

Introduction And Analysis Of DSR Protocol

Pillai Unnikrishnan
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
Unni.Krishnan@hut.fi

Abstract

The Dynamic Source Routing Protocol is a reactive on demand routing protocol used in multi hop wireless ad hoc networks. DSR makes the network self-organizing and self-configuring. Two important mechanisms in DSR are Route Discovery and Route Maintenance. Nodes discover and maintain routes through the network using these mechanisms. DSR uses source routing, which allows routing of packets to be loop free and also allows caching of routes in nodes for future use. This paper describes the design of the DSR protocol and the important mechanisms of the protocol. Then the paper describes the support in DSR for Heterogeneous Networks and Interconnection to Internet and Mobile IP. The DSR protocol is then compared to another reactive protocol called AODV. Based on certain earlier simulation results DSR protocol is analyzed and conclusions are drawn.

KEYWORDS: Ad Hoc networks, DSR, AODV, Heterogeneous Networks.

1 Introduction

An ad hoc network is a collection of communication devices or nodes that wishes to communicate but have no fixed infrastructure or pre-determined organization of available links. Nodes are using Internet Protocol and IP addresses are assigned to each of the nodes. Individual nodes discover dynamically which other nodes they can communicate with. Laptop computers, personal digital assistants are examples of nodes in an ad hoc network. [2] An ad hoc network is not centrally administrated and the network will not collapse if one of the nodes moves out of range of the others [3]. In addition to sending packets directly, some nodes may need other nodes to transmit information to some others, which is called multi hopping. Multihop networking increases network scalability, reduces interference, increases overall network throughput, decreases the delay and reduces energy consumption. [4]

Figure 1 illustrates an example of a small ad hoc network with 8 nodes along with the links between them. The nodes are able to move relative to each other and when that happens the links between them are broken and other links may be established. Here, M1 moves away from M2 and establishes new links with M7 and M8. Most algorithms also allow for the appearance of new mobile nodes and the disappearance of previously available nodes. As the ad hoc network is not centralized and does not have a fixed infrastruc-

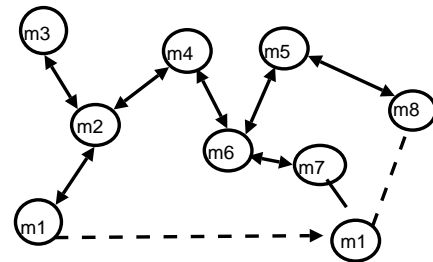


Figure 1: example of a small ad hoc network

ture it should be distributed. Functions like addressing and authentication should be designed in such a way for them to work in a distributed environment. The Internet protocols and mobility issues should be addressed and designed to adapt to the ad hoc networking environment. As ad hoc networking is a multiplayer problem, the physical layer should address link changes, the MAC layer should minimize collisions and allow fair access, the network layer needs to determine and distribute information and maintain efficiency and the transport layer must be able to handle delay and packet loss. Applications need to be designed to handle frequent disconnection and reconnection with peer applications. Ad hoc networks can be deployed or used in space exploration, undersea operations, military purposes, and network of computers in a conference having no infrastructure. [5] In mobile ad hoc networks there are two types of routing protocols called proactive and reactive. Proactive protocols are protocols that keep track of routes for all destinations in the ad hoc network. These protocols store route information in a table and the route can be selected from the table when an application starts. Advantage of proactive protocols is that it ensures minimal delay when communication with an arbitrary destination. The disadvantage of proactive protocols is that they suffer from additional control traffic that is needed to continually update scale rout entries. Since the ad hoc network contains mobile nodes and the routes are broken frequently, repairing those broken routes can cause scarce bandwidth resources to be wasted and can cause further congestion at intermediate network points. Taking into consideration all these factors on-demand reactive protocols have been designed so that routing information is acquired only when it is actually needed. Reactive routing protocols use less bandwidth for maintaining the route tables at each node, but the latency for applications increase. In Reactive routing protocols a route to the destination has to be acquired before communications can begin and due to this aspect applica-

