

PERFORMANCE ANALYSIS ON MULTIHOP TRANSMISSION USING ARP ROUTING PROTOCOL IN IEEE 802.11 AD HOC NETWORK

Ida S. Md Isa¹, Balakrishnan.Sopna², N. Latif A.Shaari³, A.T.I Fayeez⁴

¹ Telecommunication Department, University Teknikal Malaysia Melaka, Melaka, Malaysia, idasafiza@utem.edu.my

² University Teknikal Malaysia Melaka, Melaka, Malaysia, sopnabalakrishnan123@gmail.com

³ Mechatronic Department, University Teknikal Malaysia Melaka, Melaka, Malaysia, latifazyze@utem.edu.my

⁴ Computer Department, University Teknikal Malaysia Melaka, Melaka, Malaysia, fayeez@utem.edu.my

Abstract

Mobile Ad Hoc Network (MANET) are becoming more and more important in the modern environment. It can be used instantly to connect to the local or remote network without using the pre-existing infrastructure. The mobile or user in the network can together establish the infrastructure. In order to improve the limited range of radio transmission, multiple network 'hops' are needed so that the communication between the mobiles can be establish. There are varieties of protocol that had been proposed for the hopping methods but most of them suffer from high overhead. This project proposed a new method of hopping protocol for IEEE 802.11b using the existing network protocol which is Address Resolution Protocol (ARP). The ARP message is used in the network to find the MAC address of the destination. This can also be done by having multi hops where the proposed method using ARP designed will make an intermediate node act as a router in order to find the destination address and forward the data successfully. In this proposed method, the data is directly passed to the intermediate node and the intermediate node will help to find the route to the destination and passed the data to the destination node. This will reduce the transmission time. From the simulation obtained, it proved that the proposed method using the ARP protocol can works well as the existing network protocol which is Ad Hoc On-Demand Distance Vector (AODV). The simulation is composed into two types of environment which are with and without obstacles. The throughput, the packet loss and the round trip time for various distances is simulated and the results shows that the performance of the proposed method using ARP is much better compared to the AODV.

Index Terms: Address Resolution Protocol (ARP), Ad-Hoc, 802.11 Wifi, Hopping

-----***-----

1. INTRODUCTION

Recently, an ad hoc network is one of the communication technologies that provide the possibility for wireless devices to communicate directly with others. It provides benefits such as reduction of transmission output and decreased battery consumption. The wireless mesh network has become an exciting research area and a popular commercial application of the ad hoc network [1]. Ad hoc network allows the wireless devices to operate within the range of each other in order to communicate in peer-to-peer fashion without the existing of access point. The network has the ability of self-healing structure and this makes the possibility of failing links in communication low even the communicating devices are removed or added in the network.

However, each of the communicating devices has it owns limited range. Due to this, sometimes the data exchange between nodes may not be successful across the network. Thus, multiple 'hops' networks are needed to exchange data across the network In order to do so, a routing protocol is needed where each node in the networks will act as a router to find the destination node. In general, traditional routing protocol used in wired network cannot be applied directly to

wireless and mobile network [2]. There are several considerations are needed before embark on the development of a protocol for a wireless network which is on-trivial due to nodes high mobility [2]. There are many of routing protocol that had been proposed by researches such as Ad Hoc On-Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing (DSR) and etc. However, most of the existing protocol suffered from high overhead network traffic. This paper introduced a new method for ad hoc routing that utilized less overhead network traffic and less computational resources by extending the existing protocol, Address Resolution Protocol (ARP). The simulation is done using the OMNET++ simulation software for three nodes. In this paper, there are two types of environment which are with and without obstacles with different distance and different size of data are done for the ARP and AODV protocol.

2. LITERATURE REVIEW

Several ad hoc routing protocols have utilized topology established routing approach [5]. There are three types of topology established routing which are proactive routing, reactive routing and hybrid routing [6]. The proactive routing protocols focuses on the shortest path algorithms are the most

active routing protocol. All nodes that are connected will be updated in each of the node's table to maintain the configuration of the protocol and were shared among themselves. Therefore, if there are any changes in the network topology, each node will update its routing table [7]. These types of routing are applied in the link-state routing and distance vector routing.

Optimized link state routing (OSLR) maintains routing data by dispatching link state information [8]. If there are any changes in the topology such as movement of nodes, each of the nodes will updates to the discerning nodes so that every nodes in the networks will be updated merely once.

Source-Tree Adaptive Routing (STAR) is another link central protocol. In STAR, the favored paths from each node to other nodes are saved in each of nodes which act as router. This reduced the overhead in the network by removing the periodic updates. This protocol is suitable for a colossal scale networks but it needs colossal recollection and processing since it has to be uphold colossal trees for finished network.

