ADTART - MANET :- ACCELERATED DATA TRANSMISSION BASED ON AGGRESSIVE ROUTING TECHNIQUE IN MOBILE AD HOC NETWORK

P.Sajitha[1] | R.Sujitha[2]

[1](UG Student, Christ the King Engineering College, sajithasaji10aug96@gmail.com)
[2](Assistant Professor, Christ the King Engineering College, srisuji14@gmail.com)

Abstract— *The energy consumption in MANET is optimized by applying the Fitness Function technique in Ad Hoc On Demand Multipath Distance Vector (AOMDV) routing protocol. The proposed protocol is called Ad Hoc On Demand Multipath Distance Vector with the Fitness Function (FF- AOMDV). The fitness function is used to find the optimal path from the source to the destination to reduce the energy consumption in multipath routing. The performance of the proposed FFAOMDV protocol was evaluated by using Network Simulator Version 2 (NS-2), where the performance was compared with AOMDV and Ad Hoc On Demand Multipath Routing with Life Maximization (AOMRLM) protocols, the two most popular protocols proposed in this area. Mobile Ad hoc Networks (MANETs) consists of a set of wireless mobile nodes communicating to each other without any centralized control or fixed network infrastructure and can be deployed quickly. The potential applications include emergency disaster relief, battlefield situations, mine site operations, and wireless classrooms or meeting rooms in which participants wish to share information or to acquire data. Anycast is an important way of communication for replicated service applications in terms of resources, robustness and efficiency, when mobility and link disconnections are frequent. Anycast allows a source node to transmit packets to a single destination node out of set of several destination nodes.*

Keywords— Fitness Function, Multipath Routing, Wireless Mobile Nodes, Efficiency

1. INTRODUCTION

As the wireless network technology exploded, it has opened a new view to users and expanded the information and application sharing very conveniently and fast. Mobile ad hoc networks (MANETs) use wireless technology without a pre-existing infrastructure (access points). As the name states, MANETs consists of mobile nodes, which can vary from notebooks, PDAs to any electronic device that has the wireless RF transceiver and message handling capability. Mobility and no- infrastructure forms the basis of this network type.

Mobility gives maximum freedom to users, as they can be connected to the network, whether they are fixed or moving, unless they are in the range of the network. Also, it is highly dynamic, as the new nodes come, they can be connected to the network very easily. Unlike the fixed networks or traditional wireless networks, MANETs don't need any infrastructure to create and maintain communication between nodes. This property provides the ability to create a network in very unexpected and urgent situations very quickly, also without any extra cost.

As we said any electronic device that has the wireless transmission capability with proper processing hardware can be a part of a MANET. So, firstly the nodes have to have RF wireless transceivers as the network interface. But since the wireless transmission ranges according to transmission type of the antenna (omnidirectional, bidirectional), and the variations between transceivers at different nodes effect the network structure of the MANETs.

However, members of the MANETs can be fixed without any constraint, they consist of mobile nodes. So, their processing capability is limited. Also, power consumption of the mobile nodes is a very great factor on the structure of the MANETs. So, to make MANETs applicable and get maximum performance from them, we have to consider these two factors, and design any algorithms appropriately. MANETs are autonomous and decentralized networks. So, they can operate no matter which nodes are connected or not connected to the network. Connectivity of nodes only affects the topology and routing of the network, not the general operations. Since, MANETs don't have any centralization; operations are done distributed, so each node has to have sufficient information about the network and have to operate independently.

Two nodes that want to communicate with each other can send and receive messages directly, if they are both in their transmission range. Otherwise, every node is also capable to be a router, and the messages between nodes are relayed by the intermediate nodes, from the originator of the message to the destination.

