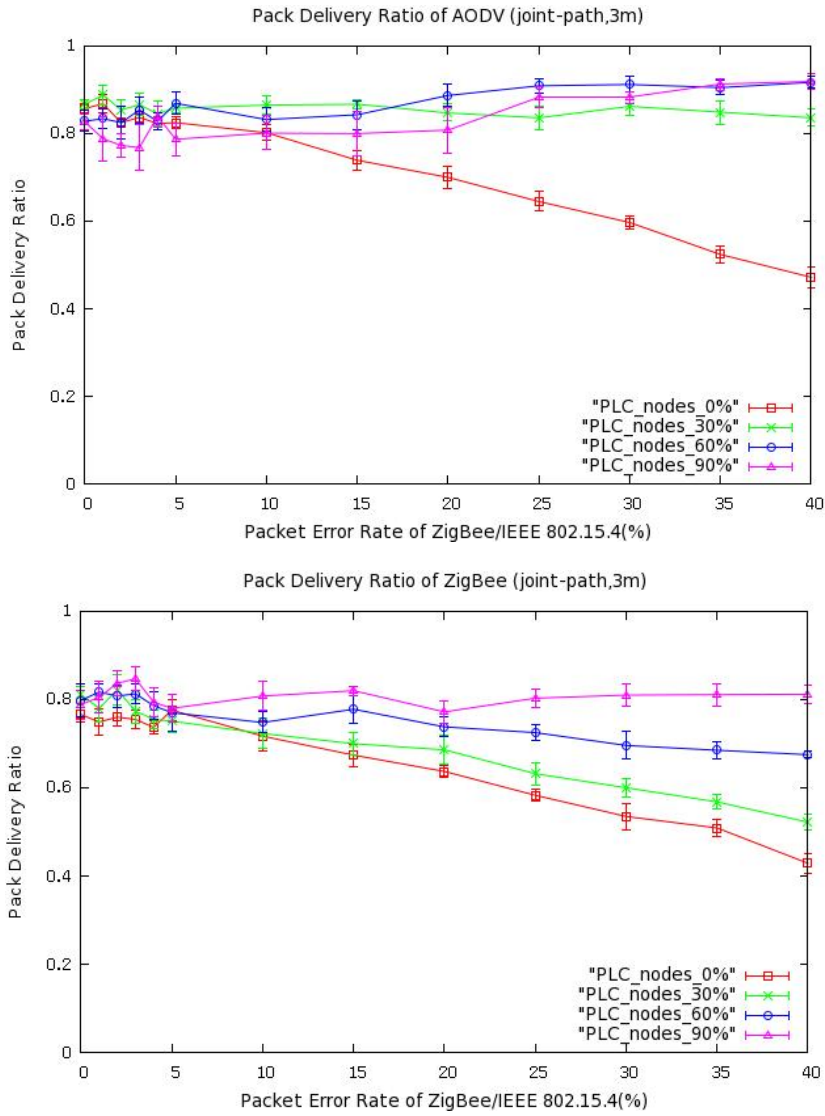


Figure 71 The PDR of AODV and ZigBee vs. varying wireless error rates

Likewise, a routing-based combined network (AODV or ZigBee) could effectively offset the impact of wireless errors in that routes packets rejected at the wireless interfaces could travel through the backbone to destination nodes for the purpose of route establishment at the cost of transmission delay, as shown in Figure 72. Eventually, the existence of PLC nodes statistically reduces the possibility of packet loss for both routes packets and RBDS packets accordingly.



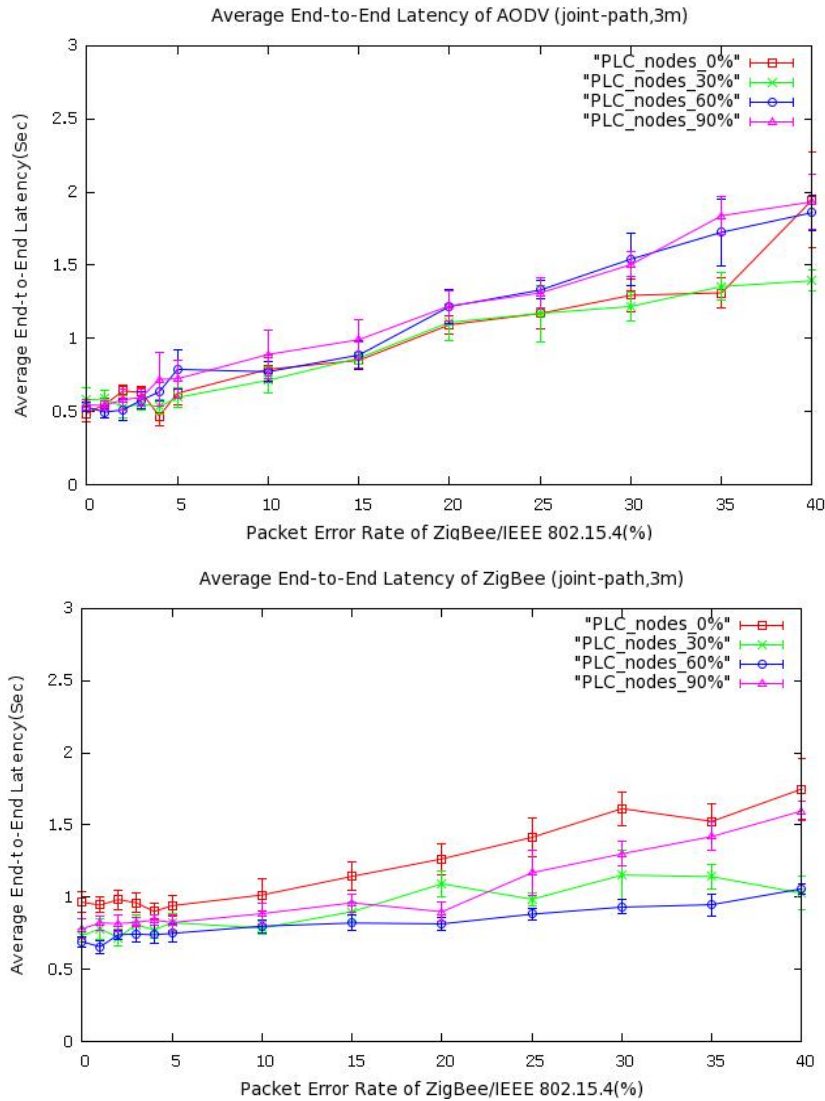


Figure 72 The average latency of AODV and ZigBee vs. varying wireless error rates

Additionally, the response of the AODV-based network to wireless errors is more sensitive than that of the ZigBee-based network since the wireless interface and wired interface of PLC nodes in the AODV-based network operates independent from each other in the context of the asynchronous mode. In spite of the limitation of synchronous mode inherent in the ZigBee protocol, the ZigBee-based network is capable of enhancing the PDR of network with the increase of PLC nodes, which meets our previous anticipation from the perspective of implementation in our project.

## 6.3 Conclusions

According to the simulations results and the corresponding analysis carried out above, the findings of the general performance of a combined network in comparison with that of a wireless network featured with various protocols/routing strategies are categorized into several aspects based on the impact of the dynamic factors involved.

- (1) A wireless network consumes more power than a combined network (including the energy cost upon the reception of RBDS packets at the central controller), regardless of the network layer protocol, since the network energy cost only covers wireless nodes that are powered by batteries rather than the backbone. Increasing the percentage of PLC nodes helps to effectively reduce the network energy cost of a combined network with a fixed node density. The node density indirectly influences the network energy cost by increasing the number of wireless nodes engaged in data transmission. A Flooding-based network consumes less power than the other two routing-based networks in that the nodes energy is only used to transmit data packets rather than to determine packet routes or retransmission. Given a fixed node density, an AODV-based or ZigBee-based network employing the backbone-based path strategy will lead to a lower energy cost as compared to the dual-path strategy and the joint-path strategy due to the difference in implementation.
- (2) The node density statistically makes little difference to the overhead of a Flooding-based network, regardless of whether Flooding occurs over the wired or the wireless links. In terms of an AODV-based/ZigBee-based network, the overhead of the wireless link remains considerably higher than that of the wired link with the increase of node density due to the multiple wireless hops and the accompanying packet loss/retransmission. Hence, the deployment of the backbone as much as possible effectively reduces the overhead of the routing-based network.
- (3) Except for a higher average latency incurred by the multiple hops via the wireless link, changing node density as well as the percentage of PLC nodes statistically makes trivial difference to a Flooding-based network, whether in a wireless network or in a

combined one. In contrast with the joint-path strategy, an AODV-based/ZigBee-based network featured with the backbone-based path strategy or the dual-path strategy experiences a better PDR compared to a Flooding-based network at the cost of a longer delay mostly due to the lower data rate of the backbone on the basis of the mechanism of timer-driven packet forwarding. Besides, the difference of performance metrics between an AODV-based network and a ZigBee-based network with the increase of node density as well as the percentage of PLC nodes mostly stems from the difference of details in their implementation, such as the route establishment, the data transmission mode, the timer setting, and so forth.

- (4) The time threshold of protocols to complete a round of RBDS packet transmission covers the time spent on forwarding data packets to all destination nodes and the time spent on establishing routes intended for routing-based networks. Thus, a high RBDS traffic rate exceeding the time threshold will prevent destination nodes from successfully receiving data packets from the central controller, which ultimately leads to a diminishing PDR of the network. Similar to the impact of the RBDS traffic rate, a high intensity of status update traffic in a reverse direction significantly reduces the PDR and extends the average latency by disturbing the normal progress of route establishment as well as data packet transmission afterwards. Likewise, large RBDS packets or a higher wireless error rate enhances the possibility of packet loss and retransmissions existing in the wireless link, which results in a reduced PDR and a longer average latency. Hence, a combined network is capable of offsetting the influence from large RBDS packets or an increased wireless error rate by forwarding packets through the wired link when possible.

In general, a network combining ZigBee/IEEE 802.15.4 and HomePlug C&C outperforms a pure ZigBee/IEEE 802.15.4 network in most aspects. In terms of the protocol configuration at the network layer, each protocol or routing strategy has its own strengths and weaknesses when put in use. Therefore, specific applications to a smart home, the demands of network energy cost and the average latency should be taken into careful consideration when choosing protocols/routing strategies intended for residences.

## 7 Conclusions and Future Work

### 7.1 Conclusions

The main emphasis of our study is to explore what kind of networking technology is advantageous to smart homes in the context of DR message delivery from utilities to residences for the purpose of energy saving. Taking other factors into account, including openness of the protocol stack, interoperability based on layering and cost-effectiveness, we propose a backbone network of HomePlug C&C plus ZigBee/IEEE 802.15.4, which is designed and implemented as an experimental model in NS-2 in an effort to investigate the overall performance of the combined network. Although our experimental model is integrated with routing protocols and underlying links specific to our project, the model framework could be extended with the implementation of existing or emerging network technologies to support more generic cases on the principle of multiple interfaces and multiple channels.

