ABSTRACT

REDEFINING INSTEON HOME CONTROL NETWORKING PROTOCOL

By

Mohamed Shoaib Khan, Abdul Azeez Khan

January 2015

The two main purposes of developing a home control networking protocol are to offer indoor lifestyle sophistication and for the security of our residences. There are numerous protocols based on ZigBee, Z-Wave, Wavenis, X10 and Insteon technologies. These technologies do have good indoor lifestyle sophistication features. Insteon provides wide range of products in this aspect and is the latest and improved version. But the existing Insteon protocol is functional in only smaller Power Line Communication networks. There will be demand for the implementation of Insteon home control networking protocol in larger residential areas and in industrial areas due to its steady growth and popularity. Implementing the existing protocol in larger networks is infeasible because of data collision due to flooding. Therefore, there is a need to redefine and expand the protocol, such that the network could accommodate many devices and increase the size of the network. To achieve the same gradient based routing is implemented that helps to choose a particular path to reach a particular end device. This eventually reduces flooding and useful data packets can be saved from collision. After implementation of gradient based protocol, collision has reduced by 56.63%, delay decreased by 65% and throughput increased by 105.6%.

REDEFINING INSTEON HOME CONTROL NETWORKING PROTOCOL

A THESIS

Presented to the Department of Electrical Engineering

California State University, Long Beach

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Electrical Engineering

Committee Members:

Mohammad Mozumdar, Ph.D. (Chair)
I-Hung Khoo, Ph.D.
Chit-Sang Tsang, Ph.D.

College Designee:

Antonella Sciortino, Ph.D.

By Mohamed Shoaib Khan, Abdul Azeez Khan

B.E., 2011, A.M.S. College of Engineering, Anna University, Chennai, Tamil Nadu, India

January 2015

TABLE OF CONTENTS

Page

LIST OF TABLES v

LIST OF FIGURES vi

CHAPTER

1. INTRODUCTION TO HOME NETWORK TECHNOLOGIES 1

Important Characteristic Features and Requirements of a Home Network 2
Technical Requirements and Specifications 4
ZigBee Technology 6
Z-Wave Technology 7
Wavenis Technology 8
IP-Based Technology 8
X10 Technology 10

2. INTRODUCTION TO INSTEON 17

History of Insteon 18
Important Characteristics of Insteon Technology 18

3. THE INSTEON TECHNICALITIES 21

The Insteon Network 21
The Insteon Communication Protocols 24
The Insteon Messages 26
The Insteon Packets 34
Insteon Data Rates 38
Insteon Devices 40
Frequency of Operation and Modulation Technique 43
Security in Insteon Devices 44
Platform for Development of Application 44
Insteon Signaling 44

CHAPTER Page

4. INSTEON COMMUNICATION 50

Powerline Communication 50
Classification 50
Communication Model 51
Multihop Data Transmission in Powerline Communication 54
Attenuation Characteristics of Carrier in Powerline Communication 57
Advantages of Powerline Communication 58
Limitations of Powerline Communication 59
Applications of Powerline communication 59

5. IMPLEMENTATION OF GRADIENT BASED ROUTING IN PLC 61

Need for Gradient Based Routing in Insteon Protocol 61
Gradient Based Routing Protocol in PLC 64

6. SIMULATION AND RESULT 75

Existing Protocol 75
Proposed Protocol 76
Results 78

7. AUTOMATED DISASTER REPORTING SYSTEM 90

REFERENCES 94

LIST OF TABLES

TABLE Page

1. Standard Message Field Size 27

2. Flag Fields in a Standard Message..... 28

3. Details of Message Type Field in a Standard Message 29

4. Extended Message Field Size 32

LIST OF FIGURES

FIGURE Page

1. X10 message format 11

2. Representation of bit ‘1’ 13

3. Representation of bit ‘0’ 14

4. Insteon network 23

5. Standard message structure 27

6. Extended message structure 32

7. Start packet structure 35

8. Body packet Structure 35

9. Powerline standard message packet 36

10. Powerline extended message packet 36

11. RF standard message packet 37

12. RF extended message packet 38

13. Simple insteon network device function without a repeater 42

14. Insteon network with an intermediate repeater 42

15. Simple BPSK modulation with dissimilar bit values 45

16. BPSK modulation with similar continuous bit values 46

17. Powerline signal with insteon packet timing 47

18. Standard powerline packet transmission 48

FIGURE Page

19. Extended powerline packet transmission 49

20. Powerline communication source 51

21. Powerline communication destination 53

22. Simple multihop demonstration 56

23. Sample attenuation characteristics in powerline communication 58

24. BP demonstration 65

25. PSQ demonstration 66

26. No PSQ response 67

27. PD packet transmission 68

28. BP response to PD 69

29. NAP demonstration 70

30. FBP demonstration 71

31. EDJ demonstration 73

32. Existing insteon protocol 75

33. Proposed protocol with 10 nodes 76

34. Proposed protocol with 30 nodes 77

35. Collision at high data rate 79

36. Collision at medium data rate 80

37. Collision at low data rate 80

38. Average collision 81

39. Percentage change in collision 82

40. Delay at high data rate 83

FIGURE Page

41. Delay at medium data rate 83

42. Delay at low data rate 84

43. Average delay 84

44. Percentage change in delay 85

45. Throughput at high data rate 86

46. Throughput at medium data rate 86

47. Throughput at low data rate 87

48. Average throughput 87

49. Percentage change in throughput 88

50. Performance comparison 89

51. Flow chart--existing disaster reporting system 91

52. Proposed automated disaster reporting system 92

CHAPTER 1

INTRODUCTION TO HOME NETWORK TECHNOLOGIES

Sophistication before advancement of technology was furnishing home with all types of furniture to make a home look beautiful and lead a cozy lifestyle. Now as science and technology is heading towards its pinnacle level, expectations amongst the people are more in order to lead the Jetson kind of life style: To open the entrance door of your home with the help of your own mobile phone and the lights turn on automatically once you enter, hot coffee waiting for you in the microwave that was prepared with the help of a command triggered when you start from office to return home, the microwave itself downloads the recipes for the next day's meals, the couch automatically changes its position depending upon the posture you want to lie comfortably and start massaging your body automatically after fetching the magnitude of strain through a group of sensors called Body Area Network (BAN), then your television automatically switches on and plays a movie or your favorite songs list. All of this should happen at a single touch of a button, lights going into the dim state for a pleasant watching of a movie, simultaneously maintaining temperature in the home apartment to make you fall asleep, later waking you up in the morning with the help of an alarm automatically for you to prepare for the day and aiding you to be on time to office. Apart from having a cozy lifetime, there is always a concern by the people regarding the security of their homes. A system that could sense intrusion, water leakage, fire, etc., all

of them in one package connected within a network and to your mobile phone, fully controlled by humans just tapping on their phone touch screens is what could be a proper definition for sophisticated lifestyle. The criterion of Insteon is to achieve this type of definition in home network control and management protocol. Apart from Insteon, there are other technologies namely X10, ZigBee, Wavenis, Z-wave and IP-based Technology that are used to implement Home automation networks [1].

Important Characteristic Features and Requirements of a Home Network

Following is discussed about some of the important features to be considered when designing a home automation network [1].

1. According to the above discussion, it is clear that there is always a rising demand for home automation and sophistication from the people, to satisfy the same, it is mandatory to have many devices involved in the system. Some of the vital applications are monitoring elderly people, children and patients at home, security of the home that could detect fire, smoke, leakage, intruder, also well secured locking system and one more important application is energy saving mechanism, to nullify the wastage of energy. This efficient energy management system requires devices that alert users at high peak energy utilization. Now it is well comprehensible, that the network of interest could include as many as hundred devices.

2. Secondly, mode of communication between the devices is considered, to study how the information is passed from one device to the other, whether wireless or wired, single-hop or multi-hop, point to point, etc., selecting the type of communication should be based on functionality.

3. Determination of devices to be mobile or static also depends upon the applications and it is to be considered that network should function without any hamper.

4. Memory is a major consideration for size constraint devices. Saved running configuration, useful information sensed and saved dynamically should be able to accommodate in the available space. The sizes of ROM and RAM respectively in a ZigBee network are 45 to 128 Kbytes and 2.7 to 12 Kbytes and in 6LoWPAN are 24 Kbytes and 3.6 Kbytes. In Z-Wave, the flash memory is of size 32 to 64 Kbytes and SRAM is 2 to 16 Kbytes. Insteon contains 7 Kbytes of flash, 4 Kbytes of external EEPROM, 256 bytes of internal EEPROM and 256 bytes of SRAM. The memory in Wavenis comprises of 48 Kbytes of flash, 400 bytes of RAM and 20 bytes of non-volatile memory.

5. At the time of emergency like sudden fire, patient abnormality and activities of an interloper data has to be transmitted immediately without any delay and to respond spontaneously in order to overcome the trauma. Therefore, the factor delay should be negligible or should be brought to zero.

6. Residences installed with home automation protocol, located near industries and hospitals would be prone to signals of ISM band. Therefore, care has to be taken to prevent the effect of interference, and avoid loss of data.

7. Security of the data though in a home automation network is not of so important, it is to be noted that at certain areas this plays a vital role. But in general less intense or basic security protocols are used like Data Encryption Standard (DES), Advanced Encryption Standard (AES) with different key size and rolling codes.

8. Lastly, cost of the system should be maintained, such that it is affordable by an average income earning families. High cost would make this burgeoning home automation and management technology defunct.

Now, let us discuss the technical aspects of a home automation management network.

Technical Requirements and Specifications

The technical characteristic requirements for different technologies are expounded layer wise below [1].

Physical Layer

1. The range of distance within which the devices could communicate with each other is higher in Wavenis which is about 200--1000 meters, next is Insteon with the range of 150 m. Least is about 100 m in ZigBee and Z-Wave.

2. Radio Frequency band used for data transfer is around 915 MHz, which is in the ISM band, usable and unlicensed. This frequency is adopted by Wavenis, Insteon, and ZigBee. Z-wave transmits at 908 MHz and ZigBee also allows data to transmit at 2.4 GHz.

3. ZigBee can send data at the rate of 250 Kbps maximum; Z-wave transmits data at the rate of 200 Kbps. Insteon can send instantaneously at 13.16 Kbps. Wavenis transports data at 100 Kbps maximum.

4. The modulation technique used in ZigBee is Binary Phase Shift Keying (BPSK) with Direct-Sequence Spread Spectrum technique. Z-Wave follows Binary Frequency Shift Keying (BFSK) with no spreading technique. Insteon follows Binary Phase Shift Keying (BPSK) and with no spreading techniques. The modulation

technique found in Wavenis is Gaussian Frequency Shift Keying (GFSK) with Fast Frequency Hop Spread Spectrum (Fast FHSS) technique.

Link and MAC Layer

1. Mechanisms applied in this layer can be TDMA, CSMA or Simulcast. CSMA is used in almost most of the techniques as in ZigBee, 6LoWPAN, Z-Wave, Wavenis. CSMA and TDMA are both applied in ZigBee, Wavenis. TDMA and Simulcast are used in Insteon.

2. Insteon takes only 24 Bytes maximum to transmit the information. Whereas, Z-Wave uses 64 Bytes and ZigBee takes 127 Bytes.

3. Error control mechanism used in link layer is Cyclic Redundancy Check (CRC) in majority by Insteon and ZigBee. Whereas, Forward Error Check (FEC) in Z-Wave, apart from FEC other techniques like scrambling, data interleaving, window acknowledgements are implemented. Acknowledgement is also used in Z-Wave along with check-sum.

Network Layer

1. This layer is generally concerned about routing the packet to a particular device or network. Insteon follows simulcast instead of multihop, ZigBee works with mesh, tree and source routing, Z-Wave also adopts source routing, and in Wavenis tree routing is implemented.

2. The hop count is a major factor in a network, this tells us how reliably, efficiently, rapidly a message can be sent. Insteon and Z-wave restricts the hop count to four. 6LoWPAN allows a maximum count of 255. Depending on the type of ZigBee routing protocol the network follows, the hop count could be 30 or 10 or 5.

Transportation Layer

This layer is assigned with the task of reliable transmission from source to destination. Reliable transmission can be achieved by incorporating protocols like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which is found in 6LoWPAN. Other technologies do not support TCP or UDP, but simpler concept like acknowledgment and duplicate packets are adopted.

Application Layer

This layer directly involves devices or this layer can be defined as the intermediate between the devices and all the transmission protocols. As discussed earlier, number of devices is directly proportional to the various applications. ZigBee and Insteon can add up to 65,536 devices in a single network. A Z-Wave network can have 32,768 devices. Different networks have different set of devices like end devices, coordinators, routers, hosts, mesh nodes, edge routers, controllers, slaves depending upon the number of technologies. Some technologies have only one kind of devices, which can perform all the duties of a sender, receiver and repeater.

ZigBee Technology

ZigBee is a wireless technology, which finds its application not only in home automation network including Automatic Meter Reading (AMR) and Heating Ventilation and Air-Conditioning system (HVAC), but in other domains like military, fleet application, medical applications, etc.

Out of the existing four layers, physical and MAC layer follow the traditional Wireless Personal Area Network (WPAN) IEEE 802.15.4 standard. While the other network and application layers abide ZigBee specification. The devices that participate

in the functioning of the network are ZigBee coordinator, ZigBee router and ZigBee end devices. ZigBee coordinator obeys IEEE 802.15.4 standard, whereas end devices are ZigBee protocol specific. There are two types of topologies like Tree and mesh possible in ZigBee technology. Tree topology is used for data aggregation. Mesh topology facilitates routing of data utilizing Ad hoc on-demand Distance Vector (AODV), because in this type of networking topology all the nodes are interconnected with each other. In the routing process ZigBee coordinators and routers take part.

ZigBee applications are divided into two profiles, one for home automation and control and the other profile for energy saving and management.

Z-Wave Technology

The devices involved in Z-wave are controllers, slaves and end devices. Collision avoidance mechanism is used in this protocol, that checks the condition of the channel whether it is feasible for data transmission. If the condition is favorable, then data is transmitted else transmission is postponed. This protocol offers reliable transmission for short messages between the controllers and the end devices. Physical, MAC, transfer, routing and application are the different layers that come to play, where transfer layer aids communication between two adjacent nodes and allows ACK mechanism to recover lost data by applying the concept of retransmission. The routing protocol used here is source routing protocol. When the packet is sent out from the controller the path is recorded, which in future aids in the scenario of retransmission. The controller maintains a table, containing the topology of the network. Four hops are permitted for the packet to reach the destination, which is sufficient for a home network protocol. Pertaining to situation, slaves act as routers and store static route to the destination nodes.

Wavenis Technology

Wavenis defines following layers physical, MAC and LLC, Network and upper layers services are acquired in terms of Application Programming Interface. But Wavenis defines only one type of device. In Wavenis two schemes namely synchronized and non-synchronized schemes are available in the MAC layer. Synchronized scheme functionality is defined to have both TDMA and CSMA work together. To explain briefly, if a node has to send out a data, a random time slot is defined at which the node senses the carrier medium; whether the medium is free to allow the data to travel through. If the medium is free, the date is transmitted, else the node has to wait for next time slot and sense the medium to send the data. Therefore in this concept both TDMA and CSMA is applied. In the non-synchronized scheme only CSMA is used, here reliability is compromised to an extent. LLC layer as usual takes care of flow and error control using ACK mechanism. The network layer is not just routing, but aids data aggression. In this layer the devices in the network are allowed to find their parent and form a tree topology with four level of hierarchy, wherein the root collects all the data and acts like a gateway. A node selects a parent by first broadcasting a request packet to all the nodes. The request packet demands for QoS information, which is a bundle of information like number of nodes attached to it, battery energy level, received signal strength indicator. The best of value is chosen as the parent.

IP-Based Technology

There are various protocols in home networking; internet of things seems to be in its rapid phase of development. IP-based technology has one unique system called DOMOSEC a platform form of Domotics and Security [2]. This provides the owners to

monitor and control their home remotely with setting up local gateway. Also third party security concerns can also monitor the residence in the case of owners' negligence.

There had always been research to collaborate sensor networks and IP networks. IP networks consist of larger devices and larger data transmission when compared to the sensor networks, therefore compatibility should be put into the networks to derive best reliability. It can be affirmed that the technology in sensor networking has attained its pinnacle if this idea of collaboration is successful. Efforts have been taken to standardize incorporation IP-Based technology in sensor network by IETF with the help of the promoter named IP for Smart Object (IPSO) alliance. Already the IP network has commenced utilization of IPv6 addresses, which will accommodate lot of devices including sensor nodes. The collaboration is termed as 6LoWPAN, which defines IPv6 protocol for Wireless Personal Area Networks. For the effective collaboration, following few factors is required. Fragmentation: Packet size of IPv6 is of 1280 Bytes, whereas IEE 802.15.4 packet structure size is of 127 Bytes. Therefore the packet size should be adapted such that there is no impediment in data transmission. Header Compression: Sensor data packet with heavier header size of 40 Byte as in IP network is not feasible, therefore data header should be compressed for successful collaboration of the two different networks. Thirdly, sensor network should adopt the concept of IPv6 address auto configuration. Neighbor Discovery protocol: There are a lot of protocols standardized for neighbor discovery. Maintaining neighbor details in a table through neighbor discovery protocol is essential for proper network topology maintenance. Huge amount of memory size is required to store the table which is possible by the devices associated with IP network, but devices in sensor network are tiny and have memory

constraints in them to store the high volume of table, therefore a protocol has to be designed such that, it is suitable for devices in a sensor network. Apart from these many more factors can be designed like routing protocol, type of devices and its characteristics. But if it is very successful, in the home automation protocol, the devices can be controlled from different remote places, like the way people from different places could send SMSs or email to people in different parts of the world. Some other few disadvantages of IP-Based technology that would make users to choose Insteon home networking technology is that currently IPv4 is facing address depletion and even though IPv6 would overcome it, it would become difficult to migrate devices from IPv4 to IPv6. And IPv4 features complex routing protocol to determine the best path to find the destination, which would consume a lot of time, but Insteon which avoids complex protocols works very rapidly, keeping response time, which is very minimum as one of the major characteristics while building this technology.

X10 Technology

A company called Pico Electronics in Scotland developed X10 Standard in 1975 for the purpose of automated home management network. As said succinctly above, X10 data packet, which is a combination of an address and a command is sent at every zero crossing of the power signal which is of 60 Hz, using 120 KHz carrier signal. Each bit is sent thrice and each message is sent twice. This phenomenon of sending data in burst-mode is to achieve high data throughput, but this could cause wastage of energy and time. Also in this protocol, data sent is not acknowledged back. Therefore, these two factors contribute to the disadvantages of X10.

X10 Data Format

The Data packet generally consists of four sections: Firstly, start code, which is equal to the binary digits 1110, then follows four bits of home code, which ranges from the English letter A to P, then follows four bits of unit code within the range of numbers 1 and 16. Lastly, the four bits make up the command field. Having home code and unit code gives secure data transaction, because the data is found to travel within a home or a zone containing devices of same home code. Therefore the data packet cannot escape out from the particular zone, which implies no leakage of information and prevention of data attenuation due to collision of packets from different zones.

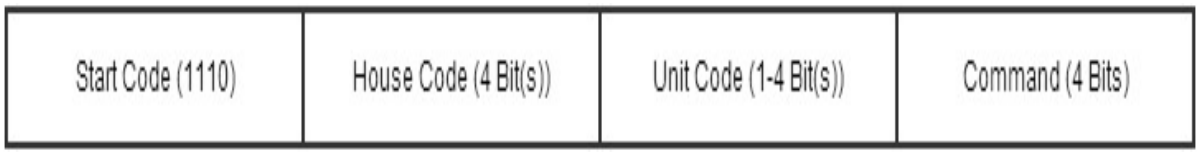

FIGURE 1. X10 message format.

With the combination of home and unit codes, 256 addresses can be generated. Each device's module is configured with one of the available 256 addresses, hence the devices respond to the data packets addressed to their corresponding module alone.

`X10 Signaling Details

When the binary digit '1' is transmitted, it is indicated by the presence of the carrier signal in the first zero crossing, then absence of the same in the second zero crossing of the powerline. For bit '0' carrier signal is absent in the first zero crossing and

present in the second zero crossing, as shown in the Figure 2. This protocol sends data at the rate of 20 Kbps, therefore the X10 protocol is very slow and led to the invention of a faster protocol.

X10 Devices and Modules

Controllers. One or four X10 devices active at low operational power can be controlled by simple controllers that are involved in simple lamp or wall switch module. One of simple controller's scenarios is switching on or off small devices like low watt bulbs. If more than four devices are to be controlled and those devices that operate at high power as in appliance mode, then sophisticated controllers are required. Controllers are responsible for sending the command to the devices, depending upon the user input. Command travels throughout the available powerline wiring.

Modules. The devices are connected to the power socket through modules. These modules are responsible to pick up the signal for the devices connected to it. The module learns that the incoming packet is meant for the device connected to it by comparing the home and unit codes in the signal and the device. Modules ignore the signals that are not meant for the devices connected directly to them.

Bridges. X10 devices are said to work using powerline to transmit data. To provide more comfort to the users, certain devices can be indirectly controlled wirelessly using RF communication. Bridges are the devices which convert RF data packets to X10 readable powerline packets.

Other common devices are repeaters that come into the picture at times when signal from one phase has to be passed through the other phase, couplers aid connection

of two different networks for the transmission of data from a sender to farther located receiver in the home.