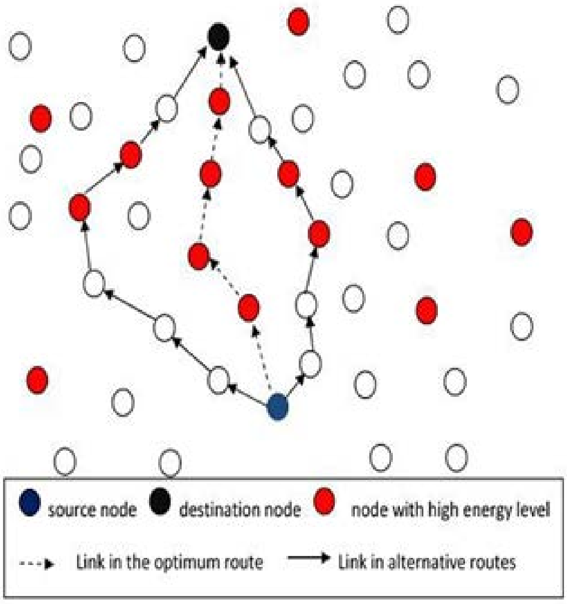
2 RELATED WORK

2.1Protocol architecture for mobile ad hoc networks

Most of the proposed MANET protocols view mobile ad hoc networks as an IP-centric view of the network, and the use of a layered architecture. Recently there has been increased interest in protocols for wireless networks that rely on significant interactions between various layers (Cross Layer Design) of the network stack. In this paper we would study the various Cross Layer Design Approaches and their significance in MANET while having an insight into the problems of Cross Layer design mode. According to the definition of IEEE 802.11: A network composed solely of stations within mutual communication range of each other via the wireless medium (WM). An ad hoc network is typically created in a spontaneous manner. The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent. These limitations allow the act of creating and dissolving the ad hoc network to be sufficiently straightforward and convenient to be achievable by nontechnical users of the network facilities. No specialized "technical skills" are required and little or no investment of time or additional resources is required beyond the stations that are to participate in the ad hoc network.

The term ad hoc is often used as slang to refer to an independent basic service set (IBSS). The applications of MANET have a wide range of network requirements as well as different energy constraints for different network nodes. The network requirements must be met despite variations in the link characteristics on each hop, the network topology, and the node traffic. It is very difficult to ensure performance of the network or the support of real-time or mission critical data in the face of these random variations. Current ad hoc wireless network protocol design is largely based on a layered approach TCP/IP Model as shown in Fig. The TCP/IP stack design is highly rigid and strict, and each layer worries only about the layer directly above it or the one directly below it. This results in nonexistent collaboration between the different layers. In TCP/IP Model each layer in the protocol stack is designed and operated independently, with interfaces between layers that are static and independent of the individual network constraints and applications. This paradigm has greatly simplified network design and led to the robust scalable protocols in the Internet. However, the inflexibility and sub optimality of this paradigm result in poor performance for ad hoc wireless networks in general, especially when energy is a constraint or the application has high bandwidth needs and/or stringent delay constraints. In a MANET some functions cannot be assigned to a single layer. As shown in the Figure Energy management, security and cooperation, quality of service, Mobility

Management among the others cannot be completely implemented in a single layer but they are implemented by combining and exploiting mechanisms implemented in all layers. An efficient implementation of these functions can thus be achieved by avoiding a strict layering approach in which the protocols at each layer are developed in isolation, but rather within an integrated and hierarchical framework to take advantage of the inter dependencies between them. Relaxing the Internet layered architecture, by removing strict layer boundaries, is therefore an open issue in the mobile ad hoc networks evolution.


source node
destination node
node with high energy level
Link in the optimum route
Link in alternative routes

2.2 Different types of attacks on integrated MANET-internet communication
Security is an important issue in the integrated MANET-Internet environment because in this environment we have to consider the attacks on Internet connectivity and also on the ad hoc routing protocols. The focus of this work is on different types of attacks on integrated MANET-Internet communication. We consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network and find out the security issues which have not solved until now. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently Mobile ad hoc network has been a challenging research area for the last few years because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc. If we consider only a stand-alone MANET then it has limited applications, because the connectivity is limited to itself. MANET user can have better utilization of network resources only when it is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET. Because we have to consider the attacks on access point also through which MANET is connected to Internet.

