Improved Performance of Wireless Mobile Ad Hoc Networks (MANET) by using PWAODV Mechanism

BUSHRA NAJIB TALIB ALSUNBULI1, DR M.NAGARATNA2, HASAN FALAH MOHISIN FAKHRULDEEN3

M.Tech, ECE Dept, JNTU, Hyderabad, AP-INDIA. Email:bosh_1986@yahoo.com. Prof, CSE Dept, Hyderabad, AP-INDIA. E-mail: mratnajntu@gmail.com. M.Tech, ECE Dept, JNTU, Hyderabad, AP-INDIA. E-mail: hfmuhsen@yahoo.com.

Abstract: This project deals with wireless Mobile Ad hoc Networks (MANETs). In this project, an improved AODV– PWAODV (Piggyback and weighted neighbor stability Ad- hoc On-demand Distance Vector routing) protocol with lower route cost and smaller delay is presented. In the algorithm we introduce a piggyback mechanism and weighted neighbor stability algorithm. Essentially, the route cost can be reduced greatly by the use of piggyback mechanism and the link stability algorithm decreases the delay because of ensuring the robustness of the network topology. Finally, by comparison in the simulation via NS2, our newly-mentioned protocol could acquire better route cost and delay performances.

Keywords: Mobile Ad hoc Networks (MANETs), PWAODV, NS2, Performance.

I. INTRODUCTION

Recently, the mobility model is considered generally as an important aspect in the area of wireless network, especially in Ad hoc networks. Then the probability of breaking of links may increase and the disruption will lead to higher route cost and longer delay in view of frequent route repair. So exploring the stability of links has become necessary and important particularly. In order to enhance the link stability, GPS position system and the idea of cross-layer have some contribution to this. Unfortunately, the cost of GPS is too high in order to meet the strict requirements of hardware and the algorithms of cross-layer are so complex to achieve. Then, some new link stability algorithms begin to appear. One of them bases on the neighbor change ratio, which overcomes the faults mentioned above so it is simple and cheap. But the problem of the method is that the nodes still need to send Hello packets periodically in spite of forwarding control packets or data packets which have carried the neighbor messages of their neighbors. To solve the issue, we introduce the piggyback mechanism into the neighbor stability algorithm, as this the route cost will be reduced greatly. To make the links more stable to get smaller delay, the stability of two parts included the current time and historical time is considered. Finally, the thought is implemented in AODV protocol. A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed wireless networks. AODV as an on-demand hop-by-hop based routing protocol is applied to Ad hoc networks, and it will start to create route when the source requires.

II. MOBILE AD_HOC NETWORKS (MANETs) ISSUES&AODV

A. Wired Vs Wireless Networks

The different types of networks available today are Wired and Wireless networks. Wired are differentiated from wireless as being wired from point to point. The biggest difference between these two types of networks is one uses network cables and one uses radio frequencies. A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2,000 feet. A wireless network is a lot less secure and transmission speeds can suffer from outside interference. Although wireless networking is a lot more mobile than wired networking the range of the network is usually 150-300 indoors and up to 1000 feet outdoors depending on the terrain. The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network, and their higher cost is offset by the benefit of easier installation and built-in security features.

Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may cost three or four times as
much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g. Wired LANs offer superior performance. A traditional Ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs a little more and is readily available. Fast Ethernet should be sufficient for file sharing, gaming, and high-speed Internet access for many years into the future. Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub. Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. Furthermore, wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint.

As more wireless devices utilize the 802.11 LAN more heavily, performance degrades even further. The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the wireless network range. However, many computers are larger desktop models, and even mobile computers must sometimes be tied to an electrical cord and outlet for power. This undermines the mobility advantage of wireless networks in many organizations and homes. For any wired network connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls.

However, firewall software products like Zone Alarm can be installed on the computers themselves. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software. In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted. The weaknesses of wireless security are more theoretical than practical. Wireless networks protect their data through the Wired Equivalent Privacy (WEP) encryption standard that makes wireless communications reasonably as safe as wired ones. No computer network is completely secure. Important security considerations for organizations tend to not be related to whether the network is wired or wireless but rather ensuring that the firewall is properly configured, employees are aware of the dangers of spoof emails, they are away of spy ware and how to avoid and that anyone outside the organization does not have unauthorized access to the network.

