ISSN 2047-3338

Performance Evaluation and Improving Bandwidth Utilization of AODV Protocol by Finding Hidden Terminals in Wireless Networks

Teena Arora[1], Parminder Singh[2] and Sandeep Singh Kang[3]

[1,2]Department of IT, C.E.C. Landran, India
[3]Department of CSE, C.E.C. Landran, India

***Abstract*– Ad-Hoc on demand distance vector routing protocol is designed for use in Ad-Hoc mobile networks. AODV is an on-demand distance vector routing protocol that determined a route to a destination only when a node wants to send a packet to that destination. This paper focuses to improvement of AODV protocol in wireless networks by finding the hidden terminals in the mobile network and improved the bandwidth utilization by using Fair share algorithm. The bandwidth is the combination of width and range of frequency and due to this we have to also solve the hidden terminal problem. These hidden terminals degrade the performance of Ad-Hoc networks for sharing resources on the same bandwidth. The fair share algorithm had been used and run under the network simulator (NS2). In this we improved the performance of Ad-Hoc networks and calculated the congestion level during the experimentation. With the removal of collision and congestion we improved the bandwidth and focuses to implement the method of RTS/CTS. The further use of RTS/CTS methods to finding the hidden terminals and update the table so that the chance of collision has been less. The simulated scenario of Ad-Hoc networks performed over 802.11 networks by using simulator NS2.**

***Index Terms*– AODV, Bandwidth, FA algorithm, RTS and CTS**

I. INTRODUCTION

THE new generation of wireless mobile computers can temporarily form Multi-hop networks without the aid of fixed infrastructure. This activity is usually called ad hoc networking .As this technology matures, Adhoc networks will increasingly need to support distributed multimedia communication. Adhoc on demand distance vector routing protocol is designed for use in Ad hoc mobile networks. AODV is an on demand routing algorithm in that it determines a route to a destination only when a node wants to send a packet to that destination. In AODV the routing table is expended by sequence number to every destination and by time to live for every entry.

The Adhoc on demand distance vector (AODV) algorithm enables dynamic, self starting, multi hop routing. Routing between participating mobile nodes wishing to establish and maintain an Adhoc network [1]. AODV is an example of reactive and stateless protocol [2] that establishes routes only as desired by a source node using route request (RREQ) and route reply (RREP) messages AODV is capable of both unicast and multicast routing. A mobile ad-hoc network [20] is a wireless network in which nodes can communicate the packets without any pre installed infrastructure. This is most suitable for applications such as military communications, search and Rescue operations, and multiparty conferencing. Secure AODV (SAODV) [14], [15], [16] is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity.The SAODV routing protocol proposed in [3] is used to protect the routing messages of the original AODV. SAR is an extension framework to existing on demand ad hoc routing protocols [9].

The AODV routing protocol [11] is one of several published reactive routing protocols for mobile ad-hoc networks, and is currently extensively researched. In AODV, every node maintains a table, containing information about which neighbor to send the packet to in order to reach the destination. Wireless ad-hoc network hosts can use protocols such as the IEEE 802.11 media-access Control standard to communicate via the same frequency, or they can apply Bluetooth or other frequency-hopping technology [8]. A Mobile Ad-Hoc Network (MANET) [7] is a specific type of ad-hoc network, where the nodes are mobile and use the IEEE 802.11 standard. This means that every node has the ability to act as a router. In AODV there is maintenance of nodes in according to the time based of each node. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries [4].

There are various types of control packets are used. The first one is route request message route request message is follow when the node requiring a route to another node then it send the route request message .The second one is route reply message route reply message is the response given back to the node by the server. The third type of control packet is route error message. Route error message is generated due to some error in nodes. It is referred to as RERQ. These control packets are used vary widely. These message types are received via UDP, and normal IP header processing applies. When a route to new destination is needed, the node broadcasts a RREQ to find a route to the destination.

A route can be determined when RREQ reaches either the destination itself, or an intermediate node with a 'fresh enough' route to the destination. A 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. The route is made available by unicasting a RREP back to the origination of the RREQ. Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. The RERR message indicates those destinations which are no longer reachable by way of the broken link. There is an optimization of AODV using an expanding ring (ESR) technique when flooding RREQ messages [12], [13]. Every RREQ carries a time to live (TTL) value that specifies the number of times this message should be re-broadcasted. This value is set to a predefined Value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

In AODV, the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.