In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the ad hoc routing protocols. Due to this reason, almost all possible attacks on the traditional ad hoc networks also exist in the integrated wired and mobile ad hoc networks. Whatever the attacks are, the attackers will exhibit their actions in the form of refusal to participate fully and correctly in routing protocol according to the principles of integrity, authentication, confidentiality and cooperation. Hence to design a robust framework for integrated MANET-Internet communication we have to minimize attacks on the internet connectivity and also on the ad hoc routing protocols. The rest of the paper is organized as follows. In this section we consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network. We also discuss some secure routing protocols for integrated MANET-Internet communication and find out the security issues which have not solved until now. Finally section 4 is about conclusions and future work. We have discussed security issues related to integrated mobile ad hoc network (MANET)-Internet and stand alone MANET. The proposed mechanisms until now have solved many security issues related to integrated MANET-Internet communication but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks. In future, we will propose to design a robust framework that uses minimal public.

2.3AODV routing protocol implementation design

To date, the majority of ad hoc routing protocol research has been done using simulation only. One of the most motivating reasons to use simulation is the difficulty of creating a real implementation. In a simulator, the code is contained within a single logical component, which is clearly defined and accessible. On the other hand, creating an implementation requires use of a system with many components, including many that have little or no documentation. The implementation developer must understand not only the routing protocol, but all the system components and their complex interactions. Further, since ad hoc routing protocols are significantly different from traditional routing protocols, a new set of features must be introduced to support the routing protocol. In this paper we describe the event triggers

required for AODV operation, the design possibilities and the decisions for our Ad hoc On-demand Distance Vector(AODV)routing protocol implementation, AODV-UCSB. This paper is meant to aid researchers in developing their own on-demand ad hoc routing protocols and assist users in determining the implementation design that best fits their needs Simulation is an important tool in the development of mobile ad hoc networks; it provides an excellent environment to experiment and verify routing protocol correctness. However, simulation does not guarantee that the protocol works in practice, because simulators contain assumptions and simplified models that may not actually reflect real network operation. After a protocol is thoroughly tested in simulation, an implementation is the logical next step.

A working implementation is necessary to validate that the routing protocol specification performs under real conditions. Otherwise, assumptions made by the protocol design cannot be verified as correct. Additionally, an implementation can be used to perform tested and field tests. Eventually it can be used in a deployed system, such as. Creating a working implementation of an ad hoc routing protocol is non-trivial and more difficult than developing a simulation. In simulation, the developer controls the whole system, which is in effect only a single component. An implementation, on the other hand, needs to interoperate with a large, complex system. Some components of this system are the operating system, sockets, and network interfaces. Additional implementation problems surface because current operating systems are not built to support ad hoc routing protocols. A number of required events are unsupported; support for these events must be added. Because these events encompass many system components, the components and their interactions must also be explored. For these reasons it takes significantly more effort to create an ad hoc routing protocol implementation than a simulation. In this paper we analyzed the design possibilities for an AODV implementation. We first identified the unsupported events needed for AODV to perform routing. We then examined the advantages and disadvantages of three strategies for determining this information. This analysis supported our decision to use small kernel modules with a user-space daemon. Finally, we presented the design of many publicly available.

3.METHODOLOGIES

3.1Protocol Initialization

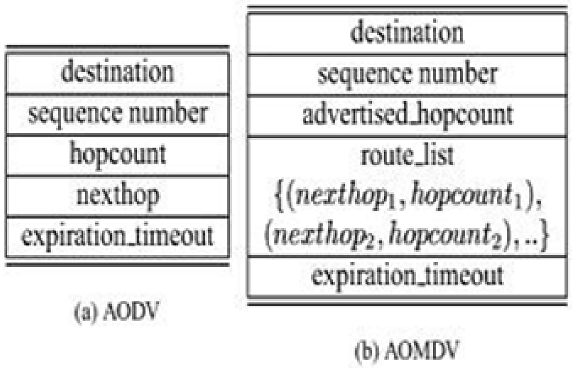
Multipath routing protocols flood a route request to learn more than one path to the destination to forward packets through them. It is not necessary that the source will always find the optimum or the shortest path available. Since the power source of the mobile nodes is limited, the power consumption by these nodes should be controlled to increase the network lifetime. Multipath routing protocols have several issues. One of them is finding an optimum path from the sources to the destinations. The issue becomes more complicated with a large number of mobile nodes that are connected to each other for transferring the data. In this case, most of the energy is going to be consumed at the time of investigating for shortest routes. Subsequently, the more energy is wasted at data transfer.

