Review Paper on AODV Protocol for link stability in mobile ad-hoc network

Amanpreet Singh (Student), Ashish Dutt (Assistant Professor)

***Abstract*— The mobile adhoc networks is the self-configuring type of networks in which mobile nodes can join or leave the network. The adhoc networks is the decentralized type of network due which various issues like security, quality of service and routing arise in the network. The reactive routing is the efficient routing technique in which source node gather information about the network at the time of path establishment from source to destination. As described earlier, in mobile adhoc network mobile nodes can join or leave the network due which link failure problem may occur in the network. In this work, novel technique will be proposed which can recover and reduce the chances of link failure in the network.**

***Index Terms*— Wireless networks, ad hoc networks, multicast routing.**

1. INTRODUCTION

1.1. Introduction

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. 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

In ad hoc networks, nodes communicate witheach other by way of radio signals, which are broadcastin nature.Broadcast is a unique case of multicast, wherein all nodes in the network should get the broadcast message.

Manuscript received Dec, 2015

Amanpreet Singh (Student), *Computer Science and Engineering Department, Shaheed Udham Singh college of Engineering and Technology, Tangori (Punjab), India.*

Assistant Professor Ashish Dutt, *Computer Science and Engineering Department, Shaheed Udham Singh college of Engineering and Technology, Tangori (Punjab), India,*

Multicasting isa communication process in which thetransmission of packets(message) is initiated by a single user and the message isreceived by one or more end users ofthe network.Multicasting in wired and wireless networks has beenadvantageous and used as a vital technology in manyapplications such as audio/ video conferencing, corporatecommunications, collaborative and groupware applications,stock quotes, distribution of software, news and etc. Undermulticast communications, a single stream of data can beshared with multiple recipients and data is only duplicatedwhen required.

1.2. CHARACTERISTICS OF MANET

- They are easy to deploy.
- Do not need backbone infrastructure support.
- Useful when infrastructure is absent, destroyed or unreasonable.
- Flexible.
- In MANET each node acts like a router and host.
- Nodes have less memory, power and light weight features.
- MANET is distributed in nature.
- Dynamic network topology.

1.3. APPLICATIONS OF MANET

- Local Level: MANET may be used at local level for example at home networks where devices can communicate directly to exchange information between them.
- Military environments: Military equipment consists of some sort of computer equipment. Ad-hoc network can be used in military to maintain the information network between the soldiers, vehicles, and military information head-quarters.
- Commercial Sector: In rescue or emergency operations mobile ad hoc network can be used, e.g. flood, earthquake or in fire.
- Wireless sensor Networks: Mobile nodes contain small sized sensors that can be used to collect real time data i.e. pressure, temperature, etc.

1.4. MANETs Routing Protocols

One of the most important and a difficult method tomaintain in ad hoc networking is the routing mechanism. An ad hoc routing protocol is nothing but a concurrence between nodes as to how they control routing packets in the middle of themselves. The nodes in an ad hoc network discoverroutesasthey do not have any previous knowledge about the networktopology. Routing protocols in MANETs are classified intothree different categories.

ISSN: 2278 – 1323

Reactive protocols: It is On Demand routing protocol. Routeonly create when it required. If a node needs to transmit apacket to another node first check route through ondemandand after that create the connection between the nodes. Thesource node initiates the route discovery segment.There aremainly two stages in reactive routing mechanism after thenode needs to send data to the destination. The source nodebroadcasts Route Request messages and is extend across thecomplete network. Routes are added to the list onetime theRoute Reply packets derive from the destination reach thesource using different forwarders. Reactive protocols such as
DSR, AODV.
Proactive Protocols: It preserves the route data when it is needed. It uses an already existing route. These protocols maintain routes to all possible destinations even while a few of the routes may not be required. Every node in the network maintains tables of routes and when the network topologychanges, updates are sending across the network. These protocols require nodes to send control packets sometimes to maintain the routes. To maintain all possible routes in anetwork is difficult because the control packets for route preservation use a lot of bandwidth on links where there is no need of data transfers. These protocols invite a lot of routingoverhead. Proactive Protocols are DSDV, OLSR.
Hybrid protocols:It is association of proactive and of reactive routing. ZRP and TORA are Hybrid Protocols.

