DEVELOPMENT OF NEW ARP ROUTING PROTOCOL FOR MULTIHOP TRANSMISSION IN AD HOC IEEE 802.11 NETWORKS

Ida Syafiza Binti Md Isa

Final Project Report
Short Term Grant
Faculty of Electronic Engineering and Computer Engineering
Universiti Teknikal Malaysia Melaka
1 November 2013

ABSTRACT

Ad hoc networks are becoming more important in the modern complex environment. The ad hoc network can be used to instantly connect to the local or remote networks such as the Internet without the need of pre-existing infrastructure or centralized administration. The users of the network together will establish the infrastructure. Limited radio range transmission is one of the major problems in ad hoc network. Due to this, multiple network 'hops' are needed to send data across the network. The devices in the network will act as a router in order to forward the data to the final destination. There are varieties of routing protocols targeted for this environment that have been proposed and developed. However, most of them suffer from high overhead data traffic. The main purpose of this project is to implement the ad hoc network with the existing network protocol that had been already used in network environment which is the Address Resolution Protocol (ARP). ARP was designed to announce or find MAC addresses. However, in this work we have extended the usage of the ARP protocol as routing protocol in wireless ad hoc network. Our ARP route provides two new operation types, ARP Forward Request and ARP Forward Reply to allow the multihop transmission using intermediate nodes to forward the request and reply. These two operation types only used the current operation codes which are '0x0001' for request and '0x0002' for reply. The current studies on this routing protocol create a new operation code for the ARP forwarding scheme which is '0x000c' for forwarding. We have successfully managed to create a multi hop transmission in an ad hoc network by using the current existing operation code for the ARP forwarding. The 802.11b test-bed has been configured and the ARP routing protocol has been implemented for multi hop transmission. The experiment in the open space provides the comparison of environment with obstacles and without obstacles. We manage to get more than 50% of packet receive at a place with no obstacles and more than 45% in a place with obstacles. In order to show the effectiveness of the proposed methods, a simulation using OMNET++ has been simulated for the three nodes and the results are compared with the current protocol which is Ad Hoc On Demand Distance Vector, AODV protocol. The data can be sent through multi hop transmission until it reaches the destination. From the simulation it shows that ARP protocol works better than ADOV. The proof of method is shown by using several graphs namely in terms of time, packet loss and also throughput.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TITLE **PAGE**

LIST OF ABBREVIATIONS

ARP		Address Resolution Protocol
DSR		Dynamic Source Routing
AODV	-	Ad-Hoc On Demand Distance Vector
IEEE	-	Institute of Electrical and Electronics Engineers
LAN	-	Local Area Network
WLAN	-	Wireless Local Area Network
PIC	-	Programmable Interface Controller
NLOS	-	Non-Line Of Sight
LOS	-	Line Of Sight
LCD	-	Liquid Crystal Display

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Problem Statement

Ad hoc is one of the communication technologies that provide the possibility for wireless device to communicate without using central access point. An Ad hoc network allows all the wireless device to communicate directly or peer-to-peer fashion within its radio range. However, the transmission of data cannot be done if the wireless device is out of its radio range. Due to this, multiple network 'hops' are needed to exchange data between the nodes to the destination. Many routing protocol has been proposed for the multi hop methods but most of them suffered from high overhead. With high overhead, the possibility of the unsuccessful transmission may happen. Besides, the time for the data transmission will be longer.

1.2 Project Objectives

- To configure the low rate IEEE 802.11 platforms using Microchip WiFI Development Board.
- To develop a multi hop routing protocol in C language.
- To implement the multi hop routing protocol on the wireless Ad Hoc network in a test-bed.
- To investigate the performance of ARP and AODV protocol for different environment and packet size using OMNeT++ simulation software.

The performance of the proposed routing protocol will be evaluated based on the packet loss, the round trip time for the successful transmission and the throughput.

1.3 Scope

The scope of this project includes developing software for the low rate 802.11b platform in C language. The routing protocol using the ARP is developed and the software will be embedded in the low rate 802.11b radio. The nodes will acts as a transceiver and also as a router. The proposed routing method will be tested using the real test-bed environment. Besides, a simulation using the OMNeT++ software is also involved. The test-bed are developed using three 802.11b nodes, a laptop to run a Wireshark. The performance metrics such as packet loss, the round trip time and the throughput are analyzed.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

An ad hoc network is one that comes together as needed and it does not necessarily come with assistance from the existing Internet infrastructure. An ad hoc network is simply a collection of wireless mobile hosts that form a temporary network without centralized administration [1].