The research in this paper presents an energy efficient multipath routing protocol called Ad-Hoc On demand Multipath Distance Vector with the Fitness Function (FF-AOMDV). The FF- AOMDV uses the fitness function as an optimization method, in this optimization, we seek for two parameters in order to select the optimum route are; energy level of the route and the route distance in order to transfer the data to the destination more efficiently by consuming less energy and prolonging the network lifetime.

Based on the results of the simulation, the FF-AOMDV routing protocol outperformed both Ad-Hoc On demand Multipath Distance Victor (AOMDV) and Ad-Hoc On demand Multipath Routing with Life Maximization (AOMR-LM) routing protocols in terms of throughput, packet delivery ratio, end-to-end delay, energy consumption, network lifetime and routing overhead ratio except the AOMR-LM when comparing with energy consumption and network lifetime where it has better performance than FFAOMDV with these two metrics.

3.2Routing Scheme

An on-demand routing protocol, AOMDV has its roots in the Ad hoc On-Demand Distance Vector (AODV), a popular single-path routing protocol. AOMDV creates a more extensive AODV by discovering, at every route discovery process, a multipath (i.e. several other paths) between the source and the destination. The multipath has a guarantee for being loop-free and link-disjoint. AOMDV likewise offers two key services: route discovery and route maintenance. Since it greatly depends on the AODV route information, which is already available, AOMDV incurs less overhead than AODV through the discovery of multiple routes. Compared to AODV, AOMDV's only additional overhead is extra RREPs and RERRs intended for multipath discovery and maintenance, along with several extra fields to route control packets (i.e. RREQs, RERRs and RREPs). Adding some fields and changing others modified the structure of the AOMDV's routing presents the routing table entries' structure for AODV and AOMDV. In AOMDV, advertised_hopcount is used instead of the hopcount in AODV . A route_list stood as a replacement for nexthop; this change essentially defining multiple nexthops with respective hopcounts. All nexthops, however, are still allotted the same destination sequence number. Every time the sequence number gets updated, the advertised_hopcount is initialized.



destination
sequence number
hopcount
nexthop
expiration_timeout

(a) AODV

destination
sequence number
advertised_hopcount
route_list $\{(nexthop_1, hopcount_1), (nexthop_2, hopcount_2), ..\}$
expiration_timeout

(b) AOMDV

3.3 Route Discovery

Route discovery and route maintenance involve finding multiple routes from a source to a destination node. Multipath routing protocols can try to discover the link-disjoint, node disjoint, or non- disjoint routes. While link-disjoint routes have no common links, it may have nodes in common. Node-disjoint routes, which are also referred to as totally disjoint routes, do not have common nodes or links. No disjoint routes, on the other hand, can have both nodes and links that are in common. AOMDV's primary idea is in discovering multiple routes during the process of route discovery. The design of AOMDV is intended to serve highly dynamic ad-hoc networks that have frequent occurrences of link failure and route breaks. A new process of route discovery is necessary in the event that all paths to the destination break. AOMDV utilizes three control packets: the route request (RREQ); the route reply (RREP); and the route error (RERR). Initially, when a source node is required to transmit data packets to a specific destination, the source node broadcasts a RREQ . Because the RREQs is a flooded network-wide, several copies of the very same RREQ may be received by a node. In the AOMDV, all duplicate copies undergo an examination to determine the potential alternate reverse path. However, of all the resulting set of paths to the source, only the use of those copies, which preserve loop-freedom and disjointedness, get to form the reverse paths. In the event the intermediate nodes get a reverse path through a RREQ copy, it conducts a check to determine the number of valid forward paths (i.e. one or many) to the destination. If so, a RREP is generated by the node and the request is sent back to the source using the reverse path. Since this route discovery, the RREP has a forward path that was not employed in any prior RREPs. The RREQ is not further propagated by the intermediate node.