B. Wireless Networks

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users who no longer need wires to stay connected with their workplace and the Internet. Ironically, the very devices that provide wireless service to these clients need lots of wiring themselves to connect to private networks and the Internet. A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier. As shown in fig.1

The last link with the users is wireless, to give a network connection to all users in a building or campus. The backbone network usually uses cables. A wireless network, which uses high-frequency radio waves rather than wires to communicate between nodes, is another option for home or business networking. Individuals and organizations can use this option to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure. An ad-hoc or peer-to-peer.

---

Fig. 1 wireless network.

Wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. An infrastructure wireless network consists of an access point or a base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect or bridge the wireless LAN to a wired LAN, allowing wireless computer access to LAN.
resources, such as file servers or existing Internet Connectivity. There are four basic types of transmissions standards for wireless networking. These standards define all aspects of radio frequency wireless networking. They have established four transmission standards: 802.11, 802.11a, 802.11b, 802.11g. The basic differences between these four types are connection speed and radio frequency. 802.11 and 802.11b are the slowest at 1 or 2 Mbps and 5.5 and 11Mbps respectively. They both operate off of the 2.4 GHz radio frequency. 802.11a operates off of a 5 GHz frequency and can transmit up to 54 Mbps and the 802.11g operates off of the 2.4 GHz frequency and can transmit up to 54 Mbps. Actual transmission speeds vary depending on such factors as the number and size of the physical barriers within the network and any interference in the radio transmissions.

Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal. Interference can be caused by other devices operating on the same radio frequency and it is very hard to control the addition of new devices on the same frequency. Usually if your wireless range is compromised considerably, more than likely, interference is to blame. A major cause of interference with any radio signals are the materials in your surroundings, especially metallic substances, which have a tendency to reflect radio signals. Needless to say, the potential sources of metal around a home are numerous—things like metal studs, nails, building insulation with a foil backing and even lead paint can all possibly reduce the quality of the wireless radio signal. Materials with a high density, like concrete, tend to be harder for radio signals to penetrate, absorbing more of the energy. Other devices utilizing the same frequency can also result in interference with your wireless. For example, the 2.4GHz frequency used by 802.11b-based wireless products to communicate with each other. Wireless devices don't have this frequency all to themselves. In a business environment, other devices that use the 2.4GHz band include microwave ovens and certain cordless phones.

On the other hand, many wireless networks can increase the range of the signal by using many different types of hardware devices. A wireless extender can be used to relay the radio frequency from one point to another without losing signal strength. Even though this device extends the range of a wireless signal it has some drawbacks. One drawback is that it extends the signal, but the transmission speed will be slowed. There are many benefits to a wireless network. The most important one is the option to expand your current wired network to other areas of your organization where it would otherwise not be cost effective or practical to do so. An organization can also install a wireless network without physically disrupting the current workplace or wired network.

Wireless networks are far easier to move than a wired network and adding users to an existing wireless network is easy. Organizations opt for a wireless network in conference rooms, lobbies and offices where adding to the existing wired network may be too expensive to do so.

1. **Infrastructure Networks**

Infrastructure network have fixed network topology. Wireless nodes connect through the fixed point known as base station or access point. In most cases the access point or base station or connected to the main network through wired link. The base station, or access point, is one of the important elements in such types of networks. All of the wireless connections must pass from the base station. Whenever a node is in the range of several base stations then it connect to any one of them on the bases of some criteria. As shown in fig.2.

![Fig 2. Infrastructure wireless network](image)

2. **Mobile Ad-hoc Networks (MANETs)**

Internet usage has skyrocketed in the last decade, propelled by web and multimedia applications. While the predominant way to access the Internet is still cable or fiber, an increasing number of users now demand mobile, ubiquitous access whether they are at work, at home or on the move. For instance, they want to compare prices on the web while shopping at the local department store, access Internet “navigation” aids from their car, read e-mail while riding a bus or hold a project review while at the local coffee shop or in the airport lounge. The concept of wireless, mobile Internet is not new. When the packet switching technology, the fabric of the Internet, was introduced with the in 1969, the Department of Defense immediately understood the potential of a packet switched radio technology to interconnect mobile nodes in the battlefield. The DARPA Packet Radio project which began in the early 70’s helped establish the notion of ad hoc wireless networking. This is a technology that enables...
In the next period of time, the MANETs need efficient protocols for these networks is a complex issue. Despite the advances in radio technology, major success have been reported in military and quite recently in civilian applications. The MANETs can be used in battlefields, disaster recovery, homeland defense, etc. The MANETs can be used in battlefields, disaster recovery, homeland defense, etc.