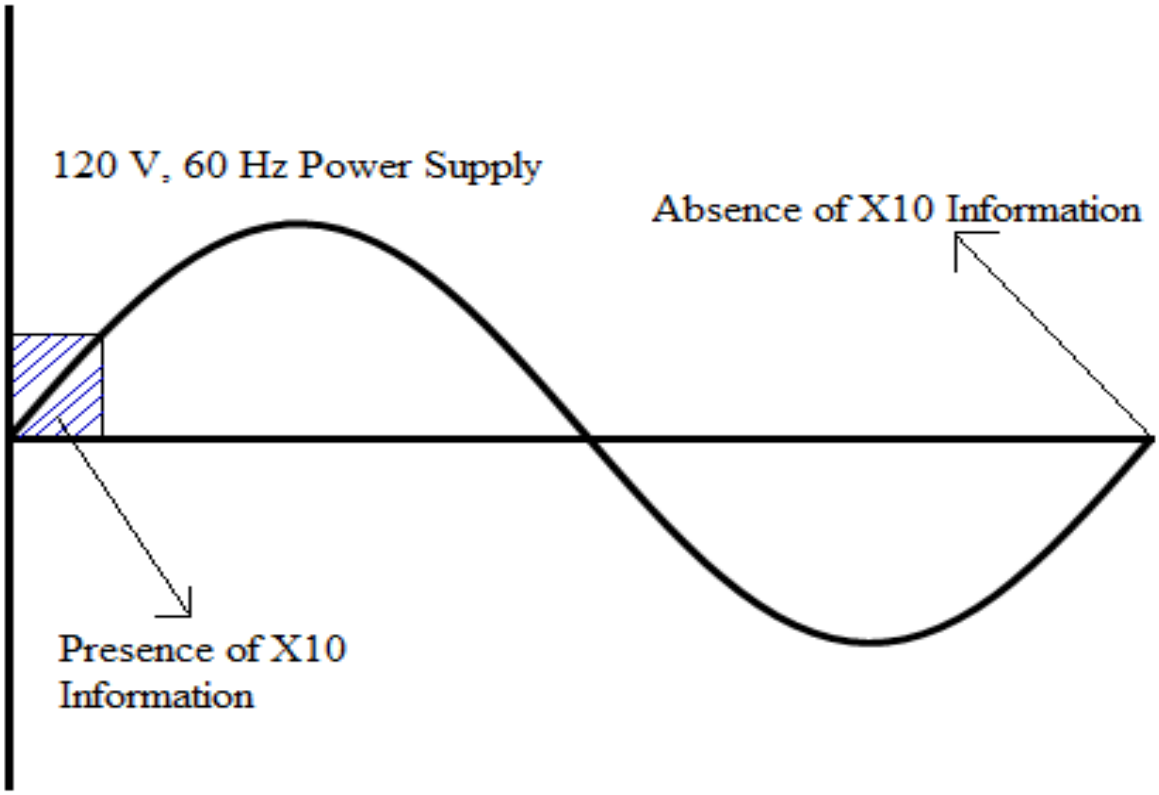

FIGURE 2. Representation of bit ‘1’.

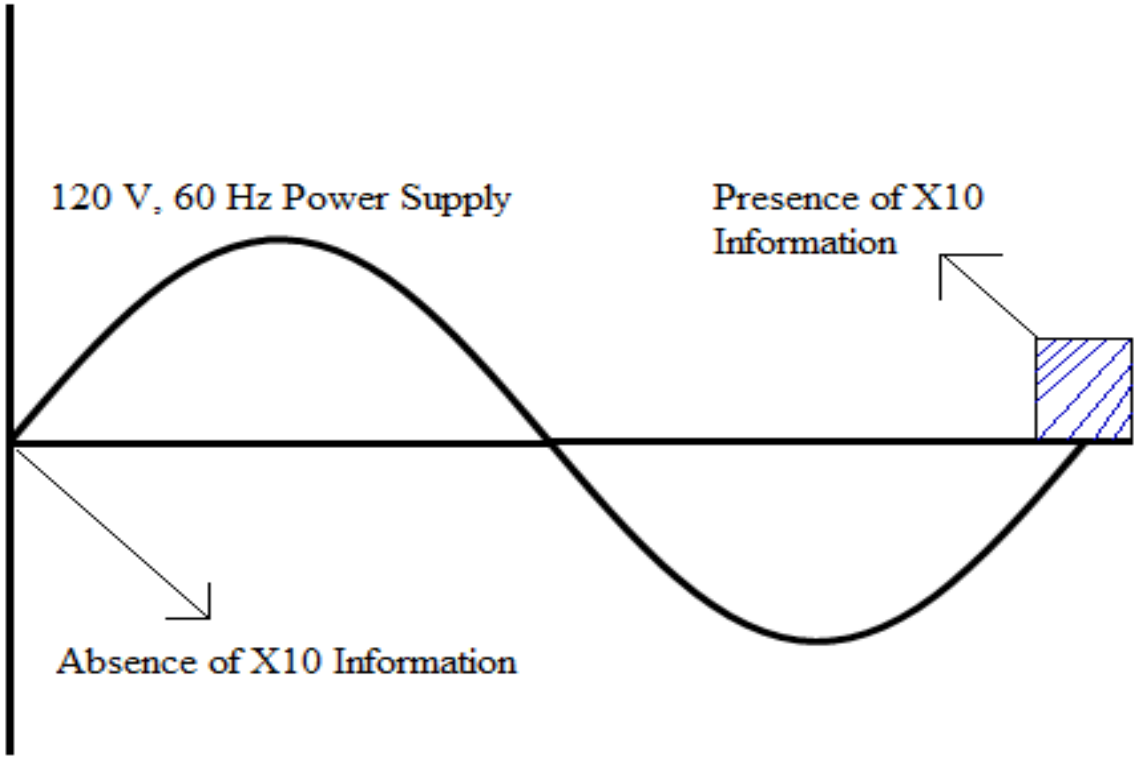

FIGURE 3. Representation of bit '0'.

Disadvantages of X10 Protocol

Loss of data. X10 protocol allows data to be transmitted once at a time. If two or more packets are sent at the same time, then collision is the resultant. Some times this may lead to incorrect functioning of devices.

Low data rate. Message is transmitted at the speed of 20 Kbps, which cannot be accepted at this era, where people expect processes to happen at almost lightning speed. Generally it takes for the device almost three forth of a second to respond, once the command is issued.

Less functionality. Fewer operations are supported by X10 technology than Insteon like switching on / off or dimming lamps and other low watt appliances. Also upgrading to more advanced devices to add more options requires many changes from modules to circuitry.

Lack of data security. Data encryption process is not integrated in X10 protocol. This is one serious disadvantage because data is not protected while transmitting.

All of these above discussed demerits lead to the evolution of more upgraded Insteon technology.

One advantage of X10 is that the products are kept at lesser cost than Insteon.

Comparison between Insteon and X10

Firstly, Insteon supports two way communications, whereas simple X10 devices follow simplex communication. Some advanced X10 controllers, though allow two way communications, demand for all devices to be duplex compatible. This increases the price more than four times making the technology lot expensive for fewer features. Also there is no acknowledgement message sent to confirm reception in either case. In case of Insteon protocol, the devices are capable of acknowledging the data received.

The carrier signal frequency is 120 KHz in X10, whereas Insteon works with carrier signal at frequency 131.65 KHz using powerline to transmit the data.

The response time in X10 is very slow, because the data rate is very low, which is about 20 bps only. Insteon has really higher data rate than X10, the data rate ranges between 180 bps and 13.165 Kbps.

Installing X10 is lesser expensive than Insteon devices. This could be due to the less options and outdated technology of X10. Most of the controllers of X10 are wired

and people for ease, demand wireless for domotics or home automation, therefore Insteon is highly welcomed product nowadays. Though bridges could translate information from RF packet to powerline packet, bridges in the automation kit makes the package costlier at the rate at which better product i.e., Insteon package could be bought.

Commonalities between Insteon and X10

Only one similar aspect could be inferred after the study of X10 and Insteon. In both the cases, powerline is used to transmit the data at every zero crossings of the power supply with 60 Hz frequency. Insteon could also communicate wirelessly via RF communication without any alteration of the network, so as X10 which uses bridges as discussed above and is not very feasible idea.

CHAPTER 2

INTRODUCTION TO INSTEON

Smartlabs which was found in 1992, California Irvine is the birth place of Insteon and Smarthome. Smartlabs is the leading authority in the field of home automation and control. Insteon is a networking technology that is designed for home network management protocol. Smarthome is the retailer outlet for the end products developed out of Insteon technology. There are a various kinds of products developed for peoples' comfort and home security like dimmers, HVAC System, LED bulbs, low voltage controllers, on the security side devices like sprinkler control, garage door monitor, hidden door sensor, motion sensor detector and transmitter, leak sensor, smoke detector, energy monitoring device, camera.

Nowadays, the security system consists of sprinklers, fire detectors, smoke detectors, cameras etc., but all not interconnected and use traditional technology. Insteon concept is that it connects all devices to form a mesh network. And the most important concept that attracts all engineers is its dual band technology. This technology includes transmission of data through powerline and RF communication. All the devices form peer-to-peer network such that any device in the network can transmit, repeat or receiver. Some devices follow only RF communication or communicate via powerline and some devices use both to communicate and are called dual-band devices. Though it uses both RF and powerline the networking concept is very simple and not complicated that

includes routing table, addressing, easily comprehensible data packet, simple error check mechanism and other cumbersome tasks. All of these together make working of the network without any impediment. These concepts to be further discussed in the coming topics.

History of Insteon

To satisfy the need of more equipped home automation system than X10 technology, which is more than three decade old and works only using existing powerline. Reliability, response time and efficiency of the X10 system is not as expected. A system which overcomes all of these is required. This lead to the invention of Insteon network protocol in June 2004. Insteon network protocol uses dual band, both RF and powerline, this improves reliability. Insteon is proved 30 times faster than X10, this promotes response time. Both of these together increases overall efficiency of the system. Hence Insteon is a successful home network management protocol and now the authority in the same domain. Due to the network's rapidness, the name of the protocol Insteon is derived from the phrase "Instant on."

Important Characteristics of Insteon Technology

Reliability

Insteon's dual band nature of communication helps sender to send data to nodes in different routes, such that if one fails the other successfully transmits the command. This holds good because of another concept of repeating messages. The function of a node as a repeater is to check the received packet and take actions accordingly. Once the node receives the packet it checks for the "to address," if the packet's to address is not equal to the address of the node that received the packet, the node sends out the packet

for retransmission instead of dropping it. These features thus aid reliable transmission of the message and proper outcome is achieved.

Installation

The users can install their Insteon product by themselves without requirement of any specialized trained engineers. The Insteon nodes are pre-addressed at the time of manufacturing process. Therefore there is no initialization process to occur once the nodes are powered on. Secondly, Insteon setup demands no separate wiring to form network, but uses the existing powerline to communicate within the devices. The installation is said to be called as "Plug and Tap" process, which has two simple steps: First is to plug a device like lamp or a bulb or any other device that has to be controlled automatically into the Insteon module, which is plugged to the power line via power socket. Second step is to press the set buttons in the module and in the mobile phone Insteon application, which is used to control the device automatically is well explained and wide range of products are shown in the website [3]. Therefore installation Insteon home networking devices is easy.

Utilization

Controlling and using Insteon devices is simple, because it does not require complicated programming or functions to make the network operational by the user. Just pressing buttons and switches is involved. Therefore Insteon products can be termed as user friendly devices.

Response Time

Due to dual band feature and due to high speed of the travelling signal, the network does not experience any delay in the transmission of commands. Insteon system

is build such that a function can be executed in 0.04 seconds. Hence the name Insteon derived from “Instant On” as explained earlier.

Affordability

The network is not made to engage into performing cumbersome algorithms to determine the route to destination and the software used is simple too. These together make the networking protocol affordable to users.

Backward Compatibility

X10 technology mostly uses existing powerline to communicate with devices. Also X10 was the recent technology before Insteon was evolved. Insteon technology can work on both RF and powerline. Insteon can function with some X10 devices, therefore Insteon is called as backward compatible technology.

CHAPTER 3

THE INSTEON TECHNICALITIES

The Insteon Network

Dual Band Technology

Network is defined as the relationship of a device with its associates. The Insteon home network has many devices connected to each other that can communicate and deliver outcome satisfying users' desire to possess automatically controllable house appliances and to have a sophisticated life style at the users' residence. This main concept would not have established successfully, if network with only one type of communication network is considered. In Insteon two different types of networks are integrated to achieve the main purpose of home automation network. Traditionally, networks are formed by connecting the devices in the network with the help of wires and is called wired network. But nowadays, to avoid dense networks and as a result of technology reaching to its pinnacle, wireless networks are designed. Wireless networks require no physical connectivity between the devices, but takes air as medium to communicate. These types of networks are apt for home automation network. Some devices are wired compatible, whereas some can adopt wireless communication.

Considering all of the above discussed necessities, Insteon network is designed to support both wired and wireless communication and this is called Dual Band technology.

Wireless network use RF (Radio Frequency) to communicate, while the wired network devices use existing powerline to communicate or in other words, devices can communicate through wired and wireless medium. These devices are called as dual band devices. These devises are RF compatible to transmit data wirelessly and uses powerline to transmit through a wire.

Mesh Topology

There are many topologies that a network can form: Star topology, Ring topology, Bus topology, Tree topology and Mesh topology. Star topology consists of a central or a master device to which all other devices are connected. There would be unnecessary communication to the central device for every packet transmission between source and destination, this increases load to the central device. If the central device fails then the whole network is not operational. In Ring topology, the network is formed as a ring by connecting the adjacent devices. If a data is transmitted from a device at the beginning of the network to a device at the end of the network, the data passes through all the intermediate devices between the source and the destination. Again delay is at the maximum level. If anyone node in the network fails, the overall transmission is disrupted. Bus topology consists of only one single wired bus to which all the devices are connected to it. Communication is possible in one direction at once. There is possibility of collision if more than two transmissions of the data take place simultaneously. If the central bus fails then the whole network fails. Tree topology is the combination of Star and Bus topology and it is not suitable for home automation network. The best suitable topology for home networking protocol is Mesh topology considering the following features. Mesh topology is a network topology in which all the devices of

the network can communicate with each other, which means all the devices are interconnected with each other. The advantages of this topology are, that more than one communication within the network is possible simultaneously and more than one routes are available between source and destination. The below Figure 4 shows a mesh topology, in which all the devices are interconnected.

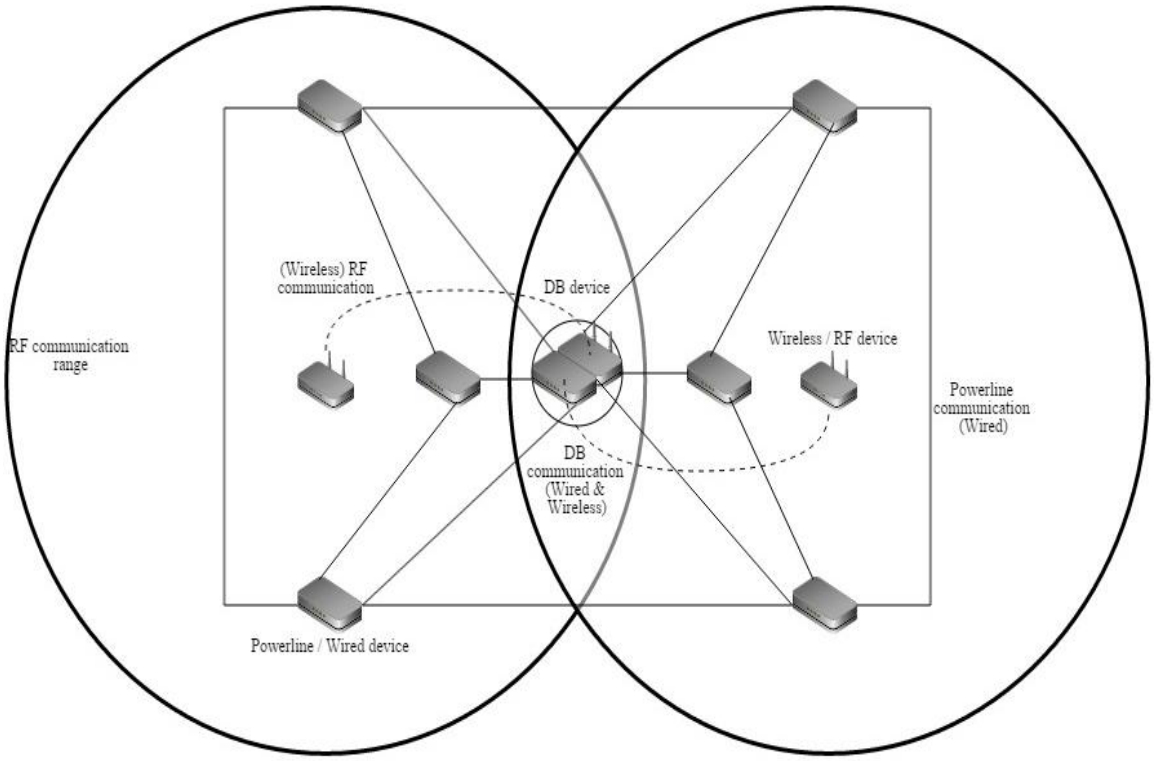

FIGURE 4. Insteon network.

The Figure 4 demonstrates a basic Insteon network, which consists of nodes that can communicate using a wired medium via powerline and nodes that can communicate

wirelessly via RF communication. One node in the center of the network in the figure is called as a DB device, supports communication wirelessly and on a wired medium.

Peer-to-Peer Communication

In Peer-to-Peer network, all the devices of the network possess same and equal responsibilities. All the devices have equal rights to access the resource. The process is decentralized; there is no master to control the other devices as in server and client communication, where server is considered to be the master. Here, in Insteon any node can perform the duties of a sender or a receiver or an intermediate node that just passes the data it receives.

The Insteon Communication Protocols

Protocol is defined in step by step procedure, that a data message should follow starting from sending end device, till it reaches the receiver. There are a various protocols that Insteon packets should adhere for successful transaction between source and destination.

1. All devices are capable of receiving a message and resending it. Therefore all devices act as repeaters. A node receives a packet, checks for to address and if it is destined to it, it decodes the information. If the packet is destined to some other node, then the device sends the packet out without any alteration. Therefore all devices follow two-way repeater communication.

2. Sender who sends a packet to the destination node should know whether, it has reached the destination without any impediment or loss, therefore all the messages that are received by the destination are acknowledged to the sender, that the receiver got the packet successfully. In Insteon, all the messages that are received are acknowledged back

to the sender, except for the broadcast message. This procedure in communication helps successful transmission of data with high reliability and reduces loss of packets. In the case of no acknowledgement or ACK is received, the sender retransmits the packet.

3. The concept of Negative Acknowledgement or NACK Adds more reliability to data communication. Circumstances at which NACK should be sent out to the sender, informing about the data disruption are: When data is dropped or lost or in the intermediate node in the path of communication, NACK is to be sent to the sender that notifies the sender that the message has been dropped. Secondly, NACK is issued to the sender, when the data receiver erroneous packet. In all cases after NACK is received by the sender from the receiver that encounters packet loss and / or erroneous data, the packet is retransmitted by the sender.

4. Above all discussed concepts, the following protocol aids to attain complete reliability. The Error Detection or Error Control Mechanism Protocol. There are various error control mechanisms like Cryptographic hash function, Parity bits, Repetition codes, Checksum, Cyclic Redundancy Check or CRC. As already discussed that, X10 Technology has no error detection mechanism. This is a drawback for a protocol to be called as a reliable and well defined protocol.

The receiver may receive erroneous message and respond wrong according to the message received. This could be fixed using the parity check method [4], wherein a bit field included in the message byte informs whether all the bits in the message hold even or odd parity. Whereas Insteon as CRC using the polynomial long division method determines the quotient, the digital equivalent of the quotient is appended to the message in the CRC field.

In Insteon home networking technology, CRC Protocol is used. Every message that is sent out from a device has a field in it that stores a value. This value is called as Cyclic Redundancy Check or CRC value. The sender before sending the packet and after encoding the information into the packet, the data bits in the packet are subjected to error control algorithm. The result of the process is saved into the CRC field. Now the packet is sent out of the sender, the receiver receives the packet, runs the CRC algorithm with input to the algorithm as the bits in the packet received. The receiver obtains the value as the result of CRC algorithm, compares the value with the CRC field in the original packet it received. If the value is same, the packet is categorized as accurate packet and the receiver starts to decode the information in the packet. If the values are dissimilar, then the received packet has error and is dropped, notifies the sender about the error in the packet by sending negative acknowledgement.

The Insteon Messages

Message Size and Type

The Insteon message is of less size, which aids faster transmission of data. Therefore commands can be executed rapidly in about 0.04 seconds. Users can expect instant switching on of lamps or lights and other household electronic products. There are two types of messages in Insteon: standard message and extended message. An extended message can carry the information in a standard message, whereas a standard message is incapable of carrying all the information as in an extended message. For basic communication, like just to turn on the lights, a standard message is enough. And for functions beyond some basic communication, an extended message is required. The standard message is of size 10 Bytes and the extended message is of size 24 Bytes.

Message Format

Message format describes each and every field and its significance in the Insteon message. Let us now look in to the fields of the two available types of message in detail.

Standard Message

This basic and simple message, which is of size 10 Bytes has the following fields as presented in the Figure 5.

FIGURE 5. Standard message structure.

The table below presents the data size of each field, which is then followed by description of each field.

TABLE 1. Standard Message Field Size

Field	Size in Bytes
From Address	3
To Address	3
Flags	1
Command	2
Error Detection Value	1

From Address. This field is a 3 bytes or 24 bits field that holds source address. This field is used to determine the sender by the receiver node, and in the case of loss of

data negative data should sent by the receiver, hence it is a necessity for the receiver to know the sender address to send the negative acknowledge.