Otherwise, the node would broadcast the RREQ copy again in case any other copy of this RREQ has not been previously forwarded and this copy has led to the updating or the formation of a reverse path.

3.4Fitness Function

The fitness function is an optimization technique that comes as a part of many optimization algorithms such as genetic algorithm, bee colony algorithm, firefly algorithm and particle swarm optimization algorithm. The fitness function finds the most important factor in the optimization process, which could be many factors depending on the aim of the research. In MANET, the fitness factor is usually energy, distance, delay, and bandwidth. This matches the reasons for designing any routing protocol, as they aim to enhance the network resources. In this research, the fitness function used is part of the Particle Swarm Optimization (PSO) algorithm as proposed. It was used with wireless sensor networks to optimize the alternative route in case the primary route fails. The factors that affect the choice of the optimum route are:

- The remaining energy functions for each node
- The distance functions of the links connecting the neighboring nodes
- Energy consumption of the nodes
- Communication delay of the nodes

The PSO algorithm is initialized with a population of random candidate solutions, conceptualized as particles. Each particle is assigned a randomized velocity and iteratively moved through the problem space. It is attracted towards the location of the best fitness achieved so far by the particle itself and by the location of the best fitness achieved so far across the whole population. The PSO algorithm includes some tuning parameters that greatly influence the algorithm performance, often stated as the exploration– exploitation trade-off: "Exploration is the ability to test various regions in the problem space in order to locate a good optimum, hopefully the global one. Exploitation is the ability to concentrate the search around a promising candidate solution in order to locate the optimum precisely. In this case, the particles are attracted towards two fitness parameters which are; energy level of the mobile nodes and the distance of the route. With these two parameters, the optimization could be found by forwarding traffic through the route that has the highest level of energy and less distance in order to minimize the energy consumption related studies. Mail et al. proposed an energy- efficient multipath routing protocol, called Ad hoc On-demand Multipath Routing with Lifetime Maximization (AOMR-LM), which preserves the residual energy of nodes and balances the consumed energy to increase the network lifetime.

They used the residual energy of nodes for calculating the node energy level. The multipath selection mechanism uses this energy level to classify the paths. Two parameters are analysed: the energy threshold and the coefficient. These parameters are required to classify the nodes and to ensure the preservation of node energy. The AOMR-LM protocol improves the performance of MANETs by prolonging the lifetime of the network. This novel protocol has been compared with both AOMDV and ZD-AOMDV. The protocol performance has been evaluated in terms of network lifetime, energy consumption, and end-to end delay.

This information include:

- Information about network’s each node’s energy level
- The distance of every route
- The energy consumed in the process of route discovery.

The route, which consumes less energy, could possibly be (a) the route that has the shortest distance; (b) the route with the highest level of energy, or (c) both. The source node will then sends the data packets via the route with highest energy level, after which it will calculate its energy consumption. Alike to other multipath routing protocols, this protocol will also initiates new route discovery process when all routes to the destination are failed. In the event when the selected route fails, the source node will then selects an alternative route from its routing table, which represents the shortest route with minimum energy consumption.

The pseudo-code for the fitness function

```
1: Select the Source and Destination.
2: Source Initialize the route Discovery.
3: Broadcast the Routing Packet to direct nodes.
4: Update the routing information in the Source Routing Table.
5: Source Initialize the Beacon.
6: Broadcast the Routing Packet to direct nodes.
7: Update the Energy and location information in the Source Energy Table for all the nodes in the entire network.
8: check If(ene>= High &&dist<= Low &&hop Count<= Low) Select that route for Communication.
Else if (ene>= High &&dist>= high &&hop Count<= Low) Select that route for Communication.
Else if (ene<= Low&&dist<= Low &&hop Count<= Low) Select that route for Communication
9: Send the periodic route discovery.
10: Send the periodic beacon message.
```

4. CONCLUSION AND FUTURE WORK

Node’s movement stability, channel load, node congestion level and route expiry time are the important QoS metrics among several QoS parameters for providing an efficient, low overhead QoS support for anycast routing in MANETs. We proposed mobility and QoS based anycast routing in MANETs. The proposed work is simulated for various MANET network environments to validate its performance. From the simulations, we observed that the proposed scheme performs better than traditional flooding, DSR and DIASD scheme in terms of control overhead, packet delivery ratio and end-to- end delay.

