IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A Comparative Evaluation of Various MANET Routing Protocols based on Performance Matrices

Vinod Kumar[1], Sameer Srivastava[2], Jagdeep Singh[3]

M. Tech. Computer Science and Engineering, CSE Department, KNIT Sultanpur[1, 3]

Professor, CSE Department, KNIT Sultanpur[2]

Abstract: Emerging technologies need network connection every time and everywhere. MANET can be created anywhere and anytime and well suited for these technologies. Mobile Ad Hoc Networks are the flexible and low cost of deployment. The properties of MANET are attracting the attention of developers for the future applications. Routing protocol design is the important issue of Mobile Ad Hoc Network. Dynamic network feature of MANET is creating a major technical challenge. MANET has been the attention of research area in the network. Many MANET protocols having their some specific property have been modified to enhance their performance. The performance of these protocols depends on network size and pattern of node mobility thus designing of these protocols varies. This paper presents the survey of modified MANET routing protocols. The aim of this paper is to provide the performance comparison in modified protocols. Here we will compare only those properties which are common among routing protocols.

Keywords: MANET, Destination Sequence Distance Vector (DSDV), Fisheye State Routing (FSR), Wireless Routing Protocol (WRP), Dynamic Source Routing (DSR), Zone Routing Protocol (ZRP).

I. INTRODUCTION

Mobile AD Hoc Networks (MANET) are the emerging type of wireless networking. MANET is a type of network that can change its location and configure itself on the fly. It deals sharing of IP-based information in that environment where fixed infrastructure based network is impractical. This network is formed between more than two nodes. Nodes as well as the network is free to move from one place to another place and continues data sharing while moving. Due to its mobility nature, they use a wireless connection to connect various networks. This cabe a standard wireless connection communication infrastructure has been destroyed. It is best option for the rapid deployment of communication infrastructure or another mode of connection such as satellite medium. Some MANETs are created for the purpose of local area network while other may be connected to the internet. VANET is a type of mobile ad hoc network that communicates with the roadside equipment for the purpose of sending and receiving data over the internet. Because of its mobility nature, MANET uses dynamic topology and it is not very secure thus it is very important to be cautious about the data sending over the MANET.

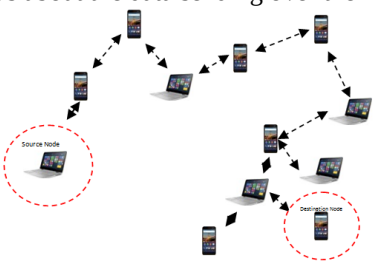


Fig.1: Diagrammatic view of MANET.

II. ARCHITECTURE OF MANET

This model for MANETs which preserves the integrity of the IP architecture while allowing for the requirements of MANET.

A. Node Morphology

This model considers MANET nodes as routers with hosts. These hosts may be external or internal. From the point of view of the hosts, and the applications running on these hosts, connectivity is through classic IP link. Nodes and their applications are not exposed to the specific characteristics of MANET interfaces and they are connected to Mobile Ad Hoc Network through routers, which have one or more MANET interfaces. This is symmetric with how hosts on an Ethernet

B. Addresses and Prefixes

If routers of MANETs are delegated to prefix a: this prefix will be assigned to IP links. Hosts can be assigned addresses from these prefixes.

C. Interface Configuration & Properties.

MANET environment is exclusively exposed to the MANET interfaces of the Routers. MANET routing protocols and interface and link characteristics the following characteristics deserve particular mention since they distinguish MANET interfaces and the MANET link model from the classic IP link model:

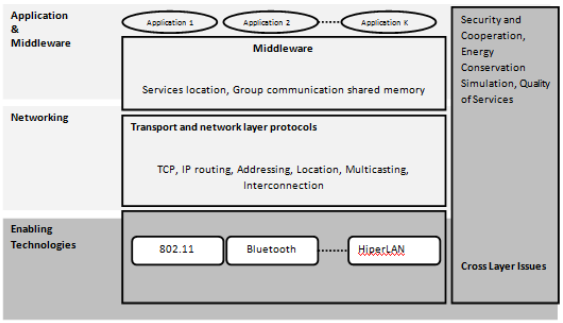
D. Unique Prefixes:

MANET interfaces must be configured using unique prefixes so that no two or more MANET interfaces are configured such that they appear within the same IP subnet.

