A Survey on Performance Evaluation using DSR in Mobile Ad-Hoc Network

Manish Kumar[1], Prof. S. R. Yadav[2]

[1] PG Scholar, MITS, Bhopal (India) [2] Head P.G., CSE, MITS, Bhopal (India)

Abstract - The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use. Survey carried out on the DSR with its enhancement and also evaluates the performance.

Keywords - MANET, DSR, MDSR, Routing, AODV, DSDV.

1. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop network, maintaining connectivity in a decentralized manner [1], [2]. It consists of a set of mobile hosts communicating amongst themselves using wireless links, without the use of any other communication support facilities such as base-stations. The nodes in a MANET can be PDAs, laptops or any other device that is capable of transmitting and receiving information. Each node in such a network acts as a host or end system as well as a router at the same time. The nodes in a MANET are generally mobile and may go out of range of other nodes in the network. Therefore, Routing in MANET is difficult since mobility causes frequent network topology changes and requires more robust and flexible mechanism to search for and maintain the routes. When the network nodes move, the established paths may break and the routing protocols must dynamically search for other feasible routes. With a changing topology, even maintaining connectivity is very difficult. In addition, keeping the routes loop free is more difficult when the hosts move. Besides handling the topology changes, routing protocols in MANET must deal with other constraints, such as low bandwidth, limited energy consumption, and high error rates; all of which may be inherent in the wireless environment. Furthermore, the possibility of asymmetric links caused by different power levels among mobile hosts and other factors such as environment conditions make routing protocols more complicated. Because of these challenging features of MANET, it has been under tremendous scrutiny and interest from the time of its emergence and by this time, numerous works have tried to address various issues. Routing in MANET is one of the well-addressed topics. Though many routing protocols have already been proposed and well-accepted in the research community because of their given promise and performance, there still remains the necessity of a flexible, user-friendly simulation tool that can make the task of simulation and visualization of routing protocols easier. The *Dynamic Source Routing* protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple “hops” between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing. The DSR protocol allows nodes to dynamically discover a *source route* across multiple network hops to any destination in the ad hoc network. Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use.

A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes that are capable of communicating with each other. There is no use of a static network infrastructure such as base station or any centralized administration in MANET. Due to the limited transmission range of wireless network interfaces, multiple hops (intermediate hosts) may be needed for one host to transfer data to another across the network. In MANET, each mobile host may operate not only as a terminal but also as a router, forwarding packets from other mobile hosts. The mobile hosts are free to move around, thus changing the network topology dynamically. Thus routing protocols for MANET should be adaptive and able to maintain routes in spite of changing the network connectivity. Such networks are very useful in military and other tactical applications such as emergency rescue or exploration missions, where static cellular phone infrastructure is unavailable or unreliable. Commercial applications are also likely where there is a need for ubiquitous communication services without the present or use of a fixed network infrastructure. Design and analysis of routing protocols are the key issues in MANET. The primary goal of a MANET routing protocol is to establish a correct and efficient route between a pair of two hosts for delivering message in a timely manner. Many different routing protocols [3,4] have been proposed for MANETs. They can be classified into two categories: table-driven and on-demand. The table-driven routing protocols are similar to and come as a natural extension of those for the wired networks including Internet. They essentially use proactive schemes, which attempt to maintain consistent up-to-date routing information from each host to every other node in the MANET. These protocols require each host to maintain one or more tables to contain latest routing information, and any change in network topology needs to be reflected by broadcasting updates information throughout the network in order to maintain a consistent network view. On the other hand, the on-demand routing protocols take a lazy approach to routing. The motivation behind the on-demand protocols is to reduce large amount of overhead for maintaining the routing table in the table-driven protocols in the dynamic MANET. They are source-initiated schemes which do not maintain or constantly update their route tables with the latest route topology. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once one or more routes are found or all possible route permutations have been examined. However, routing overhead for on-demand protocols may be still large mainly because the flooding process used in discovering routes, where the source (i.e., the host seeking a route) floods the entire network with a query packet in searching a route to the destination.