tions would have to suffer a long delay. Reactive routing protocols are suitable for Ad Hoc networks where the topology is extremely dynamic. A reactive on demand routing protocol called Distance Source Routing is the focus of attention here. [5] The Dynamic Source Routing protocol (DSR) [1] is a simple and efficient routing protocol designed for use in multihop wireless ad hoc networks of mobile nodes. Network is self-organizing and self-configuring when using DSR. When the nodes in an ad hoc network move and join the network while forwarding packets, all routing is automatically determined and maintained by DSR. DSR 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 [5]. Distance Source Routing Protocol can interoperate with Mobile IP and nodes using Mobile IP and DSR have seamlessly migrated between WLAN's, cellular data services and DSR mobile ad hoc networks [5]. The main aim of designing DSR was to create a routing protocol that reacts quickly to network changes and provides highly reactive service for successful delivery of data packets and has very low overhead. DSR allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets. In an ad hoc network nodes should be willing to participate in the network protocols and should be able to move continuously at any time without notice. Nodes can enable promiscuous receive mode and nodes should be able to operate bi-directionally although DSR can support and operate over unidirectional links as well. DSR supports very rapid rates of arbitrary node mobility. DSR can take advantage of additional optimizations like route reversal when used on top of MAC protocols. [5] DSR is composed of two main mechanisms: Route Discovery and Route Maintenance. These two mechanisms work together to allow and maintain routes to arbitrary destinations in the ad hoc network. Route Discovery is used when a node does not know the route to a destination node and attempts to send a packet to the destination node. Route Maintenance indicates that the source route is broken or can invoke the Route Discovery again to find a new route. [5]

2 DSR Protocol Design Overview And Important Properties

Route Discovery and Route Maintenance, which are the main mechanisms of the DSR protocol, allows the discovery and maintenance of source routes in the ad hoc network. DSR works entirely on an on-demand basis. DSR does not rely on functions like periodic routing advertisement, link status sensing or neighbor detection packets and because of the entirely on demand behavior, the number of overhead packets caused by DSR scales down to zero. As DSR works entirely on demand and as nodes begin to move continuously, the Routing packet overhead automatically scales to only that needed to react to changes in the route currently in use. In response to a single Route Discovery if a node

learns and caches multiple routes to a destination, it can try another route if the one it uses fails. The overhead incurred by performing a new Route Discovery can be avoided when the caching of multiple routes to a destination occurs. In wireless networks, differing antenna, propagation patterns or sources of interference can cause the link between two nodes to not work efficiently in either direction. DSR improves the overall performance and network connectivity in the system by allowing unidirectional links to be used when necessary. Routing in DSR is integrated into standard Internet routing and Mobile IP routing and supports internetworking between different types of wireless networks. [5]

2.1 DSR Route Discovery

The header of the packet, which originates from a source node S to a destination node D, contains the source route, which gives the sequence of hops that the packet should traverse. A suitable source route is found normally when searching the Route Cache of routes obtained previously but if no route is found then the Route Discovery protocol is initiated to find a new route to D. Here S is the initiator and D the target. [5] Node A transmits a ROUTE REQUEST

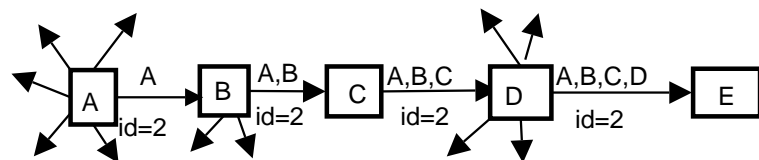


Figure 2: Node A is the initiator and Node E is the target

message, which is received by all the nodes in the 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. The initiator of the Route Discovery initializes the route record to an empty list. [5] When the target node receives the ROUTE REQUEST message, it returns a ROUTE REPLY message to the ROUTE Discovery initiator with a copy of the accumulated route record from the ROUTE REQUEST. This route is cached in the Route Cache when the initiator receives the ROUTE REPLY and is used in sending subsequent packets to this destination. When the target node finds a ROUTE REQUEST message from the same initiator bearing the same request ID or if it finds its own address is already listed in the route record of the ROUTE REQUEST message, it discards the REQUEST. If the target node does not find the ROUTE REQUEST message from the initiator, then it appends its address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet. When Route Discovery is initiated the copy of the original packet is saved in a local buffer called Send Buffer. The Send Buffer contains copies of each packet that cannot be transmitted by the sending node. The packets are kept until a source route is avail-

able or a timeout or Send Buffer overflow occurs. As long as a packet is in the Send Buffer, the node should initiate new Route Discovery until time out occurs or overflow of Buffer occurs. An exponential Back off algorithm is designed to limit the rate at which new ROUTE Discoveries may be initiated by any node for the same target. [5]

2.2 DSR Route Maintenance

When a packet with a source route is forwarded, each node in the source route makes sure that the packet has been received by the next hop in the source route. The confirmation of receipt will be received only by re-transmitting the packet for a number of times. [5]