Ad Hoc on Demand Distance Vector Routing (AODV) is an example of pure reactive routing protocol [5]. AODV routing protocol works exclusively on demand basis after it is needed by networks, which fulfilled by nodes inside the networks [9]. Route invention and path maintenance is additionally grasped out on demand basis even if merely two nodes demand to converse alongside every single other. AODV cuts down the demand of nodes in order to always stay alert and to unceasingly notify routing data at every single node. In other words, AODV maintains and discovers paths merely after there is a demand of contact amid disparate nodes [10].

AODV is capable of both unicast and multicast routing. It keeps these paths as long as they are desirable by the sources. The sequence numbers are utilized by AODV to safeguard the freshness of routes [11]. It is loop free, self-starting, and scales to colossal numbers of mobile nodes. AODV has uttered that there were three kinds of manipulation memos for path maintenance that are RREQ, RREP and RERR.

A route request message is transmitted by a node requiring a route of the destination node. As an optimization, AODV uses an expanding ring technique when flooding these messages [13]. Every RREQ carries a time to live value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Every node maintains two separate counters which are a node sequence number and a broadcast id. Route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The

reason one can unicast the message back is that every route forwarding a RREQ caches a route back to the originator.

Nodes monitor the link status of the next hops in active route [13]. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a precursor list which contains the IP address for each of its neighbors that are likely to use it as a next hop towards each destination.

3. ARP PROTOCOL

3.1 Address Resolution protocol (ARP)

ARP is used to find the MAC address by using the IP address in a local area network segment where hosts of the same subnet reside [3]. Each node in the network must have a media access control (MAC) address which has been set and will never change for the life of the device, and an Internet Protocol (IP) address which can be change in the different part of the network. This protocol operates between the layer 2 and layer 3 in the OSI system model. Since this protocol operates in lower level, so the process time at the receiver is decrease thus it will save the battery power. The ARP protocol is used to find the MAC address of the destination via the IP address of the destination. It consists of two types of message which are ARP Request and ARP Reply. Each of these messages has its own operation code. This protocol has been standardized by the Internet Engineering Task Force (IETF) in RFC 826. The typical packet size of an ARP messages is 28 bytes. With this small size of the ARP, this will utilized less overhead.

3.2 ARP routing in ad hoc network

As mentioned before, there are two types of ARP messages that are used to find the MAC address of the destination which established the route to the destination before transmitting the data. There will be a handshaking procedure and the ARP protocol is used in order to find the route to the destination. The ARP Request is broadcast by the sender with an appropriate IP address of destination. In this packet, it contains the destination IP address, the IP and the MAC address of the sender. Once the destination receive this message, the destination will responds by sending the ARP Reply message contains its MAC address and also the IP and MAC address of the sender. When the sender receives this message, then only the data is send through the established route. Besides, the ARP cache is used where there will be no necessary route request needed since it is assume that the MAC and IP address are rarely change. The ARP cache has also a pre-configured timeout to allow the ARP cache to remove the unused entries of route. The purpose of ARP cache is to allow the communicating devices to start communicating faster without interference of the ARP messages and thereby utilized the less network resources [4]. Fig -1 shows the operation of the handshaking between two nodes using the ARP protocol.

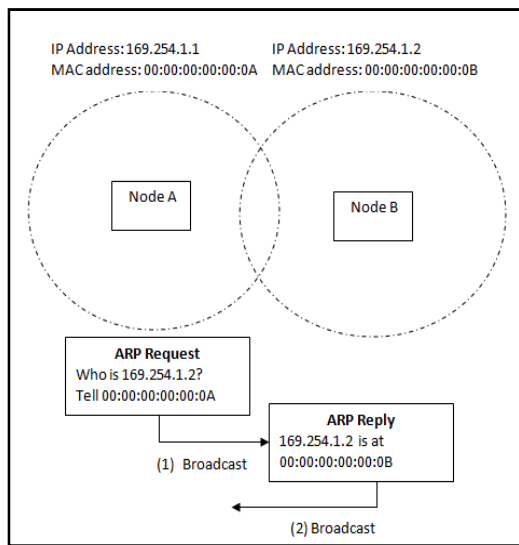


Fig -1: The ARP message used for handshaking

3.3 Multi-hop transmission using ARP protocol

Multi hop transmission happened when the communication between two nodes are out of its limited range. In order to route the data to the destination, an intermediate node is needed. The intermediate node will help the sender to send the data to the destination. In this paper, the proposed method of multi hop is introduced using the ARP protocol. The intermediate node will get the data from the sender and acts as a sender to retransmit the data to the destination. This is done by using the ARP protocol messages which are ARP Reply message and ARP Request message. The flow of the proposed method is shown as in Fig -2.