Wireless ad hoc networks are characterized and they do not have same static nature as an ordinary wired network infrastructure [2]. Ad hoc networks maintain control through a decentralized concept. Ad hoc also provide a dynamic topology network where it has the ability of self-healing structure that makes the communication less vulnerable for failing links. This means that even when the communicating devices are removed or added in the network the information can still make its way through the network to its final destination.

In ad hoc network, each nodes is equipped with a wireless antenna that can receives and transmits in an isotropic manner, directed or steer able or a combination of all three. The nodes are stand-alone devices. It usually operated by using batteries.

The existence of ad hoc network is useful for the Vehicular Ad Hoc network, VANET application. VANET is a form of Mobile Ad Hoc network, MANET to provide the communication among the nearby vehicles and between vehicles besides nearby fixed equipment [3]. In this application, each of the vehicles will be nodes in the network and each of them will be provided with the VANET device. So the vehicles among themselves can receive and relay other message through the wireless network. The vehicles will acts as a sender, receiver and also a router to broadcast the information or the message to the vehicular network. Usually, the information in the VANET application is used to ensure the safety and the free flow of the traffic.

In order to hops the data in an ad hoc network, a protocol is needed. They are many protocol have been proposed such as Ad Hoc On Demand Distance Vector, AODV, Dynamic

Source Routing, DSR and many more. Each of these protocols has its own assumption and intuition. Ad hoc network is what underlies the establishment of the paths where VANET nodes can communicate with each other. The routing will maintains the routes and makes it transparent to the user.

2.2 Routing Protocol for Multi Hop in Ad Hoc Network

Routing is important in sending data from the source node to the destination nodes. Besides, it is also used to minimize the network performance. It also included the procedure in establishing a route, decision in forwarding and action on maintaining the route from routing failure [4]. Since the topology of the network can changed constantly, the route between sources and destinations may changed and become inefficient. Due to this, routing information is needed to be updated regularly than in traditional wired network. In order to maintain the route, a routing algorithm or a routing protocol is needed. In order to create a new algorithm of routing, several performances are needed such as dynamic topology, multi hop, energy constrained operation and also bandwidth constrained. All of this performance needs to be considered in order design new routing protocol.

Dynamic topology is where the nodes in the ad hoc network moved randomly. Due to this, routing information need to be update frequently so that the route between the nodes maintain. However, with frequent updated may also cause the routing overhead. This will increase the use of the radio medium resources.

Multi hop is one of the important parameter that needs to be concerned in order to have a great performance in the network. Usually, in ad hoc network the nodes do not have peer-to-peer contact between themselves. The connection between the nodes is not guaranteed. Sometimes, in order to send a data from a sender to a destination, multiple hops are needed to forward the data. The source and destination may not in the communication range. So the other nodes in the network are needed to forward the data. This is also where the nodes in the network will acts as a router or an intermediate node to route the data to the destination. In VANET application, the topology may change constantly and a good routing protocol is needed in order to send data to the destination.

Energy constrained is the most critical issue in wireless sensor network. Most of the nodes may rely on batteries for their energy. With lower energy the nodes may not acts perfectly. In order to develop or design new protocol, the designer needs to consider this parameter.

Bandwidth constrained is another parameter that needs to be considered in designing the protocol. Nowadays, the communication over wireless medium will continue to have less bandwidth capacity. Dues to this, many problem on transmitting signal may happened such as interference, noise and also fading. In order to this, with less transmitting and receiving the signal when delivering data need to be minimized.

2.2.1 Topology Based Routing in Ad Hoc Network

There are several ad hoc routing protocols utilized the topology established routing approach. The established topology routing protocol is used to dispatch the data packets from sender to the destination nodes. The topology routing protocol can be divided into three groups which are proactive routing, reactive routing and hybrid routing [6]. Figure 2.1 shows the diagram of the topology based routing.

