A Survey Paper on Dynamic Source Routing Protocol (DSR) in Ad-Hoc Network

Nimpal Patel[1] Professor Anjuman Ranavadiya[2] Professor Shreya Patel[3]

[2,3]Professor

[1,2,3]Department of Computer Engineering

[1,2,3]Growmore Faculty Of Engineering, Berna, Himmatnagar

Abstract— Dynamic source routing protocol (DSR) is an on demand routing protocol suited for ad-hoc network. An ad hoc network is a network that is composed of individual devices communicating with each other directly. And another word to say an ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration.[10] Many ad hoc networks are local area networks where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point. In this research we use optimized routing protocols in mobile ad hoc network (MANET), the optimization is done on the routing protocol DSR (Dynamic Source Routing) which is reactive routing protocol using ant algorithm. Then we analysis and evaluated the performance of this routing protocol in various scenario and compared the result with standard DSR routing protocol. The results of this research indicate the performance of DSR-ant has a better performance In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. For all but the highest rates of host movement simulated, the overhead of the protocol is quite low, falling to just 1% of total data packets transmitted for moderate movement rates in a network of 24 mobile hosts.

Key words: DSR, MANET, Route Discovery

I. INTRODUCTION

A computer network is an interconnected collection of Autonomous computers. In recently, there has been more and more growth in the sales of laptop and mobile Computers. Moreover, many of these small computers on operate for many hours with battery power, users are free to move about at their convenience without being constrained by wires. If you have mobile device it make sense only if you are exchanging the information with other nodes. Mobile hosts such as notebook computers featuring powerful CPUs, large main memories, hundreds of megabytes of disk space, multimedia sound capabilities, and colour displays, are now easily affordable and are becoming quite common in every business and personal life At the same time, network connectivity options for use with mobile hosts have increased dramatically, including support for a growing number of wireless networking products based on radio and infrared. With this type of mobile computing equipment, there is a natural desire and ability to share information between mobile users. Often, mobile users will meet under circumstances that are not explicitly planned for and in which no connection to a standard wide area network such as internet is available. Impractical due to the time or expense required for connection these kinds of networks of mobile hosts have been known as Ad – hoc Networks. Ad hoc Network (MANET) is a wireless network with no infrastructure in which every node or the user has the ability to searches the best route. Ad-Hoc networks are infrastructure less and have no fixed routers.[6] Each node (mobile) in the ad-hoc network can set up as and play the role of a base station in that it can transmit to and receive from other nodes in the network. A node in an ad-hoc network to other nodes if they are within line-of-sight. Non-line-of-sight-nodes are called hidden node.[1] Communication between a pair of hidden nodes needs to hop over one or more intermediate nodes ,in this sense, it is called multi hop networks. Ad-hoc networks are highly dynamic and are generally used for military services.

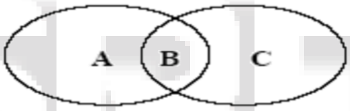

Fig 1: Example Ad Hoc Network

For Example in Fig 1 mobile host C is not within the range of host A "s wireless transmitter. And host A is not within the range of host C "s wireless transmitter. If A and C wish to exchange packets, they may in this case enlist the services of host B to forward packets for them, since B is within the overlap between A"s range and c" range.

II. DYNAMIC SOURCE ROUTING PROTOCOL

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. Dynamic source routing protocol is reactive protocol. It is based on source routing. In which source specifies the complete ordered route in packet header before sending data. Intermediate nodes simply forward packet to the next hop given in the source route. In DSR, intermediate nodes do not have to maintain routing information.

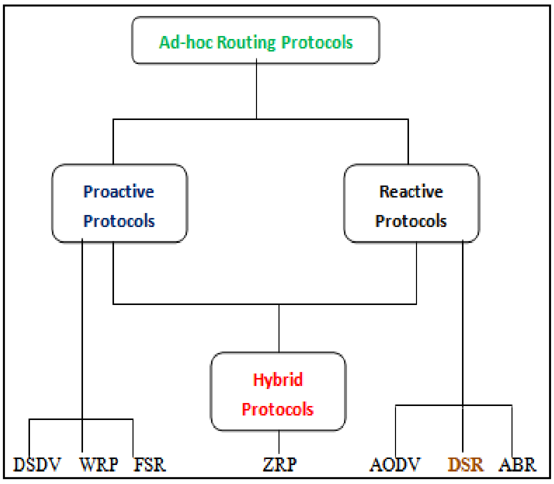

Fig. 2: Types of ad hoc routing protocols

Several routing protocols have been proposed for mobile ad hoc networks. These can be categorized as proactive (also known as table driven) protocols, reactive (known as source initiated or demand-driven) protocols or the hybrid of the reactive and proactive protocols. Types of the ad hoc routing protocols are shown in Fig2. The protocol has two components: route discovery and route maintenance.