By introducing the RBDS network into our model to mimic various scenarios of DR data transmission, our research shows that the combined networking solution distinguishes itself as a competitive and promising candidate in the field of smart home networking from the perspective of energy saving. A combined network helps to reduce the energy cost due to the fact that all PLC nodes engaged in the network could obtain infinite power from the backbone for data transmission instead of batteries that supply wireless nodes. Given that packets are forced to be forwarded through the backbone, a combined network also contributes to a lower network overhead by limiting route lengths to one hop from the central controller to forwarding PLC nodes or destination PLC nodes. As compared to a wireless network, a wired network shows strong reliability and robustness when exposed to different kinds of dynamic network environment, covering the size of RBDS packet, the status message traffic issued from nodes to the central controller and the wireless error rate. Given first priority to packet reception, a combined network is capable of guaranteeing a better PDR to smart homes by offsetting such disturbances with the aid of backbone.

When forwarding RBDS packets to all destination nodes in the network, the AODV protocol and the ZigBee routing protocol perform worse than the Flooding protocol in terms of the network energy cost, the network overhead and the average latency, due to the mechanism of timer-driven route establishment and issues of packet loss and retransmission inherent in the high-rate wireless link. Even though a ZigBee-based network is restricted to the synchronous mode in data transmission, it still shows a high performance comparable to an AODV-based network through the tradeoffs of design in adapting its implementation to our requirements of multiple interfaces and multiple channels. Considering the popularity and availability of ZigBee-based devices in the market as well as the comprehensiveness of the ZigBee technical specification, the ZigBee protocol should be treated as a strong candidate as with the AODV protocol when focusing on forwarding packets to individual nodes under the same circumstances.

With regard to the configuration of routing strategy, a dual-path strategy and a backbone-based path strategy preset in an AODV-based/ZigBee-based network are superior to a joint-path strategy in terms of PDR, in addition to their capability of resisting the impact of RBDS packet size in the combined network. The backbone-based path strategy is employed where the control and management of network energy cost is essential to smart homes, whereas the dual-path strategy should be taken into account where a comparatively low average latency is required by both utilities and residents from the perspective of the operational mechanism of DR programs on the smart grid infrastructure.

## **7.2 Future Work**

From the perspective of software implementation, the experimental model needs to be extended to mimic the scenario of how the central controller monitors target nodes involved by periodically communicating with them, which frequently occurs in smart homes. With the support of the node addressing scheme, it should be taken into serious consideration how to accommodate multiple smart homes coexisting in a single simulation scenario in an effort to mimic the delivery of DR messages from utilities or

third-party service providers to multiple residences on a large scale. To further evaluate the feasibility of the model in real environments, it is indispensable to establish a test-bed equipped with wireless/PLC devices for the purpose of cross-validation of the simulation results produced in our model. Finally, security issues associated with smart homes should be treated as an independent topic to be explored, ranging from the device registration/management in the combined network to the secure communication between the central controller and smart devices in the house.

## References

- [1] Federal Energy Regulatory Commission, “Staff Report-Assessment of Demand Response and Advanced Metering”, September 2007, [Online]. Available: <http://www.ferc.gov/legal/staff-reports/09-07-demand-response.pdf>
- [2] Peak Load Management Alliance, “Interaction of Advanced Metering Initiative (AMI) and Demand Response”, Spring 2006 Conference, March 13, 2006, [Online]. Available: <http://www.peaklma.com/documents/Haynes.pdf>
- [3] Joshua Horton, “AMI as Demand Response Enabling Technology”, Automation Insight, February 2009, pp. 1-2, [Online]. Available: <http://kema.fr/cn/Images/Automation%20Insight%20-screen%202-09.pdf>
- [4] Ontario’s Smart Grid Forum, “Enabling Tomorrow’s Electricity System: Report of the Ontario Smart Grid Forum”, February 2009, [Online]. Available: [http://www.ieso.ca/imoweb/pubs/smart\\_grid/Smart\\_Grid\\_Forum-Report.pdf](http://www.ieso.ca/imoweb/pubs/smart_grid/Smart_Grid_Forum-Report.pdf)
- [5] Yousuf, M.S., El-Shafei, M., “Power Line Communications: An Overview - Part I”, 4th International Conference on Innovations in Information Technology, November 2007, pp. 218-222.
- [6] Gonzalo Delgado Huitrón, “Reducing Home Power Consumption with Wireless Controllers”, [Online]. Available: [http://www.freescale.com/files/archives/doc/support\\_info/LOW\\_POWER\\_CONSUMPTION.pdf](http://www.freescale.com/files/archives/doc/support_info/LOW_POWER_CONSUMPTION.pdf)
- [7] Williams, E.D., Matthews, H.S., “Scoping the potential of monitoring and control technologies to reduce energy use in homes”, Proceedings of the 2007 IEEE International Symposium on Electronics & the Environment, May 2007, pp.239 - 244.
- [8] “Smart Grid: Enabler of the New Energy Economy”, December 2008, [Online]. Available: <http://www.oe.energy.gov/DocumentsandMedia/final-smart-grid-report.pdf>
- [9] Brian Atchinson, “Home Energy Use: Making Smart Choices”, New York State Conservationist, October 2007, [Online]. Available: [http://www.dec.ny.gov/docs/administration\\_pdf/1007energy.pdf](http://www.dec.ny.gov/docs/administration_pdf/1007energy.pdf)
- [10] “Small Wind Electric Systems: A U.S. Consumer's Guide”, March 2005, [Online]. Available: [http://www.windpoweringamerica.gov/pdfs/small\\_wind/small\\_wind\\_guide.pdf](http://www.windpoweringamerica.gov/pdfs/small_wind/small_wind_guide.pdf)
- [11] FLOYD ASSOCIATES, “ADVANTAGES OF PLUG-IN HYBRIDS”, APRIL 10, 2009, [Online]. Available: <http://www.floyd-associates.com/phev.pdf>

- [12] Jim Lazar, John Joyce, and Xavier Baldwin, "Plug-In Hybrid Vehicles, Wind Power, and the Smart Grid", January 2008, [Online]. Available: [http://www.raponline.org/Pubs/Jim\\_Lazar\\_PHEV\\_and\\_Smart\\_Grid\\_Final\\_12-31-07.pdf](http://www.raponline.org/Pubs/Jim_Lazar_PHEV_and_Smart_Grid_Final_12-31-07.pdf)
- [13] Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., Jansen, E., "The Gator Tech Smart House: a programmable pervasive space", Computer, Volume 38, Issue 3, March 2005, pp.50 - 60.
- [14] Programmable thermostat, [Online]. Available: [http://en.wikipedia.org/wiki/Programmable\\_thermostat](http://en.wikipedia.org/wiki/Programmable_thermostat)
- [15] "UtilityAMI 2008 Home Area Network System Requirements Specification", Version 1.04, August 19, 2008, [Online]. Available: <http://www.utilityami.org/docs/UtilityAMI%20HAN%20SRS%20-%20v1.04%20-%20080819-1.pdf>
- [16] Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., Loge, C., "The Smart Home Concept: our immediate future", 1ST IEEE International Conference on E-Learning in Industrial Electronics, Dec. 2006, pp. 23-28.
- [17] Energy conservation, [Online]. Available: [http://en.wikipedia.org/wiki/Energy\\_conservation](http://en.wikipedia.org/wiki/Energy_conservation)
- [18] Yousuf, M.S., El-Shafei, M., "Power Line Communications: An Overview - Part I", 4th International Conference on Innovations in Information Technology, Nov. 2007, pp.218 - 222.
- [19] X10 (industry standard), [Online]. Available: [http://en.wikipedia.org/wiki/X10\\_\(industry\\_standard\)](http://en.wikipedia.org/wiki/X10_(industry_standard))
- [21] David Liu, Dao Xian, "Home environmental control system for the disabled", Proceedings of the 1st international convention on Rehabilitation engineering & assistive technology, April 2007, pp.164-168.
- [22] Rashid, R.A., Sarijari, M.A., Abd Rahim, M.R., Tan Zun Yang, "Flood transmission based protocol for home automation system via power line communication", International Conference on Computer and Communication Engineering, May 2008, pp.867 - 870.
- [20] Chundururu, V., Subramanian, N., "Effects of Power Lines on Performance of Home Control System", International Conference on Power Electronics, Drives and Energy Systems Dec. 2006, pp.1 - 6.
- [23] INSTEON, [Online]. Available: <http://en.wikipedia.org/wiki/INSTEON>
- [24] INSTEON Details, [Online]. Available:



<http://www.insteon.net/pdf/insteondetails.pdf>

- [25] INSTEON Compared, [Online]. Available:  
<http://www.insteon.net/pdf/insteoncompared.pdf>
- [26] “Born of PLC-BUS technology”, [Online]. Available:  
<http://www.plcbus.com.cn/Html/news/1304.html>
- [27] “The PLCBUS bidirectional communication technology reveals - digital PLCBUS”, [Online]. Available:  
<http://www.autooo.net/EN/10806.html>
- [28] Kastner, W., Palensky, P., Rausch, T., Roesener, Ch., “A closer look on today's home and building networks”, 7th AFRICON Conference in Africa, Volume 2, 2004, pp.1239 - 1244.
- [29] “Implementing the LonTalk Protocol for Intelligent Distributed Control”, [Online]. Available:  
<http://www.stites.com/CN/lonworks/LonTalk%20Protocol%20Seminar.pdf>
- [30] Byoung-Hee Kim, Kwang-Hyun Cho, Kyoung-Sup Park, “Towards LonWorks technology and its applications to automation”, Proceedings of the 4th Korea-Russia International Symposium on Science and Technology, Volume 2, July 2000, pp.197 - 202.
- [31] Yanbin Pang, Xiangyu Wei, Youhua Wu, “The sensor network based on LONWORKS technology”, the 38th Annual Conference Proceedings of the SICE, July 1999, pp.897 - 900.
- [32] Sergey Chernishkian, “Building Smart Services for Smart Home”, Proceedings of IEEE 4th International Workshop on Networked Appliances, 2002, pp.215 - 224.
- [33] Koon-Seok Lee, Seung-Myun Baek, Yong-Tae Kim, Kyung Chang Lee, Kyoung Nam Ha, Suk Lee, “Performance Evaluation of MAC Layer of LnCP and LonWorks Protocol as Home Networking System”, SICE-ICASE International Joint Conference 2006, Oct. 18-21, 2006, pp.435 - 440.
- [34] Mianyu Wang, Erwei Lin, Edward Woertz, Moshe Kam, “Collision resolution simulation for distributed control architectures using LonWorks”, Proceedings of the 2005 IEEE International Conference on Automation Science and Engineering, August 1-2, 2005, pp.319 - 326.
- [35] Marek Mikowicz, “Access delay in LonTalk MAC protocol”, Computer Standards & Interfaces, Volume 31 Issue 3, Mar. 2009, pp.548 - 556.
- [36] Yousuf, M.S., Rizvi, S.Z., El-Shafei, M., “Power Line Communications: An

Overview - Part II”, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, April 2008, pp. 1 - 6.