Therefore one can say that ad hoc networks basically have two forms, one is static ad hoc networks (SANET) and the other one is called mobile ad hoc networks (MANET). Mobile Ad-hoc Networks (MANETs) are self-organizing, self-configuring and infrastructure-less multi-hop wireless networks, where each node communicates with other nodes directly or indirectly through intermediate nodes without any infrastructure. Such temporary networks can be used in battle-fields, disaster areas, military applications, mining operations and robot data acquisition. Besides these characteristics they present challenges like limited energy, dynamic topology, low bandwidth and security. The description of the arrangement of the MANETs, called topology, is usually temporary or dynamically changed with time. In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. As shown in fig.3, the set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining aviable routing paths and delivering messages in a decentralized environment where network topology

un tethered, wireless networking in environments where there is no wired or cellular infrastructure (e.g., battlefield, disaster recovery, etc); or, if there is an infrastructure, it is not adequate or cost effective. The term “ad hoc” implies that this network is a network established for a special, often extemporaneous service customized to applications. So, the typical ad hoc network is set up for a limited period of time. The protocols are tuned to the particular application (e.g., send a video stream across the battlefield; find out if a fire has started in the forest; establish a Videoconference among 3 teams engaged in a rescue effort).

The application may be mobile and the environment may change dynamically. Consequently, the ad hoc protocols must self-configure to adjust to environment, traffic and mission changes. What emerges from these characteristics if the vision of an extremely flexible, malleable and yet robust and formidable network architecture. An architecture that can be used to monitor the habits of birds in their natural habitat, and which, in other circumstances, can be structured to launch deadly attacks onto unsuspecting enemies. Because of its mobile, non-infrastructure nature, the ad hoc network poses new design requirements.

The first is self-configuration (of addresses and routing) in the face of mobility. At the application level, ad hoc network users typically communicate and collaborate as teams (for example, police, firefighters, medical personnel teams in a search and rescue mission). These applications thus require efficient group communications (multicasting) for both data and real time traffic. Moreover, mobility stimulates a host of location based services nonexistent in the wired Internet. The complexity of mobile ad hoc network designs has challenged generations of researchers since the 70’s. Thanks in part to the advances in radio technology, major success have been reported in military as well as civilian applications on this front (e.g., battlefield, disaster recovery, homeland defense, etc). At first look, these applications are mutually exclusive with the notion of “infrastructure networks and the Internet” on which most commercial applications rely.

This is in part the reason why the ad hoc network technology has had a hard time transitioning to commercial scenarios and touching people’s everyday lives. This may soon change, however. An emerging concept that will reverse this trend is the notion of “opportunistic ad hoc networking”. An opportunistic ad-hoc subnet connects to the Internet via “wireless infrastructure” links like 802.11 or 2.5/3G, extending the reach and flexibility of such links. This could be beneficial, for example, in indoor environments to interconnect out of reach devices; in urban environments to establish public wireless meshes which include not only fixed access point but also vehicles and pedestrians; and; in Campus environments to interconnect groups of roaming students and researchers via the Internet. It appear thus that after more than 30 years of independent evolution, ad hoc networking will get a new spin and wired Internet and ad hoc networks will finally come together to produce viable commercial applications. Ad-hoc networks also called infrastructure less networks are complex distributed systems consist of wireless links between the nodes and each node also works as a router to forwards the data on behalf of other nodes. The nodes are free to join or left the network without any restriction. Thus the networks have no permanent infrastructure. In ad hoc networks the nodes can be stationary or mobile. Therefore one can say that ad hoc networks basically have two forms, one is static ad hoc networks (SANET) and the other one is called mobile ad hoc networks (MANET).
fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network.