For multi hop transmission, an intermediate nodes is needed so that the data can be hop to the destination when the sender and the destination node is out of their range. Fig -2 shows the mutihop transmission method in an ad hoc network using the ARP protocol. Node A wants to communicate with Node C but the each of them are out of their range. So, Node B is used as an intermediate node and is positioned in between Node A and Node C. As we can see in Fig -2, the radio range for Node B is overlap with radio range of Node A and Node C. So, Node B can relay the messages between these nodes. The flows of the scenario are illustrated as follows:

1. Node A start its communication by broadcast an ARP Request message asking the location of the destination IP number that it want to communicate with.
2. Node B hears the ARP Request by node A and check that the request is not for Node B. However it will reply an ARP Reply message to Node A to inform that it can help Node A to find the destination address and forward the data to Node A.

3. Once Node A receive reply message from Node B, it will send the acknowledge message to Node B to inform that Node A will start sending the data to Node B.
4. After the acknowledge message, then only Node A transmit a data to Node B.
5. When Node B successfully receive the data, then it will send an acknowledge message to Node A to inform that Node B already receive the data without any loss.
6. Then, Node B will broadcast an ARP Request message to find the destination since the data is not meant to Node B.
7. Since Node B and C are in the same radio boundary, Node C will hears the request message and it found that the request is for Node C and it will broadcast an ARP Reply to Node B.
8. When Node B receive the reply message, then it will send an acknowledge message to Node C to inform that Node B will start forward the data to Node C.
9. After acknowledge Node C, then Node B forward the data to Node C.
10. After Node C successfully received the data, then it will acknowledge Node B by sending an acknowledge message to Node B.
11. Node C will send an ARP Request message to find the destination address of Node A since it is the sender node. This is to inform to Node A that the data is successfully received at the destination.
12. Node B hear the request message from Node C and found that the request is not for Node B and send an ARP Reply to Node C to inform that Node B will help Node C to find the destination address and forward the data.
13. Before start transmitting the reply message, Node C send an acknowledge message to Node B to inform that Node C will start to transmit a data.
14. After acknowledge, then Node C transmit the reply message data to Node B.
15. Node B will send an acknowledge message to Node C once it finished receive the data.
16. Then, Node B will start broadcasting an ARP Request message to find the destination address (Node A).
17. Since Node A and B are in the same radio boundary, then Node A will hear the request message and found that the message is for Node A. Then Node A will broadcast an ARP Reply message to Node B.
18. When Node B get the destination address, then Node B will send an acknowledge message to Node A to inform that it will start forwarding the reply message data to Node A.
19. Then, Node B starts forwarding the reply message data to Node A.
20. When Node A receive the reply message then it will send an acknowledge message to Node B to inform that it already receive the data. Once Node A receives the reply message data from Node C through Node B, then the transmission is done.

The above process describes the communication method involving the ARP Request, ARP Reply and data forwarding. This method used the standard message of the current operation code for the ARP message. The operation code for ARP Request is '0x0001' and the operation code for ARP Reply is "0x0002". In this paper, the method using the ARP protocol is that, the nodes that hear the request message from the sender will help to pass the message to the destination when the sender and destination is out of their radio range. The intermediate node will help the sender to forward the data to the exact destination. The intermediate node will act as a sender in order to forward the data to the destination.

As mentioned before, the ARP message is only in 28 byte of size. So, this causes less overhead transmission data. Since the packet size is small, so it will increase the transmission speed compared to the AODV protocol. For this method, it consists of two steps which are the handshaking procedure where it is a process to find the MAC address of the destination by knowing the destination IP address and the data transmission. Besides, ARP Request and ARP Reply message, the ARP protocol also has an ARP cache. The ARP cache is used to store mapped link layer address and network layer address. This is used with the assumption that the MAC and the IP address rarely change and therefore the transmission of ARP messages is considered unnecessary [4].

The transmission of the ARP message is only done for the first transmission since each of the nodes that include with ARP cache will add all the other's node address in their entries and this allow the communication between the nodes become faster. This is also useful in preventing the network flooding which will caused the interferences of the ARP messages. Besides, this will also utilized less network resources. However, the ARP cache has its own preconfigured timeout. This is to allow the ARP cache to remove the entries that are no longer used or have been changed. In this paper, the timeout of the ARP cache is set to 100ms.