When a link fails, a routing error is passed back to a transmitting node, and the process repeats. The advantage of AODV is that it creates no extra traffic for communication along existing links. One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple route reply packets in response to a single route request packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption. AODV is perhaps the most well-known routing protocol for a MANET [5].The ultimate goal of any security solution for AODV should be to provide security services, such as authentication, confidentiality, integrity and non repudiation [6].

AODV forms tree which connect multicast group members. The trees are composed of group members and the nodes needed to connect the members. AODV supports unicast, Broadcast and Multicast without any further protocols. AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbours and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbours periodically its whole routing table. So they can check if there is a useful route to another node using this neighbour as next hop. When a link breaks a Count-To- Infinity could happen. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs.

In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. AODV uses IP in a special way. It treats an IP address just as an unique identifier. This can easily be done with setting the Subnet mask to 255.255.255.255. But also aggregated networks are supported. They are implemented as subnets. Only one router in each of them is responsible to operate the AODV for the whole subnet and serves as a default gateway. It has to maintain a sequence number for the whole subnet and to forward every package. One of the great advantages of AODV is its integrated multicast routing. In a multicast routing table the IP address and the sequence number of the group are stored. Also the leaders IP address and the hop count to him are stored as well as the next hop in the multicasting tree and the lifetime of it.

Wireless communication systems are increasingly being used to support multimedia services; these real-time services demand Quality of Service (QoS) mechanisms to guarantee the Bandwidth. Delay and delay jitter, etc. In mobile ad hoc networks (MANET), there are some QoS routing proposals [17], [I8], [19] for supporting real-time services. In these there is route request buffer. Route request buffer is that which prevent from resending the same messages again and again. When a node sends a route request message to its neighbor node. The buffer is present to check multiple entries if there is already a request present from this node then it will not receive more request from the same node.

Before forwarding a RREQ message, a node always checks the buffer to make sure it has not already forwarded the request. RREQ messages are also stored in the buffer by a node that originates a RREP Message. The purpose for this is so a node does not send multiple RREPs for duplicate RREQs that may have arrived from different paths [21]. Each entry consists of two pairs of value the address of the node which node originates the message and the identification number. Route request identification number is very important to identify request from which node the request is come. Bandwidth is defined as width of the range of frequency and is measured in hertz. Bandwidth is often used as a data transfer rate the amount of data that can be carried from one point to another in a given time period (usually a second).This kind of bandwidth is usually expressed in bits per second .The parameter of bandwidth is frame size, packet size, delay, data rate. AODV reacts relatively fast to the topological changes in the network and updates only the nodes affected by these changes.

AODV protocol can be used in networks with limited resources: bandwidth Energy, computational power, but with a limited number of nodes. RTS/CTS are a mechanism to prevent collisions. If we enable RTS/CTS on a particular station, it will refrain from sending a data frame until the station completes a RTS/CTS handshake with another station, such as an access point. A station initiates the process by sending a RTS frame. The access point receives the RTS and responds with a CTS frame. The station must receive a CTS frame before sending the data frame. The CTS also contains a time value that alerts other stations to hold off from accessing the medium while the station initiating the RTS transmits its data. The RTS/CTS handshaking provides positive control over the use of the shared medium. The primary reason for implementing RTS/CTS is to minimize collisions among hidden stations. RTS/CTS are only used for unicast data frames, when the packet size exceeds threshold. It does not affect management or control frames. RTS/CTS access method is used to combat the hidden terminal problem by requiring that a short Request-to-Send (RTS) and Clear-to-Send (CTS) packet should be exchanged successfully between a pair of sender and receiver before actual data packet transmission begins. To avoid unnecessary protocol overhead, only when data packet length exceeds the value of a parameter called R TSTHRESHOLD is RTS/CTS access method used.

II. PROBLEM DEFINITION

When one source node send data to two or more receiver node then there is collision occurs. When number of channel is more then there is congestion occur. There is hidden terminal problem due to hidden terminal there is degradation in bandwidth. We have to remove the congestion and overcome the collision .Due to this we utilize the bandwidth. There is hidden terminal problem also. These hidden terminals degrade the performance of Adhoc networks for sharing resources on the same bandwidth. In these we improve the performance.