Mobile Ad-hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly exile and robust. The characteristics of these networks are summarized as follows:

1. No centralized controller and infrastructure. Intrinsic mutual trust.
2. Dynamic network topology. Frequent routing updates.
3. Autonomous, no infrastructure needed.
4. Can be set up anywhere.
5. Energy constraints.

Generally, the communication terminals have a mobility nature which makes the topology of the distributed networks time varying. The dynamical nature of the network topology increases the challenges of the design of ad hoc networks. Each radio terminal is usually powered by energy limited power source (as rechargeable batteries). The power consumption of each radio terminal could be divided generally into three parts, power consumption for data processing inside the RT, power consumption to transmit its own information to the destination, and finally the power consumption when the RT is used as a router, i.e. forwarding the information to another RT in the network. The energy consumption is a critical issue in the design of the ad hoc networks. The mobile devices usually have limited storage and low computational capabilities. They heavily depend on other hosts and resources for data access and information processing. A reliable network topology must be assured through efficient and secure routing protocols for Ad Hoc networks. Application areas:

- Military or police exercises.
- Disaster relief operations.
- Mine site operations.
- Urgent Business meetings.
- Robot data acquisition.

III. PROJECT DESCRIPTION & SYSTEM ANALYSIS

Recently, the mobility model is considered generally as an important aspect in the area of wireless network, especially in Ad hoc networks. Then the probability of breaking of links may increase and the disruption will lead to higher route cost and longer delay in view of frequent route repair. So exploring the stability of links has become necessary and important particularly. In order to enhance the link stability, GPS position system and the idea of cross-layer have some contribution to this. Unfortunately, the cost of GPS is too high in order to meet the strict requirements of hardware and the algorithms of cross-layer are so complex to achieve. Then, some new link stability algorithms begin to appear. One of them bases on the neighbor change ratio which over comes the faults mentioned above so it is simple and cheap. But the problem of the method is that the nodes still need to send Hello packets periodically in spite offer warding control packets or data packets which have carried the neighbor messages of their neighbors. To solve the issue, we introduce the piggyback mechanism into the neighbor stability algorithm, as this the route cost will be reduced greatly. To make the links more stable to get smaller delay, the stability of two parts included the...
current time and historical time is considered. Finally, the thought is implemented in AODV protocol.

A. Brief Review of Piggyback Mechanism

AODV as an on-demand hop-by-hop based routing protocol is applied to Ad hoc networks, and it will start to create route when the source requires. Due to AODV protocol combining the advantages of DSR and DSDV it is a very important protocol in wireless network. In AODV protocol, some periodic Hello messages are redundant when control packets or data packets which include many messages of nodes to its neighbors are transmitted correctly. Obviously, such redundancy will increase route cost and energy consumption, even bring the deterioration of the entire network. The idea of piggyback is displayed by the way that Hello messages will not need to be broadcasted if a node has transmitted the packets such as control or data packets in a Hello interval. Although we can benefit from the lower route cost by use of the thought of piggyback, the network topology may be damaged in the case of the accidental losing of control packets or data packets. The fault will make the performance of delivery ratio weak, but overall, the advantage is more prominent.

B. PWAODV Protocol

The PWAODV is implemented based on the version ofns-2.31, with the concrete steps described as below: first, in AODV protocol, we introduce the piggyback mechanism to restrict the redundant transmission of Hello messages, and in the RREQ and RREP add the parameter of neighbor stability NCRpath which will be updated when intermediate nodes forward packets; then we only cache the recent K NCRs in the table by covering updating the oldest NCR; finally, we select the route with the largest sequence of destination node or equal sequence but more stability or the two aspects equal but less hops to send the data. As the same as AODV, our protocol also broadcasts a RREQ if the source node needs to send a data and no valid route. But the difference is that in PWAODV the NCRpath will be copied in the routing table when the intermediate node receives the RREQ firstly. Then, for the same RREQ received later, just update the routing table and reverse path only if the item of NCRpath is greater. In this way, the RREQ reaches the destination node and the final path will be the most stable one. Next, the destination node will reply a RREP and reply again only if the later received RREQ has greater sequence or equivalent one but greater NCRpath.