The Dynamic Source Routing (DSR) protocol (e.g., [1, 4]) is one of the more generally accepted on-demand routing protocols. It is natural to consider the DSR protocol with multiple routes since they may be built during the route discovery by coding. The Dynamic Source Routing (DSR) protocol proposed in [1] also has an option of maintaining multiple routes, so that an alternate route can be used upon failure of the primary one. But in DSR [1], too many routes are maintained in a trivial manner, without any regard to their ultimate usefulness. The performance study of DSR protocols has not been conducted in [1]. The concept of multipath routing has been used for circuit switched and packet switched networks□ as it provides an easy mechanism to distribute traÆc and balance the network load, as well as provide fault tolerance. For MANET, the Temporally Ordered Routing Algorithm (TORA) [5, 6] provides multiple alternate paths by maintaining a "destination-oriented" directed acyclic graph from the source. However, TORA does not have any easy mechanism to evaluate the performance of these multiple routes.

In designing DSR, we sought to create a routing protocol that had very low overhead yet was able to react quickly to changes in the network, providing highly reactive service to help ensure successful delivery of data packets in spite of node movement or other changes in network conditions.

2. SYSTEM MODEL

- **DSR Protocol Description**

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

i. *Route Discovery* is the mechanism by which a node **S** wishing to send a packet to a destination node **D** obtains a source route to **D**. Route Discovery is used only when **S** attempts to send a packet to **D** and does not already know a route to **D**.

ii. *Route Maintenance* is the mechanism by which node **S** is able to detect, while using a source route to **D**, if the network topology has changed such that it can no longer use its route to **D** because a link along the route no longer works. When Route Maintenance indicates a source route is broken, **S** can attempt to use any other route it happens to know to **D**, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when **S** is actually sending packets to **D**.

Route Discovery and Route Maintenance each operate entirely on-demand. In particular, unlike other protocols, DSR requires no periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbour detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behaviour 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 have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. In response to a single Route Discovery, a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks. The operation of Route Discovery and Route Maintenance in DSR are designed to allow unidirectional links and asymmetric routes to be easily supported. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available [9]. For example, some nodes in the ad hoc network may have only short-range radios, while other nodes have both short-range and long-range radios; the combination of these nodes together can be considered by DSR as a single ad hoc network. In addition, the routing of DSR has been integrated into standard Internet routing, where a “gateway” node connected to the Internet also participates in the ad hoc network routing protocols; and has been integrated into Mobile IP routing, where such a gateway node also serves the role of a Mobile IP foreign agent [10, 11].

- **Basic DSR Route Discovery**

When some node **S** originates a new packet destined to some other node **D**, it places in the header of the packet a source route giving the sequence of hops that the packet should follow on its way to **D**. Normally, **S** will obtain a suitable source route by searching its Route Cache of routes previously learned, but if no route is found in its cache, it will initiate the Route Discovery protocol to dynamically find a new route to **D**. In this case, we call **S** the initiator and **D** the target of the Route Discovery. Figure 1 illustrates an example Route Discovery, in which a node **A** is attempting to discover a route to node **E**. To initiate the Route Discovery, **A** transmits a ROUTE REQUEST message as a single local broadcast packet, which is received by all nodes currently within wireless transmission range of **A**. Each ROUTE REQUEST message identifies the initiator and target of the Route Discovery, and also contains a unique request_id, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. This route record is initialized to an empty list by the initiator of the Route Discovery.

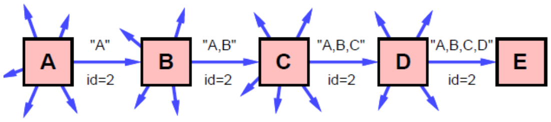

Figure 1: Route Discovery: Node **A** is the initiator, and node **E** is the target.

When another node receives a ROUTE REQUEST, if it is the target of the Route Discovery, it returns a ROUTE REPLY message to the initiator of the Route Discovery, giving a copy of the accumulated route record from the ROUTE REQUEST; when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. Otherwise, if this node receiving the ROUTE REQUEST has recently seen another ROUTE REQUEST message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the ROUTE REQUEST message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet (with the same request id).