III. LITRATURE SURVEY

Author [1] discussed about the AODV. AODV routing protocol is one of several published reactive routing protocols for mobile ad-hoc networks, and is currently extensively researched. In on-demand routing protocols a fundamental requirement for connectivity is to discover Routes to a node by request messages.

Author [2] described that the Ad hoc On-Demand Distance Vector (AODV) routing protocol provides unicast, broadcast, and multicast communication in ad hoc mobile networks. AODV initiates route discovery whenever a route is needed by a source node, or whenever a node wishes to join a multicast group. . AODV nodes maintain a route table in which next hop routing information for destination nodes is stored.

Author [3] observed that Ad-Hoc On-Demand Distance Vector (AODV) protocol, one of the on-demand routing algorithms that are receiving the most attention. However, does not utilize multiple paths. Consequently, when route disconnects, nodes of the broken route simply drop data packets because no alternate path to the destination is available until a new route is established. When the network traffic requires real time delivery (voice, for instance), dropping data packets at the intermediate nodes can be costly.

Author [4] observed that Wireless communication systems are increasingly being used to support multimedia services; these real-time services demand Quality of Service mechanisms to guarantee the bandwidth. Delay and delay jitter, etc.

Author [5] observed that the Ad hoc networking has emerged as one of the most focused research areas in the field of wireless networks and mobile computing. Ad hoc networks consist of hosts communicating one another with portable radios. These networks can be deployed impromptu without any wired base station or infrastructure support. In ad hoc mobile networks, routes are mainly Multihop because of the limited radio propagation range and topology changes frequently and unpredictably since each network host moves randomly. Therefore, routing is an integral part of ad hoc communications, and has received interests from many researchers.

Author [6] defined that Routes are maintained as long as they are needed by the source node or as long as the multicast group exists, and the routes are always loop-free through the use of sequence numbers.

Author [7] observed that there is an optimization of AODV using an expanding ring (ESR) technique when flooding RREQ messages. Every RREQ carries a time to live (TTL) value that specifies the number of times this message should be re-broadcasted. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.

Author [8] observed that Wireless communication systems are increasingly being used to support multimedia services; these real-time services demand Quality of Service mechanisms to guarantee the bandwidth, delay and delay jitter, etc.

Author [9] observed that Supporting QOS in an ad hoc environment entails the coordination of several system activities. The first is route discovery and route repair. Since ad hoc network topologies are highly dynamic, routes between two nodes often need to be produced or discovered upon demand, at the time of connection establishment in the case of a QOS connection, since previous routes may no longer exist.

Author [10] described that various schemes have been proposed in the literature for end-to-end QOS provisioning in ad hoc networks. These schemes are mostly related to TCP adaptable transport protocols that react to congestion events.

Author [11] discussed that Quality of Service support in mobile Ad hoc networks is a very challenging task because of the dynamic topology, limited resources and wireless link characteristics. Routing algorithm is a very important mechanism for QOS guaranteeing in networks. The Ad hoc On-demand Distance Vector (AODV) protocol chooses a path with small bandwidth consumption.

Author [12] observed that Supporting QOS in an ad hoc environment entails the coordination of several system activities. The first is route discovery and route repair. Since ad hoc network topologies are highly dynamic, routes between two nodes often need to be produced or discovered upon demand, at the time of connection establishment in the case of a QOS connection, since previous routes may no longer exist.

Author [13] observed that in AODV there are various security techniques like SAODV, SAR. In these there is use of IPSec protocol by which the node transfers secure data to each other. There is not any chance of loss of data.

Author [14] observed that Security Aware routing enables the use of security as s negotiable metric to improve the routing. Security ad hoc is an approach to routing that incorporates security level of nodes in to traditional routing metrics.

IV. METHODOLGY USED

When one source node send data to two or more receiver node then there is collision occurs. Due to hidden terminal problem there is degradation in bandwidth .In these we use the RTS and CTS access method [10]:

```
Switch (receive packet type)
{
RTS:
If (dest ID! =local ID)
{
Weo+= Trts; Update Tedata
}
Else
Send CTS packet; Weo+= (Trts+Tcts)
}
```

The basic idea is that whenever a station receives a packet, it will update its estimation of either its own share or others' share based on type and role of the packet. If a station receives a CTS packet destined to it, the station sends a data packet and updates estimation of its own share as the data packet transmission request was originated by itself. If destination id is not equal to local id then its update the data else it send CTS packet.

```
CTS
If (dest id!= local id)
{
Weo+=(Trts+Tcts); UpdateTedata
}
else
{
Send DATA packet;
Wei+=(Trts+Tcts+Tdata)
}
```

If destination id is not equal to the local id then the estimated share of other stations update the data packet otherwise it sends the data packet to the estimated share of the estimating station itself.