IJARCCE

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

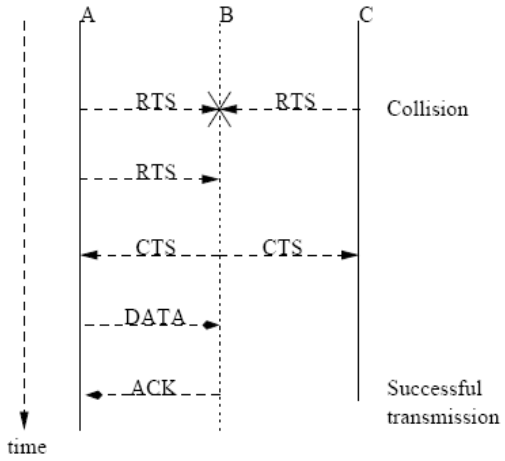
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016



III. DESIGNING ISSUE OF MANET

A. Error Prone Chanel State: Link characteristics of the wireless network varies and this is called the interaction between routing protocols. When this issue arises, the best way is to find an alternate route.

B. Hidden Node Problem: MANET is not limited to the number of nodes participating in the network. Two nodes communicate while they are not within each other range. Some node works as an intermediate node to ease communication between the other nodes. When the terminus nodes want to communicate with the intermediate nodes simultaneously, the signal collides at the intermediate node and intermediate node does not receive any transmission from either node. The solution for this is called hidden terminal problem in which nodes coordinate themselves by asking and granting permission to send and receive data packets. This is called Request to Send/Clear to Send (RTS/CTS).



C. Exposed Terminals: If a node is added which is reachable from only node C, consider node B wants to communicate with node A while node C transmits data packets to node D. When node A and node B are communicating, node C senses that the channel is busy, in this node C falsely thinks that no transmission has been successful while both the transmission was successful. These problems are often called to as "the exposed terminal problem". Both the hidden and the exposed terminal problem cause reduced the throughput of the network when traffic is highly loaded.

D. Variable capacity of links: Wireless networks have low bandwidth capacity. In addition, the throughput of transmission in a wireless network multimode environment when more than one node is communicating, noise, fading, and interference etc. is less than the maximum. The congestion problem is normal and congestion can be easily controlled and the network bandwidth is exceeded frequently. As mobile networks are often the extension of the field network infrastructure, the services demanded by MANET users are similar. These demands increase in the field of multimedia computing, collaborative networks and in other fields.

E. Energy Constrained Operation: MANET relays on batteries power of mobile nodes or the other power sources compatible for the mobile nodes. Considering the limitation of battery power, it is very important to design MANET for the minimum power requirement to save energy. The nodes consume the high battery power while sending the data and some less while receiving the data and less in route discovery and route maintenance. Considering the facts that when the nodes are in the idle mode they do not receive any data but still they consume little amount of energy. This amount approaches the amount that is consumed in the receive operation. Idle energy is a wasted energy that should be eliminated or reduced through energy-efficient schemes. Through energy consumption measurements studies, experiments have also been conducted to determine the power consumption patterns in the different active modes. In some experiments, the instantaneous power consumption per communication mode, e.g. send, receive, idle and sleep modes, has been measured. Some experiments went even further to include more details about the energy consumption pattern per subtype of the operation, for example, the cases of unicast and broadcast are considered to have different costs.

F. Security Issue: MANETs are more prone towards security threats than Ethernet. It has increased possibility of spoofing, eavesdropping and denial-of-service attack should be considered. . It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device. In network layer wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack, the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. In Black hole attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listens to the requests for routes in a flooding based protocol. When

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created.

IV. ROUTING IN MANET

MANET Protocol → can be divided into

1. Proactive routing or table driven routing.
2. Reactive routing or on demand routing
3. Hybrid routing.

Proactive Routing the nodes in a mobile ad hoc network continuously evaluate routes to all reachable nodes and attempt to maintain consistent, up-to-date routing information. When a network topology change occurs, respective updates must be propagated throughout the network to notify the change.. Using proactive routing algorithms, mobile nodes proactively update network state and maintain a route table and route.

Reactive routing protocols for mobile ad-hoc networks → routing paths are searched only when needed. A route discovery operation invokes a route determination procedure. The discovery procedure terminates either when a route has been found or no route available after examination for all route permutations. In a mobile ad hoc network, active routes may be disconnected due to node mobility. Hence route maintenance is an important operation of reactive routing protocols. On comparison to the proactive routing protocols for mobile ad hoc networks, less control overhead is a distinct advantage of the reactive routing protocols.. However, when using reactive routing protocols, source nodes may suffer from long delays for route searching before they can forward data packets.

For eg. { AODV, DSR}

Hybrid routing protocol: to combine the merits of both proactive and reactive routing protocols and overcome their shortcomings. Hybrid routing protocols for mobile ad hoc networks exploit hierarchical network architectures. Proper proactive routing approach and reactive routing approach are exploited at different hierarchical levels, respectively. For eg. { ZRP,HARP}

V. APPLICATIONS OF MANET

Military battlefield- Mobile ad-hoc network allows the military to maintain the communication between the military base, vehicles and soldiers. Collaborative work- In business, sometimes collaborative computing outside the office is more important than inside, for exchanging the information of the projects. Local level- MANET allows sharing the information on local area and providing access directly to the nodes. Personal area network and Bluetooth- Personal area network is a small range network in which many mobile nodes are connected. Small range network like Bluetooth simplify the inter communication between the node (Laptop, Mobile etc.). Commercial sector- Ad-hoc networks can be used for the relief from disaster such as flood, fire, gas leakage, earthquake etc.