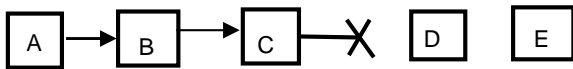


Figure 3: Node C is unable to forward a packet from A to E over the next node D

Node A is the originator of a packet to the desired destination E. The packet has a source route through intermediate nodes B, C and D. Node A is responsible for receipt of the packet at B, node B at C, node C at D and node D at E. Node B confirms receipt of packet at C by overhearing C transmit the packet to forward it to D. The confirmation of acknowledgement is done by passive acknowledgements or as link-layer mechanisms such as option in MAC protocol. The node receiving the packet can return a DSR specific software acknowledgement if neither of the acknowledgements is available. This is done by setting up a bit in the packet's header and then requesting a DSR specific software acknowledgement by the node transmitting the packet. When a node is unable to deliver a packet to the next node then the node sends a ROUTE ERROR message to the original sender of the packet. The broken link is then removed from the cache by the originator of the packet and retransmissions to the same destination are done by upper layer protocols like TCP. [5]

2.3 Additional Route Discovery Features

Caching Overhead Routing Information: When a node is forwarding a packet, the routing information of the packet is added to the Route Cache of the node. A node may cache the source route, the accumulated route record and the route being returned in a ROUTE REPLY. The presence of unidirectional links in the ad hoc network is a limitation on caching of overhead information. [5]

Replying to Route Requests using Cached Routes: Before forwarding packets, nodes receiving a ROUTE REQUEST examine their Route Caches even if they are not targets. A ROUTE REPLY is sent to the initiator when the ROUTE is found. The ROUTE REPLY contains the route record to list the sequence of hops and the route from the node to the target from the node's Route Cache. There should be no duplicate nodes listed in the route record of the resulting route being returned in the ROUTE REPLY. [5]

Preventing Route Reply Storms: When a packet is sent to the local broadcast address, it might cause a large number of nodes to send Route Replies back to one source. If a node puts its network interface into promiscuous receive mode, it delays sending its own ROUTE REPLY for a short period. During the delay, the node receives and can verify all data packets from the initiator and can infer whether the initiator of the Route Discovery has already received a ROUTE REPLY showing a better route. [5]

Route Request Hop Limits: This mechanism is used to determine whether the target is a neighbor of an initiator or if the neighbor node has a route to the target cached. A hop limit is used to limit the number of intermediate nodes allowed to forward the copy of the ROUTE REQUEST. Before finding the target and when the REQUEST is forwarded, the limit is decreased and the REQUEST packet is discarded if the limit reaches zero. [5]

2.4 Additional Route Maintenance Features

Packet Salvaging: A node may want to salvage the data packet that caused the ROUTE ERROR. The Route Cache of the node is searched for a route from itself to the destination of the packet causing the ERROR. The original source route on the packet with the route from its Route Cache is replaced for the route being found. The packet is forwarded to the next node in the source route. Backtracking from a current node to an earlier node is allowed in this method of packet salvaging but the packet can be salvaged only once. [5]

Automatic Route Shortening: Automatic shortening is the method when one or more of the intermediate hops become unnecessary, the source route gets shortened. Automatic shortening of routes is similar to passive acknowledgements. A node by operating its network interface in promiscuous receive mode is able to overhear a packet carrying a source route. If so, then the node examines the route's unused portion. The intermediate nodes in the source route are not needed if the node is not the intended next hop for the packet but is named in the later unused portion of the source route of the packet. [5]

Increased Spreading of Route Error Messages: When a source node receives a ROUTE ERROR for a data packet that it originated, it propagates it to its neighbors by piggy-backing it on its next ROUTE REQUEST. Stale information in the caches of nodes around this source node will not generate ROUTE REPLYs that contain the same invalid link for which this source node received the ROUTE ERROR [5].

3 Support For Heterogeneous Networks

When configuring and deploying an ad hoc network all nodes are equipped with the same type of wireless network interfaces, allowing simple routing between nodes over arbitrary sequence of network nodes. A subset of nodes with a network interface consisting of longer-range wireless network interface is the most flexible configuration in an ad hoc network, which enables high-speed communication among cooperating nodes and at the same time allows communication

with distant nodes without requiring very large number of network hops. [5]

