ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

A Simulation and analysis of DSR Protocol in Mobile ad hoc Networks

Sesha Bhargavi Velagaleti[1], Dr.M.Seetha[2], Dr.S.Viswanadha Raju[3]

Assistant Professor, IT Departmnet, GNITS, Shaikpet, Hyderabad, India[1]

Professor, CSE Departmnet, GNITS, Shaikpet, Hyderabad, India[2]

Professor, CSE Departmnet, JNTUK, Hyderabad, India[3]

Abstract: A MANET can be treated as a network in which the nodes have the capability of self-configuring among themselves. These nodes are connected by wireless links to form an distributed topology without the help of any pre-existing infrastructure. Each node in a MANET can itself act as a router on its own. To perform effective routing operation in MANETS , several routing protocols were proposed, addressing several issues in MANETS. In this paper ,we tried to study the operation of DSDV protocol ,which is a proactive protocol and analyse the results obtained by simualting the DSDV protocol using NS-2 Simulator.

Keywords: MANET, Network Simulator, DSDV, nodes

1. INTRODUCTION

With the recent changes and advancements in computer and communications technologies, particularly under wireless communications, there is a widespread use of mobile computing applications using the TCP/IP protocol stack. MANETS were mainly introduced to provide enhanced support for wireless networking applications by adding the routing functionality into the entities. These type of networks are composed of wireless links most of which are bandwidth-constrained, with dynamically changing multi hop topologies .The main goal of MANETS is to enhance mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes themselves form the network routing infrastructure in an ad hoc fashion. MANETS provide more flexibility in the creation of a network in situations like where there is no possibility or less possibility in setting up the predefined infrastructure. The topology of the network changes unpredictably and rapidly. Less configuration, no need of a centralized authority and fast deployment features make MANETS most suitable for emergency situations like natural calamities, emergency medical situations, military applications etc., Unlike a node in an infrastructure based network, all the nodes in a MANET cooperate with each other to perform routing. All the nodes in a network are very free to move and hence change the links very easily. Because the radio transmission range is very less, there is a lot of overhead involved with respect to routing , security in particular. This is because the nodes are more prone to failures and compromises in ad hoc networks because of their mobility.

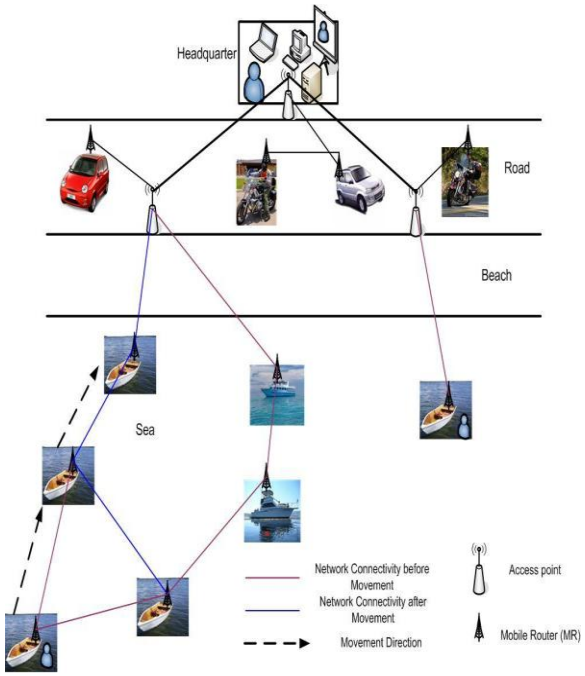


Fig1: A Mobile Ad hoc Network

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

In the recent days, research on MANETs has became quite popular with the widespread use of wireless networking devices.Mobile ad hoc networks became a popular for r esearch as laptops and 802.11/Wi-Fi wireless networking became widespread from 1990s. Many researchers are evaluating the protocols with different degrees of mobility within a bounded space, usually with all nodes within a few hops of each other, and usually with nodes sending data at a constant rate. The packet drop rate, the overhead introduced by the routing protocol, and other measures are also evaluated for different protocols.