C. Existing System

Existing system is AODV protocol; Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. Some periodic Hello messages are redundant when control packets or data packets which include many messages of nodes to its neighbors are transmitted correctly. AODV does not play any role. When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. The route is made available by unicasting a RREP back to the origination of the RREQ. A node may offer connectivity information by broadcasting local Hello messages. A node should only use hello messages if it is part of an active route. Every HELLO_INTERVAL milliseconds, the node checks whether it has sent a broadcast within the last HELLO_INTERVAL.

D. Proposed System

In the algorithm we introduce a piggyback mechanism and weighted neighbor stability algorithm. The idea of piggyback is displayed by the way that Hello messages will not need to be broadcasted if a node has transmitted the packets such as control or data packets in a Hello interval. We add the weighted neighbor stability algorithm to acquire more robust route whose delay time must be smaller.

E. Piggybacking

Table1: Example of Piggybacking Mechanism

<table>
<thead>
<tr>
<th>No.</th>
<th>A Node</th>
<th>Intermediate Step</th>
<th>Piggybacked Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>a1 a2</td>
<td>a1 a2</td>
<td>a1 a2</td>
</tr>
<tr>
<td>2</td>
<td>a3 a4</td>
<td>a3 a4</td>
<td>a3 a4</td>
</tr>
<tr>
<td>3</td>
<td>a5 a6</td>
<td>a5 a6</td>
<td>a5 a6</td>
</tr>
<tr>
<td>4</td>
<td>a7 a8</td>
<td>a7 a8</td>
<td>a7 a8</td>
</tr>
<tr>
<td>5</td>
<td>a9 a10</td>
<td>a9 a10</td>
<td>a9 a10</td>
</tr>
<tr>
<td>6</td>
<td>a11 a12</td>
<td>a11 a12</td>
<td>a11 a12</td>
</tr>
</tbody>
</table>

This example illustrates one method of piggybacking for reducing data read during systematic node repair. Consider two instances of a (6, 4) MDS code as shown in table 1a, with the 8 message symbols {ai} 4 i=1 and {bi} 4 (each column of table3.1a depicts a single instance of the code). One can verify that the message can i=1 be recovered from the data of any 4 nodes. The first step of piggybacking involves adding 2 iai to the second i=1 symbol of node 6 as shown in table1. The second step in this construction involves subtracting the second symbol of node 6 in the code of table.1 from its first symbol. The resulting code is shown in table.1. This code has 2 sub stripes (the number of columns in table.1).

We now present the repair algorithm for the piggybacked code of table1. Consider the repair of node
Improved Performance of Wireless Mobile Ad Hoc Networks (MANET) by using PWAODV Mechanism

1. Under our repair algorithm, the symbols $b_2, b_3, b_4$ and $b_i$ are downloading from the other nodes, and $b_1$ is decoded. In addition, the second symbol $(4b_i + 2ai)$ of node 6 is downloaded. Subtracting out the components of $i=1$ gives the piggyback 2. Finally, the symbol $a_2$ is downloaded from node 2 and subtracted to obtain $i=1$ which is $a_1$. Thus, node 1 is repaired by reading only 6 symbols which are 75% of the total size of the message. Node 2 can be repaired in a similar manner. Repair of nodes 3 and 4 follows on similar lines except that the first symbol of node 6 is read instead of the second. The piggybacked code is MDS, and the entire message can be recovered from any 4 nodes as follows. If node 6 is one of these four nodes, then add its second symbol to its first, to recover the code of Fig. 1b. Now, the decoding algorithm of the original code of Fig. 1a is employed to first recover $\{ai\}$, which then allows for removal of $i=1$ the piggyback $(2ai)$ from the second sub stripe, making the remainder identical to the code of Table I. To cache information efficiently to reduce the control overhead, Piggybacking literally refers to carrying someone on one’s back. Same idea is implemented in networking to improve the communication such as the process of sending data along with the acknowledgment is called piggybacking in networking. Piggybacking technique applied in MAC layer has following advantages.

1. It can reduce the transmission of control packets and reduce overhead.
2. Stations can allocate/reserved bandwidth resources by extracting the piggybacking information.