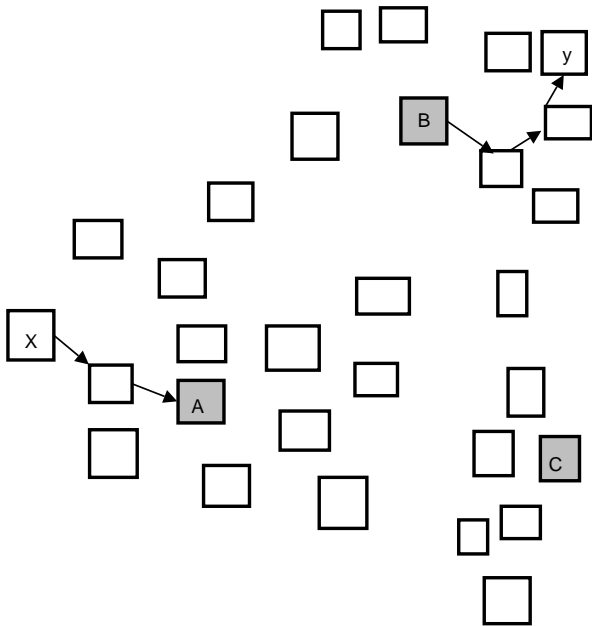


Figure 4: A heterogeneous Ad Hoc Network

3.1 Interface Indices in DSR, Internet Inter-connection and Mobile IP

Through its logical addressing mode, DSR gives support for automatic seamless routing to heterogeneous configurations. Each node in an ad hoc network when using DSR chooses one of the differing IP address for individual network interfaces. One of these IP addresses is used as the home address for all communication in the ad hoc network. DSR has the ability to treat the overall network as a single routing domain. Each node assigns a locally unique interface index to each of its own network interfaces. This interface index is an opaque value and should be unique. [5] DSR supports seamless interoperation between an ad hoc network and the Internet. Interoperation is enabled when one or modes in the ad hoc network are connected to the Internet in such a way that it participates in the ad hoc network and the Internet through DSR and standard IP routing respectively. Such a node is called a gateway node and it operates as a Mobile IP home agent and allows nodes to visit the ad hoc network as a Mobile IP foreign network and also allows nodes whose home network is the ad hoc network to visit other networks using Mobile IP. Gateway nodes use two special reserved interface index values to identify their interconnection to the Internet. When a node has a separate physical network interface other than the network interface, which is used for the ad hoc network then the reserved index value, is used to identify that network interface. Through standard IP routing it is also possible to use a single network interface both for ad hoc network participation and for Internet connection. The reserved index values for mobility agents and routers allow mobility agents to advertise their existence at low cost [5].

4 Comparison Of DSR Protocol With AODV Protocol

The Distance Source Routing Protocol and the Ad Hoc On Demand Routing protocol are two dynamic routing protocols that initiate routing activities for ad hoc networks on an on demand basis. These protocols were designed for reducing the routing loading in ad hoc networks. The routing mechanism in DSR uses source routing, while AODV uses a table driven routing framework and destination sequence numbers. AODV relies on certain timer-based activities while DSR does not rely on such options. In DSR the sender knows the hop-by-hop route to the destination because of the use of source routing in the protocol. In DSR, the routes are stored in route cache. The packet header contains the source route. Route Discovery is used to dynamically determine a route when the route is not known. Route Request packets are send to flood the network and Route Error packets are send when any link in the source route is broken. DSR makes use of source routing and route caching. DSR uses Route Maintenance mechanism to repair routes that get broken when sending packets from the sender to the destination. Packet Salvaging, Automatic Route Shortening, Increased Spreading of Route Error Messages are some of the mechanisms, which are used under Route Maintenance. [7]

AODV discovers routes on an on-demand basis using a similar route discovery process as in DSR. AODV uses traditional routing tables, one entry per destination for maintaining routing information. DSR on the other hand maintains multiple route cache entries for each destination. To propagate route reply back to the source and to route data packets to the destination, AODV relies on routing table entries. Sequence numbers at each destination determines freshness of routing information and prevents routing loops. Routing packets carry the sequence numbers. The maintenance of timer-based states in each node for utilization of individual route entries is an important feature of AODV protocol. Sets of predecessor nodes are maintained for each routing table entry, which indicates the set of neighboring nodes. Route Error packets are used to notify these nodes when the next-hop link breaks. All the routes using the broken link are erased when the route error packets are send to its own set of predecessors. Route Error packets in AODV are intended to inform all sources using a link when a failure occurs. In AODV, Route Error propagation is visualized as a tree structure where the root is the node at the point of failure and all sources using the failed link as leaves. An optimizing technique in AODV to control Route Request flood in the route discovery process is to use an expanding ring search to discover routes to unknown destination. [7] DSR with the influence of source routing and promiscuous listening of data packet transmissions has access to a significantly greater amount of routing information than AODV. AODV can gather only limited amount of routing information. DSR uses route caching aggressively by replying to all requests reaching a destination from a single request cycle. In AODV, the destination replies only once to the request arriving first. The rest of the requests are ignored. Since DSR does not have any mechanism for the expiration of stale routes stored in the cache, some of these stale routes may start polluting

other caches. AODV when faced with the choice of stale routes would choose the fresher one. The entry in the routing table if not used recently gets expired. [7]