In returning the ROUTE REPLY to the initiator of the Route Discovery, such as node **E** replying back to **A** in Figure 1, node **E** will typically examine its own Route Cache for a route back to **A**, and if found, will use it for the source route for delivery of the packet containing the ROUTE REPLY. Otherwise, **E** may perform its own Route Discovery for target node **A**, but to avoid possible infinite recursion of Route Discoveries, it must piggyback this ROUTE REPLY on its own ROUTE REQUEST message for **A**. It is also possible to piggyback other small data packets, such as a TCP SYN packet [12], on a ROUTE REQUEST using this same mechanism. Node **E** could also simply reverse the sequence of hops in the route record that it trying to send in the ROUTE REPLY, and use this as the source route on the packet carrying the ROUTE REPLY itself. For MAC protocols such as IEEE 802.11 that require a bi-directional frame exchange as part of the MAC protocol [13], this route reversal is preferred as it avoids the overhead of a possible second Route Discovery, and it tests the discovered route to ensure it is bi-directional before the Route Discovery initiator begins using the route. However, this technique will prevent the discovery of routes using unidirectional links. In wireless environments where the use of unidirectional links is permitted, such routes may in some cases be more efficient than those with only bi-directional links, or they may be the only way to achieve connectivity to the target node. When initiating a Route Discovery, the sending node saves a copy of the original packet in a local buffer called the Send Buffer. The Send Buffer contains a copy of each packet that cannot be transmitted by this node because it does not yet have a source route to the packet's destination. Each packet in the Send Buffer is stamped with the time that it was placed into the Buffer and is discarded after residing in the Send Buffer for some timeout period; if necessary for preventing the Send Buffer from overflowing, a FIFO or other replacement strategy can also be used to evict packets before they expire.

While a packet remains in the Send Buffer, the node should occasionally initiate a new Route Discovery for the packet's destination address. However, the node must limit the rate at which such new Route Discoveries for the same address are initiated, since it is possible that the destination node is not currently reachable. In particular, due to the limited wireless transmission range and the movement of the nodes in the network, the network may at times become partitioned, meaning that there is currently no sequence of nodes through which a packet could be forwarded to reach the destination. Depending on the movement pattern and the density of nodes in the network, such network partitions may be rare or may be common. If a new Route Discovery was initiated for each packet sent by a node in such a situation, a large number of unproductive ROUTE REQUEST packets would be propagated throughout the subset of the ad hoc network reachable from this node. In order to reduce the overhead from such Route Discoveries, we use exponential back-off to limit the rate at which new Route Discoveries may be initiated by any node for the same target. If the node attempts to send additional data packets to this same node more frequently than this limit, the subsequent packets should be buffered in the Send Buffer until a ROUTE REPLY is received, but the node must not initiate a new Route Discovery until the minimum allowable interval between new Route Discoveries for this target has been reached. This limitation on the maximum rate of Route Discoveries for the same target is similar to the mechanism required by Internet nodes to limit the rate at which ARP REQUESTs are sent for any single target IP address [14].

▪ Basic DSR Route Maintenance

When originating or forwarding a packet using a source route,each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. For example, in the situation illustrated in Figure 2, node **A** has originated a packet for **E** using a source route through intermediate nodes **B**, **C**, and **D**. In this case, node **A** is responsible for receipt of the packet at **B**, node **B** is responsible for receipt at **C**, node **C** is responsible for receipt at **D**, and node **D** is responsible for receipt finally at the destination **E**. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use (such as the link-level acknowledgement frame defined by IEEE 802.11 [13]), or by a *passive acknowledgement* [15] (in which, for example, **B** confirms receipt at **C** by overhearing **C** transmit the packet to forward it on to **D**). If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR-specific software acknowledgement be returned by the next hop; this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is unidirectional, this software acknowledgement may travel over a different, multi-hop path. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. In Figure 2, if **C** is unable to deliver the packet to the next hop **D**, then **C** returns a ROUTE ERROR to **A**, stating that the link from **C** to **D** is currently "broken." Node **A** then removes this broken link from its cache; any retransmission of the original packet is a function for upper layer protocols such as TCP. For sending such a retransmission or other packets to this same destination **E**, if **A** has in its Route Cache another route to **E** (for example, from additional ROUTE REPLYs from its earlier Route Discovery, or from having overheard sufficient routing information from other packets), it can send the packet using the new route immediately. Otherwise, it may perform a new Route Discovery for this target.

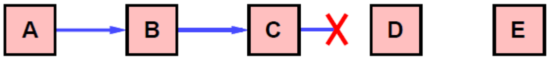

Figure 2: Route Maintenance: Node **C** is unable to forward a packet from **A** to **E** over its link to next hop **D**.