To Address. To identify the message's destination, to address is encoded into the packet from the database. If a receiver receives a message, it first checks the to address. If the to address is same as its own receiver device address, then it is understood that the message is intended to this device that has received the message, otherwise the message is retransmitted to the neighbors.

Flags. This field, which is of 1 byte size describes the type of the message and controls retransmission of the message at the device holding this message.

TABLE 2. Flag Fields in a Standard Message

Flag Field	Size in Bits	Bit Position	Description
Message Type	1	7	NACK / Broadcast
	1	6	Group message
	1	5	ACK
	1	4	Extended / Standard message
Message Retransmission	2	2 and 3	Hops left
	2	0 and 1	Maximum Hops

Message type field in a standard message. The message type field holds the information on the type of the message. From the fourth bit position, we can learn that, whether the message is standard or extended type of message. If that field contains the bit value '1' then the message is an extended message, otherwise the message is standard message, if it contains the bit value '0'. The rest of the bits in the fifth, sixth and seventh positions play very important role in the classification of the message. Group cleanup message has always a bit value '1' in the sixth position. For broadcast and NACK type

of messages, the fifth bit position carries bit value ‘1’. For the purpose of NACK and ACK message the seventh bit position takes the bit value ‘1’. The following TABLE 3 displays the significance of each bit of the field.

TABLE 3. Details of Message Type Field in a Standard Message

Bit Position			Significance
5	6	7	
0	0	0	direct message
0	0	1	ACK for direct message
0	1	0	group cleanup direct message
0	1	1	ACK for group cleanup direct message
1	0	0	broadcast message
1	0	1	NACK for direct message
1	1	0	Group broadcast message
1	1	1	NACK for group cleanup direct message

Let us now get into details of the message type field in a standard message.

Direct Messages. The direct message is nothing but a normal message that carries command to the receiver. This message can also be called as point to point message.

Broadcast Message. This is not a point to point message, because the message is not sent to just one device, but sent to all the device s in the network, it can be also called as one to all message.

Group Message. This type of message is sent to a group of devices from one device, therefore can be called as one to many message.

Acknowledgement Message. This is a positive response sent by the receiver to the sender for the successful receipt of the packet received by the device from the sender.

There is acknowledgment message for a direct message, group cleanup message, but there is no acknowledgement for broadcast message.

Negative Acknowledgement. This is the negative response to a garbled message or a message with error or garbled by the receiver. This is a kind of request for the retransmission of the message with proper computation by the source, this is one of the conditions for retransmission of message at the time of reception of a message with error.

Outcome of the combination of these above type of messages gives us many more messages depending upon the purpose, serving many functions.

Message Retransmission. This is one of the most important concepts in Insteon technology that serves to increase reliability. The two fields called Hops left and Hop count plays vital role in message retransmission technique.

Hop count is a two bits information field that can store numbers from zero to three in binary form, because messages are encoded with binary digits for digital transmission of the packets. The purpose of this field is to store the value of the maximum number of transmission allowed in a single transaction of the packet between the sender and the receiver.

Hops left field is again a two bit information field capable of storing numbers from zero to three. The value in the field decrements by one count for every retransmission of the packet. Retransmission is done within the limit of the value in the hop count field. The hop left field is initially loaded with the value in the hop count field. After every retransmission, as the value decrements, at one stage the value turns to zero in the hops left field. At this condition the packet is dropped, and there is no more retransmission.

Command Field. There are a lot of predefined commands against each value of the two Byte command field. This field provides additional functionality to the message with the above mentioned functions. Since there are two bytes of size, this field can hold around 65,536 commands for each transaction. The huge number states that, 65,536 commands can be created, but depends on the application of Insteon protocol in each residency. These commands are stored in a database, and at every time the user tries to use the application, the source fetches the command byte from the database.

Cyclic Redundancy Check. This is an important field that validates the correctness of the message. CRC involves a protocol in which first a polynomial is generated, which is called as the divisor. The message bits are called as the dividend. Then binary long division mathematical calculation is computed, which gives us two results, the quotient and the reminder. The reminder is omitted, while the quotient is considered and added as the tail of the message and transmitted, which is redundant information later, therefore the mechanism is called as Cyclic Redundancy Check. The message with the CRC value which is of 1 Byte is received by the receiver. The receiver again performs CRC process with the same message bits as dividend and divisor polynomial. The outcome of the process, which is the quotient is acquired, then checked with the value in the received message CRC field. The value should be the same, meaning the message is correct and can be used to decode the information. If not the message has to be discarded.

Cyclic Redundancy Check is very simple to compute, because it does not involve complex algorithms to fetch the result, it is just a simple binary long division operation. This reason has made CRC mechanism popular and is widely used in various applications

like mobile networks, ATM, telecom systems, and many other fields, apart from Insteon Technology.

Extended Message

The Extended message is same as the standard message except the additional user data field which is of size 14 bytes, making the size of the extended message equal to 24 bytes in total, whereas the standard message is only 10 bytes. The purpose of having the user field is for advanced applications.

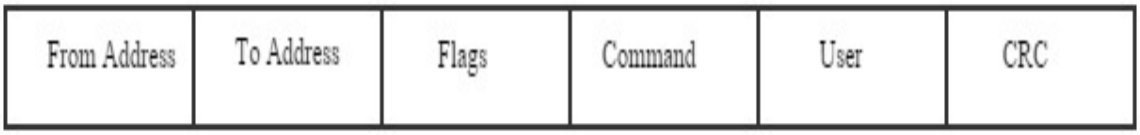

FIGURE 6. Extended message structure.

The table below presents the data size of each field, which is then followed by description of each field.

TABLE 4. Extended Message Field Size

Field	Size in Bytes
From Address	3
To Address	3
Flags	1
Command	2
User Data	14
Error Detection Value	1

The user data field is placed in between the command and the CRC field. Though the user data field is 14 bytes and increases the overall size of the message, the speed is maintained, Insteon is still instantaneous. Most of the below fields are already mentioned above

From Address. This address holds the originators address. All the devices have a unique 24 bit address, the address is burnt in to the device at the time of manufacturing. When a sender sends the message out, the device address is taken into the from address field.

To Address. The destination address of a message. In case of direct message, the actual destination device address is the to address. In the case of broadcast message, the field holds two bytes of device type and 1 byte of firmware version. In the case of group message, the lowest significant byte takes the group ID or number and the rest two most significant bytes take zero [5]. When the data has to be sent to destination, the command and to address can be fetched from predefined database. Here, the to address is the device address of the destination node.

Flags. This field functions same as the standard message, except for the fourth bit position. If it carries one, then it is extended message and if it has zero, then it is standard message.

Command Field. For easy understanding of command field which is of 2 bytes, let us consider the application of controlling a fan. The user wants to switch on the fan and wants to maintain the speed at a particular level also. The first byte of the command field should contain the command to switch on the fan and the second field the desired speed, at the time of encoding the information into the message.

User Data. The user data is the only addition to the standard message that leads to the formation of extended message. This field is encrypted to render a secure and private connection between the source and destination. If the information encoded in the user field exceeds the 14 bytes data field, more Insteon extended messages can be appended. The receiver has the ability to receive and put them together in order using packetizing process [5].

Cyclic Redundancy Check. Since multiple extended messages are transmitted, maintaining the integrity of the message is important. CRC helps in maintaining the integrity of the message and error detection from the message.

The Insteon Packets

Insteon messages are broken up to form packets. Packet structure is different for powerline communication and RF communication.

Powerline Packet

Each packet consists of 24 bits. At the start of standard message packet, there exists a special type of packet called start packet (SP). And the source packet is followed by body packet (BP).

Start Packet. This packet has three subdivisions: Sync bits, Start code bits, Message data bits.

The start packet has initial eight sync bits, which indicates the start of packet and consists of alternate pattern of 1s and 0s as shown in Figure 7. Then follows four start code bits, which indicates the start of message data bits and takes the bit value 1001. Lastly, the start packet has the message data packet, which is of length 12 bits.

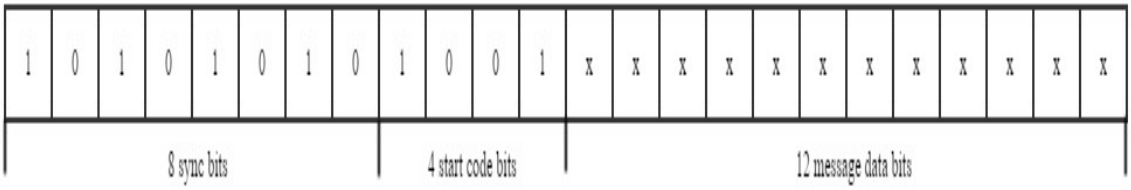

FIGURE 7. Start packet structure.

Body Packet. The body packet follows the start packet.

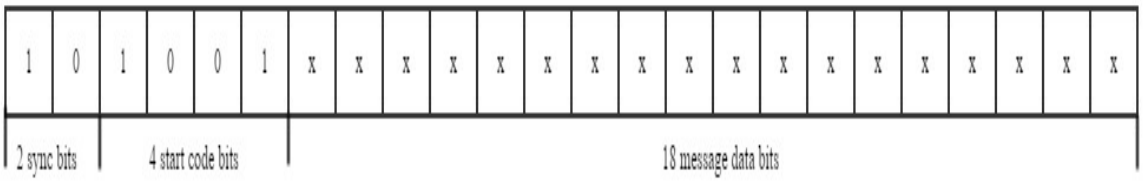

FIGURE 8. Body packet structure.

The body packet has two sync bits, to identify the start of the packet, which has the binary value 10. Four start code bits follow the sync bit and the trailer is the message data bits, which is of 18 bits size.

Powerline Standard Message Packet. The standard message packet comprises of one start packet in the beginning, followed by four body packet. Since each packet is of 24 bits size. The total length of the packet is 120 bits. Start packet has 12 bits of message data and the body packet has 18 bits of message data, therefore ((1 SP * 12 bits) + (4 BP * 18 bits)) yields 84 bits. Considering 80 bits, which is 10 bytes gives us the size

of one standard message. Therefore, as told earlier, transmission of one standard message requires one start packet and four body packet. The total standard packet is of 120 bits or 15 bytes.

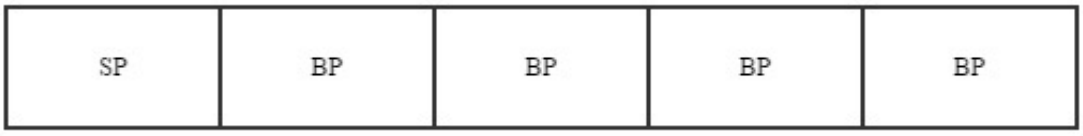

FIGURE 9. Powerline standard message packet.

Powerline Extended Message Packet. The extended message packet comprises of one start packet and ten body packets. As we know the start packet has 12 bits of data message and the body packet has 18 bits of data message, therefore ((1 SP * 12 bits) + (10 BP * 18 bits)) summing to 192 bits, which is equal to 24 bytes, which is exactly the size of extended message size. The total size of the extended packet is 264 bits or 33 bytes.

FIGURE 10. Powerline extended message packet.

RF Packet

Unlike in powerline packet, RF packets are not broken down into start packet and body packet. Due to this reason, Insteon packet sent via RF communication is faster than the data sent via powerline. The RF standard message packet and RF extended message packet is almost same, except the inclusion of data bits, which is 80 bits or 10 bytes in the case of standard data message and 192 data bits or 24 bytes in the case of extended data message.

RF Standard Message Packet. This single packet has two sync bytes that indicate the start of the RF packet, followed by start code byte, which is of one byte size, indicates the start of data message packet, then follows the 80 bits or 10 bytes of data message bits. The trailer attached to this packet is CRC redundant value for error detection mechanism. The total packet size comes to 14 bytes.

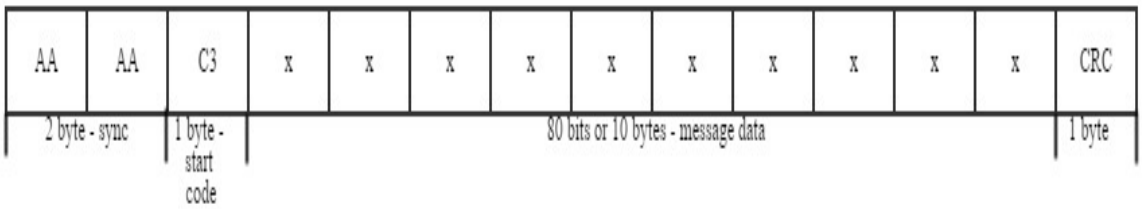

FIGURE 11. RF standard message packet.

RF Extended Message Packet. This again has two sync bytes, which specifies the start of a packet, followed by one start code byte that specifies the start of message data.

The date message of 192 bits or 24 bytes follow and the packet ends with the trailer, which is of one byte that stores CRC redundant value.

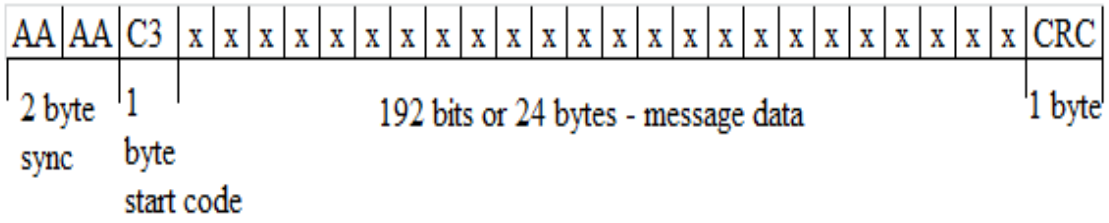

FIGURE 12. RF extended message packet.

The total size of the packet is 28 bytes or in the terms of bits, the size of extended message packet is 224 bits.

Insteon Data Rates

We had come across various types of messages and the primary ones are the standard and the extended type of message. Extended message carries 112 (14 bytes * 8 bits) bits of excess data when compared to the standard one, and sometimes multiple extended messages are sent. Therefore a favorable data rate should be set.

There must also be circumstances at which large amount of multiple data has to be transported spontaneously for certain applications, to achieve this we have Instantaneous data rate, which is 13,165 bits / s. With this data rate, we can send around 49.8 powerline extended message packets in one second and in the case of standard message approximately 109.7 powerline standard message packets can be sent out in a

second. Thus this data rate called Instantaneous data rate is apt for applications that use heavy data messages and demands rapid transmission.

Previously, it was considered that communication via powerline impossible due to heavy loss and noise. Nowadays we have strong error detection and error correction mechanism and modulation techniques which support data transmission through powerline successful, hence development in home networking protocol. There is research going on to provide internet access to the users carried by existing powerline that would provide downloading speed of 14 Mbps and more research to attain the speed of 30 – 60 Mbps using powerline [6].

Now for RF packets, using instantaneous data rate of 13165 bits / s, the standard message packet which is of 112 bits or 14 bytes, with 10 bytes or 80 bits data message, the number of RF standard message packets that can be sent in one second is 117.5 RF standard message packets. For RF extended message packet which is of 224 bits or 28 bytes, with 192 bits or 24 bytes of data message, the number of RF extended message packet that can be sent is 58.7 message packets.

There is also another data rate provided in Insteon home networking protocol, which is called as sustained data rate and the speed is 2,880 bits / s. With this data rate we can send around 10.9 powerline extended data message packets in one second. And in the case of standard message packet type, we can send 24 powerline standard message packets in one second [5].

With sustained speed of 2880 bits / s, 25.7 RF standard message packets can be sent in one second. And in the case of RF extended message packet 12.8 packets can be sent in one second.

From the above information we can infer that, using instantaneous data rate we can send powerline extended data message packet, 4.5 times the powerline extended data message sent with sustained data rate. And in the case of powerline standard message, we can send powerline standard message using instantaneous data rate again 4.5 times the standard message sent with the help of sustained data rate.

Considering RF standard message packets, with instantaneous speed, we can send RF standard message packet 4.5 times the RF standard message packet sent using sustained speed of 2880 bits / s. Similarly with RF extended message packet, with instantaneous speed, 4.5 times the RF extended message packet with sustained speed can be sent.

Instantaneous data rate is faster than the sustained data rate, though sustained data rate is actually fast. Thus analyzing the data rate we can come to a conclusion that Insteon Technology is faster and can operate and respond to applications much faster in about 0.04 seconds.

Insteon Devices

Device Function

Primarily the Insteon devices can function as following types: Controllers, Repeaters and Responders. These simple device functions enable Insteon home-control network protocol to work without any impediment.

Controllers. The function of a control is to transmit data, therefore it's an originator or a source or a sender. The controller's task is to get the destination device address from the database and apply the same into the to address field and simultaneously adding command from the database into the command field as per the request by the user.

Before this process, the node adds its own device address into the from address field. Other formalities to build the data packet take place. Once the packet is formed it is set out to reach the destination from the controller.

Responder. The responder is nothing but the destination host. It receives the data packet sent out from the controller and decodes the packet to get necessary information to operate specific application. The to address in the data packet is the device address of the responder.

Repeater. Repeater plays a vital role in the Insteon protocol. It is an intermediate between the repeater and the responder. Sometimes there might not be an involvement of Repeater during message transmission, only the controller and the responder can carry out transmission of data packet. There is a limitation on the number of repeaters an Insteon message can be passed. This condition limits data flooding and creation of loop in the network.

In Insteon network any device can act as a controller or a repeater or a responder, which means the device can work as responder, repeater and controller, irrespective of whether the device is dual band device or only RF device or only powerline device. Therefore there is no master slave communication, whereas Insteon technology exhibits peer to peer communication.

Figure 13, demonstrates simple direct message transmission between a controller and the responder. This type of communication is possible, when the responder is just one step away from the controller. Figure 14, whereas consists of the intermediate device or the repeater. This type of condition occurs when the responder and the controller are faraway, hence require repeater to help transmission of the data.

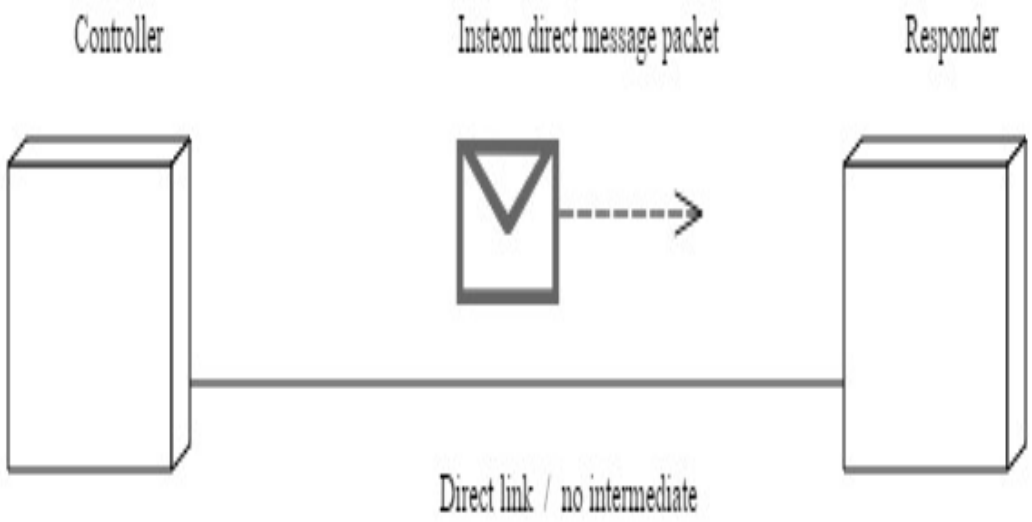

FIGURE 13. Simple insteon network device function without a repeater.

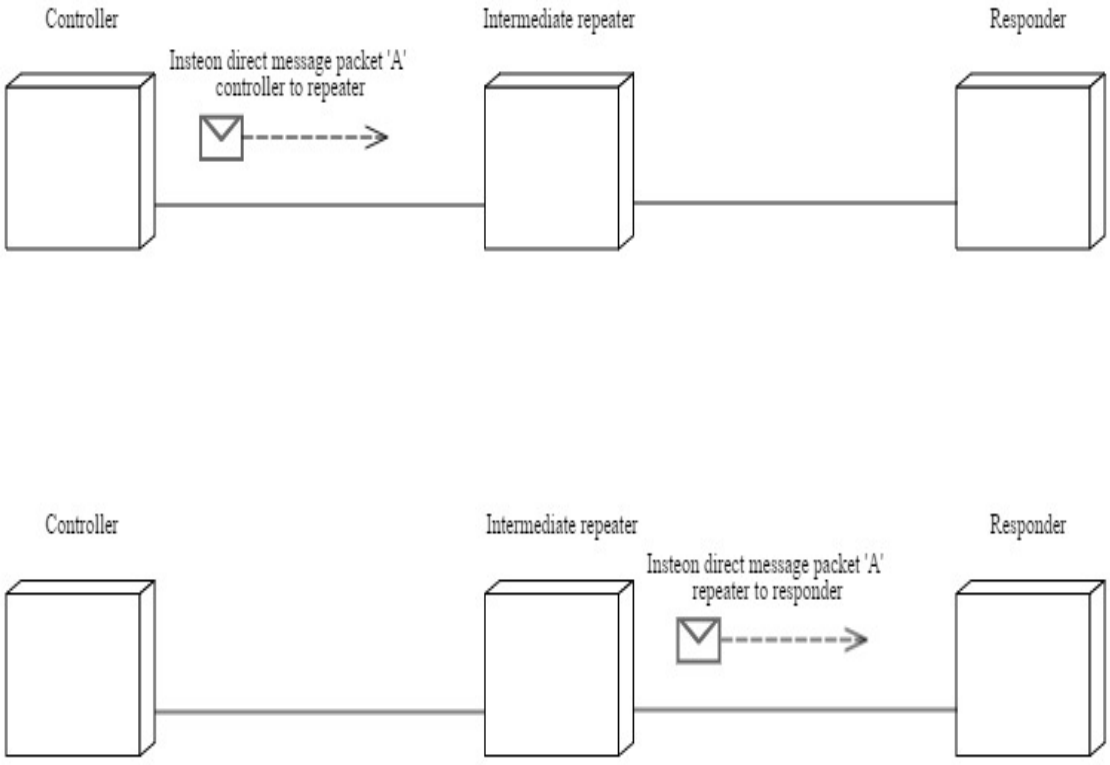

FIGURE 14. Insteon network with an intermediate repeater.