- [37] HomePlug Command & Control, [Online]. Available:  
[http://www.homeplug.org/tech/homeplug\\_cc1/](http://www.homeplug.org/tech/homeplug_cc1/)
- [38] Yu-Ju Lin, Latchman, H.A., Minkyu Lee, Katar, S., “A power line communication network infrastructure for the smart home”, IEEE Wireless Communications, Volume 9, Issue 6, Dec. 2002, pp. 104 - 111.
- [39] Min Young Chung, Myoung-Hee Jung, Tae-Jin Lee, Yutae Lee, “Performance analysis of HomePlug 1.0 MAC with CSMA/CA”, IEEE Journal on Selected Areas in Communications, Volume 24, Issue 7, July 2006, pp.1411 - 1420.
- [40] Campista, M.E.M., Costa, L.H.M.K., Duarte, O.C.M.B., “Improving the Data Transmission Throughput over the Home Electrical Wiring”, 30th Anniversary. The IEEE Conference on Local Computer Networks, Nov. 2005, pp.318 - 327.
- [41] Chatschik, B., “An overview of the Bluetooth wireless technology”, IEEE Communications Magazine, Volume 39, Issue 12, Dec. 2001 pp. 86 - 94.
- [42] M. Al-Qutayri, H. Barada, S. Al-Mehairi, J. Nuaimi, “A Framework for an End-to-End Secure Wireless Smart Home System”, the 2nd Annual IEEE Systems Conference, April 2008, pp. 1 - 7.
- [43] Luis Carlos Aceves Gutiérrez, Og Jamir Ramos Juraidini, Carlos Alberto Garza Frias, “Wireless control of Bluetooth “on/off” switches in a smart home using J2ME in Mobile Phones and PDAs”, [Online]. Available:  
<http://www.luiscarlosaceves.com/wirelesscontrolofbluetoothswitchesinasmarthomeusingj2meinmobilephonesandpdas.pdf>
- [44] Matt Maupin, “ZigBee: Wireless Control Made Simple”, [Online]. Available:  
[http://www.mobiusconsulting.com/papers/MattMaupin\\_FreescaleSemiconductor.pdf](http://www.mobiusconsulting.com/papers/MattMaupin_FreescaleSemiconductor.pdf)
- [45] Yu-Ping Tsou, Jun-Wei Hsieh, Cheng-Ting Lin, Chun-Yu Chen, “Building a Remote Supervisory Control Network System for Smart Home Applications”, IEEE International Conference on Systems, Man and Cybernetics, Volume 3, Oct. 2006, pp.1826 - 1830.
- [46] Mikhail Galeev, “Home networking with Zigbee”, [Online]. Available:  
[http://www.eetindia.co.in/ARTICLES/2005JUN/B/2005JUN16\\_NETD\\_TA.pdf?SOURCE=DOWNLOAD](http://www.eetindia.co.in/ARTICLES/2005JUN/B/2005JUN16_NETD_TA.pdf?SOURCE=DOWNLOAD)
- [47] Patrick Kinney, “ZigBee Technology: Wireless Control that Simply Works”, [Online]. Available:

[http://www.zigbee.org/imwp/idms/popups/pop\\_download.asp?contentID=5162](http://www.zigbee.org/imwp/idms/popups/pop_download.asp?contentID=5162)

- [48] Byoung-Kug Kim, Sung-Kwa Hong, Young-Sik Jeong, Doo-Seop Eom, “The Study of Applying Sensor Networks to a Smart Home”, Fourth International Conference on Networked Computing and Advanced Information Management, Volume 1, Sept. 2008, pp.676 - 681.
- [49] Gonzalo Delgado Huitrón, “Reducing Home Power Consumption”, [Online]. Available: [http://www.freescale.com/files/archives/doc/support\\_info/LOW\\_POWER\\_CONSUMPTION.pdf](http://www.freescale.com/files/archives/doc/support_info/LOW_POWER_CONSUMPTION.pdf)
- [50] Shah, P., Shaikh, T., Ghan, K., Shilaskar, S., “Power Management Using ZigBee Wireless Sensor Network”, First International Conference on Emerging Trends in Engineering and Technology, July 2008, pp.242 - 245.
- [51] Surie, D., Laguionie, O., Pederson, T., “Wireless sensor networking of everyday objects in a smart home environment”, International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Dec. 2008, pp.189 - 194.
- [52] Z-Wave, [Online]. Available: <http://en.wikipedia.org/wiki/Z-Wave>
- [53] Mikhail Galeev, “Catching the Z-Wave”, [Online]. Available: [http://www.eetindia.co.in/ARTICLES/2006OCT/PDF/EEIOL\\_2006OCT01\\_EMS\\_NETD\\_RFD\\_TA.pdf?SOURCES=DOWNLOAD](http://www.eetindia.co.in/ARTICLES/2006OCT/PDF/EEIOL_2006OCT01_EMS_NETD_RFD_TA.pdf?SOURCES=DOWNLOAD)
- [54] “Z-Wave Overview presentation”, 2008, [Online]. Available: [http://www.shortrangewireless.dk/C1257306002B260C/sysOakFil/100608\\_Z-Wave%20technical%20presentation%20ver%203/\\$File/080609%20Z-Wave%20technical%20presentation%20ver%203.pdf](http://www.shortrangewireless.dk/C1257306002B260C/sysOakFil/100608_Z-Wave%20technical%20presentation%20ver%203/$File/080609%20Z-Wave%20technical%20presentation%20ver%203.pdf)
- [55] G. Ferrari, P. Medagliani, S. Di Piazza, and M. Martal’o, “Wireless Sensor Networks: Performance Analysis in Indoor Scenarios”, EURASIP Journal on Wireless Communications and Networking, Volume 2007 Issue 1, January 2007, pp.14.
- [56] Bosheng Zhou, Marshall, A., Wenzhe Zhou, Tsung-Han Lee, “Novel Wireless Mesh Networking Architectures for Future Smart Homes”, Future Generation Communication and Networking (FGCN 2007), Volume 2, Dec. 2007, pp.43 - 48.
- [57] Todd Kennedy, Ray Hunt, “A review of WPAN security: attacks and prevention”, Proceedings of the International Conference on Mobile Technology, Applications, and Systems, Sept. 2008, Article No.56.
- [58] The Network Simulator ns-2 Manual, [Online]. Available: [http://www.isi.edu/nsnam/ns/doc/ns\\_doc.pdf](http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf)

- [59] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", Springer Science+Business Media, LLC, New York, USA, 2009
- [60] The Enhanced Network Simulator(TeNs),  
[Online]. Available: <http://www.cse.iitk.ac.in/users/braman/tens>
- [61] Tzi-cker Chiueh, Ashish Raniwala, "Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network", In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, March 2005, vol.3, pp. 2223-2234.
- [62] Ramon Agüero Calvo, "Adding Multiple Interface Support in NS-2", January 2007,  
[Online]. Available:  
<http://personales.unican.es/aguerocr/files/ucMultiIfacesSupport.pdf>
- [63] Laurent Paquereau, Bjarne E. Helvik, "A module-based wireless node for NS-2", In Proceeding from the 2006 workshop on ns-2: the IP network simulator, 2006, Vol.202, Article No.4.
- [64] Laurent Paquereau,"Extensions to ns-2", October 29, 2009,  
[Online]. Available: [http://people.item.ntnu.no/~paquerea/ns/q2s\\_doc.pdf](http://people.item.ntnu.no/~paquerea/ns/q2s_doc.pdf)
- [65] Nicola Baldo, Federico Maguolo, Marco Miozzo, Michele Rossi, Michele Zorzi, "ns2-MIRACLE: a modular framework for multi-technology and cross-layer support in network simulator 2", In Proceedings of the 2nd international conference on Performance evaluation methodologies and tools, 2007, Vol.321, Article No.16.
- [66] NS-MIRACLE: Multi-InterfAce Cross-Layer Extension library for the Network Simulator, [Online]. Available:  
[http://www.dei.unipd.it/wdyn/?sez\\_alias=ricerca/signet/tools/nsmiracle](http://www.dei.unipd.it/wdyn/?sez_alias=ricerca/signet/tools/nsmiracle)
- [67] Monageng Kgwadi, "Communication Protocol for Residential Electrical Demand Response in Home Devices", Master thesis, Carleton University, July 2009
- [68] Cheng Jin and Thomas Kunz, "Design and Implementation of a Smart Home Networking Simulation", Technical Report SCE-10-08, Carleton University, August, 2010
- [69] Marina Petrova, Janne Riihijarvi, Petri Mahonen, Saverio Labella, "Performance study of IEEE 802.15.4 using measurements and simulations", In IEEE Wireless Communications and Networking Conference, April 2006, Vol.1, pp. 487-492.
- [70] Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), June 2006, [Online]. Available:  
<http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf>

- [71] Yu-Ju Lin, Latchman, H.A., Minkyu Lee, Katar, S., “A power line communication network infrastructure for the smart home”, IEEE Wireless Communications, Dec. 2002, Volume 9, Issue 6, pp. 104-111.
- [72] Min-Soo Kim, Dong-Min Son, Young-Bae Ko, Young-Hyun Kim, “A Simulation Study of the PLC-MAC Performance using Network Simulator-2”, IEEE International Symposium on Power Line Communications and Its Applications, April 2008, pp. 99-104.
- [73] ZigBee Alliance, “ZigBee Specification”, June 27, 2005, [Online]. Available: <http://www.zigbee.org/Specifications/ZigBee/download.aspx>
- [74] Runcai Huang, Yiwen Zhuang, Qiying Cao, “Simulation and Analysis of MFlood Protocol in Wireless Network”, International Symposium on Computer Science and Computational Technology, Dec. 2008, Vol.1, pp. 658-662.
- [75] J. Zheng and M. J. Lee, “A comprehensive performance study of IEEE 802.15.4”, Sensor Network Operations, IEEE Press, Wiley Interscience, 2006, Chapter 4, pp. 218-237, [Online]. Available: [http://www-ee.cuny.cuny.edu/zheng/papers/paper1\\_wpan\\_performance.pdf](http://www-ee.cuny.cuny.edu/zheng/papers/paper1_wpan_performance.pdf)
- [76] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen, Jang-Ping Sheu, “The Broadcast Storm Problem in a Mobile Ad Hoc Network”, Wireless Networks, March-May 2002, Volume 8, Issue 2/3, pp. 153-167.
- [77] Pradeep Kyasanur, Nitin H. Vaidya, “Routing and Interface Assignment in Multi-Channel Multi-Interface Wireless Networks”, IEEE Wireless Communications and Networking Conference, March 2005, Vol.4, pp. 2051-2056.
- [78] ZigBee Simulation Environment, Dimitri Marandin, [Online]. Available: <http://www.ifn.et.tu-dresden.de/~marandin/ZigBee/ZigBeeSimulationEnvironment.html>
- [79] ZigBee/IEEE 802.15.4 Module for NS2 simulator, Oct. 19, 2008, [Online]. Available: <http://www.cs.uwm.edu/~mukul/wpan.html>
- [80] Jianliang Zheng, “802.15.4 and ZigBee Routing Simulation”, 2003, [Online]. Available: [http://www-ee.cuny.cuny.edu/zheng/pub/file/WPAN\\_ZBR\\_pub.pdf](http://www-ee.cuny.cuny.edu/zheng/pub/file/WPAN_ZBR_pub.pdf)

## Appendix A Summary of NS-2 Modifications

This section presents a brief description of all files we modified and created in NS-2 v2.33 for our simulation model. To have a clear understanding of our implementation, all files involved are hierarchically categorized on the basis of functionalities and internal relationships, logically following the order laid out in the main body of thesis. In addition, it is assumed that the NS-2 package available for distribution is entirely complied by GCC v4.2.2 on the Fedora Linux v10 platform. Given the issues of backwards compatibility and the version upgrading of the GCC compiler, arbitrary migration to other Linux platforms with a lower GCC compiler version will inevitably lead to unexpected grammatical errors.