1.1 Characteristics of MANET's

1. No fixed infrastructure needed
2. Dynamic Topology
3. Rapid Deployment
4. Easily attachable to any kind of network.
5. No need of user intervention.
6. Autonomous behaviour
7. Multi-hop radio relaying
8. Symmetric Environment
9. Distributed nature of operation
10. Intermittent nodal connectivity.

1.2 MANET Challenges

A MANET environment has to overcome certain issues of limitation and inefficiency. It includes:

- Time Varying nature of the wireless links.
- Multipath Fading
- Path loss and interferences
- Limited range Connectivity
- Less coverage area for wireless transmission
- Huge suceptability to packet losses due to transmission errors.
- Dynamic Routing updates
- Presence of hidden terminals
- More frequent network changes
- Adhoc nature of the network
- Security threats like DOS, eavesdropping, spoofing etc.,

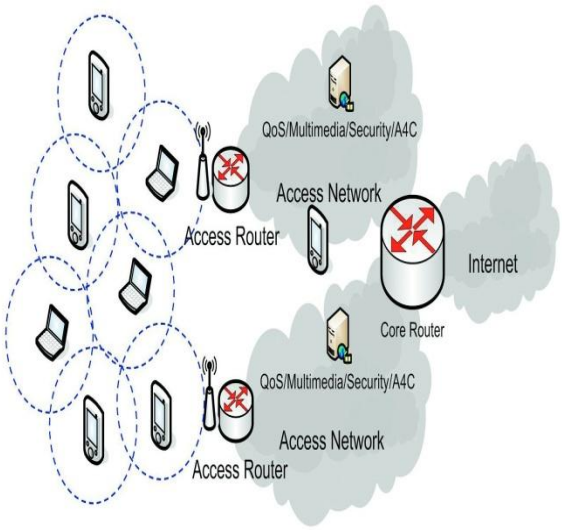


Fig3: Architecuture of MANET

1.3 Applications of MANET's

As the usage in the no of wireless and mobile devices is increasing day b day, there has been extensive scope use of MANET's in various application areas of wireless and adhoc networking.The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infra structured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment.Typical applications include:

1. Personal Area Networks
2. Military Battle field Applications
3. Search and Rescue Emergency operations
4. Civilian environments
5. Ad hoc conferencing
6. Home Networking
7. Ubiquitous Computing
8. Intelligent Transport Systems

1.4 Limitations of MANET's

1. Route discovery is a very complex task because of the constantly changing positions of the nodes
2. Additional complexity due to Out-of date routes

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

3. Assymetric links also poses additional overhead.
4. Because of the dynamic topology, the medium characteristics also change frequently, and more complex routing algorithms have to be employed.
5. Dynamic nature of the network opens doors for more security threats.

1.5 Routing protocols for MANET's

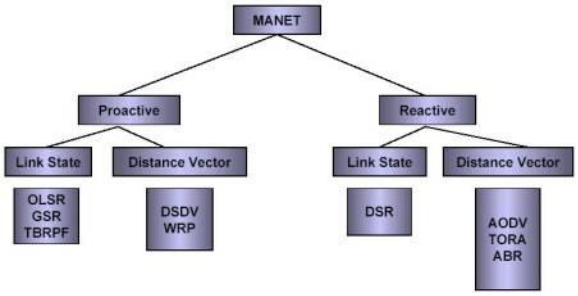


Fig4: Classification of Routing Protocols

Many routing protocols for MANET's were proposed based on several criteria like the topolgy , routing updates , location information etc.Most of them are based on when and how the nodes are informed of the routing updates in the network topology. Major classification is based on hoe nodes are informed of the routing updates and participate in route discovery process. Entire set of routing protocols were mainly classified as either proactive or reactive. If the routing updates are made before the routing decision is done statically , they are called as proactive routing protocols, which doesn't consider any changes in the topology of the network once route discovery is completed. The other class of protocols are the reactive protocols which consider the dynamic topological updates also into account. Examples of proactive protocols are OLSR, WRP, GSR etc. Examples of proactive protocols are DSDV,ODMRP,DSR,TORA etc.