Insteon Device Hardware Requirements

A normal Insteon device or module that is capable of switching on or off appliances should have some memory to run the system. Therefore the RAM memory size is of 256 Bytes. The memory that stores operating system to run the system is Flash memory and is of size 7 Kbytes. The memory that stores configuration and loads, when the system switches on is EEPROM and is also of size 256 bytes.

Installation of Insteon Devices

Installation is very easy, and no specialized engineer is required, users themselves can perform the installation process. Because it is just plug-in and tap-in or wire-in process. After connecting the device to the ports, the set button is to be pressed and in seconds the device joins the network [5].

Powering Insteon Devices

We know Insteon devices are some wired and wireless. Wireless devices that communicate via RF are battery operated. Whereas the devices that can communicate with the devices via powerline are powered with regular residential power supply, step down to required voltage.

Frequency of Operation and Modulation technique

If the device supports RF communication, to communicate devices wirelessly, the frequency of operation is 915 MHz. The modulation technique used in the communication is Frequency Shift Keying (FSK).

In wired communication, the wired devices communicate over powerline using the frequency 131.65 KHz. And the modulation technique is Bipolar Phase Shift Keying (BPSK).

Security in Insteon Devices

The security in Insteon communication is carried out by encrypting Insteon messages. Address masking is a concept of identifying by means of segregating data packet, this is adopted by Insteon technology, which provides some level of security.

Platform for Development of Application

The software to build and run Insteon application in Insteon devices is taken care by Integrated Development Environment (IDE). IDE is used for simple software creation; IDE consists of program code editor, a debugger and an automation tool to build the application. IDE makes a programmer's work easier.

Insteon Signaling

We know that Insteon devices can communicate wirelessly or through wired medium, with the help of RF or powerline respectively. In this section we are going to study about signaling techniques used in RF and powerline communication. A signal is a physical parameter that carries information between sender and receiver. Therefore the signal has to be generated depending upon the information to be passed or otherwise defined as encoding information in the form of bits into signal, which varies depending upon RF and powerline.

Powerline Signaling

Insteon uses existing wired powerline connections to transmit data. The powerline voltage is at 110 v and at 60 Hz frequency. At every zero crossing of the powerline signal, Insteon data is transferred. This is done by a signal to the powerline signal at zero crossing. The signal which is added is of peak-to-peak amplitude of 4.64

volts and the carrier frequency used is 131.65 KHz with modulation technique Binary Phase Shift Keying (BPSK).

Binary Phase Shift Keying is the concept of varying the phase of the signal depending upon the bits of information. Here, each bit of information is represented with 10 cycles of the signal.

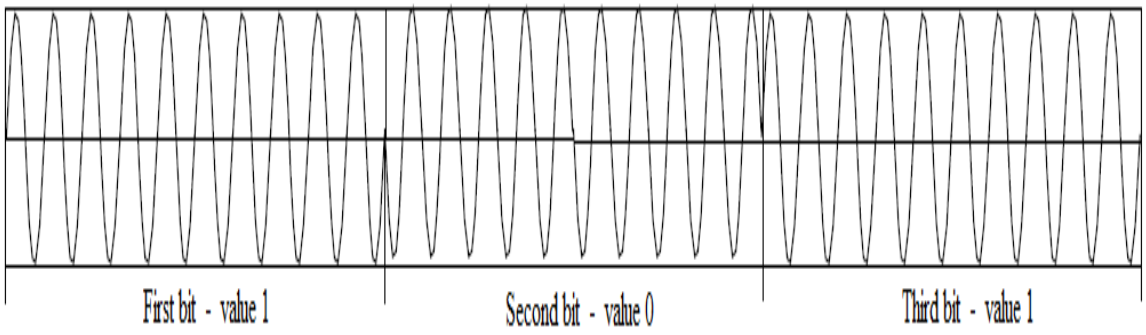

FIGURE 15. Simple BPSK modulation with dissimilar bit values.

As we can see in Figure 15 above, there exists 10 cycles representing each bit. Bit value 1 is represented with the phase starting at the positive side of the graph, next is the bit value zero, which is represented with the signal phase starting at the negative side of the graph. And finally the bit value 1, again the signal phase starting from the positive side of the graph.

Generally in BPSK, the signal phase changes with the change in bit value as shown in the following Figure 16.

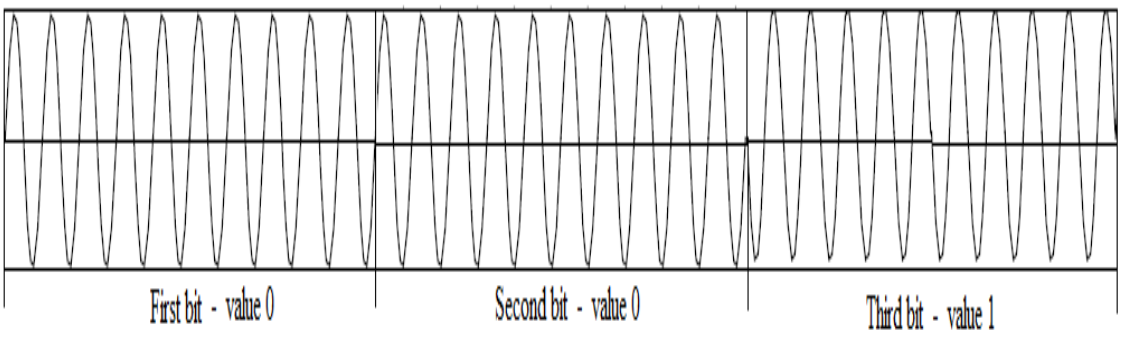

FIGURE 16. BPSK modulation with similar continuous bit values.

Here, the initial bit starts with positive phase representing the bit value 0, this bit is followed by another bit value zero, which is again represented by signal starting with positive phase. Then the bit value 1 is represented with the signal starting with negative phase. Therefore from this we can infer that, change in bit value alone will change the phase of the signal, otherwise the phase is the same for all similar continuous bit values. This type of bit coding technique is called Non-Return to Zero (NRZ).

There is an abrupt phase change, while encoding the bits to signal; thereby a high frequency component occurs in the output signal. This can be avoided by gradually changing the phase of the signal.

Insteon message packets are sent in at the zero crossing of the powerline only, because at high amplitudes, there could be noise that could disrupt Insteon packet. We know that the center frequency is 131.65 KHz, there are 24 bits in a single Insteon packet, and each bit takes 10 cycles to reach the destination. Therefore, 240 cycles are required to send a single Insteon packet. With the center frequency 131.65 KHz, the time

period is 0.007 ms. And totally for 24 cycles to carry one Insteon packet, it takes 1.823 ms or 10823.0 µs (24 cycles * .007 ms). The information is embedded into the signal as follows.

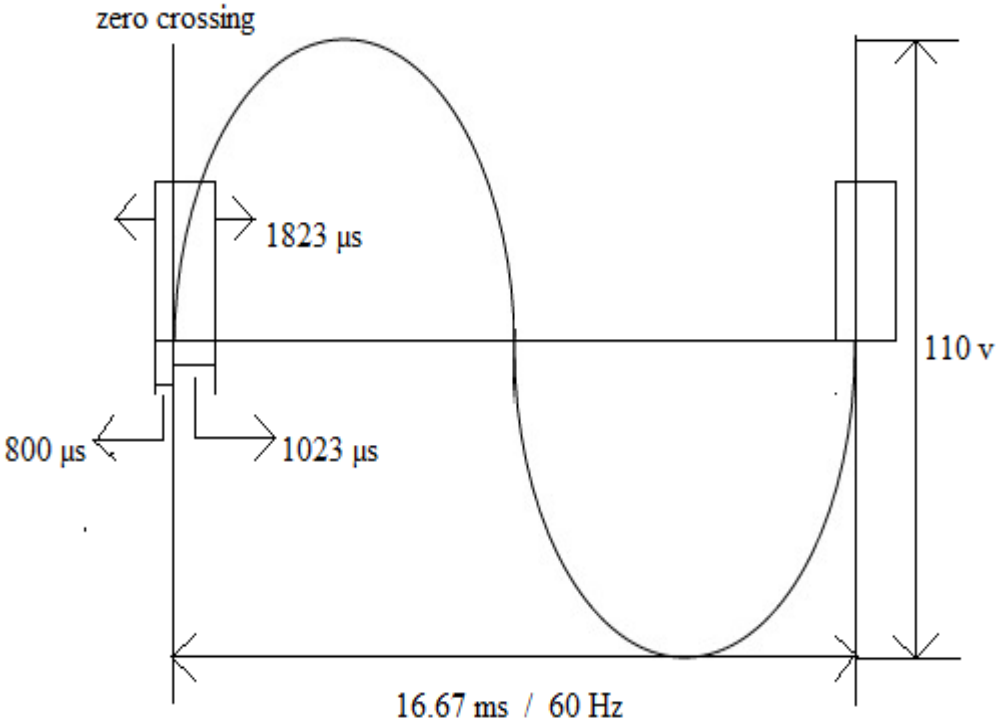

FIGURE 17. Powerline signal with Insteon packet timing.

From the above Figure, we can notice that the Insteon packet starts 800 µs before the powerline signal and it transmission goes till 1023 µs, therefore completing one full packet transmission of 1823 µs. The most important fact that lies in this concept is X10

compatibility. X10 message packet takes 1023 µs to be transmitted to destination. After the powerline signal reaches zero, both Insteon packets and X10 packets take 1023 µs to complete the transmission. Therefore, from this we can understand that both Insteon and X10 technologies are compatible and Insteon technology is actually backward compatible.

To transfer an Insteon standard powerline data, we know that one start packet and four body packet, so totally five packets are required. While sending the next data, which requires again five set of standard powerline message packets, single zero crossing of the powerline is not considered for transmission of the packet. Therefore, the next zero crossing is used to send the next set of packets, instead of taking immediate powerline zero crossing.

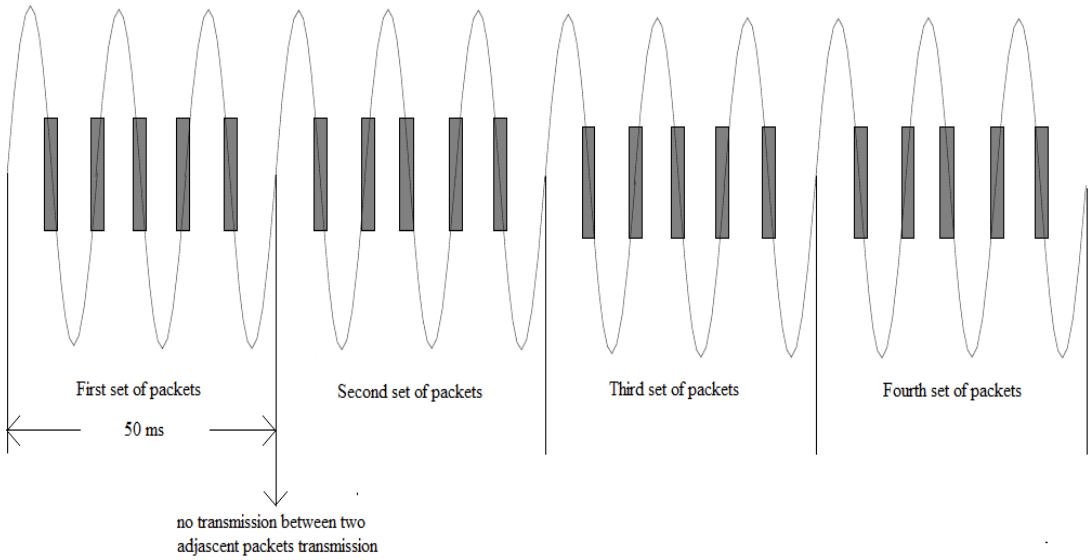

FIGURE 18. Standard powerline packet transmission.

To transfer five packets of standard powerline data, total time period of 50.01 ms is required as shown in the above diagram. Totally six zero powerline crossings are used to transmit the powerline standard packet.

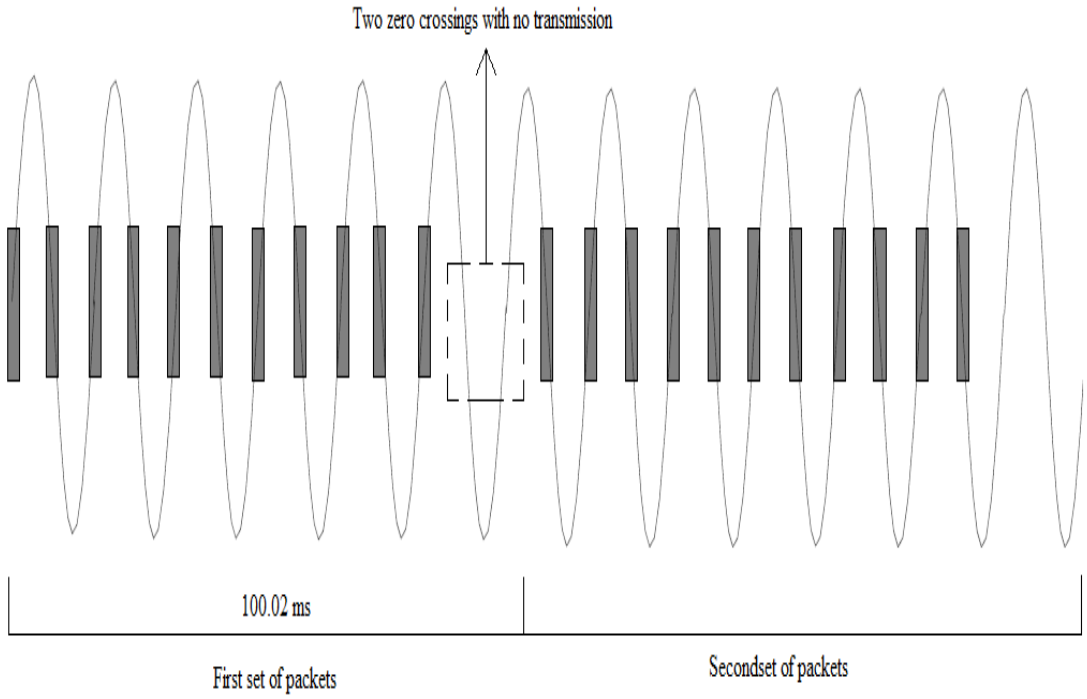

FIGURE 19. Extended powerline packet transmission.

Considering extended powerline message packets transmission, totally 11 extended packets of data are sent using 13 zero crossing, two zero crossings are left without any transmission intermediate of two packet transmission. The total time period required to transfer the extended powerline packet would be approximately around 100.02 ms.

CHAPTER 4

INSTEON COMMUNICATION

Powerline Communication

One of the means that Insteon devices communicate each other is via powerline communication. The powerline cables are generally used to provide electricity to residential and commercial buildings and we also know there are many modulation techniques to transport useful data modulating it to suit the original signal of the medium. Taking the advantage of these two concepts, the method of sending required data through a powerline implying certain type of modulation, thus found its application in many domains and especially this type of communication protocol is very much suitable method in home control networking protocol, because this does not demand for installation of a new wired infrastructure.

The powerline communication takes place by producing a signal called carrier that depends upon the information to be transported. This carrier signal should not go below 60 Hz, because the powerline signal operates with 60 Hz frequency.

Classification

Depending upon the frequency band, the powerline communication is grouped into two types:

Narrowband Powerline Communication

The frequency range of operation is between 3 KHz and 500 KHz and speed in the ranging 100s of Kbps. In this type of powerline communication long distance data transmission is possible with the use of repeaters.

Broadband Powerline Communication

This type of communication takes place in short distance data transmission, while this method of communication takes the frequency range in MHz range and provides data rate within Mbps range.

Generally, Narrowband communication is implemented in almost all the applications. This is also used in Insteon home-control networking protocol, though the system involves short distance communication, the data rate and the frequency of communication is well suitable for the application.

Communication Model

The basic communication process flow at the sender end is as shown in the Figure 20 below.

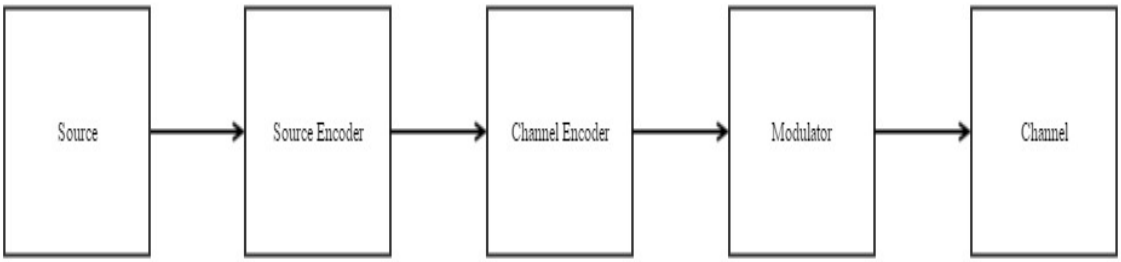

FIGURE 20. Powerline communication source.

Source

The source here should be in digital form. If the output of the source is analog, then the signal has to be digitized using converters and is sent to the next step.

Source Encoder

Here compression of the digital bits takes place. This avoids sending high volume of bits by removing redundant bits.

Channel Encoder

Here, error detection mechanism is applied to compute the useful redundant bits that carry the information of the result obtained from CRC process and used later at the receiver end.

Modulator

Now the digital processed signal is fed into the modulator to convert it into analog signal called carrier signal and made suitable for transmission over the powerline. Some of the modulation techniques that can be used are BPSK, FSK, GFSK, etc. In Insteon as already mentioned earlier BPSK is used, because of its simple method of generation of the signal.

Channel

This is the medium of communication. A channel could be wired or wireless, but in powerline communication the channel should be definitely a wired one, where the channel carries both powerline signal and Insteon data.

The receiver has the following blocks, which is the reverse of the source end process.

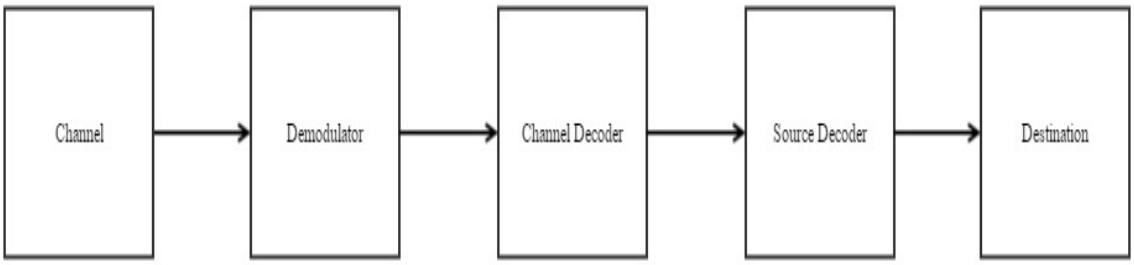

FIGURE 21. Powerline communication destination.

Demodulator

The demodulator is responsible to convert back the analog carrier signal to its digital equivalent and appropriate for further process.

Channel Decoder

Here error check process takes place. The result is compared with the redundant CRC bits from the received signal, if both match the received bits are error free and gains entry to the next level of process. Otherwise the received message is considered to have error and dropped and NACK is sent to the sender notifying the disrupted message containing error.

Source Decoder

The decoder decompresses the received signal to gain the original signal. Data compression should be performed such that there is extraction of lossless data.

Destination

This is the end point of powerline communication. The digital bits are delivered to device to decode necessary information.

Multihop Data Transmission in Powerline Communication

There are many multihop transmission in powerline communication in which some of them are explained below:

Incremental – Redundancy (IR) Multihop

If the powerline signal with data is transmitted, all the devices in the link will receive the message. After receiving the data, the nodes retransmit, and then all the adjacent nodes receive the message again. This happens multiple times, and each device receives multiple copies of the source data. Now it seems that more than once the same data is received simultaneously. This fact is actually advantageous, because by receiving more than once the same data, the device could apply various combining strategies, wherein the best suitable signal is transported, taking into account various factors [7].

With the above multihop retransmission technique, there are a few ways to choose one relay technique, which is discussed as below:

Fixed (Fi) Selection. In this method of choosing a relay route is by assigning dedicated nodes as retransmitting node. Only the assigned nodes in the multihop track can retransmit and others cannot. The retransmitting node should be placed in the way such that, its placement is between the source – destination path evenly, such that signal attenuation in minimized [7].

Channel Adaptive (CA) Selection. In this process of determining retransmitting device, a metric value is calculated at each node. The link rate depends upon metric calculation. The node that possesses maximum metric value becomes the next retransmitting node. In this type of technique, different nodes take up the responsibility of retransmitting at different time. Here, there is no specific node selected to retransmit, which might be a burden of retransmitting to one single node as in the above method [7].