F. Route Discovery

In this module, there are the two main processes taken into account.

- Route request
- Route reply

When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID. As shown in Fig.4. In the example, Node 1 wishes to send a message to Node 3. Node 1’s Neighbors are Nodes 2 + 4. Since Node 1 cannot directly communicate with Node 3, Node 1 sends out a RREQ. The RREQ is heard by Node 4 and Node 2. When Node 1’s Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast the RREQ to their set of Neighbors. The message keeps getting rebroadcast until its lifespan is up. If Node 1 does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan and a new ID number. All of the Nodes use the Sequence Number in the RREQ to insure that they do not rebroadcast a RREQ. As shown in Fig.5.

![Fig.4. Broadcasts a Route Request (RREQ) message.](image-url)
Fig. 5. broadcasts a Route Reply (RREP) message.

In the example, Node 2 has a route to Node 3 and replies to the RREQ by sending a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ. Sequence numbers serve as time stamps. They allow nodes to compare how “fresh” their information on other nodes is. Every time a node sends out any type of message it increases its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence number signifies a fresher route. This is possible for other nodes to figure out which one has more accurate information. In the example, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in its Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply.

IV. NETWORK SIMULATION & SOFTWARE REQUIREMENT

People communicate. One way or another, they exchange some information among themselves all the times. In the past several decades, many electronic technologies have been invented to aid this process of exchanging information in an efficient and creative way. Among these is the creation of fixed telephone networks, the broadcasting of television and radio, the advent of computers, and the emergence of wireless sensation. Originally, these technologies existed and operated independently, serving their very own purposes. Not until recently that these technological wonders seem to converge, and it is a well-known fact that a computer communication network is a result of this convergence. System modeling refers to an act of representing an actual system in a simply way. System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented. Traditionally, there are two modeling approaches: analytical approach and simulation approach.

A. Analytical Approach

The general concept of analytical modeling approach is to first come up with a way to describe a system mathematically with the help of applied mathematical tools such as queuing and probability theories, and then apply numerical methods to gain insight from the developed mathematical model. When the system is simple and relatively small, analytical modeling would be preferable (over simulation). In this case, the model tends to be mathematically tractable. The numerical solutions to this model in effect require lightweight computational efforts. If properly employed, analytical modeling can be cost-effective and can provide an abstract view of the components interacting with one another in the system. However, if many simplifying assumptions on the system are made during the modeling process, analytical models may not give an accurate representation of the real system.
B. Simulation Approach

Simulation is a process of designing a model of a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system. Simulation is widely-used in system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few. Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach. In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefully consider a measure under consideration and not to include irrelevant detail into the simulation. As shown in fig.6 and fig.7 below.

C. Introduction to Network Simulator 2(NS2)

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors. Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. As shown in fig.8 below.

D. Expected Output in NS2

We will show the output in two ways

Nam (Network animator) window

In this window, we can show the animation of packet transfer, packet drop.

Xgraph

In this window, we can show the result like as packet delivery radio, packet loss, and delay as graph

Fig. 6. Packet Arrival Event

Fig. 7. Successful Packet Transmission

Fig. 8. NS2 Structure

Fig. 9. Network Animator Window

Fig. 10. X graph Window
E. Turn on Tracing

To show the result we need to trace the information from network environment. For tracing information there is the two temporary files required name as nam file and trace file. Nam file is used to store the temporary information about nam window, and trace file is used to trace the network environment.

![Fig. 11. Tracing Information](image)