3. PREVIOUS WORK

AODV, DSR and DYMO are on demand routing protocols based on IEEE 802.11 are examined and characteristic summary of these routing protocols is presented. With MAC and physical layer model their performance is analyzed and compared on [16] performance measuring metrics throughput, jitter, packet delivery ratio, end-to-end delay and error reply packets and dropped packets due to non availability of routes by varying CBR data traffic load using QualNet 5.0.2 network simulator. It is observed that AODV outperforms both of the DSR and DYMO routing protocols in terms of the packet delivery ratio as it uses fresh routes and DSR performs poorer because of aggressive use of cache. The throughput is best in case of the DYMO as it avoids good routes and outperforms both DSR and AODV. It is also performs better with heavy load. The DSR performs poorer than both because of aggressive use of cache. The poor performance of DSR is also attributed to absence of proper mechanism to expire the stale routes and therefore the jitter and the average end-to-end delay is also very high in comparison to AODV and DYMO. The dropped packets due to no routes and error replies are more in case of DYMO as routes breakages are more than both AODV and DSR due to route maintenance and mobility. It is found that the Packet deliver is better in case of AODV with increased traffic load and mobility.

ViSim [17] is a new simulation tool that has a user-friendly graphical interface. ViSim could be useful for researchers, students, teachers in their works, and for the demonstration of various wireless network scenarios on computer screen. It could make the task of simulation more exciting and enhance the interest of the users without going into complex command-only text interface. ViSim is not a simulation engine rather it calls ns-2 simulations in the background and makes the task easy for the users to visualize the simulation in Windows environment. Though ViSim is mainly a simulation demonstration tool, any user with the knowledge of ns-2 and Tcl scripting is also allowed to do necessary modifications and quick configurations for any other MANET routing scenario. Using ViSim simulation tool, they measured the performances of several Mobile Ad-hoc Network (MANET) routing protocols. They present the performance analysis of three prominent MANET routing protocols; DSDV, DSR, and AODV using ViSim tool. The details of various features of ViSim. In [17], they have presented user-friendly simulation tool/prototype which can ease the task of simulation of MANET routing protocols even in Windows based environments. Many users dealing with ns-2 simulations face troubles in setting up Linux or other systems and environment. The use of ActiveTcl with graphical ViSim interface could really be beneficial for the research community in general. Using ViSim simulation tool, we obtained different graphs and analyzed the results for different scenarios which leads to the following conclusions:

1. For AODV, it is observed that it adapts quickly to the change of the network and has a relatively stable throughput with a moderate goodput. So, in an application where there is a fast change in the network topology and a requirement of stable data rate, AODV is more preferable.

2. DSDV turns out to have the best goodput and lesser routing load; however, it takes time to converge. So if there is relatively less number of nodes in the network and the mobility is somewhat steady or slow, DSDV will work more efficiently.

3. DSR, though has a very high throughput, it actually contains less data packets and it can seen that there are lots of fluctuations on the throughput curve which are not preferred in a wireless network.

The intent of [18] is to study three ad-hoc routing protocols ZRP, DSR and STAR in the presence of some misbehaving nodes and analyze them. It concentrates on evaluating the performance of routing protocols when some nodes behave as malicious ones. The performance analysis for above protocols is based on variation in speed of nodes in a network with 50 nodes. All simulation is carried out with QualNet 4.5 network simulator.

Operation of DSR is evaluated the through detailed simulation on a variety of movement and communication patterns, and through implementation and significant experimentation in a physical outdoor ad hoc networking testbed [19]. They have constructed in Pittsburgh, and have demonstrated the excellent performance of the protocol. In [19], they describe the design of DSR and provide a summary of some of simulation and testbed implementation results for the protocol. As shown in detailed simulation studies and in their implementation of the protocol in a real ad hoc network of cars driving and routing among themselves, DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network. A key reason for this good performance is the fact that DSR operates entirely on demand [20], with no periodic activity of any kind required at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbour detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behaviour and lack of periodic activity allows the number of routing 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 have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. Their goal is to create an integrated set of protocols that allow mobile computers, and the applications running on them and communicating with them, to seamlessly make the most efficient use of the best available network connections at any time. The Dynamic Source Routing protocol (DSR) is an important component of such a system.

STAR is a table driven and DSR is on demand protocols based on IEEE 802.11 are analyzed for their performance on different performance measuring metrics versus varying traffic [21] CBR load using QualNet 5.0.2 network simulator. It is observed with the simulation analysis that at low traffic load DSR performs better than the STAR-LORA protocol but as the traffic load increases STAR-LORA outperforms DSR protocol. The performance of STAR-LORA is better because of its LORA technique that enables it to find route faster and safe. The packet delivery and throughput are better in case of STAR-LORA. The end to end delay and jitter are also very high for DSR.