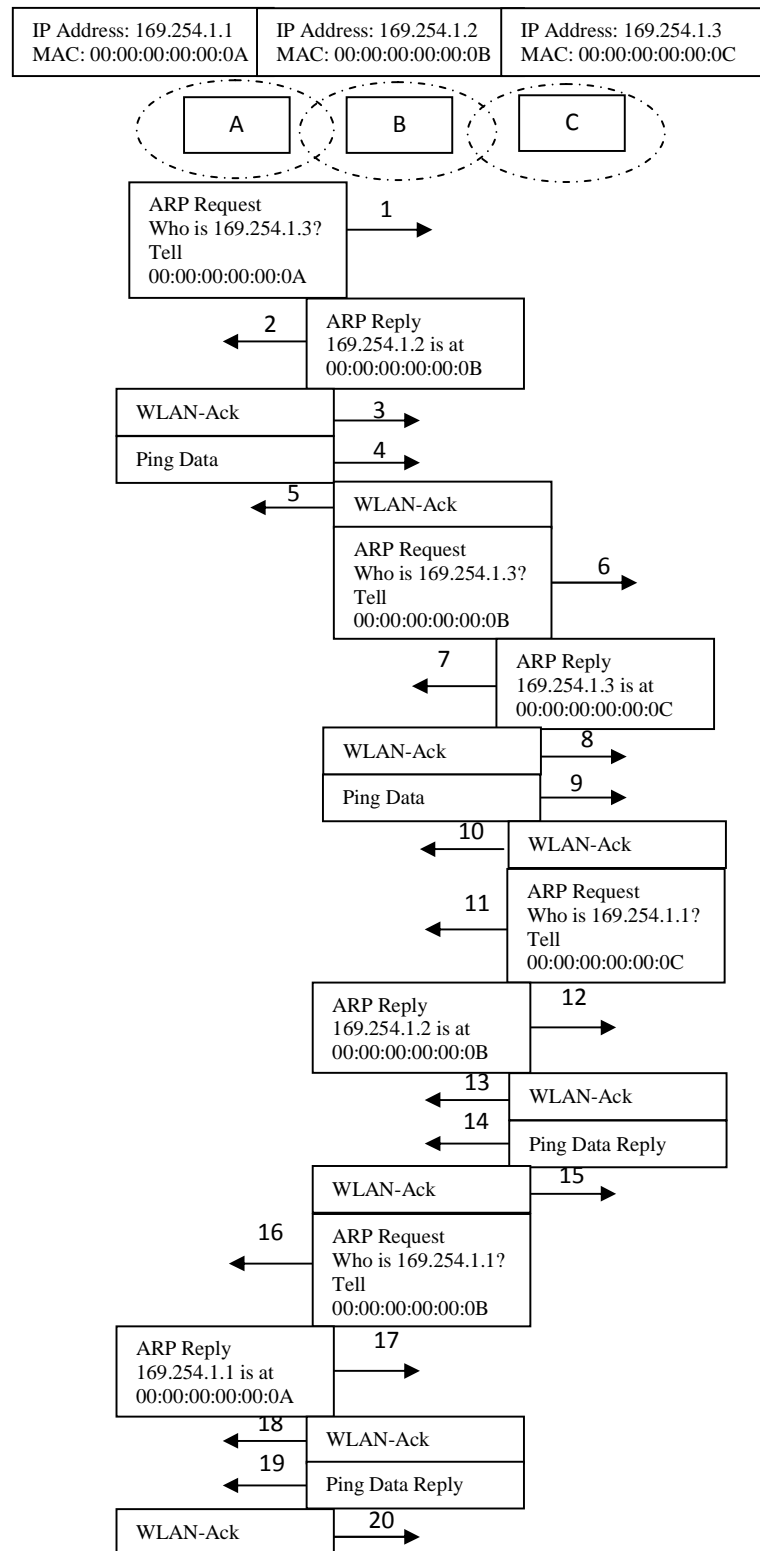


Fig -2: Multi hopping using ARP protocol

4. RESULTS AND ANALYSIS

A simulation is done using the OMNET++ software for 3 nodes of IEEE 802.11b. The parameters that are taken into consideration are the number of packet loss and the throughput. The nodes are simulated in two different environments which are with and without obstacles. The range radio boundary for each node is arranged in order to make a multi hop transmission. Besides, the simulation is done in two different distances and two different sizes of packet data in the two environments. To make the result much more reliable and efficient, a comparison is made for the proposed protocol, ARP protocol with the current existing protocol, AODV protocol.

