Route Discovery of AODV and DSR in MANET

Anurag Kushwaha
Department of IT,
GCET, Greater Noida
anurag.kush9119@gmail.com

Ashish Kumar Singh
Department of IT,
GCET, Greater Noida
ashish_sehwag@yahoo.com

Danish Khan
Department of IT,
GCET, Greater Noida
dnshkhan09@gmail.com

Dheeraj Shukla
Department of IT,
GCET, Greater Noida
dheeraj.shukla@gmail.com

ABSTRACT

''The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.''

A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. The transition from wired to wireless networks opened up new horizons for research. There is a multitude of emerging network applications designed for personal and mobile devices. To support such a variety of applications, there is an ever growing trend to optimize the performance of the wireless networks. Mobility of the different nodes makes the situation even more complicated. Multiple routing protocols especially for these conditions have been developed during the last years, to find optimized routes from a source to some destination. In other words, the higher layers and their residing protocols remained ignorant of the fact that now they are operating without a wire. This lack of knowledge about the new protocols and different characteristics of a new physical layer

(PHY) consequently caused wrong assumptions at the higher layers. While layer to layer abstraction was a goal of the layered protocol suite; in case of wireless networks it presented a few problems. In order to cope with these problems an idea of cross layer information

1.INTRODUCTION

Recent advances in technology have provided portable computers with wireless interfaces that allow networked communication among mobile users .The resulting computing environment, which is often referred to as mobile computing, no longer requires users to maintain a fixed and universally known position in the network And enables almost unrestricted mobility .A Mobile Ad hoc Network (MANET) is a special type of wireless mobile network in which a collection of mobile hosts with wireless network interface may form a temporary network, without aid of any established infrastructure or centralized administration. The application ranges from civilian to disaster recovery and military.

Routing in the MANET faces special challenges because of its infrastructure less network and its dynamic topology. The tunnel-based triangle routing of mobile IP works well only for fixed infrastructure network to support the concept of "home agent". But when all hosts move, such a strategy cannot be directly applied. Traditional routing protocols for wired networks like distance vector or link state are no longer suitable for ad hoc wireless networks. In an environment with mobile hosts as routers, changes in network topology may be slow and this process could be expensive due to low bandwidth.

Routing protocols for MANETS can be roughly divided into *proactive* and *reactive*. In proactive routing, each host continuously maintains complete routing information of the network. Both link state and distance vector belong to proactive routing. The reactive scheme, invokes a route determination procedure only on demand through a query/reply approach. Dynamic source routing protocol (DSR) is a reactive routing protocol. The source determines the complete path for each routing process. The approach consists of two steps, route discovery and route maintenance. Route discovery allows any host to dynamically discover a route to a destination host. Each host also maintains a route cache in which it catches source routes it has

ISBN: 9788175157538

learned. Unlike regular routing-table based approaches that have to perform periodic routing updates, route maintenance only monitors the routing process and informs the sender of any routing errors.*exchange was coined in the research community.In this report we are describing various methodologies given by different researchers on MANET and also describing about a method for reliable transmission of data which is energy efficient as well.*

The Dynamic Source Routing (DSR) is one of the widely used routing protocols for MANETs. Several previous studies indicate that some of the route gathering techniques and optimizations proposed in the original protocol actually hurt the performance in many situations and make DSR under perform another commonly used routing protocol—ad hoc on demand distance vector (AODV) . Because of source routing, however, DSR is considered to be desirable from security aspect Several previous studies indicate the benefit of turning off some of the "optimization" features of DSR to improve its performance .

(a) An infrastructured network with two base station.

(b) A mobile ad-hoc network.

Figure 1: Infrastructured and ad-hoc networks.

MANET has the following features:

1 **Autonomous terminal**: In MANET, each mobile host is autonomous node, which may function as both a host and a router.

2 **Distributed operation**: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals.

3 **Multi-hop routing**: Basic types of ad hoc routing algorithms can be single-hop and multi-hop.

4 **Dynamic network topology**: Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time.