VI. RESULTS AND DISCUSSIONS

Parameter	Traditional AODV	RAODV	MAODV	QAODV
Average Delay	HIGH	LOW	AVG	AVG
Packet Delivery Ratio	LOW	HIGH	HIGH	AVG
Throughput	LOW	HIGH	HIGH	AVG

The combined graph for energy levels of the protocols.

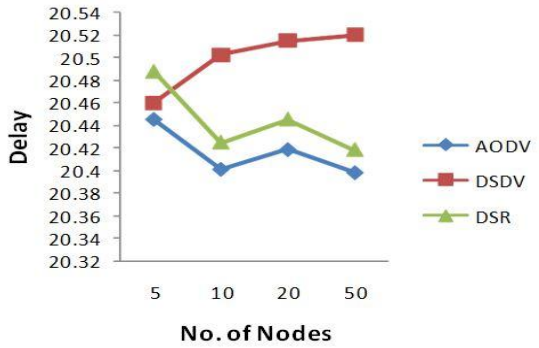


Fig 2: shows energy levels of the protocols where AODV consumes less energy compared with others. The combined graph for protocol delay.

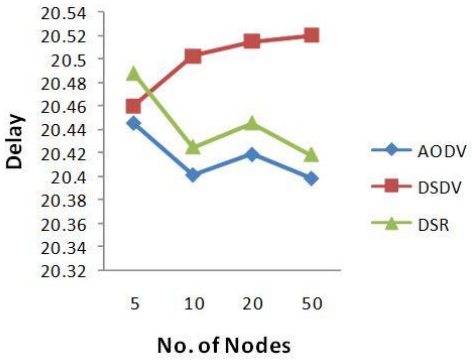


Fig 3: AODV performs well compared to the other protocols with less delay.

The combined graph for overall performance metrics of AODV, DSDV and DSR protocols.

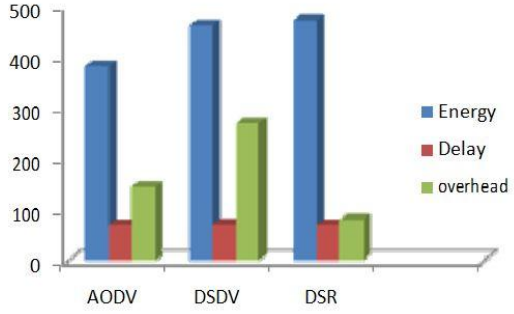


Fig 4: AODV protocol works well but DSR has less overhead.

DOI 10.17148/IJARCCE.2016.5431

VII. CONCLUSIONS

1. If we talk about energy levels of the protocols, AODV consumes less energy compared with others.DSR utilises more energy for data transfer.
2. From **(**delay) point of view, DSDV protocol delay increases with no of nodes. AODV performs well compared to the other 2 protocols with less delay.
3. Talking about performance of protocols, AODV works well but DSR has less overhead. But for routing purposes AODV is well suited than DSR.

REFERENCES

[1]. Akshatha, P.S., Khurana, N., Rathi, and A.: Optimal Path For Mobile Ad-Hoc Networks Using Reactive Routing Protocol. International Journal of Advances in Engineering & Technology, IJAET (2011) ISSN: 2231-1963

[2]. D. Chakeres and E. M. Belding-Royer. AODV routing protocol implementation design. In Proceedings of the International Workshop on Wireless Ad-hoc Networking (WWAN), pp. 698–703, Tokyo, Japan, March 2004.

[3]. E. N. et al. AODV-UU: Ad-hoc On-demand Distance Vector Routing. http://user.it.uu.se/˜henrikl/aodv.

[4]. NS -2, The ns Manual (formally known as NS Documentation)

[5]. E. Perkins, E. M. Royer, and S. R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing", Internet Draft, draft-ietf-MANETsaodv -10.txt, work in progress, 2002.

[6]. Li Ting Jun "Study On Airborne Single passive location Technology" Applied Mechanics and Materials Vols.58（2011) pp. 2006-2009.

[7]. Li Ting Jun, Lin Xueyuan, "GPS/SINS Integrated Navigation System Based On Multi-Scale Preprocessing", Journal of Wuhan University, 2011, Vols 36(1): pp. 6-9.

[8]. Li Tingjun "The Phonetic Complex Data Based on FPGA Key Engineering Materials", Vols 475 (2011） pp. 1156-1160.

DOI 10.17148/IJARCCE.2016.5431