2. Background

Recently, TCP performance in ad hoc wireless networks has become an active research field. Link failures due to mobility have been identified as one of the major factors degrading TCP performance. To combat this problem, Holland and Vaidya et al proposed Explicit Link Failure Notification (ELFN) scheme whereby the intermediate nodes notify the TCP sender when a link failure happens. This is a scheme similar to the Explicit Congestion Notification (ECN) technique originally proposed in the wired networks. With the help of ELFN, TCP senders can tell whether a packet loss is caused by link breakage or congestion. Thus, it could properly response to different kinds of packet losses. In TCP-F (TCP-Feedback), Chandran and Prakash et al proposed a scheme, very similar to the ELFN scheme, by asking the intermediate node to notify TCP sender about the network condition. When one intermediate node detects a route failure, it explicitly sends a route failure notification (RFN) to the TCP sender. The difference between TCP-F and ELFN is the response of route failures. TCP-F relies on the intermediate node to send a route reestablishment notification (RRN) to notify that the path is back up. In ELFN, the TCP sender must send probing packet periodically to detect the route recovery.

Venkatraman and Agrawal proposed a protocol based on public key cryptography. They assume the existence of a governing authority for the distribution of public keys. A source node generates a route request and digitally signs it using its private key. When a destination node sends a route reply back to the source node, public key cryptography is used for pair-wise authentication to exclude malicious nodes. If a node does not know a forwarding node's public key, they have to exchange public keys first. This pair-wise authentication is done by challenge
and response process. The purpose of this protocol is to prevent external attacks.

3. Destination-Sequenced Distance-Vector Routing

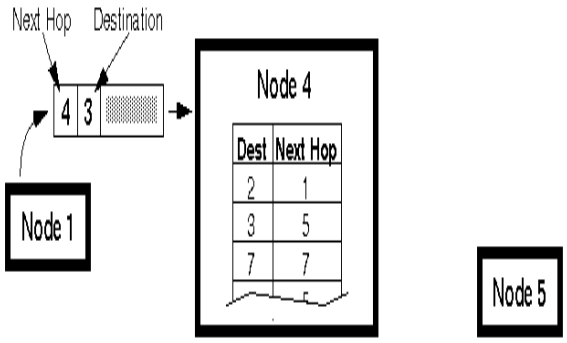
Destination-Sequenced Distance-Vector Routing (DSDV) [16] is an adaption of a conventional routing protocol to ad hoc networks. DSDV is based on the Routing Information Protocol (RIP) [9], used in parts of the Internet. Consequently, DSDV only makes use of bidirectional links. DSDV is one of the earlier ad hoc routing protocols developed. n DSDV, packets are routed between nodes of an ad hoc network using routing tables stored at each node. Each routing table, at each node, contains a list of the addresses of every other node in the network. Along with each node's address, the table contains the address of the next hop for a packet to take in order to reach the node.

In this example, a packet is being sent from node 1 to node 3 (node 3 is not shown). From node 1, the next hop for the packet is node 4 (Figure 3.1 a). When node 4 receives the packet, it looks up the destination address (node 3) in its routing table (Figure 3.1 b). Node 4 then transmits the packet to the next hop as specified in the table, in this case

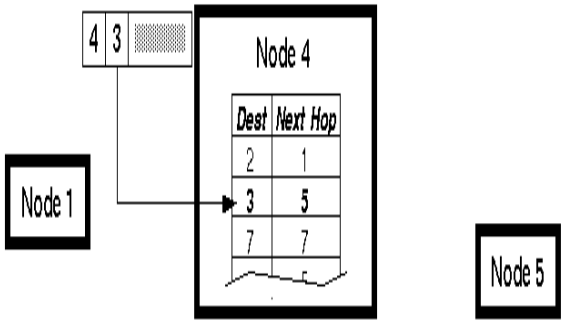
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

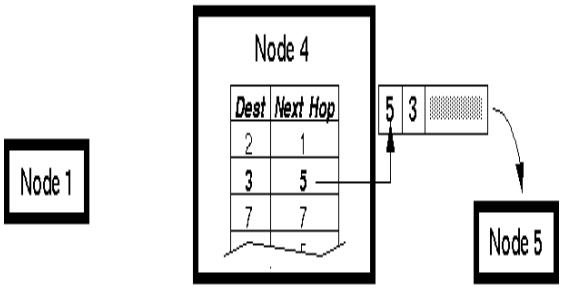
node 5 (Figure 3.1 c). This procedure is repeated as required until the packet finally reaches its destination.



a) Node 1 transmits packet to node 4 for forwarding



b) Node 4 looks up the destination in its routing table



c) Node 4 retransmits the packet to the next hop

Routing Table Management

The bulk of the DSDV protocol does not involve routing at all. Rather, the crux of DSDV is the generation and maintenance of the routing tables. Every time the network topology changes, the routing table in every node needs to be updated. As one might expect, this is no trivial task. The situation is further complicated by the fact that, when routing tables are out of sync (i.e. the routing protocol has not converged), routing loops may form.