### *(1) Protocol related parameter settings*

Filename	ns-default.tcl ns-packet.tcl packet.h (/common) ns-agent.tcl
Location	/tcl/lib, /common
Description	These files existing in NS-2 were modified to define the default value of network parameters, the naming and declaration of protocol packet header as well as the default port number, covering HomePlug C&C, the Flooding protocol, and the ZigBee routing protocol.

### *(2) Construction of nodes with multiple interfaces*

Filename	ns-lib.tcl ns-mobilenode.tcl
Location	/tcl/lib
Description	The two Tool Command Language (Tcl) files existing in NS-2 were modified so as to create a node with multiple interfaces. To be specific, the initial number of interfaces, the identification of node type, the energy model related parameter binding for each interface and the configuration of network objects (Flooding and ZigBee routing) within a node are handled in ns-lib.tcl, whereas the connection of interfaces to a node and the error model object binding with each interface are addressed in ns-mobilenode.tcl.

*(3)Node addressing scheme for multiple interfaces*

Filename	ns-node.tcl (/tcl/lib) phy.cc (/mac)
Location	/tcl/lib, /mac
Description	The two files existing in NS-2 are modified to support the node addressing scheme in multiple networks. Based on the scheme, the newly created node ID (ns-node.tcl) in the OTcl space are passed as an address to the corresponding MAC object and PHY object within each interface in the C++ space while generating a node. Thus, the function of index transferring were added in the Base PHY class in phy.cc since it already exists in the base MAC class in mac.cc (such function was also added to nodes with the RBDS interface in mac-rds.cc in that the RBDS MAC object automatically generates the MAC address)

*(4)Node organization and management of multiple channels*

Filename	mobilenode.h & .cc (/common) channel.h & .cc (/mac) power_channel.h & .cc (/mac)
Location	/common, /mac
Description	A bidirectional linked list was created for nodes across multiple channels/networks in mobilenode.h & .cc and managed and manipulated by channel objects (channel.h & .cc) during data transmission. Meanwhile, static transmission related parameters originally shared by multiple channel objects were modified to support the one-to-one relationship between a channel object and a network. A power channel (power_channel.h & .cc) that was a clone from a channel only serves nodes with the HomePlug C&C interface.

*(5)MAC/PHY layer*

Network	RBDS
Filename	mac-rds.h & .cc (/mac) prop_ricean_shadowing.h & .cc (/mobile)
Location	/mac, /mobile

Description	The new files obtained from [67] were adopted here to model the data traffic featured with a combination of the Shadowing model and the Ricean/Rayleigh fading model over the RBDS network from the RBDS originator to the central controller in a smart home. Meanwhile, an interface index was created at the RBDS MAC layer (mac-rds.h & .cc) to tag incoming RBDS packets before handing them over to the upper layer.
-------------	--

Network	ZigBee/IEEE 802.15.4
Filename	p802_15_4mac.h & .cc p802_15_4phy.h & .cc wireless-phy.h & .cc (/mac)
Location	/wpan, /mac
Description	The modification of the ZigBee/IEEE 802.15.4 MAC/PHY layer existing in NS-2 referred to the implementation issued in [79], focusing on the interconnection between the ZigBee routing protocol and the ZigBee/IEEE 802.15.4 MAC/PHY layer with some adjustments intended for our project. Meanwhile, an extra flag and an interface index were created respectively at the ZigBee/IEEE 802.15.4 MAC layer (p802_15_4mac.h & .cc) to identify outgoing packets from the ZigBee routing protocol and to tag incoming packets through the ZigBee/IEEE 802.15.4 interface.

Network	HomePlug C&C
Filename	homeplugcc-phy.h & .cc (/mac) mac-homeplugcc.h & .cc (/mac) mac-homeplugcc-timers.h & .cc (/mac) propagation.h & .cc (/mobile) shadowing.h & .cc (/mobile) ns-mac.tcl (/tcl/lan) ns-mac-homeplugcc.tcl (/tcl/lan)
Location	/mac, /mobile, /tcl/lan
Description	The HomePlug C&C MAC/PHY layer (/mac, ns-mac-homeplugcc.tcl) was cloned from the IEEE 802.11 WLAN protocol in NS-2 to model the data traffic over the HomePlug C&C network. Hence, the propagation related methods were created in the propagation models (/mobile) suitable for data transmission over the HomePlug C&C network. Meanwhile, the default values of network related parameters involved were added in ns-mac.tcl for the network initialization. Also, an interface index was created at the HomePlug C&C MAC layer (homeplugcc-phy.h & .cc) to tag incoming packets through the HomePlug C&C interface.



(6) Routing Layer

Protocol	one-hop routing protocol
Filename	dumb-agent.h & .cc
Location	/mobile
Description	The modification of dumb agent referred to the implementation in [67] to support data transmission over the RBDS network. Beyond that, the protocol was adjusted to connect the corresponding network objects intended for multiple interfaces in the OTcl space prior to the node construction.

Protocol	Flooding
Filename	rdsf_packet.h rdsf_rtable.h & .cc rdsflooding.h & .cc
Location	/RdsFlood
Description	The Flooding protocol (rdsflooding.h & .cc) was created to support the flooding of reframed RBDS message over multiple networks in a smart home. The packet forwarding mechanism (rdsflooding.h & .cc) from the RBDS network to smart homes were also established within the central controller. Besides, a packet header of the protocol was defined in rdsf_packet.h, and a sequence number table was created (rdsf_rtable.h & .cc) so as to filter out incoming flooding packets with an out-of-date sequence number.

Protocol	AODV
Filename	aodv.h & .cc aodv2.cc aodv_rtable.h & .cc
Location	/aodv
Description	These files existing in NS-2 were modified to enable AODV objects to handle all types of packets over multiple networks, depending upon the mechanism of timer-driven data forwarding as well as different routing strategies added in aodv.h & .cc. Besides, aodv2.cc was a newly created file that implemented part of the dual-path routing strategy. An interface field added in the AODV routing table (aodv_rtable.h & .cc) helps to establish routes with the minimal path cost by registering the corresponding interface indexes inserted in the header of incoming packets.

Protocol	ZigBee
----------	--------

Filename	Zigbee.h & .cc Zigbee2.cc Zigbee_routing.cc Zigbee_association.cc Zigbee_packet.h Zigbee_queue.cc p802_15_4const.h ll.h & .cc (/mac)
Location	/wpan, /mac
Description	The implementation of the ZigBee routing protocol obtained from [79], along with the part of device association, packet queue and the definition of packet header for the protocol (Zigbee_association.cc, Zigbee_queue.cc, Zigbee_packet.h) was modified to enable ZigBee objects to handle all types of packets over multiple networks on the basis of the mechanism of timer-driven data forwarding as well as different routing strategies added in Zigbee.h & .cc and Zigbee_routing.cc. Besides, Zigbee2.cc was a newly created file that implemented part of the dual-path routing strategy. An interface field added in the ZigBee routing table (Zigbee.h & .cc, Zigbee_routing.cc) helps to establish routes with minimal path cost by registering the corresponding interface index inserted in the header of incoming packets. The length of packet at the PHY layer was extended in p802_15_4const.h to insert flags used for tracing the path of packets over multiple networks for the purpose of the backbone-based routing strategy. In addition, the identification of packet type coded in ll.h to tag incoming packets forwarded by various kinds of routing objects, since ZigBee directly interconnects with the ZigBee/IEEE 802.15.4 network without support of the Link Layer in NS-2.

*(7)Application/Transport Layer*

Location	/apps
Filename	title-24.h & .cc udp.cc
Description	A Title-24 specification based application class was created in title-24.h & .cc, new files obtained from [67], to generate PCT data at fixed intervals. To ensure that the central controller properly identifies RBDS packets, a RBDS flag was created to tag RBDS packets at the application layer (title-24.h & .cc) and was converted to the packet type inserted in the header of RBDS packets at the transport layer (udp.cc) prior to data transmission.

## Appendix B Simulation Configuration and Execution

This section presents a comprehensive guideline of how to set up simulation scenarios with node featured with multiple interfaces based on our implementation, mostly emphasizing the numbering of interfaces involved in multiple networks, the simulation steps essential to the scenario scripts, the configuration and placement of nodes, as well as the network related parameter settings following that.

### B.1 Basic Setting and Interface Allocation

The Tcl script file designed for our project allows a combination of multiple network simulations as shown in Table 6:

Table 6 Interface setting of Flooding/AODV/ZigBee routing for multiple networks

		RBDS MAC/PHY(0)	ZigBee/ IEEE 802.15.4(1)	HomePlug C&C(2)
Flooding	2 interfaces/channels	√	√	
	3 interfaces/channels	√	√	√
AODV	2 interfaces/channels	√	√	
	3 interfaces/channels	√	√	√
ZigBee routing	2 interfaces/channels	√	√	
	3 interfaces/channels	√	√	√

For scenarios with both two and three interfaces/channels, the settings of Flooding and AODV/ZigBee routing are identical in terms of the allocation of interfaces/channels. In this case, node 0 is identified as the RBDS sender that issues the original RBDS messages to smart homes, whereas node 1 is identified as the central controller in smart homes that is in charge of receiving incoming RBDS messages and forwarding them to destination nodes pre-configured in the network. For the moment, it is assumed that only one smart home is allowed to be configured for receiving RBDS messages from the RBDS network due to the limitation of the software implementation mechanism in our simulation model as well as the deployment of nodes in scenario scripts.

The numbering scheme of interfaces is listed below in Table 7:

Table 7 Interface numbering for different scenarios in simulations

Interface	Node Type	Interface Numbering		
		RBDS	ZigBee /IEEE 802.15.4	HomePlug C&C
2 interfaces/channels	RBDS Sender(node 0)	0		
	Central Controller(node 1)	0	1	
	Normal Nodes		0	
3 interfaces/channels	RBDS Sender(node 0)	0		
	Central Controller(node 1)	0	1	2
	Intermediate Nodes		0	1
	Normal Nodes		0	

For any node in multiple networks, the interface ID is always gradually allocated starting from 0 regardless of the simulation scenarios. To be specific, nodes with one interface to the wireless network are allocated an interface ID numbered 0, while nodes with one interface active in the backbone are allocated an interface ID numbered 1; nodes with two interfaces are allocated two interface IDs from 0 to 1; nodes with three interfaces are allocated three interface IDs from 0 to 2. Meanwhile, the numbering scheme is forced upon each node involved in networks and directly influences the configuration of interfaces and the creation of nodes, since part of the implementation associated with the interface ID has been hardcoded for our simulations. In such case, misuse of interface ID will lead to unexpected errors during simulations.