5 **Fluctuating link capacity**: The nature of high bit-error rates of wireless connection might be more profound in a MANET.

6 **Energy-constrained operation**: Some or all of the nodes in a MANET may rely on batteries or other means for their energy. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

7 **Limited physical security**: MANETs are generally more prone to physical security threats than are fixed cable networks.

2. ADVANTAGES OF MANET:-

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

3. DISADVANTAGES OF MANET:-

Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- _Security protocols for wired networks cannot work for ad hoc networks.

4. ROUTING PROTOCOLS

4.1AODV: The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner.

ISBN: 9788175157538

The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the adhoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

Path Discovery -:

When trying to send a message to a destination node without knowing an active route2 to it, the sending node will initiate a path discovery process. A route request message (RREQ) is broadcasted to all neighbors, which continue to broadcast the message to their neighbors and so on. The forwarding process is continued until the destination node is reached or until a in- termediate node knows a route to the destination that is new enough. To ensure loop-free and most recent route information, every node maintains two counters: sequence number and broad-

cast_id. The broadcast_id and the address of the source node uniquely identify a RREQ message.

broadcast_id is incremented for every RREQ the source node initiates. An intermediate node can receive multiple copies of the same route request broadcast from various neighbors. In this case – if a node has already received a RREQ with the same source address and broadcast_id – it will discard the packet without broadcasting it furthermore. When an intermediate node forwards the

RREQ message, it records the address of the neighbor from which it received the first copy of the broadcast packet. This way, the reverse path from all nodes back to the source is being built automatically. The RREQ packet contains two sequence numbers: the source sequence number

and the last destination sequence number known to the source. The source sequence number is used to maintain "freshness" information about the reverse route to the source while the desti-nation sequence number specifies what actuality a route to the destination must have before it is

accepted by the source When the route request broadcast reaches the destination or an intermediate node with a fresh enough route, the node responds by sending a unicast route reply packet (RREP) back to the node from which it received the RREQ. So actually the packet is sent back reverse the path built during broadcast forwarding. A route is considered fresh enough, if the intermediate node's route to the destination node has a destination sequence number which is equal or greater than the one contained in the RREQ packet. As the RREP is sent back to the source, every intermediate node along this path adds a forward route entry to its routing table. The forward route is set active for some time indicated by a route timer entry. The default value is 3000 milliseconds, as referred in the AODV RFC . If the route is no longer used, it will be deleted after the specified amount of time. Since the RREP packet is always sent back the reverse path established by the routing request, AODV only supports symmetric links.

(a) Source node S initiates thepathDiscovery process

(b) A RREP packet is sent back to the Source

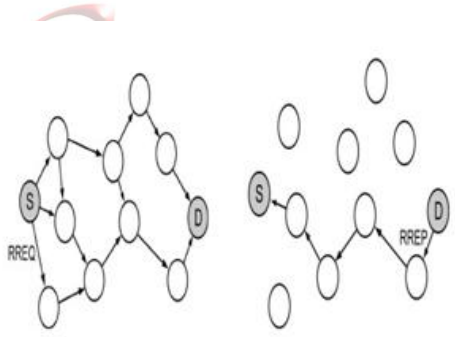

Figure 2: AODV Path Discovery Process.

4.2 DSR: Route Discovery and Route Maintenance of DSR are all operate on-demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to Each other and all routes needed for current communication.

This protocol is an origin routing protocol and is based on demand. A node maintains cache from the routes including routes from origin and it is aware of them . The entered data is updated in cache of the route when new information is obtained about current routes. Two main phases of this protocol are detection of route and maintenance and repair of routes. When origin node

ISBN: 9788175157538

wants to send a packet to destination node, it investigates its route cache to see whether it has route to destination or not. If there is a valid route to destination, it will use this route for
sending its packet. But if this node doesn't have any route, it will start route detection process through demand packet distribution. Demand packet includes address of origin and destination node and exclusive identification number. Each
intermediate node checks whether it has route to destination or not. If not, it will add its own address in this packet and will send it to its neighbors. In order to limit the number of publication of route demands, a node process route demand packet only when it has not seen it before that is its address has not been available in section route record .
A route reply is produced when destination node or and intermediate node with current information about destination node receives route demand packet. Route
record section of route demand packet which reaches a been implemented, but this implementation of GBDSR includes two essential limitations:

1- Only members of the group can send data for multiple distribution groups.