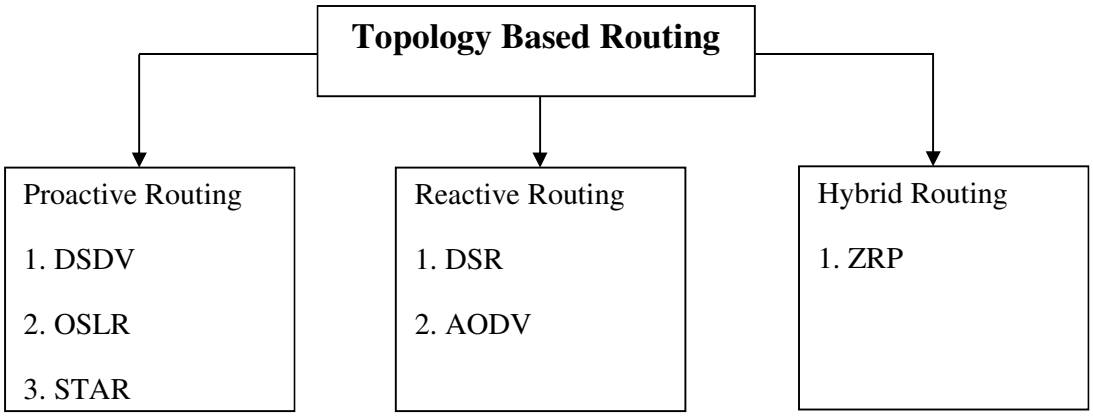

Figure 2.1: Topology Based Routing

Proactive routing is also known as table driven routing. It acts similar to the traditional fixed network routing [7]. The proactive routing protocol is used to maintain the routes to all of the destinations even there is no demand. To maintain the routes, this routing protocol will propagate the information updated regarding the network topology or connectivity throughout the network. The updated information will be topology driven. This is when the data is generated whenever there is connectivity in the network detected. This updated information can also be periodic since the connectivity in the network is generates at fixed intervals. The proactive routing protocol used a routing table to store all routes. With the aids of this routing table, there will be no route discovery when there is a demand. This will lead to the fast transmission since the delay for the route discovery is illuminated in this routing protocol. Due to this, this routing protocol is a good property since it provides low latency for real time applications. The proactive routing protocol also has its own disadvantage. The disadvantage is that it is a resource demanding where it used lots lot batteries, power and also bandwidth. This happened because each of the nodes in the network will update about themselves at interval time to update the routing table.

Reactive routing protocol is another type of topology routing. It is also known as on demand routing protocol. This is because the protocol will only determined the routes when there is data to be sent [4]. The sender will only find a route when the route is unknown. This caused a traffic flow where the query is propagated through the network. The query will be broadcast through the network and will receive by the nodes in the network. The nodes that receive the query will respond to the sender when it has a route to the requested destination node. The advantages of this routing protocol is that, it used low power, less batteries and also less bandwidth since there will only broadcast the query when there is demand. However, this routing protocol suffers from delay during the search for a route when transferring the data to the destination.

Hybrid routing protocol is a combination of proactive and reactive routing protocol technique [4]. The nodes in the network will acts as a proactive routing when it is in a limited region around and else in reactive routing. However, when the nodes in the network are moving, the protocol might sense the movement and it will switch to the proactive routing. The disadvantage of this routing protocol is that it has a complexity to the algorithm.

2.3 Existing Protocol for Ad Hoc Routing

Many routing protocol has been proposed which can be used in the ad hoc network. Each of the protocols has different characteristics and its own operation. However, all of these protocols are suitable to be used in both static and dynamic topology for wireless routing application. There are also some enhancements that have been made with the existing protocol in order to improve the performance of the routing protocols.

2.3.1 Ad Hoc On Demand Distance Vector (AODV)

AODV is characterizing into a reactive routing protocol. This type of routing protocol uses a route discovery mechanism by broadcasting the query message [8]. Besides, this routing protocol is an enhancement of the Dynamic Source Routing (DSR) algorithm which is also one of the routing protocols. Since this is a reactive routing protocol, the AODV works exclusively on demand basis. This means that, when there is a demand from the network, the nodes inside the network will together established the route to the destination. The main purpose of AODV is to reduce the routing overhead in the network where AODV cuts down the demand of nodes to always stay alert and to increasingly notify routing data at every single node. This also reduces the battery consumption. In another words, the AODV maintains and established paths merely after there is a demand of contact amid disparate from nodes [9].

AODV can be used in both unicast and multicast routing. The paths will be keeps as long as they are desirable by the sources. Moreover, it used sequence numbers to safeguard the freshness of routes [10]. AODV is a loop free, self-starting and it is suitable be used for mobile nodes. There are several message signal used in the AODV operation which are RREQ, RREP and RERR. These messages are used in order to discover the route or establish the routes.