As mentioned before, the method of this ARP protocol used the ARP cache to make the transmission much faster. The setting time for the ARP cache is set to 100ms. This is also same to the AODV protocol where the memory setting for the cache is set to 100ms. There will be 50 transmissions of data for each of the distance, packet size and for both type of environments. The round trip time (RTT) for each transmission is measured and the average of the RTT is taken. The average of the RTT is given as in equation 1:

$$T (m s) = \frac{\sum_{i=0}^{i=49} T_i}{n} \tag{1}$$

Ti is the average of the round trip time for the transmission of the successful packet send. The n is the number of the successful packet send. Besides RTT, the analysis is also made based on the throughput which is the average rate of the successful message delivery over a communication channel. The throughput is determined in bits per seconds and the size of the data packet is set to 56 bytes and 5000 bytes per packet. The throughput is calculated using the equation (2):

$$Th (bps) = \frac{ICMP \text{ Packet (bits)}}{T(msec)} \tag{2}$$

Fig -3 and Fig -4 shows the two environments of the simulated results. Each of the environments consists of three nodes. As mentioned before, the simulation is done in two different distances which are 282m and 400m.

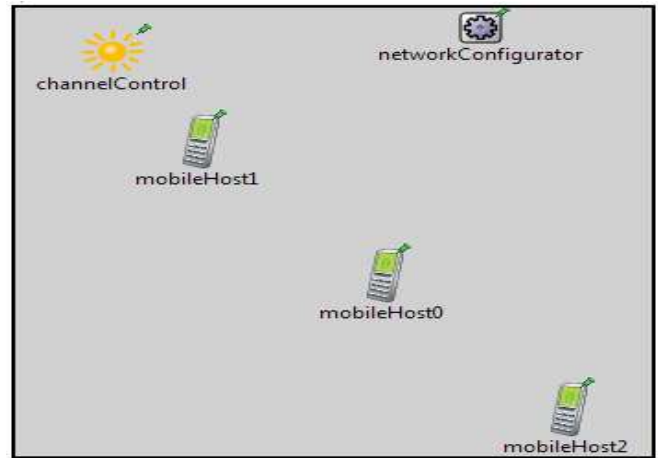


Fig -3: Nodes in a place without obstacles

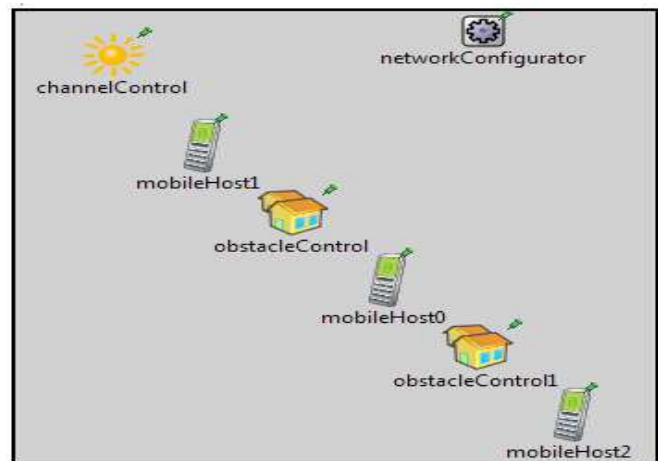


Fig -4: Nodes in a place with obstacles

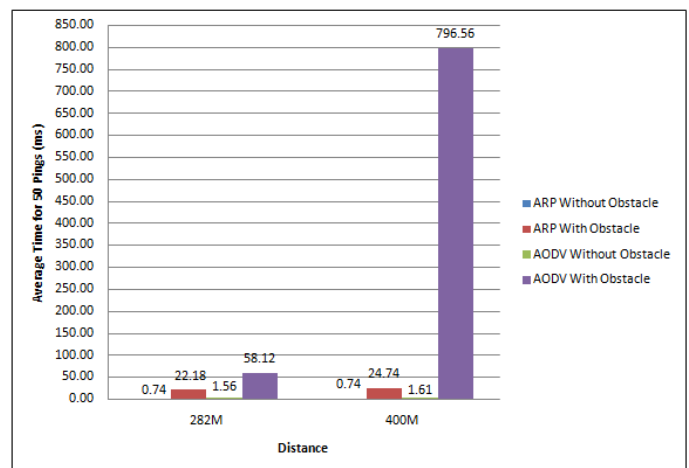


Fig -5: RTT over distances for 56 bytes of data

Fig -5 shows the results of RTT over distances for packet data transmission of 56 bytes. The average of RTT for the two environments with different distances for both protocols is shown. The RTT is calculated based on the average of the successful transmission. The lower the RTT the performance of the system is better. In the environment without obstacles, the time taken for the transmission and reception of the packet data is smaller compared to the place with obstacles for both protocols. This is because, at a place with obstacles, there are many disturbances and this caused the signal to be attenuated and reflected. This is also called as non line of side (NLOS) where the signal from the transmitter passes several obstructions before arriving at the receiver. These create the signals arrive at a receiver at different times, from different paths and with different strength. However, from the graph, it shows that the ARP protocol works well in both environments. Instead, the RTT for ARP protocol in both distances is much better compared to the AODV protocol. This is due to the packet size of the ARP message is much smaller compared to the AODV message packet. The smaller size of packet the faster the transmission and thus good performance can be achieved. Both of these protocol used the handshaking concept where finding the destination address before transmitting the data packet. In order to find the route to the destination, the ARP and the AODV used their own message packet. Since the ARP message packet is smaller compared to the AODV message, the performance of the transmission for ARP is better. By using smaller packet size also will reduce the fragmentation packet where this will cause the transmission delay and thus provide higher RTT.