Automatic Repeat – Request (ARQ). This method is an automatic self – detection process. Here the node that first receives a source signal and that could decode information properly, requests to become the next retransmitting node. The node that successfully decodes the information tends to send the acknowledgement first and this is how the node takes the responsibility of becoming the retransmitting node.

Timeslot Synchronization

This is the technique used in Insteon home control networking. The time period to send all the packets in the powerline is called as timeslot. Therefore fixed timeslots exists in this protocol. Taking advantage of this concept, multihop transmission is introduced in this protocol. Each devices either transmits, retransmits or send acknowledgement at each timeslot. If one device starts sending a message all the other adjacent devices will just listen and do nothing. In the next timeslot, the immediate adjacent device goes into the retransmitting state. Similarly for every timeslot the function of a device varies and successful retransmission is possible. With this method the devices do not retransmit the message every time they receive a packet from any node.

The advantage of this method is that we can avoid to certain extent the retransmission of the message every time slot by every devices, this in turn avoids flooding in the network.

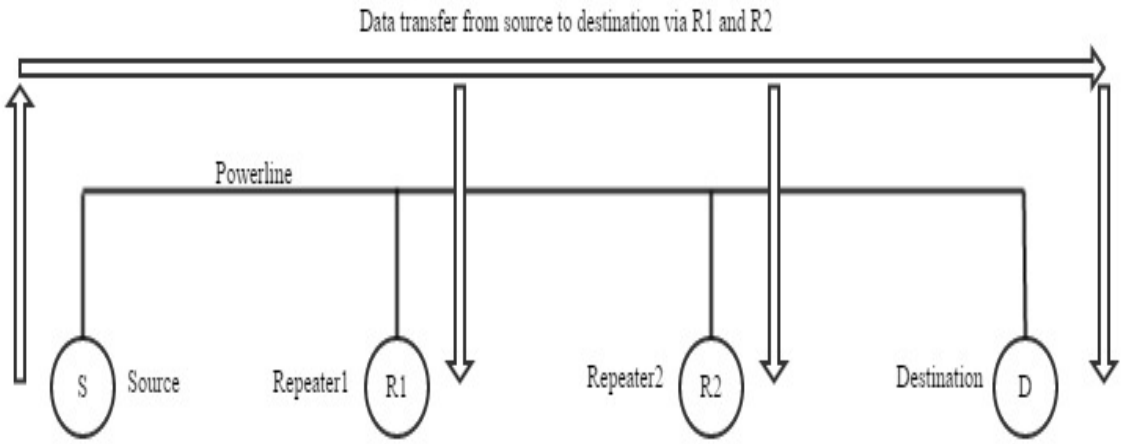

FIGURE 22. Simple multihop demonstration.

The source tends to send information to the destination, in the path the packet has to traverse through the other two nodes in between, which are the repeaters. Initially once the data leaves the source, the data is received by all the other nodes in the path, because the data uses powerline communication to travel. Now if all the devices receive the message, the received message is repeated again and there is no account of how many times the message is repeated, this situation leads to the flooding of message in the network. This problem is fixed with the introduction of timeslot synchronization concept, to avoid flooding. Where at the first timeslot the source sends the data, later in

the next, R1 retransmits the data and other devices, though they receive data, they do nothing and are in just listening state. In this way the data propagates and reaches the destination.

Attenuation Characteristics of Carrier in Powerline Communication

The major attribute of the powerline communication is that the carrier amplitude faces serious distortion with respect to distance and frequency. To measure the attenuation characteristics of the carrier the expression that can be used is

Attenuation = 20 log (Vr / Vt)

Where, Vr is the voltage value of the carrier received, Vt is the voltage value of the actual carrier voltage transmitted and as said before in Insteon protocol the carrier voltage is equal to 4.64 v.

Practically as the carrier voltage suffers serious distortion as the message passes through each node, the researchers term it infeasible to send direct message to the nodes [8], so it is a compulsory need to have many nodes between the sender and the receiver, such that the intermediate nodes as repeaters to energize the carrier and step up the carrier voltage each time the repeater receives and send it towards the receiver. In this way there will be successful transmission.

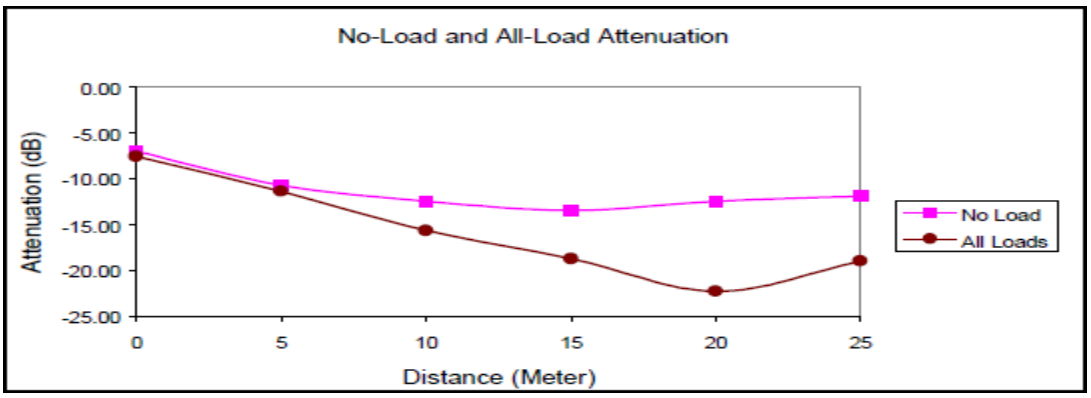

FIGURE 23. Sample attenuation characteristics in powerline communication.

The graph shows a signal is degraded as the length increases due to high rate of attenuation whether load is connected or not. In some parts of characteristic curves, we can notice some rise of curves, the reason for this condition is due to the intermediate nodes repeat the received signal [9].

Advantages of Powerline Communication

1. Additional wiring to setup the network and the devices is not required. This protocol takes the existing power transmission cable to transport data embedding the information into the power.

2. The devices involved are very simple. Installation and maintenance is very easy and requires no trained personals. The method of installation is just plugin and use, which attracts users.

3. Fast internet connectivity can be provided at any nook and cranny of the house, by passing internet signals over powerline and without the requirement of separate

Ethernet cables. This type of communication is actually faster and reliable than wireless internet

4. Powerline communication can involve encryption to secure the data passed over the powerline cable.

Limitations of Powerline Communication

1. As the current passes through the powerline cable conductor, magnetic field is produced. This could interfere with the carrier signal carrying the data that would lead to the distortion of the data.

2. The information could be subjected to various noises, traveling in the powerline conductor, because the cables used are high voltage carrying cables.

3. Though the technology is very advantageous in various aspects, it suffers standardization issues. Many technologies like ZigBee, Ethernet and all the computer communication related protocols have a proper standard, whereas powerline communication faces a serious issue of standardization.

Applications of Powerline Communication

1. Powerline communication can be deployed to offer high speed internet at homes and offices. Since powerline communication does not demand for new wiring and infrastructure, this advantageous factor can be used to install WiFi hotspots facility in public places to provide internet connection to the people, therefore this could help the user to be connected to the internet always to share their moments, internet message, video and voice calls, and use all other resources from the internet. Therefore this will increase internet users.

2. House automation is the next immediate application. To control each and every device in the house from a distance, powerline communication is the best suitable technology to implement.

3. Home security which is also a part of home automation, but considered as a separate section, because more applications and product are unavailable in the market to provide complete security at homes and offices. Therefore many applications with regards to this have to be developed.

4. Automatic Meter Reading is another application and the best in the field of automation. In certain parts of the world, there is still the practice of humans that visit each home to record the electricity meter readings to calculate the price for electricity usage in each individual house, but using Automated Meter Reading could ease this process, wherein from a distance the meter reading of the power consumption is recorded.

5. PLC can be also used airfield runways to light the runway path for the visibility that can help taxing the aircraft [8].

These are the basic applications, apart from these there are a list of applications and many more in the process of development.

CHAPTER 5

IMPLEMENTATION OF GRADIENT BASED ROUTING IN PLC

Need for Gradient Based Routing in Insteon Protocol

The existing protocol in Insteon is capable of handling small size networks. The addition of more devices in order to expand the network and its functionality with existing protocol is infeasible; therefore a simple and efficient protocol capable of routing data packet to the right destination is to be implemented that satisfies the dual band nature of Insteon protocol and overcome the short come of scalability in the existing Insteon protocol.

The existing protocol allows packets to be just broadcasted through all the links available. This might lead to collisions due to flooding in a larger network; hence this is the main factor that prevents the existing protocol to be implemented in a larger network.

With the implementation of gradient based routing in Insteon protocol, we can add more devices to the existing network and increase the size of network and the data transfer is made easy without any loss and most importantly controlling collision due to flooding. The existing protocol allows only three retransmissions, but in the proposed protocol gradient value decides the retransmission value to reach the end device which would be located farther from the transmitter may be more than three hops away from the transmitter in a larger network. Therefore this method overcomes the concept of allowing only three retransmissions in the network as in the existing protocol, which is

apt in the existing smaller networks. The novel protocol also facilitates the hub to identify the link on which the end device is located. This protocol is implemented in RF Communication [10], and changes are made to implement in PLC in this thesis.

The existing protocol which usually transmits data to the destination through all the available links to, this phenomenon is called as flooding. The advantages of flooding are that there is no computation of complex routing protocol that could cause delay in data transmission and if there is any change in the network the data would be transmitted reliably to the destination [8]. The major disadvantages due to flooding is loop creation as the data passes through all the available links and same data would be sent through the link it received such that the sender receives the same. Flooding also leads to serious issue of collision. These serious issues can be overcome with the help of the proposed protocol.

There are various protocols that avoid collision of packets in the network [11]. The protocol defines the selecting back off window depending upon the contention window size. The purpose of contention window is to compete with the other nodes to select the link to send the data packets and back of timer is used to prevent the nodes from choosing the same time slots to send the data packets. But our proposed protocol is modeled to reduce collision and aids effective routing in the links which is not explained in [11].

There are also protocols that calculate metrics to identify the best path to reach the destination node. The metrics defined are distance and channel state indicator [12]. Distance metric defines how far the destination node is available. The other metric is calculated by first initializing a variable to zero and a serious of sequential packets are

sent from the corresponding node. If a node receives these special packets sequentially in order, then the variable value is increased and affirms the path to be lossless and trusted path and if a node receives the packets not in sequence, then the variable is decreased, the path is not considered for transmission. This protocol leads to transaction of many routing packets that increases the traffic and congestion [12]. At cases with same distance and same lesser variable value then the confusion of routing to choose the best path arises.

Apart from metric determination one of the protocols is based on transmitting route request packet to determine the route [13]. The route request packet contains the following field: source, destination, unique identifier and route record. A node checks first for its address in the route record field whenever the node receives the route request packet. If it finds its address in the field then the packet is dropped in order to avoid routing loops. Then the unique identifier is checked whether the same packet is received earlier, if it had received it then again packet is dropped to avoid duplication. If the node finds both route record and the unique identifier is good, the node proceeds transmitting the packet to the neighboring nodes. This protocol is complex in terms of the route record field, because as the nodes in the path increase, the route record field has to store all the nodes available in that path.

The tree based protocol [14] also discusses level based routing where the hub is considered to be in the level zero and other nodes in the level two, in this way nodes take levels. But the protocol fails to define to check the status of the master by slave, scenario of a node at a particular node is dead or added and what happens when an end device is added. This is solved and produced in the gradient based routing.

Gradient Based Routing Protocol in PLC

The protocol can be expounded in three stages:

1. Network formation
2. End device addition
3. Information exchange

Network Formation

The first stage is the most important and multistep process starting from broadcasting Beacon Packet (BP) to form the actual network, then maintaining the network by sending out Parent Status Query (PSQ), then finding out the parent using Parent Discovery (PD) packet, to add new node New Node Addition Packet (NAP) is used and as a result Forced Beacon Packet (FBP) is used to change the gradient value of the lower nodes. This phase deals with the formation of main network.

Beacon Packet (BP). This is the initialization phase in this stage, where the hub starts the broadcasting of BP. The BP consists of following fields like packet type, sender ID or address and the gradient value. The important condition applied to this packet is that this packet is allowed only one retransmission.

Firstly, the beacon packet is broadcasted through all the links by the hub after increasing the gradient value by one and sender ID as its own ID. All the nearby nodes receive the BP because the retransmission is only once, the nodes take the gradient value and the parent ID as the sender node ID, and here hub ID is considered as the parent. The most important step after receiving BP is that every node updates its Link Database. The nodes enter from which node it hears the BP, so in the link1 column it stores the parent ID. This link defines that the node can reach the hub via its parent and through particular

link1. After the gradient value is also updated, the node increases the gradient value by one and broadcasts.

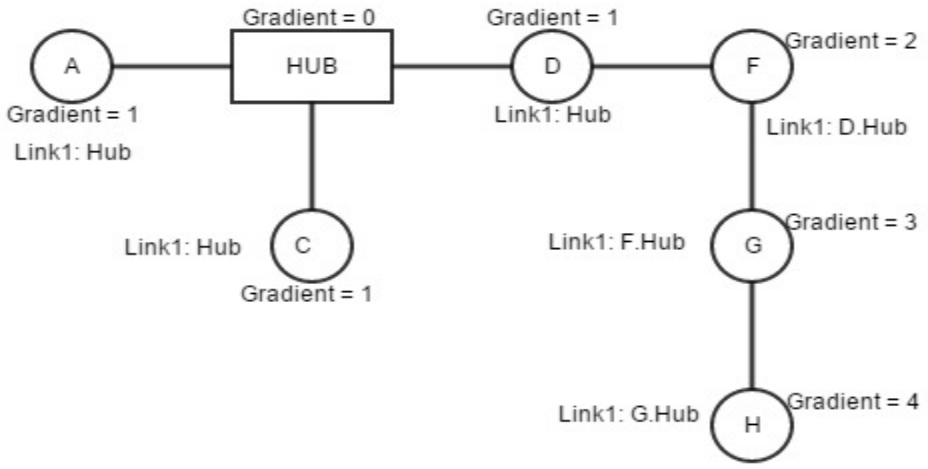

FIGURE 24. BP demonstration.

According to the above figure, Hub sends the BP first and is in the gradient level zero. The hub increases the gradient vale by one and sender ID as its own ID and broadcasts the BP, the nearby nodes which are A, C and D and lie within the rage of acceptable carrier voltage level1. The retransmission here is always once. Now A, C and D update their link state databases as entering the parent ID against Link1, here these nodes enter as Hub. Then the nodes take the gradient value, increase the gradient value by one enter their ID in the sender ID field and passed down to the other links except the Link1. Now from D, F receives the BP. F does the following, first updates the link1 of

link database with its parent ID, here F updates its link database as Link1: D.Hub, which describes that there is a hub and can be reached via Link1 through its parent D and takes the gradient value one. Now increases the gradient value by one and changes the sender ID as its ID and sends the BP to the links other than Link1. G receives and does the same as above, in this way the network is formed. G has the link state database as link1: F.Hub, similarly H has the link database as link1: G.Hub.

Parent Status Query (PSQ). The purpose of this packet is to enquire about the parent's state of a node. This packet is sent periodically. If the parent is alive, it means that there is a possibility to reach the hub and if the parent is dead, the node has to find its parent immediately, such that there could be a way to reach out to the hub.

The PSQ packet has the following fields: Packet type, Parent ID. Even this PSQ has only one retransmission and sent through link1, such that only the parent hears the PSQ. In response to the PSQ, the parent sends the PSQ Response packet.

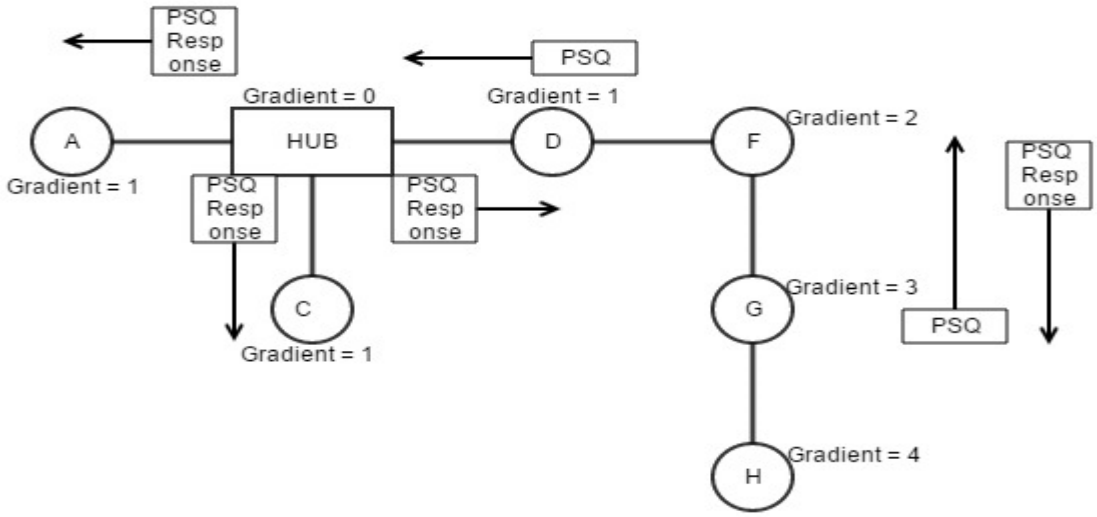

FIGURE 25. PSQ demonstration.

If all the nodes of that parent receive PSQ response as in figure 25, the nodes learn that the parent is alive and postpone the next PSQ interval.

Parent Discovery (PD). Parent discovery is the process of finding a parent, because a parent is the way to reach the hub. This process could occur in the following cases like:

1. When the node hears no PSQ response of certain period of time
2. When a node has no parent for certain period of time

The packet consists of the packet type and sender ID fields. The retransmission is only once here, because the next immediate node should hear it consider it as the parent. If there is no response for the PSQ sent, then the node understands that its parent is dead, so it should look for another node as parent in order to reach the hub and maintain the topology of the network.

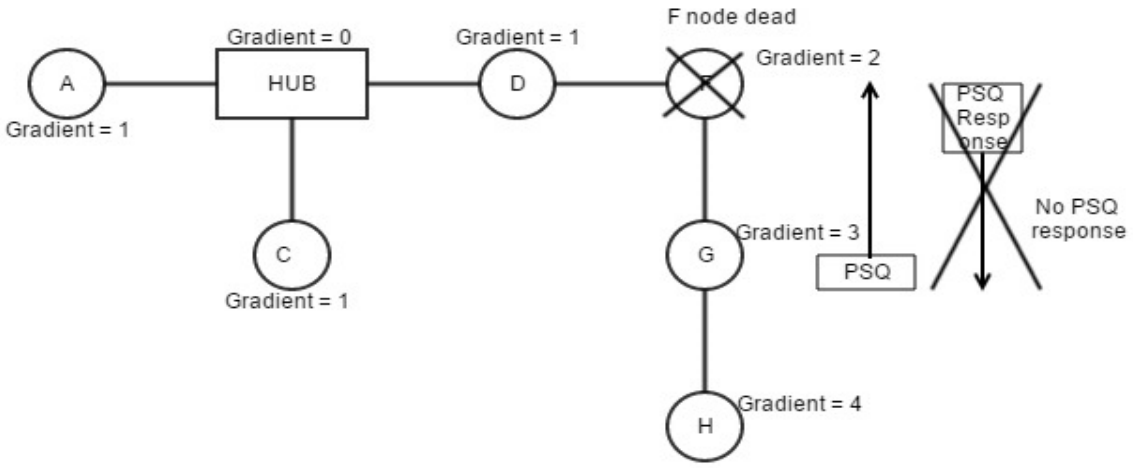

FIGURE 26. No PSQ response.

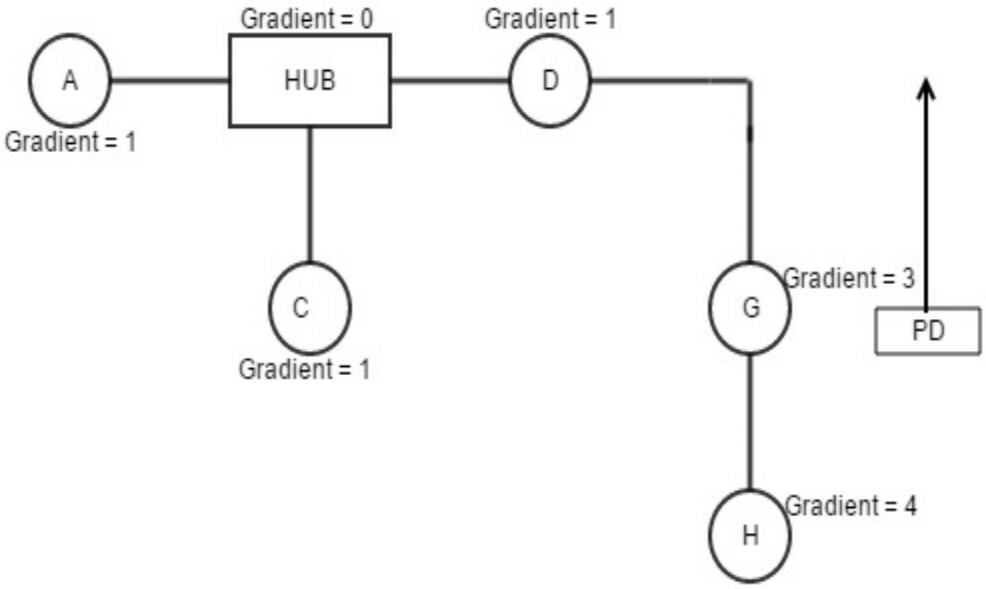

FIGURE 27. PD packet transmission.