N. Bhalaji et al. [22] propose a new approach based on relationship among the nodes which makes them to cooperate in an Ad hoc environment. The trust unit is used to calculate the trust values of each node in the network. The calculated trust values are being used by the relationship estimator to determine the relationship status of nodes. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the network simulator-2. In [22] they have discussed the characteristics of mobile ad hoc network. They also analyzed the different types of issues and attacks in an ad hoc environment. This proposed scheme of Trust Enhanced DSR protocol increases the level of security routing and also encourages the nodes to cooperate in the ad hoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing.

High overhead involved in flooding while route creation is a limiting factor of Dynamic Source Routing (DSR) protocol applied for mobile ad hoc networks (MANETs). During data delivery, it seems that we fully benefit from DSR if the route is not long enough. In [23], two modifications of DSR algorithm are proposed to enhance its performance. In the modified approach of DSR, to reduce broadcasting overhead, multicasting approach is used. Again, for shortening packet length, in case of longer route, the route is truncated after a predetermined number of hops. Some simulations show that the new modified algorithm (Enhanced DSR) performs better than the DSR algorithm. In the proposed modified DSR algorithm E-DSR with two new concepts: Reducing Route Request packet and Truncating the packet header length in DSR. Performance of E-DSR is elevated in respect of some simulation metrics such as Route Request and control packet overhead, and packet delivery ratio. Unlike other source routing protocols, the E-DSR adapts quickly to routing changes by reduction of sending route request packet as well as shortening the packet length when the size of the wireless network is large enough.

4. PROPOSED METHODOLOGY

In this paper we are proposing AODV protocol for performance evaluation. AODV protocol performs Route Discovery using control messages Route Request (RREQ) and Route Reply (RREP). Routes are set up by flooding the network with RREQ packets which, however, do not collect the list of the traversed hops. Rather, as a RREQ traverses the network, the traversed mobile nodes store information about the source, the destination, and the mobile node from which they received the RREQ. The later information is used to set up the reverse path back to the source. When the RREQ reaches a mobile node, that knows a route to the destination or the destination itself, the mobile node responds to the source with a packet (RREP) which is routed through the reverse path set up by the RREQ. This sets the forward route from the source to the destination. To avoid overburdening the mobiles with information about routes which are no longer used, nodes discard this information after a timeout. When either destination or intermediate node moves, a Route Error (RERR) is sent to the affected source nodes. When source node receives the RERR, it can reinitiate route discovery if the route is still needed. Neighbourhood information is obtained by periodically broadcasting.

5. RESULTS DISCUSSION

The use of AODV protocol at the place of DSR protocol may provide better performance because in the AODV protocol route discovery is performed using Route Request (RREQ) and Route Reply (RREP). The use of above two parameters of AODV protocol gives updated information for route discovery in the routing. Since it will provide updated information for route discovery so that it will gives better performance as compared to DSR protocol.

6. CONCLUSION

The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network. A key reason for this good performance is the fact that DSR operates entirely on demand with no periodic activity of any kind required at any level within the network. In this paper we have described the principle mechanisms of Route Discovery and Route Maintenance used by DSR, and have shown how they enable wireless mobile nodes to automatically form a completely self-organizing and self-configuring network among themselves. In this survey which includes research work which has done on DSR. Even the modified version of the DSR is also analysed for evaluation of performance of DSR.

7. FUTURE SCOPES

In future we are planning for evaluating the performance of routing using AODV protocol and we will also try to modify AODV protocol. After modification of AODV protocol we will analyzed the behaviour of AODV and modified AODV protocol.

Use of AODV protocol will provide us better results as compared to DSR protocol and modified version of AODV protocol will also gives better results as compared to modified DSR protocol.

REFERENCES

[1] A.-S.K. Pathan, C.S. Hong, Routing in Mobile Ad Hoc Networks, in: S. Misra, I. Woungang, S.C. Misra (eds.), Guide to Wireless Ad Hoc Networks, Springer London, ISBN: 978-1-84800-328-6, 2009, pp. 59-96.

[2] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, Proceedings of ACM MOBICOM 2000, Boston, MA, USA, pp. 255-265.

[3] Yu-Liang Chang, Ching-Chi Hsu, "Connection-Oriented Routing in Ad Hoc Networks Based on Dynamic Group Infrastructure," it Proc. of the Fifth IEEE Symposium on Computers and Communications (ISCC 2000), pp. 587-593, July 04 - 06, 2000.

[4] Ming-Hong Jiang, Rong-Hong Jan, "An Efficient Multiple Paths Routing Protocol for Ad-hoc Networks," The 15th International Conference on Information Networking (ICOIN'01), January 31 February 02, 2001 Beppu City, Oita, Japan, pp. 544-549.