A Route Request (RREQ) is used and transmits by a source node requiring a route to a destination node. In the RREQ packets, it contains a time to live value where it state number of hops that this message should be forwarded. This value is set to a predefined value for first transmission and it will increased at retransmissions The retransmission will occurs when there is no replies are received at the sender node. Figure 2.2 shows the RREQ packet message.

Source Address	Broadcast ID	Source Sequence Number	Destination Address	Destination Sequence Number	Hop Count

Figure 2.2: RREQ Packet Message

Route Reply is other types of AODV packet where it is used by the destination and will be sent back to the originator or the sender node. Once the sender received this reply message, the route is established where there is a valid route to the destination node. Nodes monitor the status of the link to the next hops in active routes. When there is a link breakage in the active route is detected, a route error (RERR) message is used. This is to notify other nodes in the network about the loss of the link and a new RREEQ will be initiates if necessary. The reporting of the link breakage will be enable in the AODV protocol because each node in the network will keeps a precursor list contained the IP address of each neighbour which is mostly use for the next hops towards each destination.

2.3.2 Dynamic Source Routing

DSR is one of the ad hoc routing protocols that can be sued in an ad hoc network. DSR is not only simple but also an efficient routing protocol which is designed for the multi hop purpose in wireless ad hoc networks. The network will organized itself without the need of the existing network infrastructure when using DSR. DSR did not have a routing table which is usually used to route a data packet to a destination node. This is an advantage of the DSR routing protocol since the entire route contained in the packet header [7]. Route discovery and route maintenance are the two mechanisms that is used in the DSR routing protocol. These two mechanisms are used to allow the nodes in the network to discover and maintain the routes to the desired destination. The source routing is used to allow the packet routing to be trivially loop-free [1].By having the source routing can also avoid the updated routing information in the intermediate nodes regarding to which route should they forward the data. However, these routing protocol do have some disadvantage such as DSR routing protocol requires significantly more processing resources that other protocol. Besides, this routing protocol is not applicable to be used in a large network.

2.3.3 Zone Routing Protocol

ZRP is a routing protocol which is based on the hybrid routing algorithm. This routing protocol uses both concepts of proactive and reactive routing protocol. The method of this routing protocol is that in within a certain zone around each node, the proactive routing took place while the reactive routing will be used for destination that is far away. Because of this, the transmission of data within the zone can be straight away delivered at the destination nodes. However, for transmission data to destination that is out of the zone, a route discovery need to be done. The route discovery process is done with the use of zones. The path or the route to the destination may consist of list of zones edges nodes and it does not contain the information about the nodes between them. Because of this, the size of routes to be stored is much smaller. The ZRP routing protocol is much efficient compared to the AODV and the DSR routing protocol.

2.4 IEEE 802.11 Standard

IEEE 802.11 standard is a subset of 802 Local Area network architecture (LAN). It address the functions involved wholly in the wireless networking environment [11]. The characteristics of the wireless medium and the vibrant nature of ad hoc networks make the multi hop networks vitally disparate from wired networks.

There are many wireless networking standards have been proposed by IEE 802.11 standards committee. The different between these standards are on their frequency, modulation technique and also data rate. The IEE 802.11 Wireless LAN (WLAN) standards are 802.11a, 802.11b and 802.11g. IEEE 802.11b is the most commonly used compared to the other standards since the industry, scientific and medical (ISM) band made the frequency unlicensed [12]. Table 2.1 shows the stands of IEEE 802.11 WLAN and its features.

Table 2.1: IEEE 802.11 standards characteristics

Standards	Transfer Method	Frequency Band (1,2GHz)	Data Rate (mbps)
802.11	FHSS, DSSS, IR	2.4	1,2
802.11b	DSSS, HR-DSSS	2.4	1,2,5.5,11
802.11a	OFDM	5.2,5.5	6,9,12,18,24,36,48,54
802.11g	OFDM	2.4	1,2,5.5,11,6,9,12,18,24,36,48,54

IEEE 802.11 has released in 1997. There are two data rates which are 1Mbps and 2 Mbps. The signal is transmitted via infrared (IR) signal. The ISM band for 802.11 is 2.4 GHz.

The encoding method for this first standard is Differential Phase Keying (DPSK) for 1Mbps while for 2Mbps us Differential Quaternary Phase keying 9DQPSK).