Having identified that G lost its parent, it goes into the phase of identifying a new parent. G sends out a PD, the node H will initially hear it and remains silent because G is its parent and H cannot become the parent of G. At this stage G waits from the other link too, if it does not hear anything it will increase the carrier voltage level and send such that D hears it, once hearing it locks the voltage that it can hear, then responds the PD by sending out BP. G will receive the BP and updates the link state database, saves the gradient value as two and parent ID i.e. node D's ID. G has the link state database as link1: D.Hub. Hence G has got a new parent.

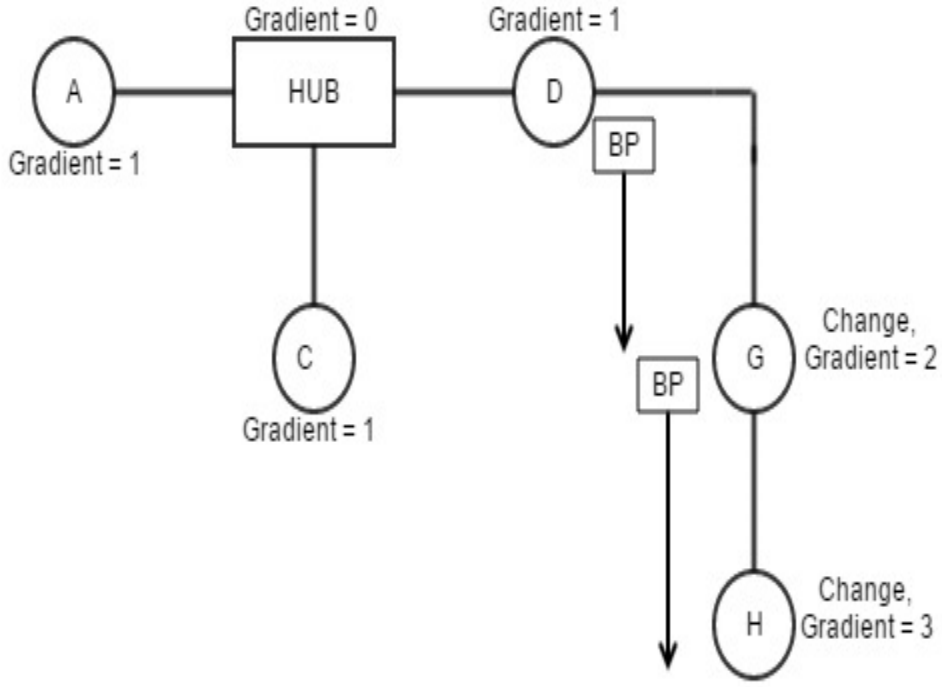

FIGURE 28. BP response to PD.

After updating the information, G then increases the gradient value by one (here three) and includes sender ID as its own ID and sends the BP to the other link such that the other nodes in the link make changes accordingly. Now H hears the BP and notices that the gradient value is lesser than it contains, so updates the link state database as Link1: G.Hub.

New Node Addition Packet (NAP). This packet is sent out whenever a new node is added and pressing the set but triggers the packet. The packet consists of packet type field and Sender ID. The retransmission is again only once. When the new node is

added and after pressing the set button, the NAP is sent, the purpose is to find the parent for the new node. The response to this node is Forced Beacon Packet.

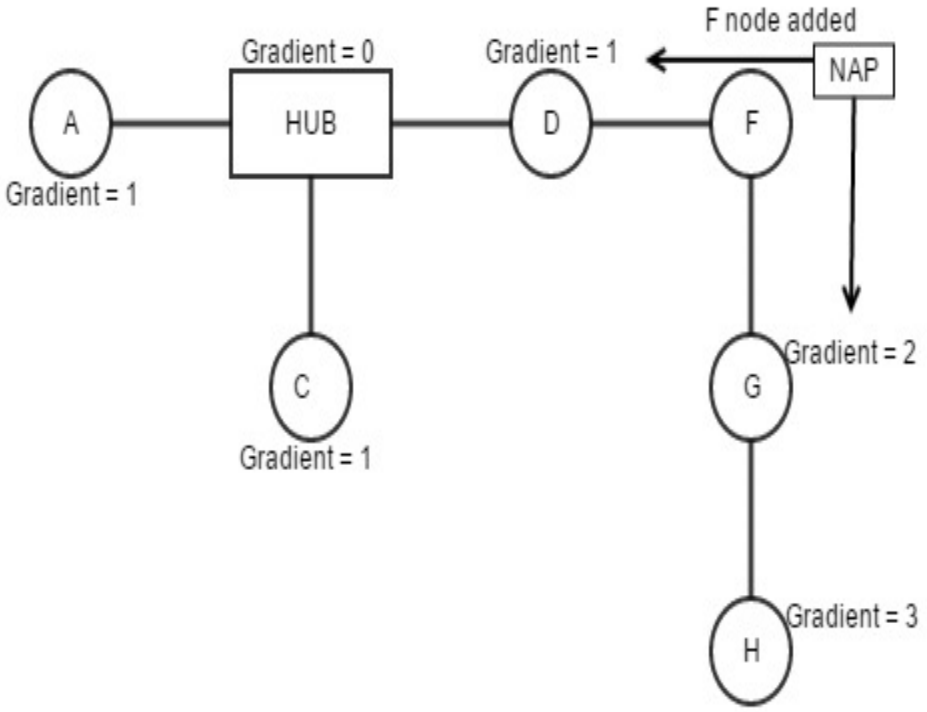

FIGURE 29. NAP demonstration.

Here node F is added again and set button is added. F sends NAP though all the link. When G receives it through link1 it understands that there are changes in the link and parent so waits for future packets. When D receives the packet it understands that there is a new node added below it so, sends another packet discussed below to make changes in the network accordingly.

Forced Beacon Packet (FBP). FBP is the response to the NAP. The FBP consists of the following fields Packet type, sender ID and gradient value. Once a node receives the NAP and according to the conditions discussed above in NAP section, it constructs FBP and sends through the link it receives and the receiving nodes by default change the gradient value and the parent.

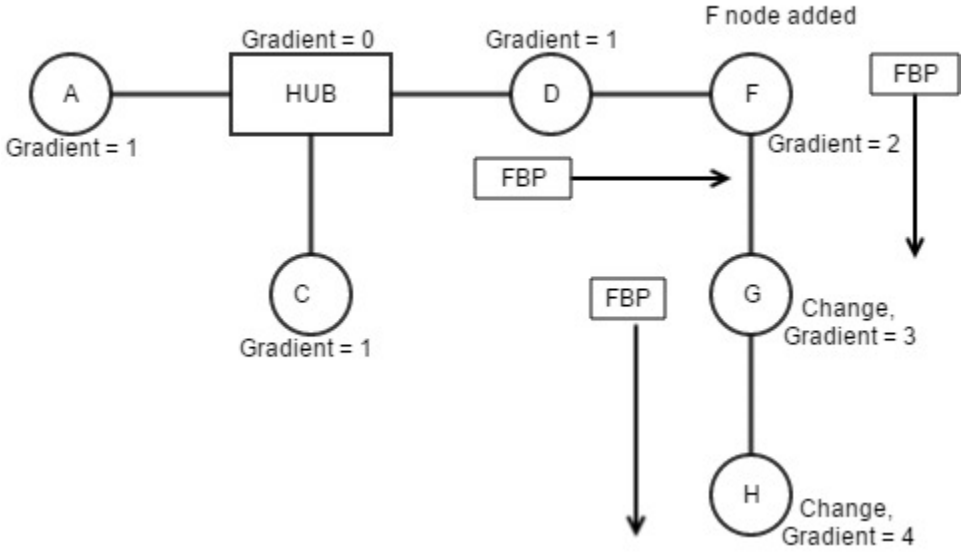

FIGURE 30. FBP demonstration.

Here F node is the new node added, the node sends the NAP after the set button is pressed. D responds to the NAP with the FBP that contains the gradient value and the Sender ID. F receives the packet and updates the ink database as link1:D.hub also changes the gradient value. Now D constructs the FBP by increasing the gradient value

by one and sender ID as its own ID and sent through the other links and not through the link1. G receives FBP changes the gradient value forcefully and without any condition, G takes F as its parent. This happens with H also, where G is taken as the parent and gradient value as the value in FBP. Respective link state databases are also updated.

With the discussion of FBP, we have reached to the end of the network formation phase, which is the first phase. Next is illustrated how the end devices are attached and made known to the hub for data transmission.

End Device Addition

This is the second phase of the protocol. This stage explains the process of addition of an End device. This stage involves transmission of End Device Join (EDJ) packet that inform the intermediate nodes and the hub about the addition of the end devices like bulbs, lights, cameras, leak, motion and gas detectors and other Insteon devices available.

End Device Join (EDJ). Each device has a unique address or ID, once the device is attached to the module or the node, which has already formed a network, that has a parent and the path to reach the hub as discussed above, the addition of the end device is informed to the hub. The packet consists of fields like packet type, End device ID and the device's gradient value. Firstly the module or node to which the end device is attached updates the link state database. The link data base will already have the parent details which mean the path to the hub and now additionally other link details to reach the end device is entered. Then the EDJ is sent to the parent such that the parent node also adds the link to reach the end device in its link state database. In this way all the parents learn about the end device and finally the hub also learns the existence of the end device

and most importantly the hub learns the gradient value to reach the end device and the link via which it could reach the same.

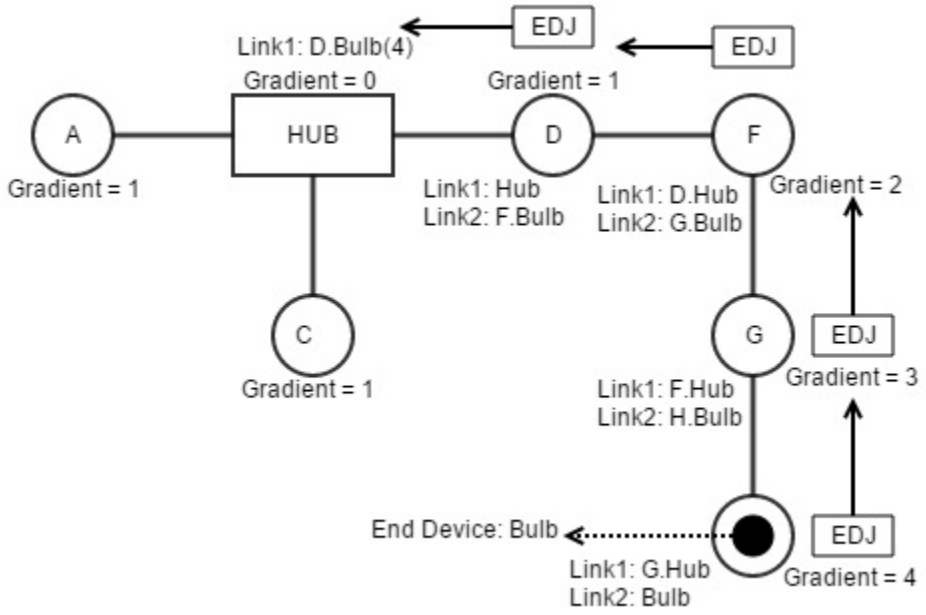

FIGURE 31. EDJ demonstration.

Here, let us consider a bulb which is termed as end device is connected to the module H. Once the bulb is attached, the module H learns the addition of new end device. The link state database of H is updated with a new link as Link2: Bulb indicating the presence of new device directly connected to it. Then EDJ from H is sent to the other node, here G. G updates the link state database by adding the link2 details like Link2: H.Bulb. In this way all the nodes after receiving the EDJ, update the link state database

and transmit the EDJ via link1 i.e. to its parent such that the end device is made know to the hub. The hub now has a link and the gradient value as shown in the figure 31 to reach the end device.

There might be many links to reach an end device, but the hub first checks the link state database and identifies the shortest path based on the gradient value. The link with the least gradient value is considered as the best link to reach the end device.

Information Exchange

This is the Third phase of this protocol where command and information is exchanged between the hub and the end devices. This phase can be discussed as upstream and downstream data transmissions. The upstream data transmission is the data information transfer from the end device and the hub, whereas downstream data is the command that is issued by the hub to the end device.

Upstream Transmission. Any information water leakage, breakage, fire outbreak, smoke detection and other data information is reported to the hub. These data is always passed through link1 via the parent to the hub. Therefore whenever there is any sensor detection the information is transmitted from the module to the hub.

Downstream Transmission. To switch ON or OFF a device, reduce the intensity of the brightness, send other commands and operate the end device downstream data transmission from the hub to the end device.

CHAPTER 6

SIMULATION AND RESULT

In this thesis work, simulation using NS2 on existing protocol with 12 nodes and the proposed protocol based on gradient value as explained in the previous chapter for 10 and 30 nodes are implemented and the results are produced.

Existing Protocol

The existing protocol is implemented using 12 nodes as shown in the figure below.

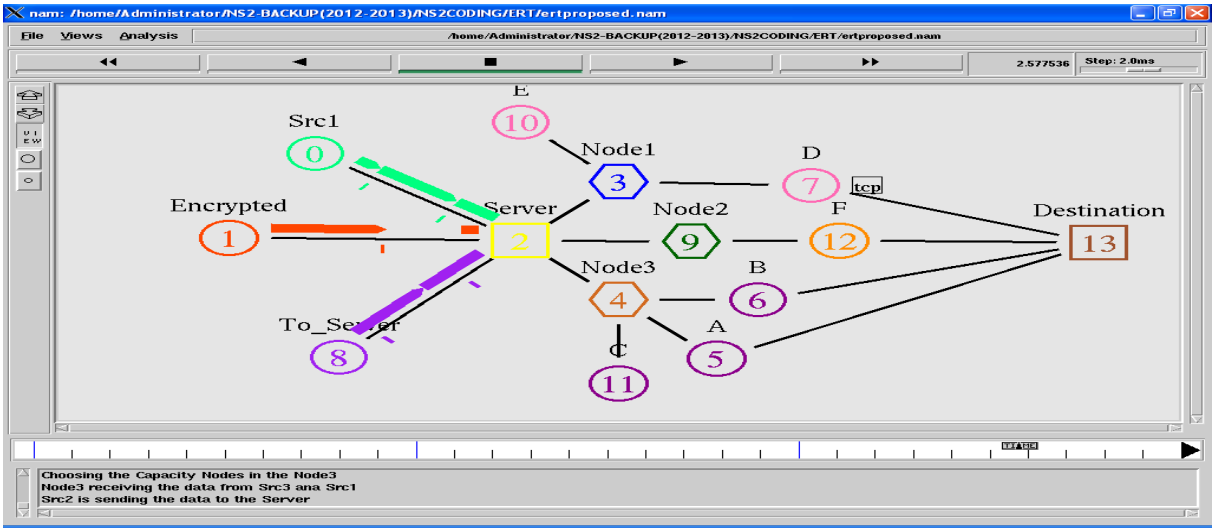

FIGURE 32. Existing insteon protocol.

Here we consider only the wired part of the protocol because the interest of study is the performance of proposed protocol on powerline medium compared with the existing protocol. The function of this protocol is as discussed in Chapter 3 under the topic titled the Insteon communication protocol. As explained in the chapter the existing protocol allows only three retransmissions and the packet destined to a node leaves the sender through all the available links. The simulation is also implemented with ACK, NACK, CRC concepts which are the advantageous factor than X10. All the devices of the network in the above figure act as controller, repeater and responder.

Proposed Protocol

The proposed protocol which deploys the gradient based routing explained in previous chapter is implemented in NS2 for 10 and 30 nodes as shown in the figures below.

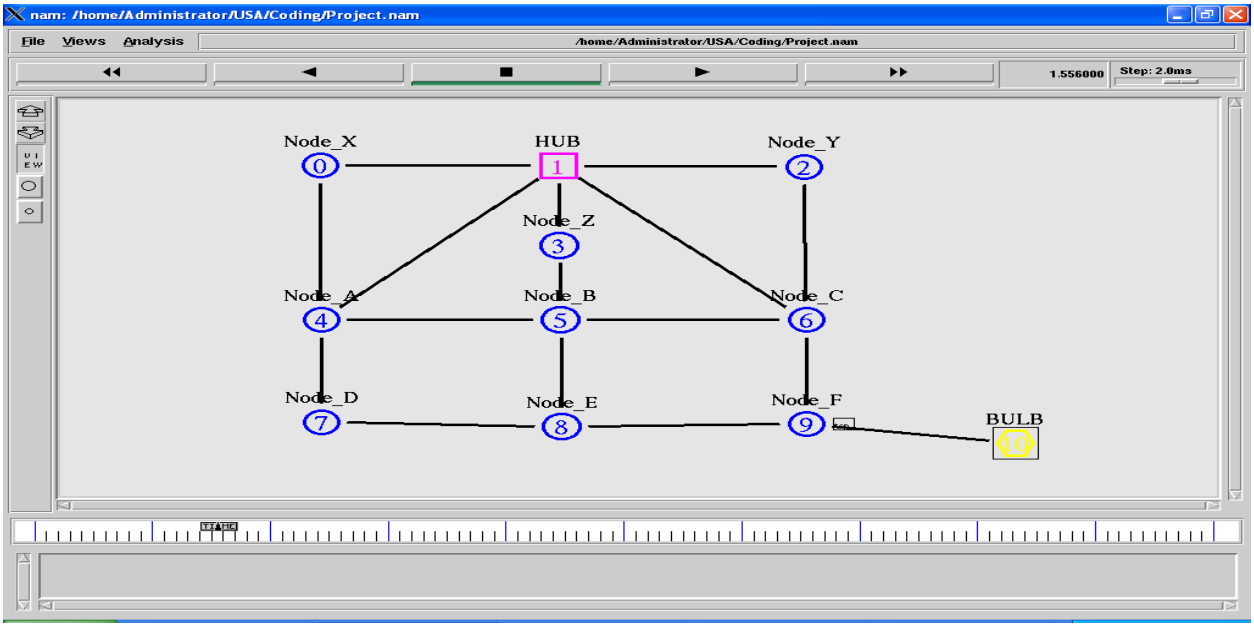

FIGURE 33. Proposed protocol with 10 nodes.

The 10 nodes include a hub; here the end device shown is a bulb. Hub takes the gradient value zero and sends BP adding one to the gradient value. Then PSQ checks the status of the parent and the parent sends PSQ Response. If no response from parent the nodes send PD to find a new parent. Addition of new node to the network is accomplished using NAP and FBP changes the gradient value based on the new node addition. Then EDJ is the packet that informs all nodes in a particular link of the hub and including hub about the addition of the end device and its status.

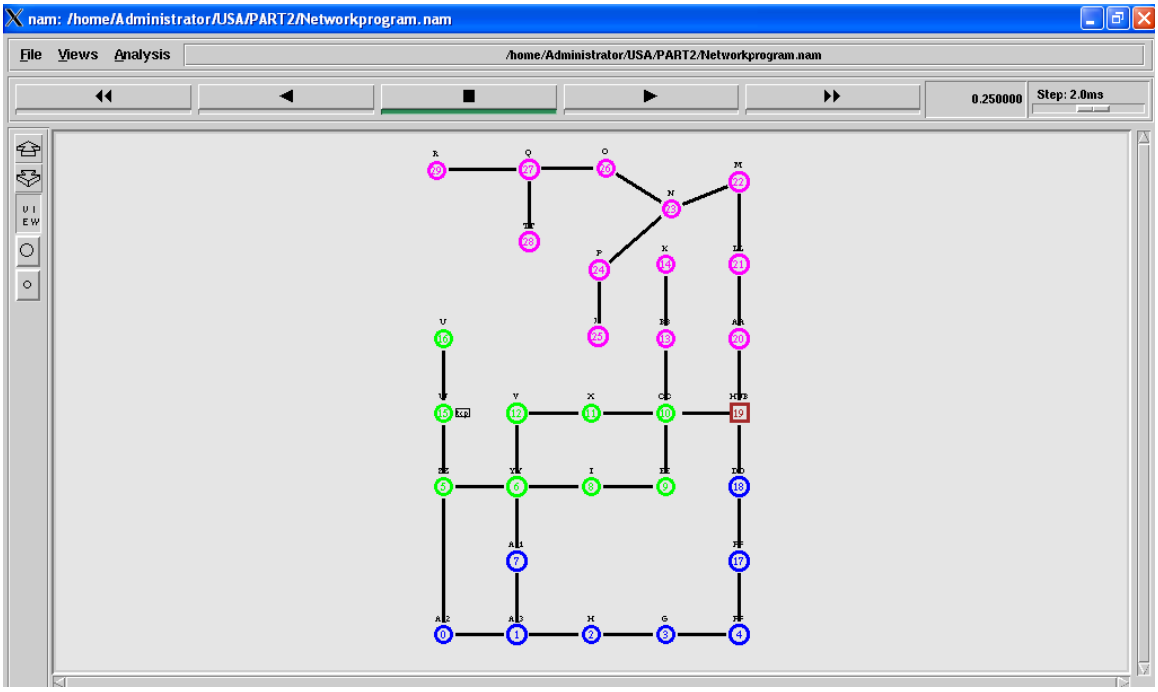

FIGURE 34. Proposed protocol with 30 nodes.