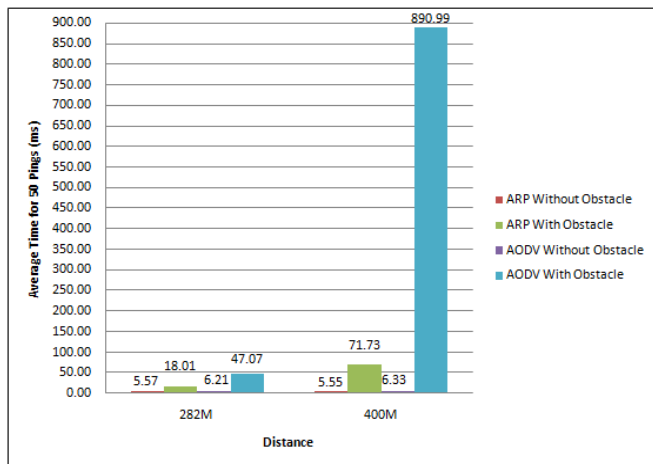


Fig -6: RTT over distances for 5000 bytes of data

Fig -6 shows the results of RTT over distances for packet data transmission of 5000 bytes. The average of RTT for the two environments with different distances for both protocols is shown. This results shows that the RTT for sending a bigger data packet data will increase the RTT. For both protocols, it shows that the RTT for both environments is much higher

when sending 5000 bytes of packet data compared to 56 bytes of packet data. This is due to the fragmentation process where the packet data will be fragment into smaller size before sending to the destination. This will cause the delay in the transmission thus increase the RTT of the transmission. Sometimes, there will also have losses of the fragment data, so the sender needs to resend the data until it received a reply message from the destination to acknowledge that the data is successfully received at the destination. However, the simulation results still shows that the RTT of ARP protocol is much better compared to the AODV protocol for both distances and both environments.

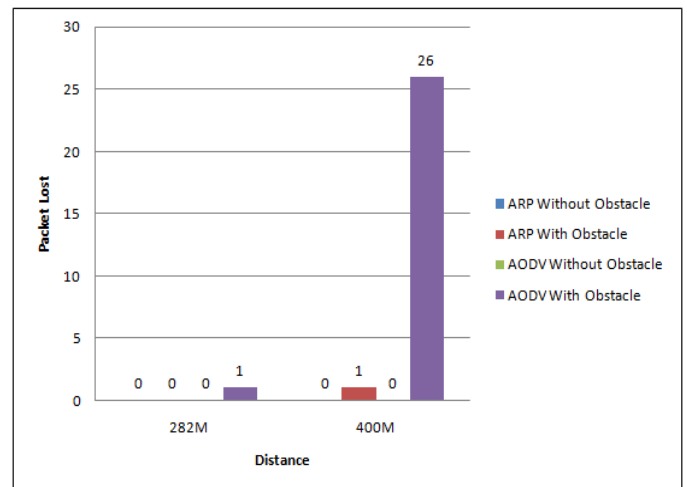


Fig -7: Packet loss over distances for 56 bytes of data

Fig -7 shows the simulation results of packet loss over the distances for packet data transmission of 56 bytes. The number of packet loss for the two environments with different distances for the two protocols is shown here. The results shows that by using the ARP protocol, there is no packet loss for the both environment at distance of 282m but the AODV protocol shows that the is 1 packet loss at this distance of 282m in an obstacles environment. At a distance of 400m, the ARP protocol only has 1 packet loss at an obstacles environment and there is no loss at a place with no obstacles. However, the AODV protocol shows no loss at a place with no obstacles but at a place with obstacles, the AODV protocol has 26 packet loss. From this result, it shows that the ARP protocol has more reliability in data transmission compared to AODV protocol. The proposed ARP methods used the passing concept where the intermediate node will received the data by the sender first then only forward the data to the destination. This caused the losses of the packet data lower. Compared to the AODV protocol, the method is find the route first then only transmit the data to the destination. The transmission of the data will follow the dedicated route when sending the data. Sometime, there is a break or link failure and this caused the

transmission of the packet data to be unsuccessful and retransmission need to be done.