1.5. *Ad hoc On Demand Vector Protocol (AODV)*

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information.

2. LITERATURE REVIEW

Hao Yang et.al, "Security in Mobile Adhoc Networks: Challenges and Solutions" IEEE, 2004
In this paper [1], they discussed about wireless networks security has become a primary concern in order to provide protected communication between mobile nodes. Due to unique characteristics of mobile ad hoc networks such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. In this paper they focused on the fundamental security problem in MANET. They identified the security issues related to MANET and discussed the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multihop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", IEEE, 2007
In this paper [2], they discussed about ad hoc networks and how these networks are constructed and their architecture. In ad hoc networks AODV is used as routing protocols. Black Hole attack is compromised the security of AODV. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the attack probability in this they proposed wait and check the replies from all the neighboring nodes to find a safe route. They discussed the results of proposed method.

Mohammad Al-Shurman and Seong-Moo YooSeungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE, 2004
In this paper [3], they discussed two possible solutions to prevent the black hole attack. The first solution they proposed is to find more than one route to the destination. The second solution is to exploit the packet sequence number included in any packet header. They compare the results to the original ad hoc on-demand distance vector (AODV) routing scheme, the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.

Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE, 2004
In this paper [4], they proposed the method for detecting the single black hole node. In this proposed method, each intermediate node send backs the next hop information when it sends back an RREP message. When the source node receives the reply message from intermediate node, it does not send the data packets quickly, but it extracts the next hop information and then sends the Further-Request to the next hop to verify that it has the route to the intermediate node. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node. If the next hop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group which is an unreal situation.

E.A. Mary Anita, V. Vasudevan , "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", IJCA, 2011
In this paper [5], they proposed a certificate authentication mechanism to counter the effect of the black hole attack. The nodes authenticate each other by issuing the certificate to neighboring nodes and generating the public key without the need of any centralized authority. There are two phases in purposed scheme: Certification Phase and Authentication phase following the route establishment process of On Demand Multicast Routing Protocol (ODMRP). Every node in the network can issue certificates to every other node within the radio communication range of each other. Certificates are stored and distributed by nodes themselves. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The certification phase is implemented in three parts: key generation and certificate issuing part, certificate update part and the certificate revocation part. The authentication phase follows the certification phase. When a source node A wants to find a

ISSN: 2278 – 1323

route to a destination node D, it broadcasts a JREQ (Joint Request) packet. The destination node or any other node has a valid route to the destination now replies to the JREQ. Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination. To overcome the black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination.

Sreenivas B.C G.C. Bhanu Prakash K.V. Ramakrishnan, "L2DB-TCP: An adaptive congestion control technique for MANET based on link layer measurements", IEEE, 2012
In this paper [6], they introduced about congestion control is a key problem in mobile ad-hoc networks. Congestion has a severe impact on the throughput, routing and performance. Identifying the occurrence of congestion in a Mobile Ad-hoc Network (MANET) is a challenging task. The congestion control techniques provided by Transmission Control Protocol (TCP) is specially designed for wired networks. There are several approaches designed over TCP for detecting and overcoming the congestion. This paper considers design of Link-Layer congestion control for ad hoc wireless networks, where the bandwidth and delay measured at each node along the path. Based on the cumulated values, the receiver calculates the new window size and transmits this information to the sender as feedback. The sender behavior is altered appropriately. The proposed technique is also compatible with standard TCP.