V. EXPERIMENTATION

Our Proposed work is on Fair share algorithm. The Algorithm will be implemented using Network Simulator 2. In these we utilize the bandwidth. The Scenario of AODV is shown in the given Fig. 1.

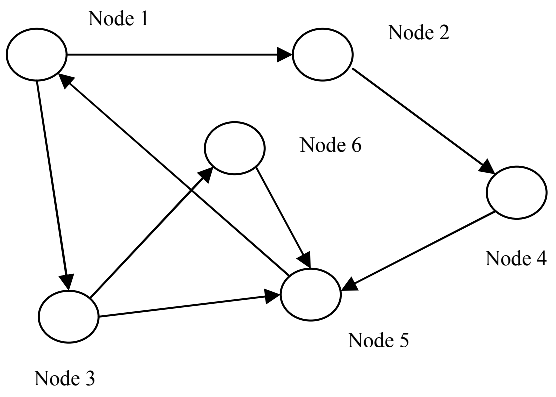

Fig. 1: Scenario of AODV protocol

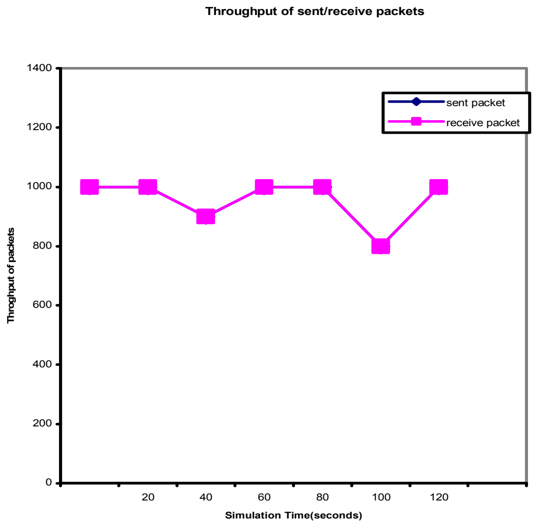

Fig. 2: Throughput vs. Time

The studied and implemented scenario consists of six nodes works on AODV. In these all nodes are communicating with each other. Each node in the mobility model or scenario show in the figure 1 has been using TCP Reno Protocol that provides End to End Connectivity. The FTP is running in this scenario for providing the connectivity and data transmission. Each mobile station begins the simulation by selecting a random destination in the defined area and moves to that destination at a random speed. In these we have to check the congestion level and we check the RTS and CTS.

The Fig. 2 shows the results of Throughput vs. Time of AODV Protocol:

The Fig. 2 represents the throughput vs. time. The throughput defined as the amount of data moved successfully from one place to another in a give time period and calculated as Bit/s.

The Throughput of AODV is calculated as total bits received by destination node per second. The delay occurs when there is no communication between nodes and throughput is zero. The data is more stable when AODV protocol runs. Though Network Topology changes, Data remains stable in AODV.

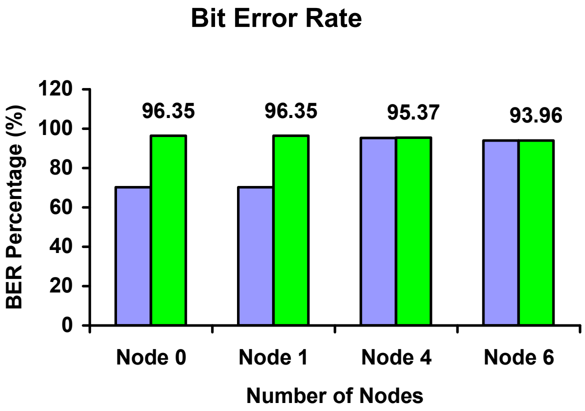

Fig. 3: BER of AODV

As shown in Fig. 3, the BER (Bit Error Rate) generated by the various nodes that communicating by using AODV protocol. The Bit error means the errors generated during the communicating with one node to another and send the error messages due some unavoidable situations like Handoff, disconnection and noise generated at 802.11 networks. The total numbers in the scenario 1 set at 10. Where, the other nodes having zero BER, it means that good put of these pending nodes high among the nodes.