To facilitate routing table maintenance, several additional pieces of information are stored in the routing tables. In addition to the destination address and next hop address, routing tables maintain the route *metric* and the route *sequence number*.

Periodically, or immediately when network topology changes are detected, each node will broadcast a *routing table update* packet. The update packet starts out with a metric of one. This signifies to each receiving neighbor they are one hop away from the node. The neighbors will increment this metric (in this case, to two) and then retransmit the update packet. This process repeats itself until every node in the network has received a copy of the update packet with a corresponding metric. If a node receives duplicate update packets, the node will only pay attention to the update packet with the smallest metric and ignore the rest.

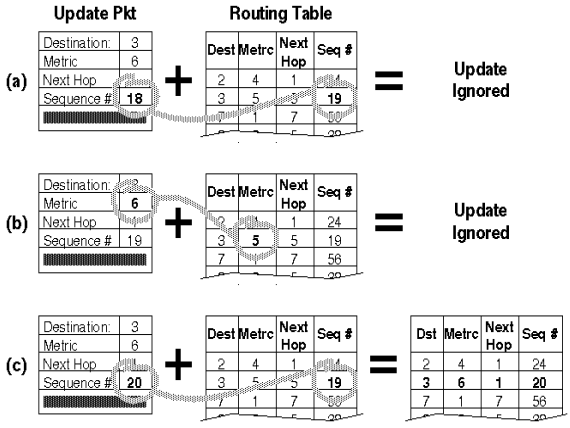
To distinguish stale update packets from valid ones, each update packet is tagged by the original node with a sequence number. The sequence number is a monotonically increasing number which uniquely identifies each update packet from a given node. Consequently, if a node receives an update packet from another node, the sequence number must be equal to or greater than the sequence number already in the routing table; otherwise the update packet is stale and ignored. If the sequence number matches the sequence number in the routing table, then the metric is compared and updated as previously discussed.

Each time an update packet is forwarded, the packet not only contains the address of the eventual destination, but it also contains the address of the transmitting node. The address of the transmitting node is entered into the routing table as the next hop (unless the packet is ignored, of course). Figure

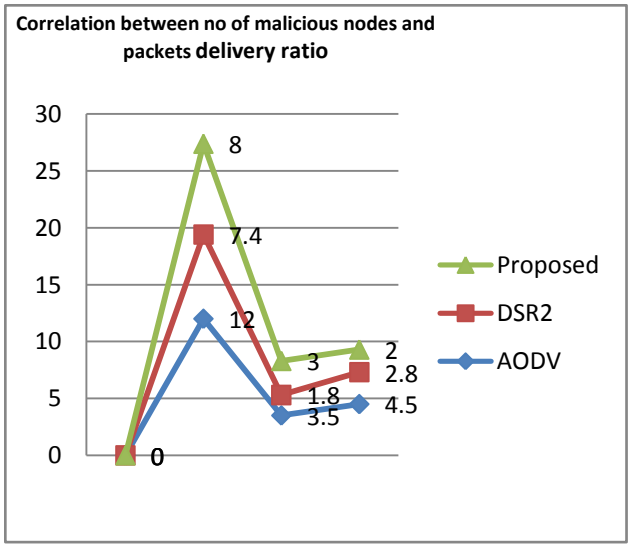
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

2.2 illustrates how a node processes an update packet under varying conditions. Note update packets with higher sequence numbers are always entered into the routing table, regardless of whether they have a higher metric or not.



delays and hence more packet delivery ratios under different no.of malicious nodes.