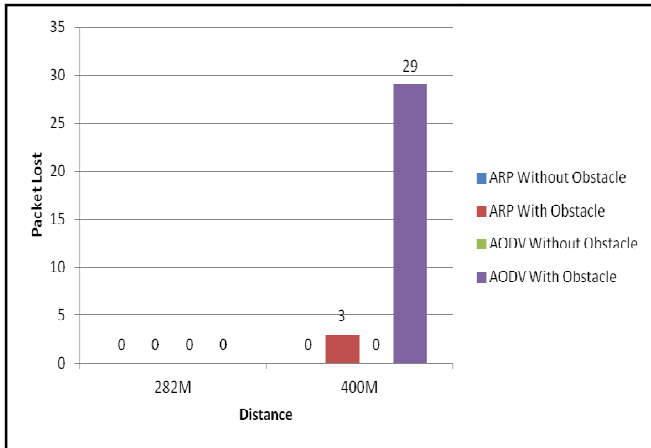


Fig -8: Packet loss over distances for 5000 bytes of data

Fig -8 shows the simulation results of packet loss over the distances for packet data transmission of 5000 bytes. The number of packet loss for the two environments with different distances for the two protocols is shown here. From the graph, it shows that there is no packet loss for ARP protocol in both environments at a distance of 282m. This is same to AODV protocol. However at a distance of 400m in an obstacles environment, there are 3 packet losses for ARP protocol and 29 packet losses for AODV protocol. The losses are much higher for 5000 bytes data transmission compared to 56 bytes at this distance. This proves that with higher packet size of data, the higher the packet loss. Higher distance also provides higher packet loss. However, this result also shows that the ARP protocol is much better compared to the AODV protocol since the ARP protocol could transmit more data with lower losses.

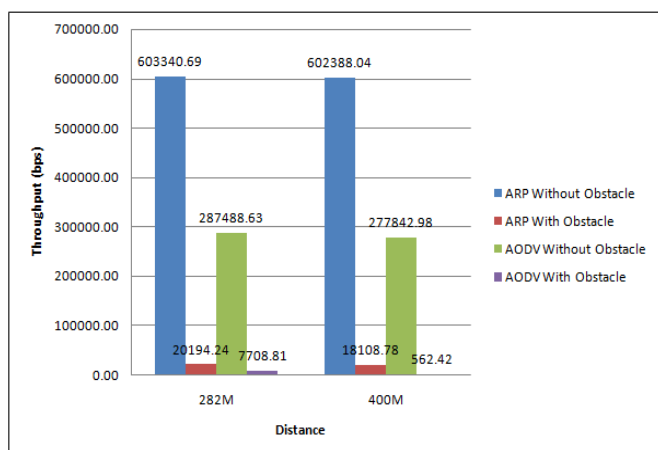


Fig -9: Throughput over distances for 56 bytes of data

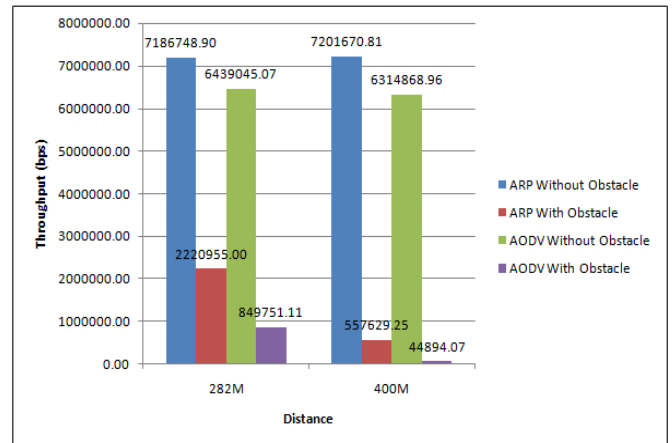


Fig -10: Throughput over distances for 5000 bytes of data

Fig. 9 shows the simulation results of throughput over the distances for packet data transmission of 56 bytes. From the graph, it shows that at both distances, the ARP protocol is much better compared to the AODV protocol for both environments. This different is due to the RTT time for the transmission. As explain before, the ARP protocol have lower RTT compared to the AODV protocol. The higher the RTT, the lower the throughput. However, in the transmission, the higher the throughput gives better performance of the transmission system. This is also same when using 5000 bytes of packet data transmission. From Fig -10, we can see that the throughput for 5000 bytes of data transmission is much lower compared to 56 bytes of data transmission. This is due to the RTT for 5000 bytes of data transmission have much higher RTT compared to 56 bytes of data transmission. However, both of the graph shows that the ARP protocol have much higher throughput compared to the AODV protocol.