Prof. S.A. Jain, Mr. Abhishek Bande, "An Improvement in Congestion Control Using Multipath Routing inManet", IJERA, 2012

In this paper [7], they presented the ad hoc connections, which opens many opportunities for MANET applications. In ad hoc network nodes are movable and there is no centralized management. Routing is an important factor in mobile ad hoc network which not only works well with a small network, but also it can also work well if network get expanded dynamically. Routing in Manets is a main factor considered among all the issues. Mobile nodes in Manet have limited transmission capacity, they intercommunicate by multi hop relay. Multi hop routing have many challenges such as limited wireless bandwidth, low device power, dynamically changing network topology, and high vulnerability to Failure. To answer those challenges, many routing algorithms in Manets were proposed. But one of the problems in routing algorithm is congestion which decreases the overall performance of the network so in this paper we are trying to identify the best routing algorithm which will improve the congestion control mechanism among all the Multipath routing protocols

3. PROPOSED WORK

3.1. Proposed Work

In a MANET(type of Ad hoc network), a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. Due to its characteristics like dynamic topology, resource constraints, No infrastructure and limited physical security, it is vulnerable to a number of attacks. The main problem occurs during transfer of data from source to destination is the problem in AODV protocol.

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes.. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. The source node broadcast the route request packets in the network and adjacent nodes to destination will revert back to source node with the route reply packets. So, the source nodes had many paths available to destination. The source nodes choose best path on the basis of hop count and sequence number. As MANET is the self-configuring type of network, the problem of load unbalancing generally exists. In the previous type various techniques had been proposed for load balancing. The most advanced and energy efficient technique is multipath routing which is based on dynamic queue threshold values. In this work enhancement in the proposed technique will be done to increase its efficiency in terms of energy, throughput and delay.

3.2. Research Methodology

The MANET is the mobile ad hoc networks which is the self-configuring type of network. The self-configuring means that any mobile nodes can join or leave the network when they want. The nodes are deployed in the network and path is established according to AODV protocol from source to destination. There are some nodes in the path having much movement than other nodes. Due to these nodes link failure problem occurs. So link failure problem is responsible for performance degradation and low reliability of the network. A novel technique is proposed to overcome link failure problem in AODV.

4. CONCLUSION

In MANET, number of nodes is present which can move freely in the area. There is no controller in the MANET. So hosts are free to move easily. It is self-configuring system. So, when the data is sent from source to destination link failure problem occurs easily due to free or easy movements of the nodes. To overcome the problem of link failure in the network various techniques of load balancing had been proposed in the previous times. Among all the proposed techniques multipath routing is the most efficient and advanced technique for load balancing in energy efficient mobile ad-hoc networks. In this, work is done to enhance the proposed AODV protocol for load balancing in MANETs. The enhancement will be based on the actual values of the networks.

REFERENCES

[1] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "Security in mobile ad hoc Networks: Challenges

ISSN: 2278 – 1323

and Solutions" UCLA Computer Science Departement 2004 IEEE.

[2] LathaTamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET" IEEE 2007

[3] Mohammad Al-Shurman and Seong-Moo YooSeungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, 2004,

[4] NeelamKhemariya, Ajay Khuntetha, " An Efficient Algorithm for Detection of Black hole Attack in AODV based MANETs" International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[5] E.A. Mary Anita, V. Vasudevan, "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", IJCA, Volume 1, 2011

[6] Sreenivas B.C G.C. Bhanu Prakash K.V. Ramakrishnan, "L2DB-TCP: An adaptive congestion control technique for MANET based on link layer measurements", IEEE, 2012

[7] Prof. S.A. Jain, Mr. Abhishek Bande, "An Improvement In Congestion Control Using Multipath Routing In Manet", IJERA, 2012

[8] JeroenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" ,2005

[9] Erik G. Nilsson and KetilStølen , "Ad Hoc Networks and Mobile Devices in Emergency Response – a Perfect Match"

[10] N.Mistry, D.C. Jinwala and M.Zaveri, "Improving AODV protocol against black hole attacks", international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong.

[11] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer 2006

[12] Priyanka Goyal, Vinit, Rishi, " MANET- A vulnerable, challenge, attacks and application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

ISSN: 2278 – 1323