2- Multiple distribution data packets are the same single distribution packets.

Route Discovery in DSR:-For route discovery, the source node starts by broadcasting a route request packet that can be received by all neighbor nodes within its wireless transmission range. The route request contains the address of the destination host, referred to as the target of the route discovery , the source's address, a route record field and a unique identification number. At the end, the source host should receive a route reply packet containing a list of network nodes through which it should propagate the packets, supposed the route discovery process was successful.During the route discovery process, the route record field is used to accumulate the sequence of hops already taken. First of all the sender initiates the route record as a list with a single element containing itself. The next neighbor node appends itself to the list and so on. Each route request packet also contains a unique identification number called request_id. request_id is a simple counter which is increased whenever a new route request packet is being sent by the source node. So every route request packet can be uniquely identified through its initiator's address and request_id. When a host receives a route request packet, it is important to process the request in the order described below. This way we can make sure that no loops will occur during the broadcasting of the packets.

(a) Building of the route record.
(b) Propagation of the Route reply.

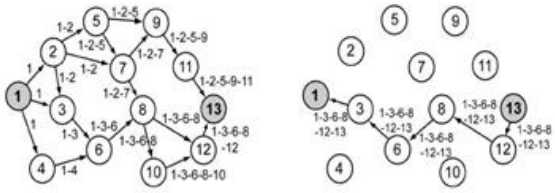

Figure 3: DSR Route Discovery Process.

request can be sent as a separate packet, piggybacked on a retransmission of the original data packet, or piggybacked on any packet with the same next-hop destination that does not also contain a software acknowledgement. After the acknowledgement request has been retransmitted the maximum number of times, if no acknowledgement has been received, then the sender treats the link to this next-hop destination as currently "broken".

5. REFERENCES

1. S. Biswas, R. Morris, ExOR: Opportunistic Multi-Hop Routing for Wireless Networks, Proceedings of ACM Sigcomm,vol.3 , no.4 , pp.412-430 Oct. 2005.
2. C. Westphal: "Opportunistic Routing in Dynamic Ad Hoc Networks: The OPRAH protocol," Proc. IEEE MASS '06, Oct. 2006, pp. 570–73.
3. Eric Rozner, Jayesh Seshadri, Yogita Ashok Mehta, and Lili Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, vol.8, no.12, pp1622-1635, December 2009.

ISBN: 9788175157538

4. Link Probability Based Opportunistic Routing Metric in Wireless Network by Yanhua Li, Yuan-an Liu, Pengkui Luo, International Conference on Communications and Mobile Computing. , vol.1 , no.4 , pp.412-430 oct 2009.

5. OM: Opportunistic Multicast Routing for Wireless Mesh Networks by Yang WenZhong , Huang ChuanHe, Wang Bo, Zhang ZhenYu, Wang Tong, Fifth International Conference on Frontier of Computer Science and Technology, ,vol.1 , no.1 , pp.312-330 jan 2010.

6. A Relay Node Selection Technique for Opportunistic Routing in Mobile Ad Hoc Networks by Nie Zhi, Liu Jing, Li Botong, Liu Hanchun, Xu Youyun. Proceedings of the 15th Asia-Pacific Conference on Communications (APCC 2009)-159,vol.3 , no.5 , pp. 10-18

7. "Opportunistic Routing for Wireless Ad Hoc and Sensor Networks: Present and Future Directions" Haitao Liu and Baoxian Zhang, Hussein T. Mouftah, Xiaojun Shen, Jian Ma**,** IEEE Communications Magazine December 2009., ,vol.3 , no.4 , pp.30-45

ISBN: 9788175157538