CONCLUSIONS

This paper introduces the new method of hopping using the ARP routing protocol which operate in an ad hoc network. The route to the destination is determined by using the ARP protocol via OMNeT ++ simulation. In order to make the results more accurate, a comparable is made by using the existing protocol which is AODV protocol. The results of these two protocols are done in term of the packet loss, throughput and the round trip time in two different environment and distances. From the results obtained, it shows that the ARP protocol works better compared to the AODV protocol in term of the RTT, the packet loss and also the throughput. This also shows that the ARP protocol also works well not only in an open space area but also at a place with obstacles. Moreover, based on the simulation, it shows that the performance of these two protocols is also affecting by the environment and also the distances between the sender and the destination nodes. However, the ARP protocol do works better compared to the AODV protocol.

ACKNOWLEDGEMENTS

We would like to thank the University Teknikal Malaysia Melaka, UTeM for making this project successful.

REFERENCES

- [1] Sung-Hee Lee, and Yong-Bae Ko, "An Efficient Multi-Hop ARP Scheme for Wireless LAN Based Mesh Networks," IEEE 2006: 1-6, Proceeding of 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks, September 2006.
- [2] Liza Bt. Abdul Latiff, "Quadrant Based Directional Routing Protocol For Mobile Ad Hoc Network", PHD Thesis, Universiti Teknologi Malaysia, 2007.
- [3] P.Limmaneewichid and W.Lilakiatsakun, "The Cryptographic Trailer Based Authentication Scheme for ARP," in ECTI-CON, 8th International Conference, May 2011.
- [4] Anders Lundstrom and Magnus Westbergh, "A New Routing Strategy for Mobile Ad Hoc Communication," Master Thesis, University of Kalmar Sweden, 2004.
- [5] Ida Syafiza Md Isa, "Implementing Multihop Transmission in Wireless Low Rate IEEE 802.11 Network" UTM, 2012.
- [6] Bernhard henchleitner and Karl Entacher, "A simple OMNET++ queuing experiment using different random number generators" 5 December, 2002.
- [7] Neha Rani, Preeti Sharma and Pankaj Sharma, "Performance Comparison Of Various Routing Protocols In Different Mobility Models", Ghaziabad: Department of Computer Science, A.B.E.S. Engineering College, 2012.
- [8] Pankaj Kumar and Suman Deswal, "Performance Comparison of Standardized Ad-Hoc Routing Protocols AODV, DSDV," pp. volume 2, no.4, July-August 2011.
- [9] Sun, Jun-Zhao, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing," Universiti of Oulum, Finland: MediaTeam, Machine Vision and Media Processing Unit, Infotech Oulu.
- [10] Lin, Clifton, "AODV Routing Implementation for Scalable Wireless Ad-Hoc Network Simulation (SWANS)," S.1: Java in Simulation Time/Scalable Wireless Ad Hoc Network Simulator, April 2004.
- [11] Akshai Aggarwal, Dr. Savita Ghandi, Nirbhay Chaubey, Pathik Shah, Madhvi Sadhwani, "A Novel Approach To Secure Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol From Insider Attacks In MANETS," International Journal of Computer Networks & Communications (IJCNC), July 2012.
- [12] Neha Rani, Preeti Sharma and Pankaj Sharma, "Performance Comparison Of Various Routing Protocols In Different Mobility Models," Department of Computer Sciences, A.B.E.S. Engineering College, 2012.
- [13] G.Ibanez, Member, IEEE, J.A.Carral, J.M Arco, D.Rivera and A.Montalvo, "ARP-Path: ARP Based, Shortest Path Bridges," IEEE Communication Letters, vol. 15, July 2011.
- [14] Amandeep and Gurmeet Kaur, "Performance Analysis of AODV Routing Protocol In MANETS," IJEST, vol. 4, August 2012.
- [15] Ida S.Md Isa, "Multi-hop Transmission in IEEE 802.11 Low rate Ad hoc Network Using ARP-Route", JTEC, ISSN No 2180-1843, Jun 2013.