## B.2 Scenario and Location of Nodes

To generate a scenario of delivering RBDS messages to from the utility to a smart home, location setting is the first element to be considered. Generally, the RBDS sender is located at (0, 0) since it is the first node generated in multiple networks. The active scope of the remaining nodes is restricted to a square of 16m×21m as an example to mimic the flat space typical to a house, as illustrated in Figure 73:

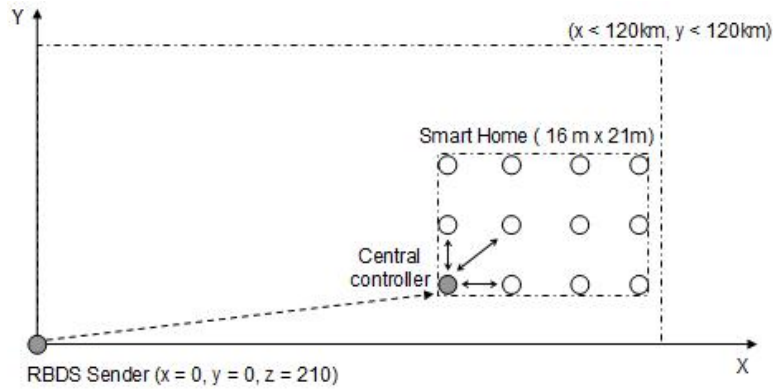


Figure 73 Scenario of RBDS message delivery in smart homes

As for the distance between the coordinate of the RBDS sender and the central controller located in a smart home, the author of the RBDS implementation demonstrated in simulation that devices up to 140 km from the transmitter are capable of receiving RBDS message 30 bytes long in size with a high reception probability of 99.5% [67]. To increase the probability of reception, RBDS messages could be transmitted multiple times (i.e. 5 times for a distance of 120km away from the transmitter).

Based on this result, we choose a distance of less than 120km to minimize the influence of RBDS message broadcasting in terms of packet loss. Meanwhile, the location of all nodes in a smart home has to be readjusted to cope with the situation. For instance, the location of nodes except the RBDS sender could be generated based on the origin of the coordinate system. Then, the X value for each node increases by 100,000 to represent the location readjustment. In this way, the smart home is always kept within the reach of RBDS message delivery.

In addition, Omni-Antenna is chosen for its ability to transmit with equal power in all directions for most wireless communications during simulations as long as the density of nodes is not intentionally restricted to a fixed location or direction. The antenna height of the RBDS message sender is set to 210m for data transmission whereas the antenna height of the central controller in a smart home is set to 1.5m in simulations [67]. Whether the antenna height of the remaining nodes in a smart home remains equal to that of the central controller is unnecessary in that there is no direct influence upon data

communication within a smart home. To simplify simulations, the height of all nodes in the house could be set to 1.5m so as to keep consistent with the central controller.

*Script sample:*

*#Coordinate of RBDS message sender*

*\$node\_(0) set X\_ 0*

*\$node\_(0) set Y\_ 0*

*\$node\_(0) set Z\_ 210*

*\$node\_(1) set X\_ 110030.0*

*\$node\_(1) set Y\_ 40.0*

*\$node\_(1) set Z\_ 1.5*

*\$node\_(2) set X\_ 110022.0*

*\$node\_(2) set Y\_ 32.0*

*\$node\_(2) set Z\_ 1.5*

### **B.3 General Steps in Simulations**

Considering the fact that scenarios in simulations deal with in multiple networks, it is necessary to arrange the order of parameter configuration and node creation to avoid problems due to any mismatch or misuse of interface ID. Therefore, the general steps for all scenarios are listed in an ordered way below:

*0. Configuration of simulation environment*

1. Parameter configuration of each layer intended for node 0 (RBDS transmitter)

*2. Creation of node 0 with one interface*

3. Parameter configuration of each layer intended for node 1 (Central Controller)

*4. Creation of node 1 with multiple interfaces*

*5. Configuration of nodes for reception of RBDS message*

6. Parameter configuration of each layer intended for intermediate nodes (if three networks involved)

*7. Creation of intermediate nodes with two interfaces*

8. Parameter configuration of each layer intended for normal nodes

9. *Creation of normal nodes with one interface*
10. *Agent setting for all nodes involved*
11. *Establishment of communication from the RBDS transmitter to the central controller.*
12. Establishment of communication from the nodes in a smart home to the central controllers (optional but not necessary)
13. Execution of simulation

It is to be noted that all steps involved have to be strictly followed in the order listed above, especially for the steps of node configuration. Any change to the order among steps could lead to unexpected errors during execution.

Those steps in italic type represent steps where special attentions should be paid in writing simulation scenarios in script files in that they are closely interconnected with the implementation specific to node configuration and communication among nodes. Therefore, all the steps involved including general settings specific to a certain layer are explained here in detail (step 10 and 11 are discussed later in Section 10.5) in order to facilitate the configuration of scenarios.

#### *1>Configuration of simulation environment*

At the beginning of the scenario script file, the number of interfaces and the number of wireless channels involved have to be initialized for current scenarios so as to be used as arguments in the configuration of node and corresponding interfaces.

*Script sample:*

```

set val(ni)          3          ;#number of interfaces
set val(nc)          2          ;#number of wireless channels

set val(chan)       Channel/WirelessChannel ;#Channel Type

# Create wireless channel
#set chan_ [new $val(chan)]
for {set i 0} {$i < $val(nc)} {incr i} {

```

```

    set chan_($i) [new $val(chan)]    ;#create a channel object for each interface
}

```

In the segment of script listed above, val(nc) is always set for RBDS and ZigBee/IEEE 802.15.4 network. For each network in the scenario, a communication channel object independent from each other has to be generated with a “for” loop to group the nodes attached to it. As for the power line channel intended for HomePlug C&C network, a brand-new channel object is created since it is cloned from Channel/WirelessChannel (detailed in HomePlug C&C in Section 6.4).

*Script sample:*

```

# Power line Channel Type
set val(pwrchan)    Channel/PowerChannel

```

*# Create power line channel*

```

set pwr_chan_ [new $val(pwrchan)]

```

In NS-2 simulations, a General Operations Director (GOD) instance is generated to store connectivity information (i.e. hop counts) of the topology by creating a matrix with the total number of wireless nodes passed as arguments. Thus, the initialization of GOD has to be updated in our project to ensure the memory management appropriate to nodes with multiple interfaces.

*Script sample:*

```

set val(mn)    14    ;# number of mobilenodes in the whole network

```

*# Create God*

```

set god_ [create-god [expr $val(mn)*$val(ni)]]

```

*2>Creation of node 0 with one interface*

Given the restriction in our implementation, node 0 is chosen to be the RBDS sender and node 1 is hardcoded to be the central controller installed in a smart home for the purpose of simplicity in the indexing of the remaining nodes.



After generation, the NS-2 simulator object enables nodes to initialize their parameters during node configuration. In this way, the number of interfaces has to be passed through for later modification when adding interface to nodes.

*Script sample:*

```
#configure and create node_(0) with DumbAgent routing in RDS network
$ns_ node-config -adhocRouting $rp_(0) \      ;#routing protocol /Dumb Agent
    -propType $prop_(0) \                    ;#propagation model
    -topoInstance $topo \                    ;#topology
    -agentTrace ON \                          ;#trace log at application layer
    -routerTrace OFF
    -macTrace OFF \
    -movementTrace OFF \
    -channel $chan_(0) \
    -ifNum $val(ni) ;#initialize the number of interfaces before the creation of node
```

Following that, the ns simulator resets the simulation environment for node 0 by changing the interface number to 1 since node 0 is only connected to the RBDS network. Meanwhile, the routing protocol is set to Dumb Agent intended for one-hop routing from node 0 to the smart home. Then, parameters of the node interface including the type of Link Layer (LL), the type of MAC layer, the queue type of the LL interface queue, the length of the queue, the type of antenna, the type of propagation model as well as a channel instance is passed through before the creation of node 0. Among them, the propagation model will be generated as an instance in order to be attached to the corresponding PHY layer in that each PHY layer of nodes with multiple interfaces holds a propagation model connected to it for private use in simulations.

*Script sample:*

```
#Add one interface for node_(0) in RDS network
$ns_ change-numifs 1
$ns_ add-ifs 0 $ll_(0) $mac_(0) $ifq_(0) $ifqlen_(0) $ant_(0) $prop_(0) $netif_(0) $chan_(0)
```

```
set node_(0) [$ns_ node 0] ;#specify the ID of node as 0
$node_(0) random-motion 0 ;#disable random motion
```

### 3>Creation of node 1 with multiple interfaces

Similar to node 0, the routing protocol is set to Flooding, AODV or ZigBee routing for node 1 (the central controller) within the smart home. Subsequently, the setting of interfaces has to be reset to 3 since node 1 holds three interfaces to the RBDS, ZigBee/IEEE 802.15.4 and HomePlug C&C network respectively (for scenarios with two networks, node 1 could be configured to connect both the RBDS and ZigBee/IEEE 802.15.4 network). As with node 0, three interfaces with corresponding parameters are added to node 1 before the node is created. In such way, node 1 is capable of handling packet transfer among the three types of network. In addition, there is no need to repeatedly add another interface 0 to node 1 since it has already been set previously for RBDS network (already coded in our implementation). Any kind of duplicate addition could lead to exceptions during simulations.

*Script sample:*

```
#configure routing protocol for nodes in a smart home
$ns_ node-config -adhocRouting $rp_(1) ;#AODV/ZigBee routing

$ns_ controller-config 1 ;#flag reserved for ZigBee routing:the central controller

#Create node_(1) that is connected to RBDS, 802.15.4 and HomePlugCC network
$ns_ change-numifs 3
#RBDS interface 0 already configured last time
#$ns_ add-ifs 0 $ll_(0) $mac_(0) $ifq_(0) $ifqlen_(0) $ant_(0) $prop_(0) $netif_(0) $chan_(0)
$ns_ add-ifs 1 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
$ns_ add-ifs 2 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_

set node_(1) [$ns_ node 1] ;#specify the ID of node as 1
$node_(1) random-motion 0 ;# disable random motion
```

### 4>Configuration of nodes for the reception of RBDS message

After generation, the controller type of node 1 has to be enabled for later execution. Meanwhile, it is mandatory to confirm how many nodes could be configured to receive incoming RBDS messages and which nodes are enabled to handle those messages. In our implementation, the central controller is capable of sending messages to the remaining nodes in the smart home or only a couple of nodes randomly chosen from the node set.

*Script sample:*

```
#exclude the first two nodes (node 0 and node 1) from the configuration set
set node_n [expr $val(mn)-2]
$node_(1) NodeType controller enabled ;#node 1 is set to be the controller
$node_(1) NodeCtrl node_num $node_n ;#initialization of the number of nodes in a house
```

*#all managed nodes are disabled by default and enable them all*

```
for {set k 2} {$k < $val(mn)} {incr k} {
$node_(1) NodeCtrl rds_pkt enabled $k
}
```

*OR*

*#node could be configured individually to receive RBDS messages*

```
$node_(1) NodeCtrl rds_pkt enabled 4 ;#node 4 is set to receive RBDS messages
$node_(1) NodeCtrl rds_pkt enabled 6 ;#node 6 is set to receive RBDS messages
```

### *5>Creation of intermediate nodes with two interfaces*

For the remaining nodes in the house, the central controller flag has to be disabled, since only one controller exists among them. Besides, interface 0 is updated to the parameters of the ZigBee/IEEE 802.15.4 network and interface 1 is reset to be configured with the parameters of the HomePlug C&C network.

In addition, the number of nodes could be randomly chosen from the node set as long as it is less than the maximal number of nodes configured in simulations. There is no restriction of how many nodes in the node set could be configured as intermediate nodes, depending on the total number of nodes in the simulations. In other words, any configuration only reflects the demand of scenarios specific to this simulation.