IEEE 802.11b is the enhancement of 802.11 where the IR has been drop from the later version. For this standard, it has maximum throughput up to 11 Mbps. However, in practise the maximum throughput is about 5.5 Mbps only since the bandwidth is used for communication overhead. The encoding method for this standard is Complementary Code Keying (CCK) while the modulation scheme is Direct Sequence Spectrum (DSSS). In this standard, there are many channels which are available and this depends on the bandwidth that had been allocated by the various national regulatory agencies. The IEEE 802.11b operates at ISM of 2.4 GHz and it can also operate well in wireless LAN with a fixed infrastructure and also in a peer to peer ad hoc networking without infrastructure.

IEEE 802.11g is a standard which has developed in June 2003. This standard works with 2.4 GHz and can operate up to 54 Mbps. The modulation technique used in this standard is OFDM. This standard suffers from interference from other product since it operates at frequency of 2.4 GHz which is heavily used to the point of being crowded.

IEEE 802.11a is a standard that can operate in 5 GHz of ISM band with a maximum data rate of 54 Mbps. This standard use OFDM as the modulation technique. The frequency that is used in this standard is relatively unused compared to another standard that used 2.4 GHz band. So, this is one of the advantages of IEEE 802.11a. However, since this standard has high carrier, so it is not too effective as 802.11b and 802.11g standards. The signal from these standards can easily absorb by walls and slid object wince it has smaller wavelength [13]. This standard can be used at indoor with 8 channels available and 4 channel available to point to point usage.

2.5 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol that is used to map a network layer address to a hardware address such as IP address to MAC address. This protocol has been standardizing by the Internet Engineering Task Force (IEFT) in Request for Comment (RFC) 826 [13].

ARP uses a simple format message which is request message and reply message. Each of these messages has its own code where the request code is 1 while the reply code is 2. The payload of each packet consists of four addresses which are hardware and protocol address of the sender and destination.

The ARP also has cache where it is used to store the mapped link layer address and network layer address. This is to avoid network flooding. Once the route to the destination is used, ARP cache will store the route it the memory. The ARP cache is used with the assumption that the MAC and IP address of the nodes in the network are rarely change.

However, the ARP cache also has its own preconfigured timeout. The AQRP cache will remove the unused entries of route. With the aids of ARP cache, the communication are much more faster without interference of ARP message and this will also utilized the network resources.

Figure 2.3 shows the packet format of ARP message. The size of the ARP message depends on the hardware and protocol used. However, the typical size of the ARP message is 28 bytes. The most important in the ARP packet is the operation codes. This is to differentiate the types of the ARP message.

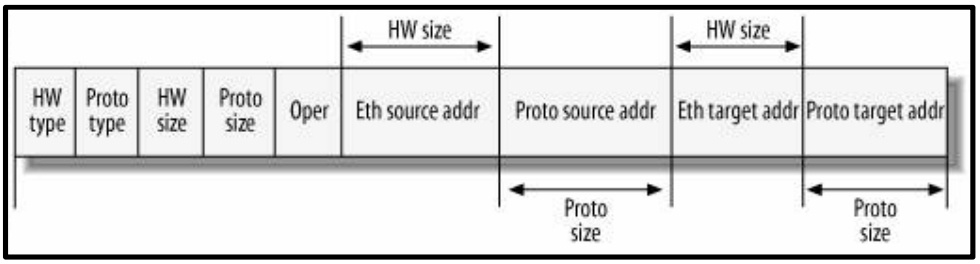

Figure 2.3: Address Resolution Protocol packet format

As mentioned before, there are two importance messages that are used in the ARP protocol which are ARP Request and ARP Reply. These messages are used for the handshaking method in order to establish a route to the destination. In order to find the route, these messages are used by broadcasting from the sender node. Figure 2.4 shows on how the MAC address is resolve by using the ARP.