[5] J. Broch, D. Johnson and D. Maltz, "Dynamic Source Routing in Wireless Ad Hoc Networks," in Mobile Computing, eds. T. Imielinski and H. Korth (Kluwer Academic, 1996).

[6] A. Nasipuri, R. Castaneda and S. Das, "Performance of multipath routing for on-demand protocols in mobile ad hod networks," ACM/Kluwer Mobile Networks and Applications, vol. 6, no. 4, pp. 339-349, 2001.

[7] Vincent D. Park and M. Scott Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. of IEEE INFOCOM '97, Kobe, Japan, April 1997, pp. 1405-1413.

[8] Vincent D. Park and M. Scott Corson, "A Performance Comparison of the Temporally-Ordered Routing Algorithm and Ideal Link-State Routing," Proc. of IEEE Symposium on Computers and Communication, Athens, Greece (June 1998), pp. 592-598.

[9] Josh Broch, David A. Maltz, and David B. Johnson. Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks. In *Proceedings of The International Symposium on Parallel Architectures, Algorithms and Networks* (ISPAN’99), Workshop on Mobile Computing, Perth, Western Australia, June 1999. IEEE Computer Society.

[10] David B. Johnson. Scalable Support for Transparent Mobile Host Internetworking. *Wireless Networks*, 1(3):311–321, October 1995.

[11] Charles Perkins, editor. IP Mobility Support. RFC 2002, October 1996.

[12] J. B. Postel, editor. Transmission Control Protocol. RFC 793, September 1981.

[13] IEEE Computer Society LAN MAN Standards Committee. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York, New York, 1997.

[14] Robert T. Braden, editor. Requirements for Internet Hosts—Communication Layers. RFC 1122, October 1989.

[15] John Jubin and Janet D. Tornow. The DARPA Packet Radio Network Protocols. *Proceedings of the IEEE*, 75(1):21–32, January 1987.

[16] Parma Nand and Dr. S.C. Sharma, " Performance study of Broadcast based Mobile Ad hoc Routing Protocols AODV, DSR and DYMO", International Journal of Security and Its Applications, Vol. 5 No. 1, January, 2011 pp. 53-64.

[17] Nazmus Saquib, Md. Sabbir Rahman Sakib and Al-Sakib Khan Pathan "Performance Analysis of MANET Routing Protocols Using An Elegant Visual Simulation Tool".

[18] Amrit Suman, Ashok Kumar Nagar, Sweta Jain and Praneet Saurav, "Simulation Analysis of STAR, DSR and ZRP in Presence of Misbehaving Nodes in MANET", Manuscript received November 15, 2009.

[19] David B. Johnson, David A. Maltz and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks".

[20] David B. Johnson. Routing in Ad Hoc Networks of Mobile Hosts. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, pages 158–163. IEEE Computer Society, December 1994.

[21] Rani Astya, and S.C. Sharma, "Traffic Load based Performance Analysis of DSR & STAR Routing Protocol", International Scholarly and Scientific Research & Innovation World Academy of Science, Engineering and Technology Vol:5 2011-08-27, pp. 415-418.

[22] N. Bhalaji, A. R. Sivaramkrishnan, Sinchan Banerjee, V. Sundar, and A. Shanmugam. "Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks", International Scholarly and Scientific Research & Innovation, World Academy of Science, Engineering and Technology Vol:3 2009-01-23, pp. 897-902.

AUTHOR'S PROFILE

Manish Kumar has received his Bachelor of Engineering degree in Computer Science and Engineering from Millennium Institute of Technology and Science, Bhopal (India) in the year 2013. At present he is pursuing M.Tech. with the specialization of Computer Science and Engineering in Millennium Institute of Technology and Science, Bhopal (India). His area of interest is Computer networking, Cloud Computing, and Image Processing.

Prof. S. R. Yadav has received his Bachelor of Engineering in Computer Science and Engineering from G.I.E.T. Gunupur under B.U. Orissa in the year 2006. M.Tech. in Computer Science and Engineering From P.G. Department of Computer Science Engineering under B.U. Berhampur, Orissa in the year 2009. M.B.A. in HR From Academy of Management Bhopal under B.U. Bhopal, M.P. in the year 2014.He is a Ph.D. Scholar of Computer science and engineering PAHER Univ. Udaipur, Rajasthan, India. At present he is working as an Associate Professor at Millennium Institute of Technology and Science, Bhopal.(India). His areas of interests are Data Mining, Intrusion Detection System using Data Mining and Neural Networks.