*Script sample:*

*#disable the flag for central controller after the creation of central controller*

```
$ns_ controller-config 0
```

*#Create intermediate nodes with both ZigBee/IEEE 802.15.4 and power line homplugC&C interfaces*

```
$ns_ change-numifs 2
```

```
$ns_ add-ifs 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
```

```
$ns_ add-ifs 1 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_
```

```
set node_(2) [$ns_ node 2] ;#specify the ID of node as 2
```

```
$node_(2) random-motion 0 ;#disable random motion
```

```
set node_(6) [$ns_ node 6] ;#specify the ID of node as 6
```

```
$node_(6) random-motion 0 ;#disable random motion
```

*... ..*

As for smart home appliances that are plugged onto the power line for data transmission, intermediate nodes could be tailored to the requirement with only the HomePlug C&C interface active in use.

*Script sample:*

*#Create intermediate nodes with only the homplugC&C interface active*

```
$ns_ change-numifs 2
```

```
$ns_ add-ifs 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
```

```
$ns_ add-ifs 1 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_
```

```
set node_(7) [$ns_ node 7] ;#specify the ID of node as 7
```

```
$node_(7) random-motion 0 ;#disable random motion
```

*#deactivate the interface to the ZigBee/IEEE 802.15.4 network (on/off)*

```
$node_(7) NodeType ZigIface off
```

*6>Creation of normal nodes with one interface to the ZigBee/IEEE 802.15.4 network*

For normal nodes in a smart home, only one interface is configured and connected to

them afterwards. Since interface 0 has already been configured with parameters for the ZigBee/IEEE 802.15.4 network, it is unnecessary to add a duplicate interface to these nodes for the same reason as node 1.

```
#Create normal nodes attached to ZigBee/IEEE 802.15.4 network
$ns_ change-numifs 1
#ZigBee/IEEE 802.15.4 interface 0 already configured last time
#$ns_ add-ifs 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)

set node_(5) [$ns_ node 5] ;#specify the ID of node as 5
$node_(5) random-motion 0 ;#disable random motion

set node_(11) [$ns_ node 11] ;#specify the ID of node as 11
$node_(11) random-motion 0 ;#disable random motion
... ..
```

#### *7>Parameters resetting with duplicate propagation models involved*

The Two-Ray Ground Model is a slightly improved version of the Free-Space model in that it considers both the direct line-of-sight connection and a ground reflection. The Two-Ray Ground model could present results more accurate than the Free-Space Model if the distance between the transmitter and the receiver is long. As compared to the Free-Space model, the Two-Ray Ground Model is more suitable for most short-distance wireless communications. The Shadowing model emphasizes fading effects for signals due to multipath diffusion in the case of wireless communications at a considerable distance. As a matter of fact, both the Two-Ray Ground model and the Shadowing model could be adopted in the situation of smart homes with a limited distance in between.

In the NS-2 environment, the parameters of the propagation model could be assigned statically through the simulation script and then be passed through the NS-2 simulator object to the corresponding model object in C++ space.

*Script sample:*

```
Propagation/Shadowing set pathlossExp_ 1.7
```

```
Propagation/Shadowing set std_db_ 7.0
Propagation/Shadowing set dist0_ 1.0
Propagation/Shadowing set seed_ 0
```

However, the central controller and the intermediate nodes may experience a situation where duplicate models for the ZigBee/IEEE 802.15.4 network and the HomePlug C&C network involved in both networks share the same propagation model with slightly different parameter values. Besides, the NS-2 execution environment provides no support for the duplicate assignment of one model. In this case, the first static assignment is replaced by the second static assignment of the same model before nodes are generated. To avoid such a problem, each instance of the propagation model corresponding to the interface attached to nodes has to be obtained from the NS-2 simulator object so as to reset the values for all nodes simulating the smart house.

*Script sample:*

```
#parameter resetting of propagation model for ZigBee/IEEE 802.15.4 network
```

```
if { $prop_(1) == "Propagation/Shadowing" } {
    set zig_prop_inst [$ns_ set propInstance_(0)]
```

```
    $zig_prop_inst set pathlossExp_ 1.7
```

```
    $zig_prop_inst set std_db_ 7.0
```

```
    $zig_prop_inst set dist0_ 1.0
```

```
    $zig_prop_inst set seed_ 0
```

```
}
```

```
#parameter resetting of propagation model for HomePlug C&C network
```

```
if { $prop_(2) == "Propagation/Shadowing" } {
```

```
    set hmplg_prop_inst [$ns_ set propInstance_(1)]
```

```
    $hmplg_prop_inst set pathlossExp_ 2.0
```

```
    $hmplg_prop_inst set std_db_ 4.0
```

```
    $hmplg_prop_inst set dist0_ 1.0
```

```
    $hmplg_prop_inst set seed_ 0
```

```
}
```

### *8>Energy model setting for nodes in smart homes*

In most cases, sensor-enabled nodes with limited energy in a smart home are mostly battery powered. Thus, it is reasonable to explore the dynamics of energy dissipation for these nodes in simulations. In the NS-2 environment, an energy model (only one generic model defined in NS-2) used to update energy consumption of a node and an initial value of energy are declared and connected to nodes through node configuration and subsequent generation.

*Script sample:*

*#Energy model type and initialization of energy value*

```
set val(energymodel)    EnergyModel           ;# Energy Model Type
```

```
set val(initialenergy)  100                   ;# initial value
```

*#set energy parameters when configuring the controller*

```
$ns_ node-config -adhocRouting $rp_(1) \  
                -energyModel $val(energymodel) \  
                -initialEnergy $val(initialenergy)
```

Considering the fact that energy consumption is only calculated by the PHY layer object, the assignment of transmission and reception power has to be done to each interface targeted for the specific PHY layer in a node with multiple interfaces.

*Script sample:*

*#set the power of transmission and reception for the controller to each interface*

```
$node_(1) setPhyPt 0  30.32e-3                ;#value is randomly chosen for generic tests
```

```
$node_(1) setPhyPr 0  34.18e-3
```

```
$node_(1) setPhyPt 1  31.32e-3
```

```
$node_(1) setPhyPr 1  35.28e-3
```

```
$node_(1) setPhyPt 2  30.32e-3
```

```
$node_(1) setPhyPr 2  34.18e-3
```

*#set the power of transmission and reception for intermediate nodes to each interface*

```
$node_(2) setPhyPt 0 31.32e-3
```

```
$node_(2) setPhyPr 0 35.28e-3
```

```
$node_(2) setPhyPt 1 30.32e-3
```

```
$node_(2) setPhyPr 1 34.18e-3
```

*#set the power of transmission and reception for normal nodes to its interface*

```
$node_(5) setPhyPt 0 31.32e-3
```

```
$node_(5) setPhyPr 0 35.28e-3
```

### *9>Error model setting for nodes in smart homes*

To support the reliability-based routing in simulations, each node in a smart home is equipped with error models, depending upon the amount of interface attached to the node. In our implementation, the unit of error is identified as packet, while the random variable used for generating packet errors is uniformly distributed from 0 to 1. Meanwhile, the packet error rate of the error model could be adjusted accordingly to cope with various scenarios. Additionally, it is assumed that each error object generated by a single procedure should be added to the target node through an interface-oriented command prior to the node construction, as exemplified as follows:

*Script sample:*

```
proc UniformErr1 {} {                                };# procedure for generating error model  
set err [new ErrorModel]                        };# error object  
$err set rate_ 0.05                               };# the packet error rate of 5 percent  
$err unit pkt                                     };# the unit of error (packet, byte and bit)  
$err ranvar [new RandomVariable/Uniform] ;# random variable uniformly distributed from 0 to 1  
$err drop-target [new Agent/Null]  
return $err  
}
```

```
proc UniformErr2 {} {  
set err [new ErrorModel]  
$err set rate_ 0.01
```



```

$err unit pkt
$err ranvar [new RandomVariable/Uniform]
$err drop-target [new Agent/Null]
return $err
}

```

```

#Create nodes with both ZigBee/IEEE 802.15.4 and HomePlug C&C interfaces
$ns_ change-numifs 2 ;# mobile node equipped with two interfaces
$ns_ add-ifs-err 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
UniformErr1 ;# bind an error object with the corresponding interface
$ns_ add-ifs-err 1 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_
UniformErr2

```

### *10>General setting of the queue model in simulations*

The Queue Model specifies the queuing mechanism in NS-2 simulations, where packets are pushed to or removed from the queue when they are ready for transmission.

As a common queue type mostly used in simulations, Drop-Tail implements the First-In-First-Out (FIFO) queuing mechanism where packets entering the queue will be handled first. Meanwhile, the last packet entering the queue will be discarded once the queue reaches its limit pre-defined in the scenario script file. In addition, the queue length has no noticeable impact upon the network performance and only depends on the efficient utilization of network resources available during executions. Thus, there is no technical restriction of how long in size it can be set in simulations.

*Script sample:*

```

set ifq_(1) Queue/DropTail/PriQueue ;# interface queue type
set ifqlen_(1) 50 ;# max packet in ifq

```

### *11>Setting of power parameters for PHY layer*

Transmission Power (*Pt\_*) is defined as the power with which the signal is transmitted. ZigBee/IEEE 802.15.4-based devices could operate at a transmit power of 0dBm (1mW) regulated by the ZigBee/IEEE 802.15.4 specification [70]. Thus, *Pt\_* could be set to

0dBm (1mW) given an ideal case in simulations.

Reception Power Threshold (RXThresh\_) identifies the least power level of packets to be detected successfully in data transmission. The packets are dropped if the received signal power is lower than the current threshold pre-defined for nodes.

Carrier Sense Threshold (CSThresh\_) specifies the sensing range of nodes in simulations. Data transmission can be sensed as long as the received signal strength is higher than the current threshold. Besides, a successful detection of packets depends on whether the nodes are capable of sensing a range at least equal to RXThresh\_ in terms of threshold.

Given the energy model specified in nodes, Transmit Power (txPower), Receive Power (rxPower) and Idle Power (idlePower) are correspondingly assigned to each PHY layer of nodes for the purpose of calculating energy consumption in different transmission states.

txPower identifies the power consumed when transmitting a data packet; rxPower identifies the power consumed by nodes to receive a data packet; idlePower identifies the power consumed by the node during the idle/sleep mode. It is to be noted that the ZigBee/IEEE 802.15.4-based devices are normally designed to operate in idle/sleep mode most of the time and are woken up to handle packets occasionally in realistic environment. Thus, it is optional for nodes to be configured with such mode in simulations, depending upon the requirements specific to the simulation scenarios.

*Script sample for the central contrller:*

```
$node_(1) setPhyPt 0 30.32e-3
```

```
$node_(1) setPhyPr 0 34.18e-3
```

```
$node_(1) setPhyPt 1 31.32e-3
```

```
$node_(1) setPhyPr 1 35.28e-3
```

```
$node_(1) setPhyPt 2 30.32e-3
```

```
$node_(1) setPhyPr 2 34.18e-3
```

These parameters at the PHY layer mentioned above are determined by the capabilities of realistic devices including the signal power of transceiver, electric current and voltage supported by devices, etc. Hence, these parameters are supposed to be configured on the basis of realistic environments with devices available for on-site experiments. In the normal case, the script segments of the RBDS network in [67], the ZigBee/IEEE 802.15.4 network with ZigBee routing in [79] as well as the examples of the ZigBee/IEEE 802.15.4 network with AODV routing included at /ns2-allinone-2.33/NS-2.33/ex/wpan could be combined to represent generic simulation scenarios.