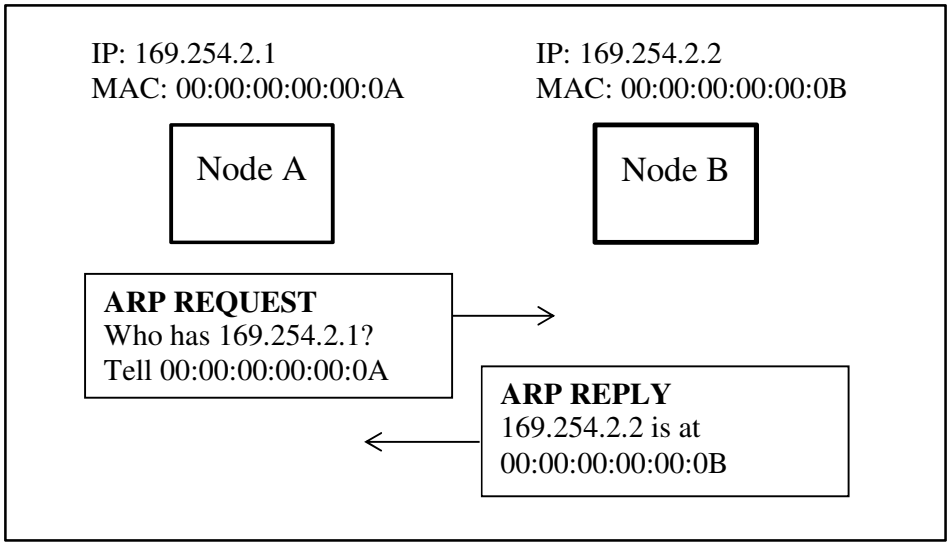

Figure 2.4: ARP resolves the MAC address

According to Figure 2.4, in order to find the MAC address of the sender, the ARP Request and ARP Reply message is used. In this scenario, the Node A is a sender node while Node B is the destination node. Node A want send data to Node B. Before sending the date, Node A will broadcast a query message to find the Mac address of the destination node. Before transmitting the query message, Node A will check its ARP cache. If there is no information regarding Node B, it will directly broadcast the ARP Request message. When Node B hears the request message and find that the request IP is itself, then Node B will reply to the sender by broadcasting ARP Reply to Node A. When Node A receives the reply message, it will send the data and updates its Arp cache.

In this project, the ARP protocol will be used for the three nodes in a network. This is done in test bed and also in simulation. The details is discussing in Chapter 3.

2.6 Internet Control Message Protocol (ICMP)

ICMP is an Internet Protocol Suite which is defining by RFC 792 [13]. ICMP message can be used for several situations such as when data cannot reach its destination, gateway did not have the buffering capacity to forward data and also when the gateway can direct the host to send traffic on a shorter route. ICMP will runs over the IP and it is not a transport layer like TCP and UDP.

Figure 2.5 shows the ICMP packet format. In the packet format, the Time to Live (TTL) is used to indicate the destination node is reach or not. This is done by referring to the TTL where if the TTL exceed 0, an ICMP error message will be generate. The nodes which act as the intermediate nodes in the network will forward the IP data and decrement the time to live field of the IP header by one. If the TTL reached 0, an ICMP error message will be generate. The ICMP messages are usually used when a source node used the Ping application to test the reachability of the destination node. ICMP Request and ICMP Reply are commonly used In the ICMP message.

The ‘differentiated services’ in the ICMP packet is used to determine the types of ICMP message is used. As mentioned before, the ICMP message can be divided into ICMP Request, ICMP Reply and also ICMP error message. The operation code for ICMP Request is ‘8’ while the ICMP Reply is ‘0’.

bit offset	0–3	4–7	8–15	16–18	19–31
0	Version	Header length	Differentiated Services	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options (if Header Length > 5)				
160 or 192+	Data				

Figure 2.5: ICMP Packet Format

\

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter explains in details on the methodology used in this project. An explanation on the hardware, software tools and the simulation software used in this project will be elaborated. In this project, the methodology is divided into four parts which are software, hardware, integration and also the simulation. In the simulation parts, it is divided into five categories which are OMNET++ architecture, AODV simulation and ARP simulation, network design, experiment scenario and experiment evaluation. The methodology of the projects is illustrated in a flow chart and a diagram. Besides, an explanation for each part will be elaborated. The theoretical, practical and simulation determination on the average time, number of packet loss and the throughput of the transmission are explained.

3.2 Hardware and Software Specification

This section elaborates on the hardware tools used in this project. The specification on the components used is also illustrated. Besides, the software tools will also be explained.

3.2.1 PIC Microcontroller (PIC24FJ128GA010)

Programmable Interface Controller (PIC) is an electronic circuit which is used to carry out a vast range of task by using programming. The PIC can be programmed to be a timer or to control any product. There are many applications that used the PIC such as alarm system. In this project the PIC24FJ28GA010 is used where it supports 16 bits and 24 bits address path. This PIC also has the ability to move the information between memory space and data. It also has an instruction set that support multiple addressing modes and it optimized for high-level languages such as ‘C’ language [15]. The overview of the Microchip PIC24FJ28GA010 is shown as in Figure 3.1 and the specification for this PIC is shown in Table 3.1.