A. Route Discovery in DSR

Route discovery is used when source needs a route to destination that is not in its route cache.The source sends a broadcast packet which contains source address, destination address, request id and path If a host saw the Packet before, discards it. Otherwise, the route looks up its route caches to look for a route to destination, If not find, appends its address into the packet, rebroadcast, If finds a route in its route cache, sends a route reply packet, which is sent to the source by route cache or the 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 header of the packet a source route giving the sequence of hops that the packet should follow on its way to D. Normally 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.[5] For example, 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 (approximately) 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. [2]

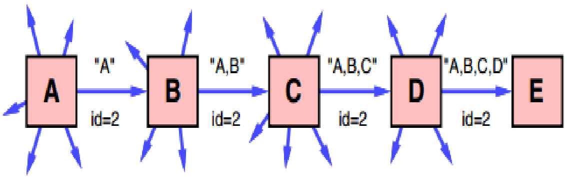

Fig. 1: Route Discovery example: Node **A** is the initiator, and node **E** is the target.

B. Route Maintenance

When original packet forwarding a 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 is received from the source. 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**. In our protocol, the MAC protocol, IEEE802.11, is used for this purpose.[5] 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 forwardedFor example, 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 ROUTEREPLYs 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.[2]

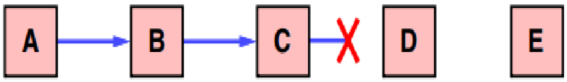

Fig. 2: Route Maintenance example: Node **C** is unable to forward a packet from **A** to **E** over its link to next hop **D**.

III. SECURITY FRAMEWORK FOR DSR

This section we propose a security framework for DSR to meet the requirements given in the previous section. We make the following assumptions:

- The scheme is based on public key cryptography.
- Node have relatively synchronized clocks
- Each node has a public and private key pair.
- Each node is capable of storing its own certificate and, as required, those of other nodes.
- Network links may be uni- or bi-directional

Security services are implemented by extending existing Control messages of the DSR protocol. There are no changes to the protocol operation itself but each node now performs additional, security related functions, when DSR messages are exchanged. We opt for a public key based system over asymmetric key based approach for the following reason.[7] Setting up shared secret keys requires pre-existing confidentiality, whereas a public key system does not. Furthermore, fewer public keys than secret keys are generally needed, because in a network with n nodes only n public keys are needed, and can potentially be broadcast, whereas n (n+1)/2 secret keys need to be set up in the case of pair-wise shared secret keys.

IV. CONCLUSION

The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad hoc networks. The proposed solution significantly increases the performance of the protocol without significantly increasing the protocol overhead. The optimization is suitable for highly mobile nodes to reduce end-to-end delay that occurs because of frequent link breaks. As shown in our detailed simulation studies and in our 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. In this Paper ,have described the principle mechanisms of Route Discovery and Route Maintenance used by DSR, and has shown how they enable wireless mobile nodes to automatically form a completely self-organizing and self-configuring network among themselves. The Dynamic Source Routing protocol (DSR) is an important component of such a system.

ABBREVIATION

DSDV	: Destination Sequence Distance Vector
WRP	: Wireless Routing Protocol
FSR	: Fisheye State Routing
ZRP	: Zone Routing Protocol
ADOV	: Ad hoc On Demand Distance Vector
DSR	: Dynamic Source Routing
ABR	: Associativity Based Routing

REFERENCES

[1] D. Johnson, D. Maltz and Y. Hu. The dynamic source routing protocol for mobile ad hoc networks. IETF MANET Working Group, Internet Draft 2003.

[2] Bantz 1994] David F. Bantz and Fr´ed´eric J. Bauchot. Wireless LAN Design Alternatives. IEEE Network, 8(2):43–53, March/April 1994

[3] R. N. Mir and A. M. Wani. Security Analysis of Two On-Demand Routing Protocols in Ad Hoc Networks. In Proceedings of ACM MOBIHOC 2001.

[4] D. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing, edited by Tomasz Emilienski and Hank Korth, Kluwer Academic Publishers, 1996.

[5] David A. Maltz, Josh Broch, Jorjeta Jetcheva,and David B. Johnson, “The Effects of On-Demand Behavior in Routing Protocols for Multi-Hop Wireless Ad Hoc Networks”, IEEE Journal on Selected Areas of Communications, 17(8):1439–1453, August 1999.’

[6] J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu & J. G. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’ 98), pp 85-97, October 1998.

[7] Y-C. Hu, A. Perrig, & D. B. Johnson. Rushing Attacksand Defense in Wireless Ad Hoc Networks. Technical report TR01-384, Department of Computer Science, RiceUniversity, June 2002.

[8] P. Johnson, T. Larsson, N. Hedman, B. Mielczarek, &M. Degermark. Scenario based performance Analysis Networking (MobiCom’ 99), pp 195-206, August 1999.

[9] IETF Mobile ad-hoc network working group http://www.ietf.org/html.charters/manet-charter.html

[10] Y. C. Hu, D.B. Johnson, and D.A. Maltz, "The Dynamic Source Routing Internet-Draft, draft-ietf-manet-dsr-09.txt, April 2003

[11] A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols, by Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, JorjetaJetcheva, http://www1.ics.uci.edu/~atm/adhoc/paper-collection/johnson-performance-comparison-mobicom98.pdf

[12] David B. Johnson, David A. Maltz: Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, Thomasz Imielinski and Hank Korth (Editors), Vol. 353, Chapter 5, pp. 153–181, Kluwer Academic Publishers, 1996

[13] T. Jiang, Q. Li, and Y. Ruan. Secure Dynamic Source Routing Protocol. In Proceedings of the Forth International Conference on Computer and Information Technology (CIT), 2004