The central idea of this work is to propose a protocol, is to expand the existing protocol such that many devices including the devices that could monitor the property for security reasons. After expansion the resultant simulated network is shown in the above figure and the results are obtained which states the feasibility to implement the algorithm for many nodes

Results

The simulation is tested on the following three parameters:

1. Throughput
2. Delay
3. Collision

For three different data rates high, medium and low data rates. The work is to expand the network by implementing the proposed prototcol and overcome the defeciencies of the exisiting propocol which can work only in the smaller networks, therefore we take number of nodes in the X-Axis for measuring performance.

Collision

This is the major problem that restricts the existing protocol to be implemented in larger networks. Collision which destroys the useful data information should be considered seriously and should be eradicated. This issue is solved in the proposed protocol.

Collision is measured in both exixting and proposed protocol by sending data packets at 1 Mbps, which is a high data rata for the type of protocols in home control networking domain. Collision increases abruptly in the exisitng protocol after 10 nodes and it is at maximum 33 Mbps for thirty nodes. We can infer that the existing protocol

cannot accommodate many nodes and scalability, a feature that determines the protocol's efficiency is not seen in the prototcol.

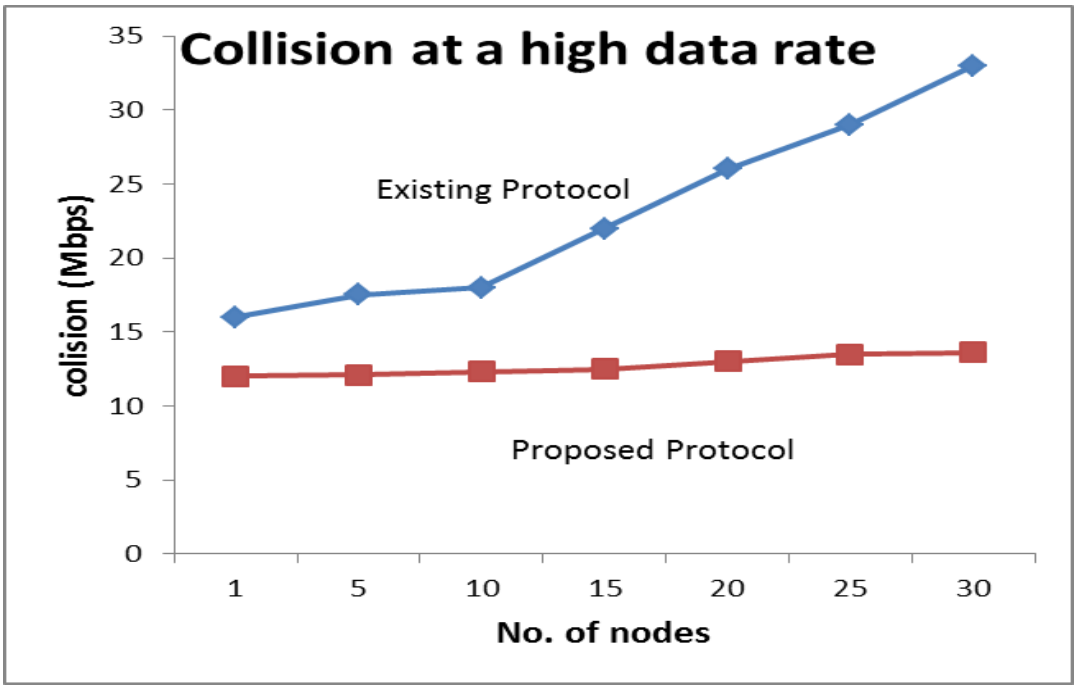

FIGURE 35. Collision at high data rate.

The medium data rate used in the simulations here is 260 Kbps. The existing protocol increases linearly with large slope which determines the inability of the existing network to be implemented in larger residential areas.

The above case is same in low data rate at 800 bps, that shows steady increse in the graph for existing prototcol and making it infeasible to beapplied in larger networks again.

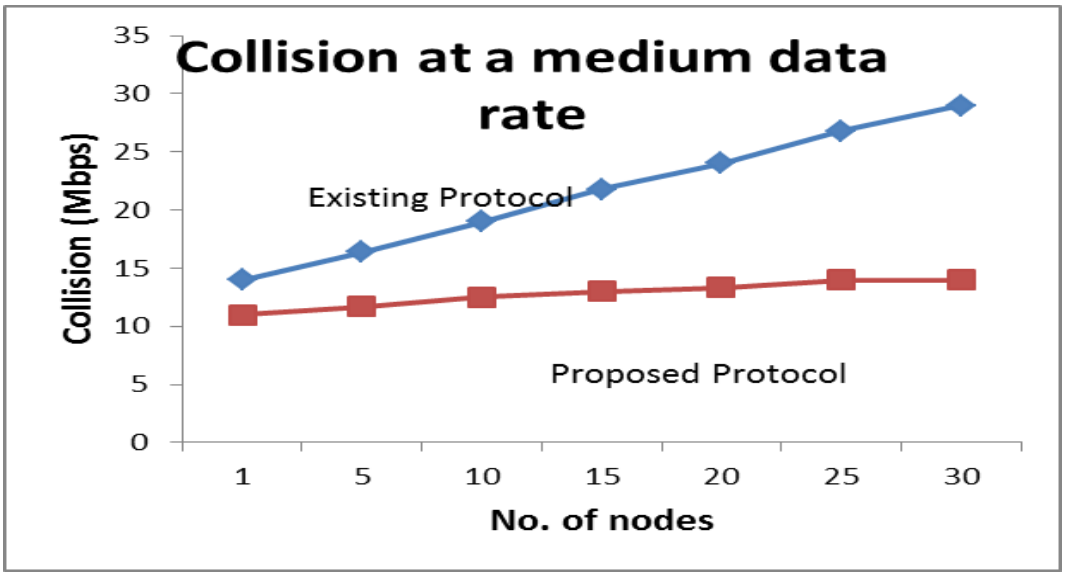

FIGURE 36. Collision at medium data rate.

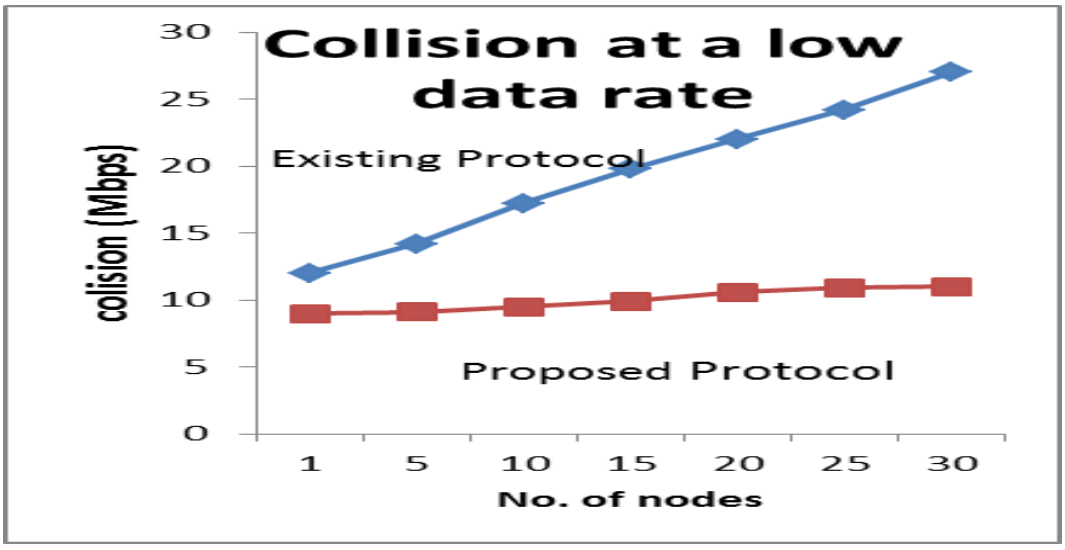

FIGURE 37. Collision at low data rate.

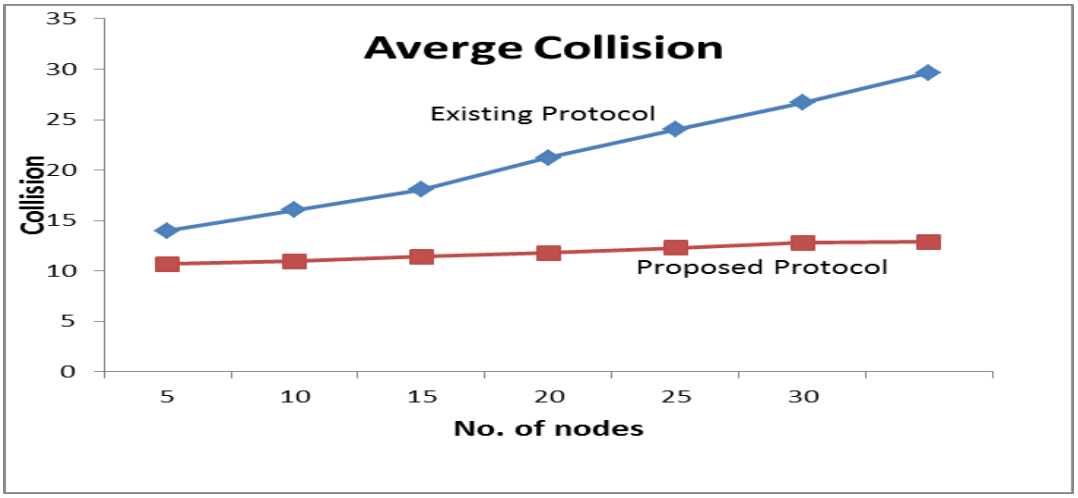

FIGURE 38. Average collision.

The above graph is based on average values of collision for all the selected data rates. For all the data rates the existing protocol increases linearly, therefore the average value for existing prototcol increases. The value here indicates to be high making the protocol to be unfit for larger residential and industrial areas.

The below graph depicts the percentage change in collision after implementing exisiting and proposed protocol. For 30 nodes, which is the maximum nodes used to implement the prototcols, the percentage decreased to 56.62% after using the proposed prototcol compared to the exisitng prototcol.

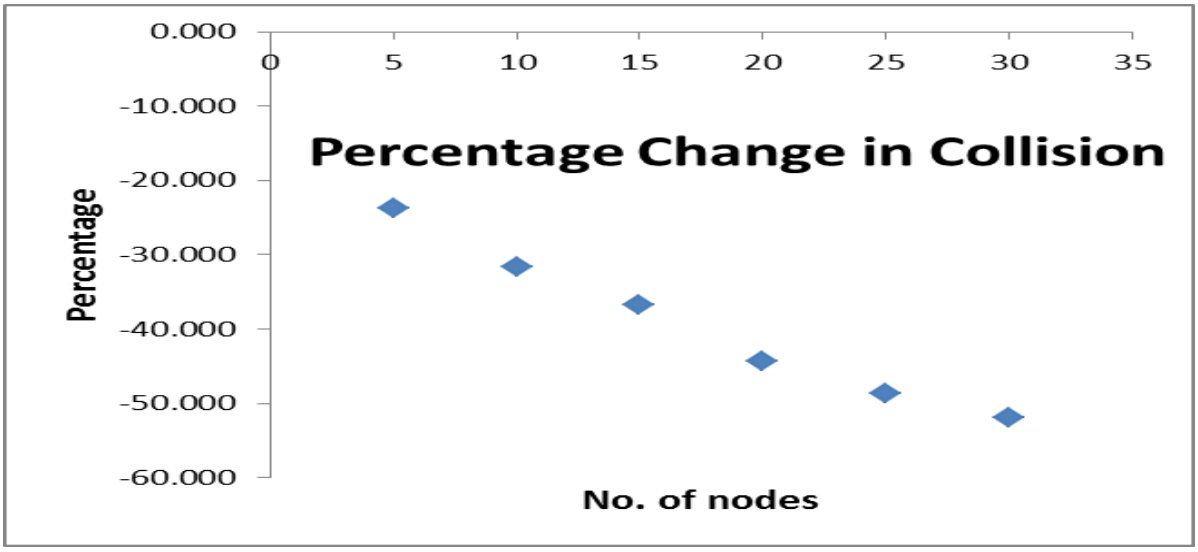

FIGURE 39. Percentage change in collision.

Delay

Delay is defined as the excess time for a packet to reach the destination. Congestion is the factor that affects delay. Existing protocol allows packet to go through all the links of a node, this leads flooding of packet and results congestion in the network leading to delay in packet delivery alongside collision. To eradicate this, the proposed protocol which aids hub and nodes to choose the best path to reach the destination is implemented instead of nodes sending through all the available links.

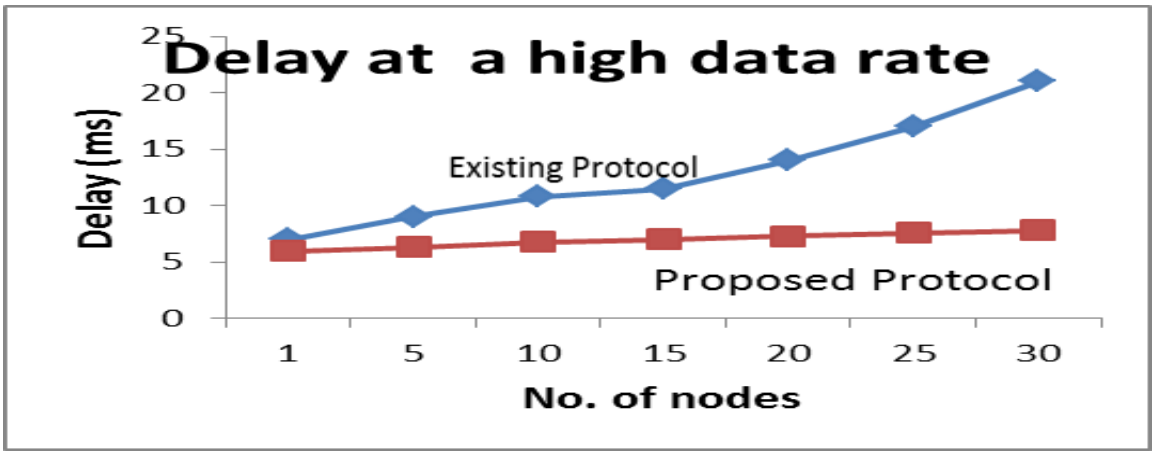

FIGURE 40. Delay at high data rate.

Delay at 1 Mbps for existing protocol is increasing curve, at maximum number of nodes the value of delay is 21 ms. But Insteon protocol's main characteristic is to maintain low response time. This nature is affected by implementing existing protocol in larger network.

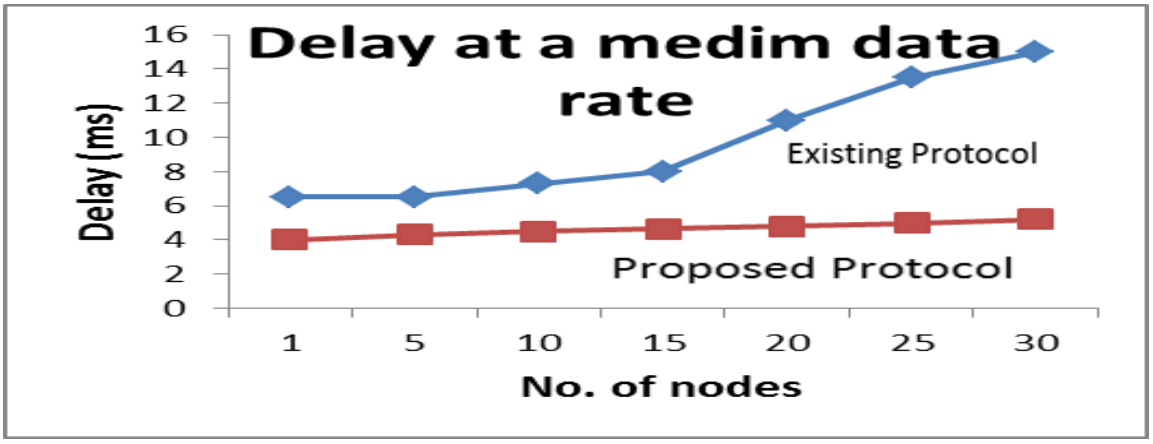

FIGURE 41. Delay at medium data rate.

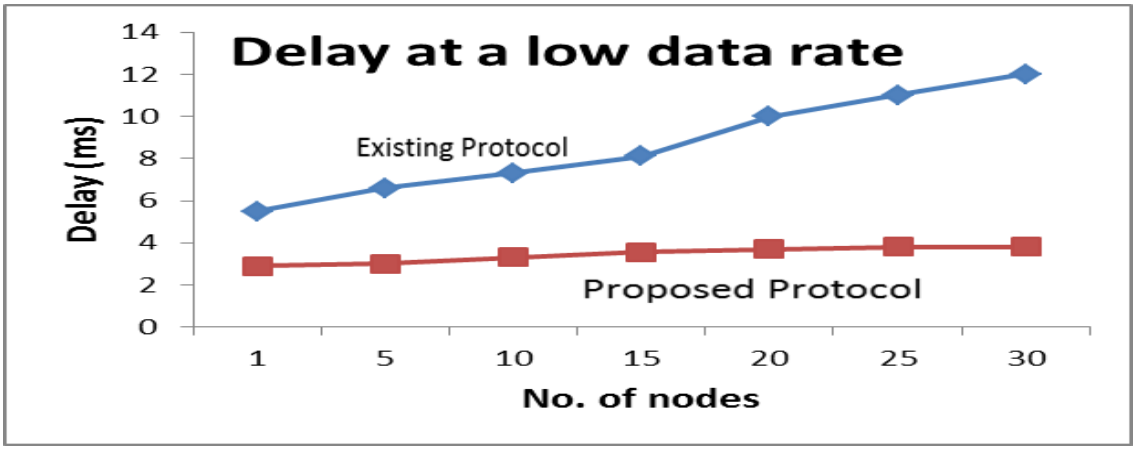

FIGURE 42. Delay at low data rate.

At medium data rate (260 Kbps), at low data rate (800 bps) and after computing the average delay values for different data rates, the existing protocol shows large increase in delay, proving the existing protocol inefficient to be implemented in larger networks.

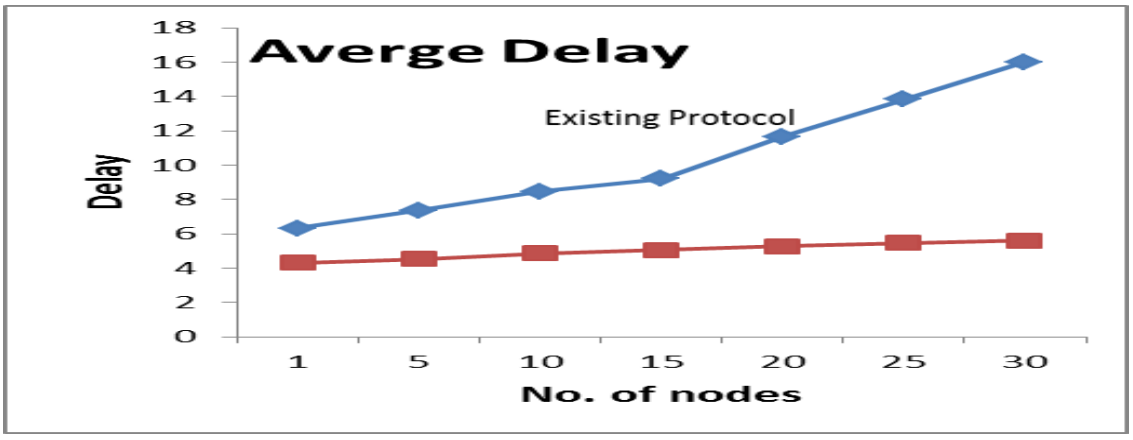

FIGURE 43. Average delay.

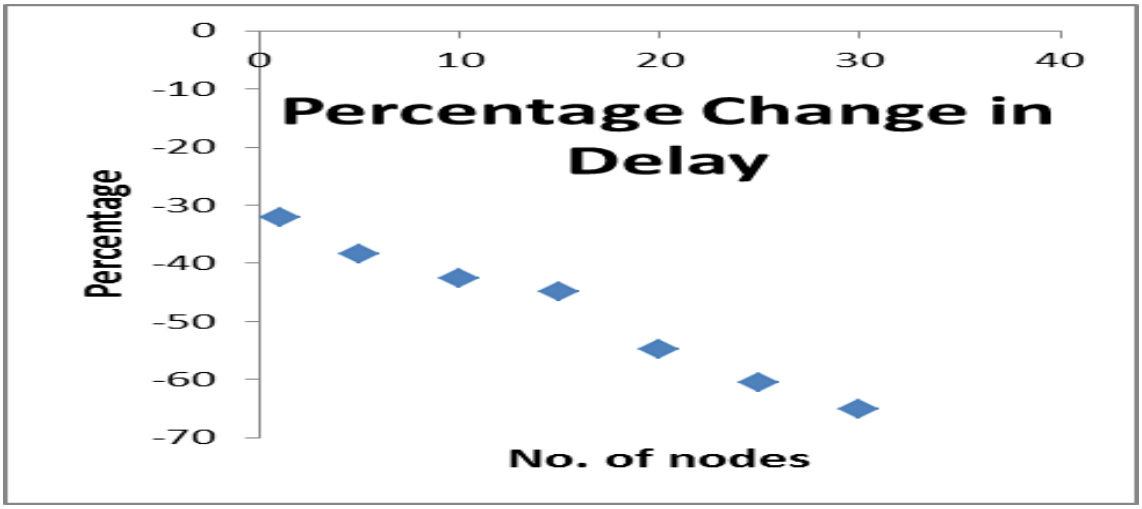

FIGURE 44. Percentage change in delay.

The percentage change has dropped by 65% for maximum nodes implemented in the simulations.