3.4 Simulation Parameters

Simulation time	3000s
No. of clusters	12
Transmission range	200m
No. of cluster heads	10
No. of nodes	100
Topology size	1000*1000m
Routing protocol	AODV
Node mobility	0 to 10m/s
Channel capacity	2Mbps
Traffic type	CBR
CBR packet size	512 bytes
Frequency	2.4GHz
Simulator	NS2
Pause time	1s
Number of packets	30000
Mobility model	Random way

3.5 SIMULATION RESULTS

DSDV protocol was developed based on the functionality of RIP protocol, and is mainly developed for ad hoc networks. Routing tables stored at each node are used to discover the route .Maintaining and managing these routing tables forms the main complexity of this routing protocol. It has been observed that our proposed protocol works with more lesser

4. CONCLUSION AND FUTURE SCOPE

In this paper, we have implemented the routing protocol DSDV for MANET's and compared the results obtained with our proposed protocol with different no. of malicious nodes to identify the performance of the network under different scenarios. The simulation results were shown and it is found that the proposed protocol delivers packets with lesser delays when compared to DSDV protocol. In future, more complex simulations could be carried out for different parameters and more detailed in-depth analysis of the entire network under various scenarios can be done. In DSDV, nodes has to periodically transmit the routing table updates, regardless of network traffic. These update packets are broadcast throughout the network so every node in the network knows how to reach every other node. As the number of nodes in the network grows, the size of the routing tables and the bandwidth required to update them also grows. As the topology changes dynamically, DSDV is unstable until update packets propagate throughout the network.

REFERENCES

1. TCP over Ad Hoc Networks : NS-2 Simulation Analysis by Ren Mao, Haobing Wang, Li Li, Fei Ye
2. SIMULATION AND COMPARISION OF AODV AND DSR ROUITNG PROTOOCLS IN MANETS by vivek kumar under the supervision of M.sumit miglani.
3. NEW SECURITY ALGORITHM FOR MOBILE ADHOC NETWORKS USING ZONAL ROUTING PROTOCOL by G.Varaprasad,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

S. Dhanalakshmi,, M. Rajaram ,Department of Computer Science and Engineering, B.M.S. College of Engineering, Bangalore, India
4. Y.Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks", ACM Wireless Networks, Vol. 9, pp. 545 – 556(2003).
5.Y. C. Hu and A. Perrig, "A Survey of Secure Wireless Adhoc Routing," IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 28-39(2004).
6.J. Li, J. Jannotti, Douglas S. J. D. Couto, David. R. Karger, and R. Morris, "A Scalable Location Service for Geographic Adhoc Routing", In Proceedings of International Conference on Mobile Computing and Networking, pp. 120-130(2002).
7. B. Karp and H. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", In Proceedings of International Conference on Mobile Computing and Networking, pp. 243-254(2003).
8. Y. A. Huang and W. Lee, "Attack Analysis and Detection for Adhoc Routing Protocols," In Proceedings of International Symposium on Recent Advances in Intrusion Detection, pp. 125-145(2004).
9. L. Zhou S. B. Fred, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority", ACM Trans. on Computer Systems, Vol. 20, No. 4, pp. 329-368(2002).
10. M. Gasser and E. McDermott, "An Architecture for Practical Delegation in a Distributed System", In Proceedings of IEEE Symposium on Security and Privacy, pp. 20-30(2004).
11. 11. Z. J. Haas, M. Perlman, "The Performance of Query Control Schemes of Zonal Routing
Protocol", IEEE Trans. on Networking, vol. 9, no. 4, pp. 427-438(2001).
12. Bradley R. Smith, Shree Murthy, and J.J. Garcia-Luna-Aceves, "Securing DistanceVector Routing Protocols", In Proceedings of Internet Society Symposium on Network and Distributed System Security, pp. 85-92(1997).
13. "Simulation Study and Implementation on Routing Protocols in MANET" IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012 ISSN (Online): 2231 –5268 Anju Yadav M.Tech Scholar, Shekhawati Engineering College, Jhunjhunu, Rajasthan.
14.Wikipedia for AODV and DSR Routing Protocols.
15. Routing in Ad Hoc Networks of Mobile Hosts,Dr. Gerard McLeanB. Cameron Lesiuk December 2, 1998Department of Mechanical Engineering,University of Victoria, Victoria, BC, Canada