## B.4 Parameter Configuration for Different Networks

### B.4.1 RBDS

A script in generic simulations mostly contains parameter configurations for a specific network, including settings of the routing protocol layer, LL, MAC/PHY layer, the queue type for LL/MAC and the maximal length of the queue involved in buffering outgoing packets, an antenna model as well as a propagation model adopted for nodes. In the RBDS network, the emphasis is placed on the parameter settings of the MAC/PHY layer and the propagation model intended for issues of burst errors due to large scale fading since it addresses the data communication at a considerable distance. The section on the RBDS network configuration refers to the annotation explained by the author in Chapter 5 and Appendix C in [67] and the configuration of parameters at the PHY layer is summarized in Table 8. There is no special requirement in terms of smart home networking simulations since our major focus is placed inside the house.

Table 8 PHY layer parameters based after calibration [67]

Transmitter Power	27kW
Transmitter Height	210m
Receiver Height	1.5m
Receiver Sensitivity (Threshold)	-103dBm (-133dB); RSSI = 0
Path-loss Exponent	3.50
Shadowing Deviation	12
Ricean K Value	0.0
Ricean max Velocity	120 km/h

*Script sample:*

```
set rp_(0)      DumbAgent      ;# routing protocol for one-hop routing
set ll_(0)      LL              ;# link layer type
```

*# interface queue type (unnecessary for RBDS, leave empty)*

```
set ifq_(0)     Queue/DropTail/PriQueue
set ifqlen_(0)  50              ;# max packet in ifq
```

```
set mac_(0)     Mac/RDS        ;# MAC type
```

*# set the bandwidth for the MAC*

```
Mac/RDS set bandwidth_ 1187.5 ;# RBDS bitrate
Mac/RDS set mode_ 1          ;# mode for RBDS 0= Normal Mode ; 1 = Real-Time mode
Mac/RDS set NTX_repeat_ 5    ;# Number of times a message is repeated
Mac/RDS set DTX_new_ 10
```

```
set netif_(0)   Phy/WirelessPhy ;# network interface type
```

*# set the carrier frequency*

```
Phy/WirelessPhy set freq_ 89.9e+6
```

*#The power levels of the transmitters and receivers*

*# transmit power*

```
Phy/WirelessPhy set Pt_ 27.00e3
```

*# Receive sensitivity.*

```
Phy/WirelessPhy set RXThresh_ 5.011872336e-14
```

```
Phy/WirelessPhy set CStresh_ 5.011872336e-14
```

```
set ant_(0)     Antenna/OmniAntenna ;# antenna model
```

*# Rayleigh and Ricean with Shadowing as the large scale fading (Propagation model for wireless channel)*

```
set prop_(0)    Propagation/RiceanShadowing
```

*# Parameters that characterize the large scale fading*

```

Propagation/RiceanShadowing set pathlossExp_ 3.5
Propagation/RiceanShadowing set std_db_ 12
Propagation/RiceanShadowing set dist0_ 45.125
Propagation/RiceanShadowing set seed_ [expr {int(rand()*64)}] ; # seed for the power deviation
random var
; # to obtain identical simulation fix this to a number between 0 and 63
; # (which indexes one of the 64 pre-defined seeds in NS-2 ) / uncomment the line below
# Propagation/RiceanShadowing set seed_ 0

if { $opt(seed) > 0 } {
    puts "Seeding Random number generator with $opt(seed)\n"
    ns-random $opt(seed)
}

set val(RiceanK)      0.0    ;# Ricean K factor
set val(RiceanMaxVel) 120    ;# Ricean Propagation MaxVelocity Parameter

# number of Nodes in the RBDS network (Node 0 is the base station)
set val(nn) 2

# Ricean Propagation: Maximum ID of nodes (Total number of nodes) used to
# compute pairwise table offsets.
set val(RiceMaxNodeID) [expr {$val(nn)-1}]
set val(RiceDataFile)  rice_table.txt           ;# Ricean Propagation Data File

# propagation settings after the node is generated
if { $prop_(0) == "Propagation/RiceanShadowing" } {
    set prop_inst [$ns_ set propInstance_(0)]

    $prop_inst MaxVelocity $val(RiceanMaxVel);
    $prop_inst RiceanK      $val(RiceanK);
    $prop_inst LoadRiceFile $val(RiceDataFile);
    $prop_inst RiceMaxNodeID $val(RiceMaxNodeID);
}

```

## B.4.2 ZigBee/IEEE 802.15.4

The parameter configuration of ZigBee/IEEE 802.15.4 for AODV routing refers to the examples provided by the authors of the ZigBee/IEEE 802.15.4 MAC/PHY layer implementation in /ns2-allinone-2.33/NS-2.33/ex/wpan. There are no special parameters to be adjusted in terms of generic tests in smart home networking scenarios.

*Script sample for AODV routing:*

```
set prop_(1)      Propagation/TwoRayGround    ;# radio-propagation model
set netif_(1)     Phy/WirelessPhy/802_15_4    ;# PHY type
set mac_(1)       Mac/802_15_4              ;#MAC type
set ifq_(1)       Queue/DropTail/PriQueue    ;# interface queue type
set ifqlen_(1)    50                        ;# max packet in ifq
set ll_(1)        LL                        ;# link layer type
set ant_(1)       Antenna/OmniAntenna       ;# antenna model
set rp_(1)        AODV                      ;# AODV routing protocol
```

*Mac/802\_15\_4 wpanCmd verbose on*

*# For model 'TwoRayGround'*

```
set dist(12m) 1.33527e-06
```

```
Phy/WirelessPhy/802_15_4 set CStresh_ $dist(12m)
```

```
Phy/WirelessPhy/802_15_4 set RXThresh_ $dist(12m)
```

*#change back to default value*

```
Phy/WirelessPhy/802_15_4 set Pt_ 0.28183815
```

```
Phy/WirelessPhy/802_15_4 set freq_ 914e+6
```

The parameter configuration of ZigBee/IEEE 802.15.4 for ZigBee routing refers to the script provided by the author of the ZigBee routing implementation in [79]. In this script, the author adopted the shadowing model instead of the two-way ground model in the simulation. Meanwhile, the values of the path loss exponent and power deviation employed in the shadowing model are obtained empirically by field measurements rather

than equation calculation. Due to the lack of support of on-site experiments based on such model, it is reasonable to directly use the parameters of propagation model and PHY layer presented by the author for generic tests in smart homes.

*Script sample for ZigBee routing:*

```

set prop_(1)          Propagation/Shadowing          ;# radio-propagation model
set netif_(1)         Phy/WirelessPhy/802_15_4       ;#PHY type
set mac_(1)           Mac/802_15_4                 ;#MAC type
set ifq_(1)           Queue/DropTail/PriQueue       ;# interface queue type
set ifqlen_(1)        50                           ;#max packet in ifq
set ll_(1)            LL                            ;#link layer type
set ant_(1)           Antenna/OmniAntenna          ;#antenna model
set rp_(1)            Zigbee                         ;#ZigBee routing protocol

```

```

Agent/Zigbee set drop_front_1                       ;#ZigBee adopts DropHead when the queue is full
Queue/DropTail/PriQueue set drop_front_true        ;#follows DropHead at the backbone interface

```

```

Propagation/Shadowing set pathlossExp_ 1.7
Propagation/Shadowing set std_db_ 7.0
Propagation/Shadowing set dist0_ 1.0
Propagation/Shadowing set seed_ 0

```

```

Phy/WirelessPhy/802_15_4 set CStresh_ 1.0e-12
Phy/WirelessPhy/802_15_4 set RXThresh_ 1.0e-12
Phy/WirelessPhy/802_15_4 set Pt_ 0.01
Phy/WirelessPhy/802_15_4 set freq_ 2.4e+9          ;#operates in the 2.4 GHz band

```

In the setting of a ZigBee/IEEE 802.15.4 network, node type configuration is closely tied to device association and beacon transmission [80]. As explained in the section on ZigBee/IEEE 802.15.4 networks in Chapter 6, device association emphasizes the formation of a cluster tree over the underlying communication link while beacon transmission or beacon-enabled transmission may result in higher overhead and delay in networks. Therefore, node type configuration for AODV routing is optional and flexible (no fundamental influence in terms of data transmission in simulations, depending on the

location of nodes and the corresponding transmission and reception power).

As compared to AODV routing, the author of ZigBee routing forced all devices to be connected into the network by locating any sub-root around it before data transmission (the central controller called coordinator is configured to be the root of the cluster tree). Any type of failure to associate with the network will lead to inaccessibility of the destination node and in turn impact the whole network traffic. To be fair to both routing approaches in terms of metric comparison, node type configuration should also be enabled for AODV routing. Taking the time spent on device association into account, it is reasonable to enable data transmission to be executed after all devices have successfully connected to the network through association.

*Script sample of the setting of node type for AODV routing:*

```
$ns_ at 0.0 "$node_(1) NodeLabel PAN Coord"  
$ns_ at 0.0 "$node_(1) sscs startPANCoord 1" ;# startPANCoord <txBeacon=1>  
<BO=3> <SO=3>  
$ns_ at 0.5 "$node_(2) sscs startDevice 1 1 1" ;# startDevice <isFFD=1>  
<assoPermit=1> <txBeacon=0> <BO=3> <SO=3>  
... ..  
$ns_ at 5.5 "$node_(7) sscs startDevice 0"  
... ..
```

*Script sample of the setting of node type for ZigBee routing:*

```
# startPANCoord <txBeacon=1> <BO=3> <SO=3>  
$ns_ at 0.0 "$node_(1) sscs startPANCoord 0 15" ;#in non-beacon mode  
  
set start_time_(2) 108.860000  
$ns_ at 1.0 $start_time_(2) "$node_(2) sscs startDevice 1 1 0 15"  
... ..
```

Normally, the group of parameters associated with ZigBee routing should be kept unchanged for proper execution in simulations.



First of all, buffLimit, buffer\_pool, and drop\_front\_ are related to the data and command buffer for data forwarding in ZigBee routing, while nwkMaxDepth represents the maximal addressing depth for data routing.

Secondly, nwkMaxRouters, nwkMaxChildren, pkt\_consume\_delay are used for device association in that it is mandatory for a ZigBee device to be connected in the ZigBee network (cluster tree structure) before data transmission.

Hence, there is no need to make any adjustment to the parameters mentioned above by default for generic tests in smart home networking simulations.