Throughput

Throughput may be defined as the successful rate of data transmission between the sender and the receiver. This parameter is dependent on collision, noise and other physical parameters. The existing protocol in a larger network can have lesser throughput; therefore the gradient based routing is developed to achieve better throughput for maximum number of nodes in the network.

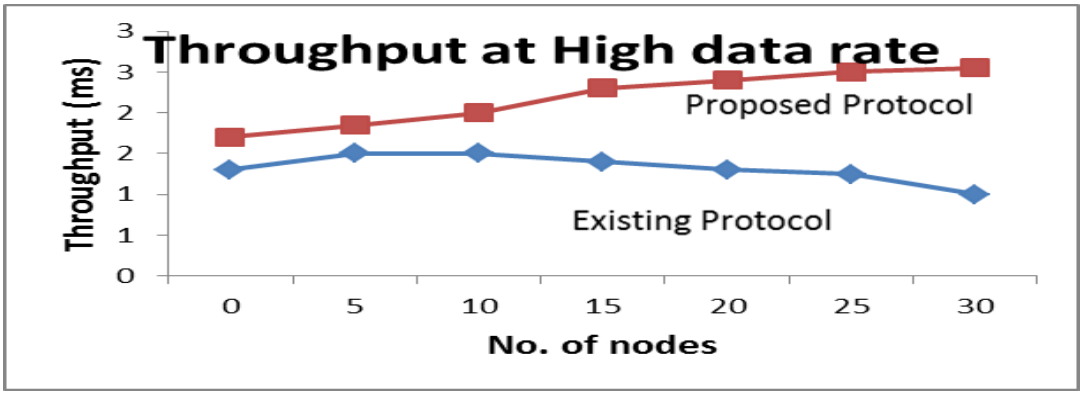

FIGURE 45. Throughput at high data rate.

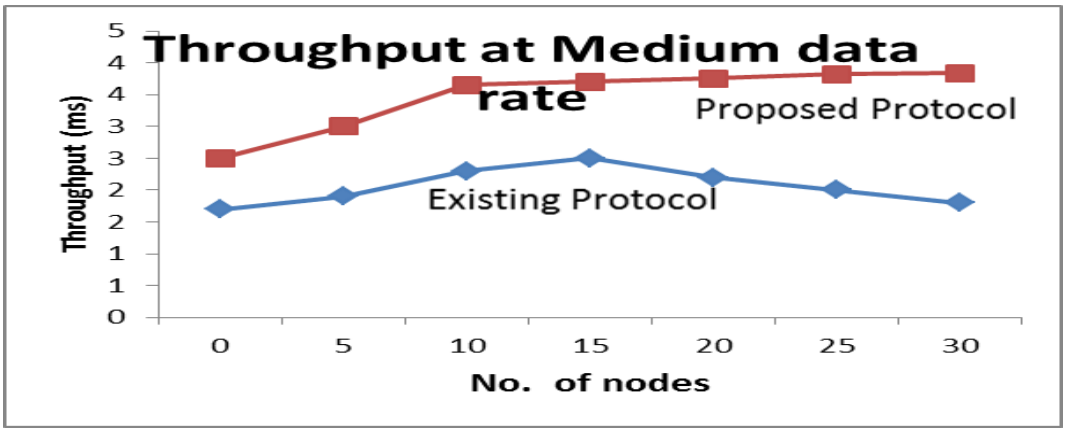

FIGURE 46. Throughput at medium data rate.

Delay and collision directly decreases the overall throughput of the system. The graphs show the result of throughput after measuring delay and collision. The throughput in the existing protocol decreases due to high rate of collision and delay, whereas the proposed protocol demonstrates better throughput.

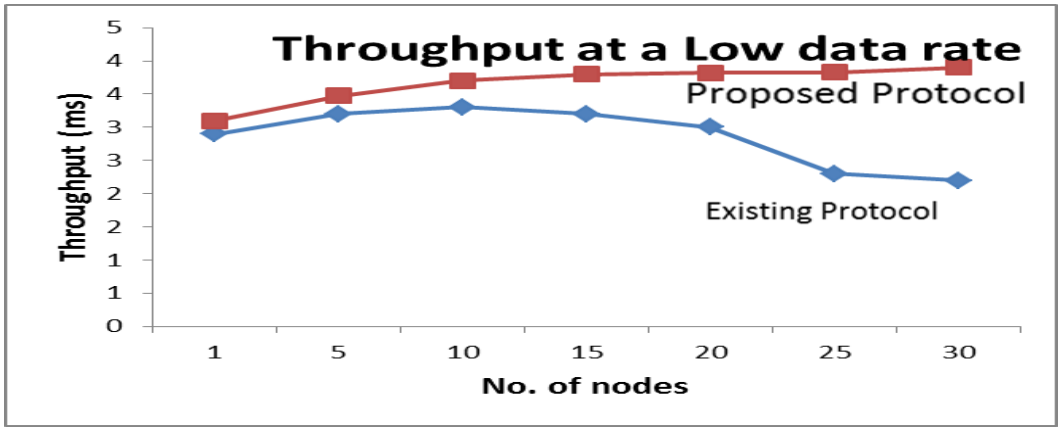

FIGURE 47. Throughput at low data rate.

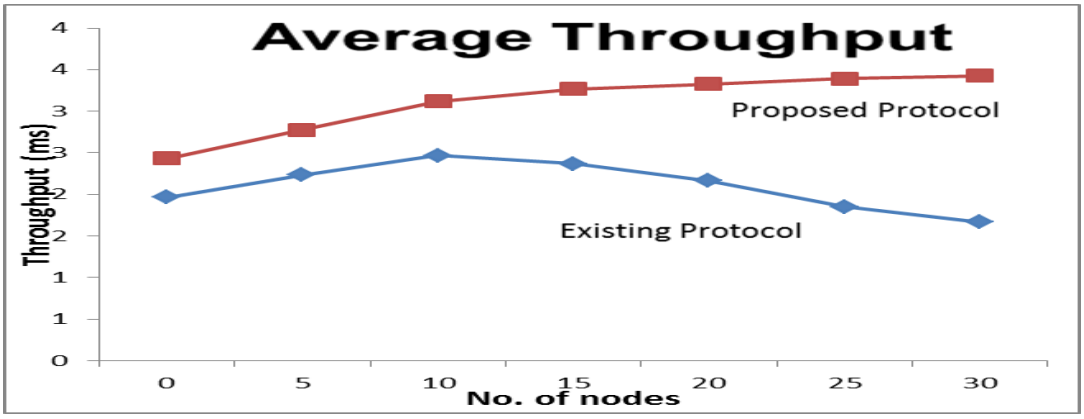

FIGURE 48. Average throughput.

The average throughput shows decreasing curve in existing protocol and the graph of proposed protocol indicates steady increase.

The percentage change in throughput increases as the number of nodes increases; the percentage change is 105% proving the proposed protocol a robust and efficient one.

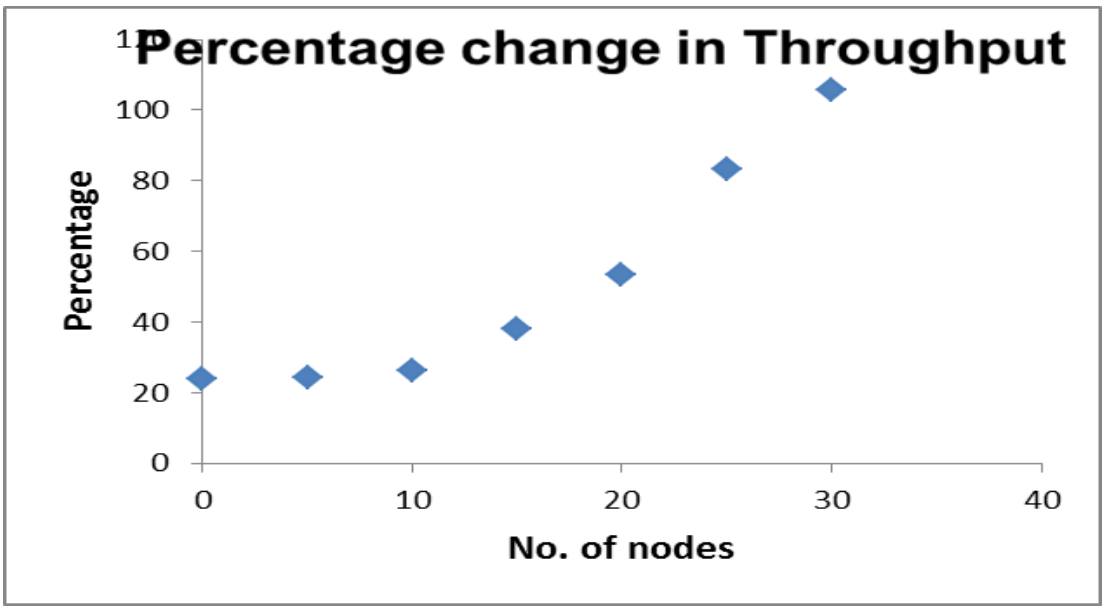

FIGURE 49. Percentage change in throughput.

Comparison of Perforrmances

The thesis is based on expanding the network, therefore the performance is measured and studied based on number of nodes, here 30 nodes are considered.

Firstly and most importantly, considering collision of the system for the 30 node the curve goes down and yields positive result and the percentage of decrease of collision is 56.63%

Secondly, measuring delay the existing protocol suffered delay and decreased by 65% using the proposed protocol.

Thirdly, throughput which is the parameter that determines the performance fo the whole system has also increased by 105.6%. Therefore the proposed protocol in this thesis can be affirmed to be a better protocol appropriate for large networks that would be

in demand in future, henceforth expanding the application of Insteon technology in larger residential areas and industrial areas.

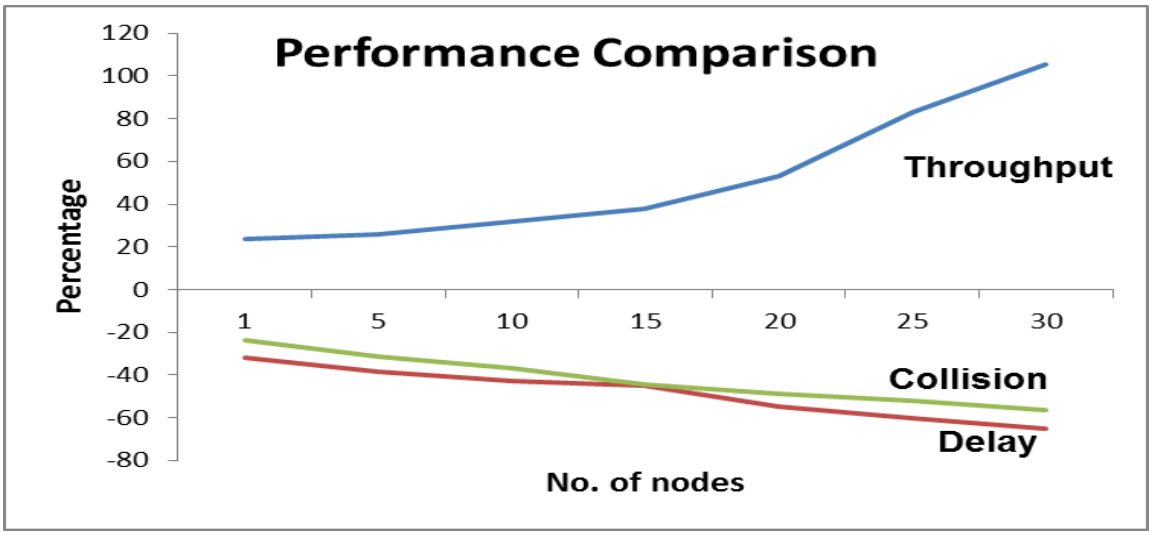

FIGURE 50. Performance comparison.

CHAPTER 7

AUTOMATED DISASTER REPORTING SYSTEM

Insteon has a range of products on indoor lifestyle sophistication to satisfy people's demand. Insteon would be an overall complete home-control networking technology, if the research area in security is fulfilled. Therefore this thesis also proposes a novel technique to handle and end the disaster as soon as possible that has occurred.

The objectives of this protocol are:

1. To stop disaster, before its effect becomes worse.

2. To increase options to call for rescue.

3. To call for immediate nearest trusted party rescue operations (with absolutely minimum or no delay).

4. To make Insteon work in absence of the user – user independent. No user intervention required here.

5. To provide affordable and 100% reliable product in security: The customers can spend $150 – 200 extra and save several $1000 worth property.

This protocol will also be beneficial to Insteon in expanding the business to the next step from residential to industrial areas. Insteon will reach the pinnacle level in home-control networking industry and no company would overwhelm Insteon.

The existing disaster reporting system just reports the occurrence of disaster to the user.

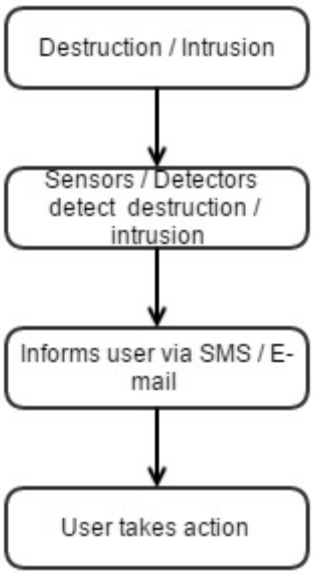

FIGURE 51. Flow chart--existing disaster reporting system.

When a sensor picks up outbreak of disaster, it is informed to the user through SMS and E-mail. Then user takes action to control the disaster. The user would call the police, fire department and 911 to control the effect of disaster and stop it.

Here the intervention of user is required compulsorily. There will be situation like the user engaged in meetings, party, out of the communicable range when the user will not be able to receive the communication about the disaster. At this situation the user cannot report the disaster to the concerned department for rescue. This new protocol can report and call for a trusted third party intervention like 911, police department, fire department.

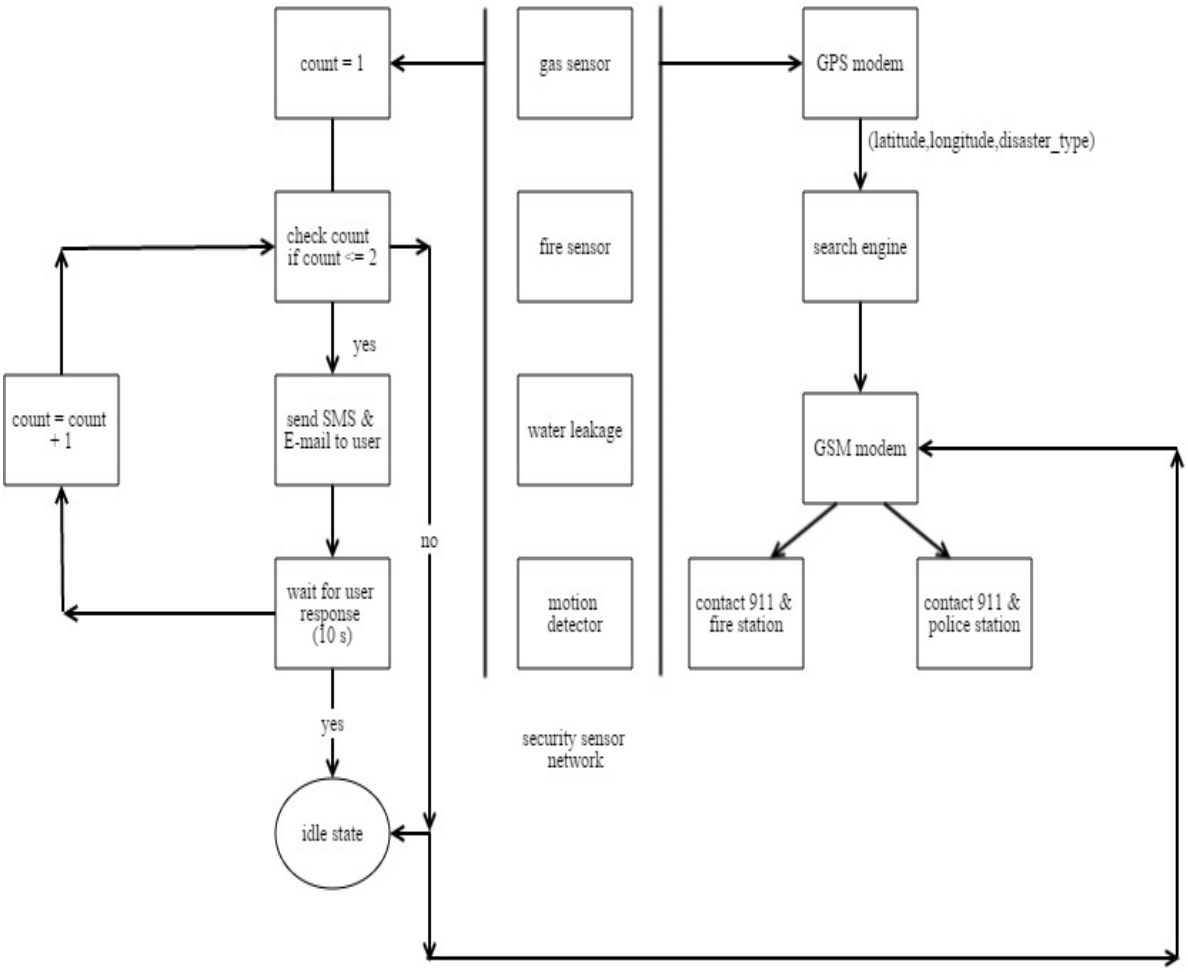

FIGURE 52. Proposed automated disaster reporting system.

The protocol consists of a set of security sensors like gas, fire, motion detectors and water leakage. If any disaster occurs the sensor detects the same and then a counter is initiated at the same time. The counter is initiated to value one and the n a SMS and e-mail is sent to the user to report the occurrence of disaster, now the system waits for 10 seconds to receive a response from the user. If there is a response, it means that the user is aware of the situation and the user takes the necessary action and the system goes to

the idle state. If there is no response from the user, the counter is incremented by one value, now the counter value is two and again the system reports the user and waits for the response. If there is no response for the second call, the system iself calls for the trusted third party for rescue.

Meanwhile the system waits for the response. The GPS modem senses the latitude and longitude of the current location along with the type of disaster and fed to a search engine. The search engine turns up with the necessary details depending upon the input. If the input type is an outcome of gas, fire and water the system contacts the nearest fire station depending upon the location. If there is an outcome from the motion or break detectors the GSM modem contacts the 911 and police department for rescue. Thus this system is a unique independent system that works without any user intervention.

REFERENCES

REFERENCES

[1] C. Gomez and J. Paradells, “Wireless home automation networks: A survey of architectures and technologies,” *IEEE Commun*. Mag., vol. 48, pp. 92-101, Jun. 2010.

[2] M. A. Zamora-Izquierdo, J. Santa, and A. F. Gómez-Skarmeta, “An integral and networked home automation solution for indoor ambient intelligence,” *IEEE Pervasive Computing,* vol. 9, pp. 66-77, Jan. 2010.

[3] Smarthome. (2015). Remote controllers. [Online]. Available: http://www.smarthome.com/controllers-apps/remote-controllers.html

[4] M. H. Mazlan, F. Mohamad, R. A. Rashid, M. A. Sarijari, M. R. A. Rahim. “Real-time communication routing protocol for home automation via power line,” paper presented at 7th Student Conf. on Research and Development, Johor Bahru, Malaysia, 2008.

[5] Insteon, "Insteon whitepaper: The details," Insteon, Irvine, CA, version 2.0, 2013.

[6] Yu-Ju Lin, H. A. Latchman, M. Lee, and S. Katar, “A power line communication network infrastructure for the smart home,” *IEEE Wireless Communications*, vol. 9, pp. 104-111, Dec. 2002.

[7] L. Lampe and A. J. Han Vinck, "Cooperative multihop power line communications,” presented at IEEE Int. Symp. on Power Line Commun. and App., Beijing, China, Mar. 2012.

[8] G. Bumiller, L. Lampe and H. Hrasnica. “Power line communication networks for large-scale control and automation systems,” *IEEE Commun*. Mag., vol. 48, pp. 106-113, Apr. 2010.

[9] C. J. Kim, and M. F. Chouikha, “Attenuation characteristics of high rate home-networking PLC signals,” *IEEE Trans*. on Power Delivery, vol. 17, no. 4, pp. 945-950, Oct. 2002.

[10] M. M. Rahman Mozumdar, A. Pugelli, A. Pinto, L. Lavagno, and A. L. Sangiovanni-Vincentelli, "A hierarchical wireless network architecture for building automation and control systems," paper presented at 7th Int. Conf. on Networking and Systems, Venice, Italy, May 2011.

[11] M. E. M. Campista, L. H. M. K. Costa, O. C. M. B., and Duarte, "Improving the data transmission throughput over the home electrical wiring," paper presented at IEEE Conf. on Local Computer Networks, Sydney, Australia, Nov. 2005.

[12] J. Heo, K. Lee, H. K. Kang, Dong-Sung Kim, and W. H. Kwon, "Adaptive channel state routing for home network systems using power line communications," *IEEE Trans.* on Consumer Electronics, vol. 53, pp. 1410-1418, Nov. 2007.

[13] H. Li, and L. Fen, "An improved routing protocol for power-line sensor network based on DSR," paper presented at Second International Conf. on Future Computer and Communication, Wuhan, China, May 2010.

[14] O. Mirabella, A. Raucea, "Tree based routing in power line communication networks," paper presented at 36th Annual Conf. on IEEE Industrial Electronics Society, Glendale, The USA, Nov. 2010.