Simulation procedure for the proposed scheme is as follows.
(1) Generate ad hoc network with given number of nodes.
(2) Estimate neighbor stability based on self node movement stability and neighbor node movement stability.
(3)Compute link congestion factor based on channel congestion and buffer congestion factors. (4) Compute LET. (5) Update link data base at each node considering their neighbors. (6) Initiate Route Discovery Process using RR, RP and RE, and accordingly update RIC. (7) Establish the path(s) from client to servers, and send the data packets, and (8) Compute performance parameters of the system.

The variation of control overhead with respect to different number of servers and client nodes. The overhead takes into account of request and reply messages. The control overhead of our scheme MQAR is reduced compared to traditional flooding, DSR and DIASD schemes. This is because, as number of servers increase, possibility of getting more connections to any other server is high. MQAR uses only paths which satisfy the node stability, QoS and congestion levels and RET, hence breakage of paths as well as failure of nodes is less. The selected path to a server will be robust and stays for a longer duration without packet loss. Impact of varying number of clients from 1 to 15 is.

When the number of clients increase, control overhead of three approaches increase. MQAR performs better compared to other schemes because it uses the forwarding control mechanism through only stable and non-congestion nodes. Hence the number of request/reply packets used are reduced. This frame work achieves high security, more energy efficiency, high packet delivery ratio, only less delay, comparing to previous frame works.

Future Enhancement

In future, improve this process security as digital signature security frame work and our proposed security scheme for centralized topology networks, so in future we improve this security using digital signature security technique for decentralized large level networks topologies. To work on anycast routing protocols to check the efficiency under high throughput applications, e.g. multimedia applications by employing negotiation parameters in route request packet in finding nearest server through non congestion paths.

REFERENCE

[1] P. S. Kiran, “Protocol architecture for mobile ad hoc networks,” 2009 IEEE International Advance Computing Conference (IACC 2009), 2009.

[2] A. Chandra, “Ontology for manet security threats,” PROC. NCON, Krishnankoil, Tamil Nadu, pp. 171–17, 2005.

[3] A. K. Rai, R. R. Tewari,and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” International Journal of Computer Science and Security, vol. 4, no. 3, pp. 265–274, 2010.

[4] D. Smith, J.Wetherall, S. Woodhead, and A. Adekunle, “A cluster- based approach to consensus based distributed task allocation,” in Parallel, Distributed and Network-Based Processing (PDP), 2014 22nd Euromicro International Conference on. IEEE, 2014, pp. 428–431.

[5] I. D. Chakeres and E. M.Belding-Royer, “Aodv routing protocol implementation design,” in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004, pp. 698–703.

[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot et al., “Optimized link state routing protocol (olsr),” 2003.

[7] M. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, “Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles,” in Advanced Information Networking and Applications Workshops, 2007, AINAW’07. 21st International Conference on, vol. 2. IEEE, 2007, pp. 249–256.

[8] J. Pojda, A. Wolff, M. Sbeiti, and C. Wietfeld, “Performance analysis of mesh routing protocols for uav swarming applications,” in Wireless Communication Systems (ISWCS), 2011 8th International Symposium on. IEEE, 2011, pp.317–321.

[9] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.

[10] N. Garg and R. Mahapatra, “Manet security issues,” IJCSNS, vol. 9, no. 8, p. 241, 2009.

[11] W. Ivancic, D. Stewart, D. Sullivan, and P. Finch, “An evaluation of protocols for uav science applications,” 2011.