VI. CONCLUSION

In this Paper, we introduce the fair share algorithm. The congestion level at every node is checked. We utilize the bandwidth with the help of fair share algorithm. Before this the bandwidth is not good due to collision and congestion. We remove the collision and congestion and therefore, hidden terminal problem eliminated and improve the overall utilization of bandwidth. RTS and CTS are used for the collision avoidance. The primary reason for implementing RTS/CTS is to minimize collisions among hidden stations. With the help of these we solve the hidden terminal problem and utilize the bandwidth.

REFERENCES

[1] C.E. Perkins, E. Belding Royer and S.R Das “Adhoc on Demand Distance Vector (AODV) routing, IETF RFC 3561, July 2003.

[2] Muhammad O Pervarz, Minaela Cardei and Jei Wu “Routing Security in Adhoc wireless Networks”, 2008, pp: 2-32.

[3] M.G.Zapata “Secure Adhoc on demand distance vector (SAODV) routing” Aug.2001.

[4] Berlein Germany, (2003), “Georgy Sklyarenko institute fiir informatik, freie universitat Berlein,Takustr.9,D-14195”. Vol.2003 pp.2-9.

[5] Mohd Anuar Jaafar, Zuriati Ahmad Zukarnain “Performance Comparisions of AODV Secure AODV and AdaptivesecureAODVroutingprotocol”vol.32, 2009, pp: 430-443.

[6] Bruce Schneir,Applied cryptography,John Wiley and sons inc,1996,pp: 1-12.

[7] Binod Kumar Pattanyak,Manoj Kumar Mishra,Jagadev Manojranjan Nayak “Mutihop Bandwidth Management protocol for mobile Ad-hoc networks” vol.2,2010,pp:11-30.

[8] Clifton Lin “AODV Routing Implementation for Scalable Wireless Adhoc Network Simulation (SWANS)”.

[9] Alain Solheid “AODV enhanced by smart antennas Alain Solheid” 2005, pp: 14-28.

[10] Yu Wang, Brahim Bensaou “Achieving Fairness in IEEE 802.11 DFWMAC with Variable Packet Lengths”2001, pp: 3588-3593.

[11] Royer E.M. Perkins C.E. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, p.90, 1999.

[12] Pucha H. Hu Y.C. Koutsonikolas D., Das S.M. On optimal ttl sequence-based route discovery in manets. Volume vol.9, p.923, 2005.

[13] Schneider S. Kaddoura M., Ramanujan R. Routing optimization techniques for wireless ad hoc networks. Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks SNPD/SAWN 2005, p.454, 2005.12.

[14] M. F. Juwad, and H. S. Al-Raweshidy, “Experimental Performance Comparisons between SAODV & AODV”, IEEE Second Asia International Conference on Modelling & Simulation, 2008.

[15] Junaid Arshad and Mohammad Ajmal Azad, “Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks”, 1-4244-0626-9/06, 2006 IEEE.

[16] Davide Cerri and Alessandro Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype”, 0163-6804/08, 2008 IEEE, IEEE Communications Magazine, February 2008.

[17] K-B. Lee, G.-S. Ahn, X. Zhang, A. T. Campbell, “INSIGNIA: an IP-based quality of service framework for mobile ad hoc network,” Journal of Parallel and Disrribured Comphng, vol. 60, pp. 374-406, Apr. 2000.

[18] C. R. Lin, “Admission control in time-slotted multihop mobile networks,” IEEEJSAC, vol. 19, no. 10, pp. 1974-1983, Oct. 2001.

[19] C. Zhu and M. Corson. “QoS routing for mobiie ad hoc networks,” Proc. IEEE ZWOCOM’OZ, New York, USA, June 2001, pp. 958967.

[20] J. P. Macke, and M. S. Coson, “Mobile Ad-hoc Networking and the IETF”, ACM SIG MOBILE, Mobile Computing and Communications reviews, vol. 2, No. 2, p. 9-14, Jan. 1998.

[21] Davide Cerri and Alessandro Ghioni “Securing AODV: The SAODV Secure Routing Prototype” 2008, PP: 120-125.