<table>
<thead>
<tr>
<th>event</th>
<th>time</th>
<th>from node</th>
<th>to node</th>
<th>pkt_type</th>
<th>pkt_size</th>
<th>flags</th>
<th>fid</th>
<th>src_addr</th>
<th>dst_addr</th>
<th>seq</th>
<th>pkt_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>1.3556</td>
<td>3 2</td>
<td>40</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>1.3556</td>
<td>0 0</td>
<td>40</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>1.3556</td>
<td>2 0</td>
<td>40</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>1.3556</td>
<td>0 2</td>
<td>tcp 1000</td>
<td>1</td>
<td>0 3 0</td>
<td>29</td>
<td>199</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>1.3556</td>
<td>2 3</td>
<td>tcp 1000</td>
<td>1</td>
<td>0 3 0</td>
<td>29</td>
<td>199</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td>1.3556</td>
<td>1 2</td>
<td>tcp 1000</td>
<td>1</td>
<td>0 3 0</td>
<td>29</td>
<td>199</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r</td>
<td>1.3556</td>
<td>1 1</td>
<td>cbr 1000</td>
<td>1</td>
<td>0 3 0</td>
<td>31</td>
<td>157 207</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>1.3556</td>
<td>1 1</td>
<td>cbr 1000</td>
<td>1</td>
<td>0 3 0</td>
<td>31</td>
<td>157 207</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 12. HELLO Message sharing

Every node in the network sharing the hello messages between them for maintaining connectivity.

Fig. 13. All Nodes Sharing Hello Message

Source node sending the route request to its neighbor nodes and every node checking the route request and forwarding that to their neighbor nodes, this process continues until it reaches the destination. Whenever route request sent by the source node is received to destination it will first check whether that information about source is already present or not. If already is there means it will check the sequence number and the packet id, if not matched means it will store that information and will give reply to that request. If matched means it will ignore to avoid multiple paths. This we can observe in the below screen shot as the RREQ in green color and RREP in red color which is sending by destination.

![Fig. 14. Sending RREQ and Getting RREP.](image)
we can observe in the below screen shot as source is sending data to destination.

Fig. 15. Overhead Function in AODV

The above screen shots show the packet delivery function of the AODV here x-axis is time and y-axis is the extra packet sizes.

Fig. 16. Overhead Function in PWAODV

The above screen shots show the packet delivery function of the PWAODV here x-axis is time and y-axis is the extra packet sizes.

Fig. 17. Overhead Function in IPWAODV

The above screen shots show the packet delivery function of the IPWAODV here x-axis is time and y-axis is the extra packet sizes.

Fig. 18. Overhead Comparison

The above screen shot shows the overhead comparison through XGRAPH, here we can observe that AODV has highly overhead but IPWAODV has lower overhead compared to PWAODV and normal AODV. The below screen shots show the packet delivery function of the
AODV, PWAODV, IPWAODV protocol in MANET environment. Here x-axis is time and y-axis is the delivered packet sizes.

![Image of Fig.19. Comparison between AODV, PWAODV AND IPWAODV.](image)

The above result is clearly showing that though Improved PWAODV has highly packet delivery fraction, and the routing overhead and delay is lower than from AODV and PWAODV.

VI. CONCLUSION & FUTURE WORKS

An improved protocol PWAODV is proposed which is based on piggyback mechanism and weighted neighbour stability is introduced. The path selected in our protocol is more stable and effective. Furthermore, it can reflect the mobility of nodes accurately. Finally, the advantage reflected in the simulation results is brought by reducing transmission of redundant packets and improving the robustness of the route. The direct result is that the performances of route cost and end-to-end delay have been improved greatly. Moreover, compared with using the GPS auxiliary hardware or the cross-layer thought we can avoid many problems. In the future, we can modify the IPWAODV by sending intelligent hello massage To checked the best way to sending data packet, the intelligent massage meaning that is not require for RREQ and RREP .we can also increase the size of data packet and reduce the packet overhead routing.

VII. REFERENCES


Author’s Profile:

BUSHRA NAJI TALIB ALSUNBULI,

Is graduated in B.Tech (CommunicationsEngineering) from Technical collage of Najaf in 2010.She obtained M.Tech in (ECE) Embedded Systems during 2013 from Jawaharlal Nehru Technological University, Hyderabad, AP-INDIA.
Dr. M Nagaratna

Computer Science & Engineering

JNTUH College of Engineering
Hyderabad (Autonomous), Official
Email1: mratnajntu@jntuh.ac.in,
Email2: mratnajntu@gmail.com.

Areas of Interest:

HASAN FALAH MOHSIN FAKHRULDEEN

Is graduated in B.Tech (Communications Engineering) from Technical collage of Najaf in 2010.He obtained M.Tech in (ECE) Embedded Systems during 2013 from Jawaharlal Nehru Technological University Hyderabad.