4.1 Analysis of DSR protocol

The behavior of DSR protocol has been simulated with the ns-2 network simulator [10,11]. The simulations were run in ad hoc networks of 50 mobile nodes. It was seen that the DSR protocol worked well in scenarios with relatively small amounts of DSR nodes. DSR does not need any periodic link status sensing or routing advertisements because of the fact that DSR embeds control information in the data packets, which is sent to the network. It can be seen that the protocol worked quite well with very little overhead when the functionalities were up to specifications. Routing instability may be a cause for concern in DSR when the protocol relies on every source to know the best path to the destination. If the path is no longer valid and the other network elements know that the source would still insist that the path is correct. Since DSR supports unidirectional links as well as bi-directional there arises no problem in the directionality of a link in an ad hoc network. [6] In DSR the header is placed after the main header. Packet filtering does not work in DSR since the packet filters need to skip over the DSR header which is not possible and so they can only see the protocol as DSR. Link failures in DSR are mild and causes of route discovery are less. Since there is a large amount of cached routes in each node in DSR, route discovery is delayed until all the cached routes fail. Caches getting stale are quite high when with high mobility and with low mobility link failures are low. [7] DSR performed better in less stressful conditions because of the aggressive caching feature in use. Finally DSR requires that every node in the network should trust each other [6].

4.2 Future Work

Scope of the applicability of DSR should be defined precisely. Security issues should be covered and studied in general, as security is an important aspect. Though DSR is not feasible to a large number of nodes, directions and perspectives to study how and what could be changed or configured to suit DSR for large networks could also be researched.

5 Conclusion

It has been found that in multi hop wireless ad hoc networks, the Dynamic Source Routing Protocol is quite effective. It has been seen that DSR is suited for small network of nodes. In an ad hoc network, DSR scales well and has very low routing overhead and can deliver all data effectively to all nodes in the network. DSR deals with both uni-directional and bi-directional links. The two most important mechanisms in DSR namely, Route Discovery and Route Maintenance enables wireless nodes to form a completely self-organizing and self-configuring network among themselves. Security features are not addressed in this document. It has been assumed that nodes communicate with each other in good faith. DSR can be secured by encrypting communication between

the nodes. Cryptographic methods could be introduced to secure DSR. New features like multicast routing, resource management, quality of service should be pondered and designed so that mobile nodes can get the best performance from DSR protocol.

References

- [1] David B. Johnson, David A. Maltz, Yih-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR). *Internet Draft, draft-ietf-manet-dsr-09.txt*, 15 April 2003.
- [2] Ram Ramanathan and Jason Redi *A Brief of Overview of Ad Hoc Networks: Challenges and Directions..* BBN Technologies.
- [3] Tony Larsson and Nicklas Hedman. *Routing Protocols in Wireless Ad-hoc Networks-A Simulation Study.* Stockholm, 1998
- [4] Klaus Nieminen. *Introduction to Ad Hoc Networking..* Networking Laboratory, Helsinki University of Technology.
- [5] Charles.E.Perkins. *AdHoc Networking..* Addison-Wesley, 2001.
- [6] Pekka Savola. *DSR: Dynamic Source Routing.* CSC/FUNET, Helsinki University of Technology.
- [7] Charles.E.Perkins, Elizabeth M Royer, Samir.R.Das and Mahesh.K.Marina. Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks *IEEE Personal Communications*, Feb 2001.
- [8] Elizabeth M Royer, Chai-Keong Toh A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *RFC 2409, IEE Personal Communications* , 1999
- [9] Yih-Chun Hu, David B.Johnson Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks *Carnegie Mellon University, Pittsburgh*
- [10] Elizabeth M Royer, Chai-Keong Toh A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *RFC 2409, IEE Personal Communications* , 1999
- [11] Yih-Chun Hu, David B.Johnson Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks *Carnegie Mellon University, Pittsburgh*
- [12] Broch .J, Maltz .D, Johnson. D,Hu. Y, Jetsceva J A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols, *Carnegie Mellon University, Pittsburgh*
- [13] Maltz.D , Broch. J, Jetsceva. J, Johnson.D The effects of On-Demand Behavior in Routing Protocols for Multi-Hop Wireless Ad Hoc Networks *IEEE Journal on Selected Areas in Communications special issue on mobile and wireless networks. August 1999.*