*Script sample intended for ZigBee routing:*

*#limitation of data and command packet buffer in transmission, -1 means no limit*

*\$ns\_ at 0.0 "\$node\_(1) sscs buffLimit -1"*

*#the size of buffer pool*

*\$ns\_ at 0.0 "\$node\_(1) sscs buffer\_pool 2500000"*

*#drop the front packets when data or command buffer is full*

*Agent/Zigbee set drop\_front\_ 1*

*#setting of maximal depth for routing in terms of radius*

*\$ns\_ at 0.0 "\$node\_(1) sscs nwkMaxDepth 20"*

*#setting for device association*

*#the maximal number of routers that can associate with this device*

*\$ns\_ at 0.0 "\$node\_(1) sscs nwkMaxRouters 200";\$ns\_ at 0.0 "*

*#the max number of children that can associate with this device*

*\$node\_(1) sscs nwkMaxChildren 200"*

*#packet delay for the reception of association request/response during device association*

*\$ns\_ at 0.0 "\$node\_(1) sscs pkt\_consume\_delay 1"*

The current implementation of ZigBee routing partially supports tree routing in the sense that all packets are first forwarded to the root of the network tree before reaching the next hop. Considering that there is no use in our project for this type of routing, `nwkUseTreeRouting` is set to 0 in the script file.

```
#flag of tree routing in ZigBee/IEEE 802.15.4 network
$ns_ at 0.0 "$node_(1) sscs nwkUseTreeRouting 0"
```

In order to keep backwards compatibility with the existing implementation of the ZigBee/IEEE 802.15.4 MAC/PHY layer in NS-2, a flag `ZigBeeRouting` is defined in our project to enable ZigBee routing when this type of routing is employed in simulations in case any unexpected collision with AODV routing occurs during execution. For AODV routing, the flag should be disabled by default.

```
#back compatibility with existing implementation in NS-2
Mac/802_15_4 wpanCmd ZigbeeRouting on ;# on/off for ZigBee routing
```

To configure a Flooding protocol in a smart home, the protocol name previously specified in simulations is replaced with “RdsFlooding” defined in our implementation except for the setting of underlying networks identical to that of AODV/ZigBee routing. Meanwhile, all other attributes associated with AODV/ZigBee routing must be removed in advance or commented out with “#” in the scenario scripts before the creation of nodes, since the Flooding protocol deployed in simulations is independent from AODV/ZigBee routing.

*Script sample for Flooding protocol:*

```
set prop_(1) Propagation/TwoRayGround ;# radio-propagation model
set netif_(1) Phy/WirelessPhy/802_15_4 ;# PHY type
set mac_(1) Mac/802_15_4 ;#MAC type
set ifq_(1) Queue/DropTail/PriQueue ;# interface queue type
set ifqlen_(1) 50 ;# max packet in ifq
set ll_(1) LL ;# link layer type
set ant_(1) Antenna/OmniAntenna ;# antenna model
```

```

set rp_(1)          RdsFlooding          ;# Flooding protocol
set val(mn)         22                   ;# number of mobile nodes in the whole network

$node_(1) NodeType controller enabled

#set node_n [expr $val(mn)-2]
#$node_(1) NodeCtrl node_num $node_n    ;#reserved for AODV/ZigBee routing

#for {set k 2} {$k < $val(mn)} {incr k} { ;#reserved for AODV/ZigBee routing
#$node_(1) NodeCtrl rds_pkt enabled $k
#}

#Mac/802_15_4 wpanCmd ZigbeeRouting on    ;#flag reserved for ZigBee routing
# $ns_ controller-config 1                ;#reserved for ZigBee routing: the central controller
# $ns_ controller-config 0                ;#reserved for ZigBee routing: the remaining nodes

```

### B.4.3 HomePlug C&C

Considering that the HomePlug C&C protocol stacks is a clone of the IEEE 802.11 wireless LAN MAC/PHY stack included in NS-2 v2.33, all parameters involved could flexibly be configured based on examples available for IEEE 802.11 in /ns2-allinone-2.33/NS-2.33/ex since IEEE 802.11 is wildly used in most simulations associated with wireless short-range communications. Specifically, the data rate of the cloned implementation is reduced to 25Kbps, which is significantly lower than that of ZigBee/IEEE 802.15.4 (250Kbps at 2.4 GHz), so as to represent an approximation to data transmission at a speed of 7.5 Kbps in the HomePlug C&C network. Further reductions of the data rate, as discussed earlier, are not possible, due to the limitation of NS-2 simulation environment as well as the complexity of event scheduling in the cloned implementation.

*Script sample:*

```

#Define options for HomePlugC&C PHY/MAC layers
set val(pwrchan)    Channel/PowerChannel ;# Power line Channel Type
set prop_(2)       Propagation/Shadowing ;# radio-propagation model

```

```

set netif_(2)          Phy/HomePlugCCPhy          ;# PHY type
set mac_(2)           Mac/HomePlugCC             ;#MAC type
set ifq_(2)           Queue/DropTail/PriQueue     ;# interface queue type
set ifqlen_(2)       50                          ;# max packet in ifq
set ll_(2)            LL                          ;# link layer type
set ant_(2)           Antenna/OmniAntenna         ;# antenna model

Mac/HomePlugCC set basicRate_ 25Kb ;# set this to 0 if want to use bandwidth
Mac/HomePlugCC set dataRate_ 25Kb ;# both control and data packets
Mac/HomeplugCC set PLCPDataRate_ 25000 ;# 25Kbps at the PHY Layer (PLCP)
Mac/HomeplugCC set bandwidth_ 25000 ;#unused if basicRate and dataRate are preconfigured

```

## B.5 Configuration for Data Traffic among Networks

In most cases, two types of data communications are involved in our project: short RBDS messages issued by the RBDS sender to the central controller, which forwards the reframed messages to nodes preconfigured, and packets of short size transmitted from nodes in a house to the central controller. Hence, data transmissions based on UDP is used in simulations. Besides, the port numbered 0 is used by all nodes for RBDS message transmission since it is hardcoded in our implementation. Consequently, data transmission in our networks could use any port number starting from 1. In this case, the communication of RBDS messages among nodes has to be configured in the first place so as to occupy the port number 0.

RBDS message transmission refers to the annotation explained in the application layer part of Appendix C in [67]. An application of Title-24 based on UDP transport layer is connected to the RBDS sender. The rest of the nodes including the central controller are configured as sink nodes for the reception of RBDS messages. Meanwhile, the RBDS communication link is only established between the RBDS sender and the central controller since nodes in a house receive the RBDS messages only through the central controller.

*Script sample:*

```

#Create a UDP agent and attach it to node 0
set RDSudp [new Agent/UDP]
$ns_ attach-agent $node_(0) $RDSudp
$RDSudp set dst_addr_ 0

#Create a Title-24 application here
set tt24 [new Application/Title-24]
$tt24 set interval_ 100.0 ;#value is randomly chosen for generic tests
$tt24 set size_ 30
$tt24 attach-agent $RDSudp

#Create sink node for reception of RBDS messages
for {set j 1} {$j < $val(mn)} {incr j} {
    set RDSnull_($j) [new Agent/Null]
    $ns_ attach-agent $node_($j) $RDSnull_($j)
}

#Connect the RBDS sender and the central controller
$ns_ connect $RDSudp $RDSnull_(1)

;#RBDS message transfer is set to the right time after all devices have connected to the network in
smart homes, depending on the time of device association..

$ns_ at 700.0 "$tt24 start"

```

As with data transmission based on the UDP layer in most simulations, packets are generated by a CBR traffic generator from intermediate nodes or normal nodes to the central controller. There are no special requirements for generic tests except that the size of the data packet and the interval of transmission should remain reasonable to smart home networking simulations.

*Script sample:*

```

proc cbrtraffic { interval src dst stime } {
    global ns_ node_
    set udp_($src) [new Agent/UDP]

```

```

eval $ns_ attach-agent \Node_($src) \Sudp_($src)
set null_($dst) [new Agent/Null]
eval $ns_ attach-agent \Node_($dst) \Snull_($dst)
set cbr_($src) [new Application/Traffic/CBR]
eval \Scbr_($src) set packetSize_ 70 ; # 70 bytes in size
eval \Scbr_($src) set interval_ $interval ;#100 seconds
eval \Scbr_($src) set random_ 1
eval \Scbr_($src) attach-agent \Sudp_($src)
eval $ns_ connect \Sudp_($src) \Snull_($dst)

$ns_ at $stime "$cbr_($src) start"
}

set appTime1 550.0 ;# in seconds
set val(traffic) cbr ;# network traffic type

if { ("Sval(traffic)" == "cbr") } {
    puts "\nTraffic: Sval(traffic)"

    $ns_ at $appTime1 "$ns_ trace-annotate \"(at $appTime1) cbr traffic from node 10 to node 1\"“
    cbrtraffic 100 10 1 $appTime1 ;#UDP packet sent from node 10 to 1 every 100 seconds
}

```

## B.6 Configuration of Routing Strategies

Preset with the AODV or ZigBee routing protocol, the combination of wired and wireless networks simulating the traffic in a smart home operates with distinct routing strategies identified in the scenario scripts. By default, all simulations run with the joint path routing option (discussed in Section 7.3). Reliability-based routing is performed with error models configured for each node with multiple interfaces in a smart home (detailed in Sections 4.2.3 and 10.1). Besides, the steps of configuring extra routing preference are detailed as follows:

### *1>Routing via the ZigBee/IEEE 802.15.4 Networks*

With regard to the routing option via only the ZigBee/IEEE 802.15.4 network, the HomePlug C&C interface attached to the corresponding nodes is disabled in the scenario scripts in that no traffic occurs over the unused network. Under such circumstances, the amount of interfaces intended for the central controller is reduced to 2 (RBDS and ZigBee/IEEE 802.15.4), whereas the remaining nodes are equipped with only one interface (ZigBee/IEEE 802.15.4).

*Script sample:*

```
set val(ni)          2          ;#total number of interface/channel

#Create the central controller with the RBDS and ZigBee/IEEE 802.15.4 interface (HomPlugC&C
disabled)
$ns_ change-numifs 2
#$ns_ add-ifs 0 $ll_(0) $mac_(0) $ifq_(0) $ifqlen_(0) $ant_(0) $prop_(0) $netif_(0) $chan_(0)
$ns_ add-ifs 1 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
#$ns_ add-ifs 2 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_

#Create nodes with the ZigBee/IEEE 802.15.4 interface (HomPlugC&C disabled)
$ns_ change-numifs 1
$ns_ add-ifs 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
#$ns_ add-ifs 1 $ll_(2) $mac_(2) $ifq_(2) $ifqlen_(2) $ant_(2) $prop_(2) $netif_(2) $pwr_chan_

#Create nodes only with ZigBee/IEEE 802.15.4 connection
$ns_ change-numifs 1
# ZigBee/IEEE 802.15.4 interface 0 already configured in NS-2
#$ns_ add-ifs 0 $ll_(1) $mac_(1) $ifq_(1) $ifqlen_(1) $ant_(1) $prop_(1) $netif_(1) $chan_(1)
```

### *2>Backbone-Based Routing and Dual Routing*

A static attribute is created separately for backbone-based routing and dual routing in our implementation, which enables the nodes in a smart home to share the same routing options when transmitting packets. To identify the routing option, the corresponding attribute is switched on prior to simulations except for the basic configuration for multiple networks. It is to be noted that both two routing options are deployed

independently from one another according to the specific scenarios. Coexistence of them in the same scenario scripts will give rise to unexpected errors in our simulation model.

*Script sample:*

*\$node\_(1) NodeType EnergyPrio on ;# Backbone-Based Routing (on/off)*

*OR*

*\$node\_(1) NodeType DualRoute on ;# Dual Routing (on/off)*