International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

A Metaphorical Review on Impact of Congestion and Route failure on the Performance Comparison of Routing Protocols in MANET

Krittika Khator[1], Prof. Nitin Manjhi[2], Prof. Manoj Ramaiya[3]

[1,2,3]Department of Computer Science, Shriram Group of Colleges, RGPV University, Banmore, Madhya Pradesh

Abstract

In Mobile adhoc network (MANETs), the movement of network nodes may quickly change the topology resulting in the increase of the overhead message in topology maintenance. MANETs focuses on reducing overhead, handling node mobility and topology maintenance etc. Routing is difficult due to its mobility trait in MANET. Mobility means each and every node is free to move within its transmission range. Due to high mobility and volatile movement of nodes network causes route failure. In MANET route failure is very frequent as the nodes are mobile and it is a very serious problem which needs to be addressed. As the number of node increases route failure also results high routing overhead. The main reasons for route failure are node mobility, interference, congestion and wireless link collision. Cross Layer is used to improve route failure in MANET. In this paper, we analyze the performance of existing routing protocols such as AODV, TAODV and CLS_AODV in mobile adhoc environment.

Keywords- MANET, AODV, Cross layer approach, signal strength.

1. INTRODUCTION

Currently mobile communications have become an important role for the people. Since these kinds of communications are considered less a luxury and more a necessity, the number of mobile users, services and devices grows quickly. Most of the researching efforts have been spent on the heterogeneous networks (integration of fixed networks with infrastructure Wireless Networks). However, during the past few years, essentials efforts have been done in the researching field of Mobile Ad-hoc Networking (MANET) [1], which is basically a wireless network without infrastructure. One of the main issues in MANET researching is the routing. Research in this area is becoming popular due to wide ranging applications supported. MANET can be established quickly anytime and anywhere[2].In this, host and topology movement is frequent. Data must be forwarded via intermediate nodes. Much of the previous research in MANET routing have focused on developing strategies, which suit one specific networking scenario. Therefore, there is no existing protocol that can work well in all different networking scenarios. Routing in ad hoc networks is different compared to normal wired networks.. In wired networks, link failure is not frequent since the network structure is mostly static. Therefore, routes in MANET must be calculated much more frequently in order to keep up the same response level of wired networks [12]. Routing schemes in MANET are classified in four major groups, namely, flooding, proactive routing, reactive routing, and hybrid routing.

Routing is the main issue in all networks. Routing is the process to moving information / packet from a source node to a destination node in a mobile ad-hoc network. During routing process, at least one intermediate node within the network is encountered. Routing protocols are the in charge of discovering and maintaining the routes in the network. A lot of research has been conducted in this field and two types of topology structure have been proposed mainly:

1. Flat topology - In a flat structure, all nodes in a network are at the same level and have the same routing functionality. Flat routing is simple and efficient for small networks. The problem is that when a network becomes large, the volume of routing information will be large and it will take a long time for routing information to arrive at remote nodes.

2. Hierarchical topology - For large networks, hierarchical (cluster-based) routing may be used to solve the problems. In hierarchical routing the nodes in the network are dynamically organized into partitions called clusters, and then the clusters are aggregated again into larger partitions called super clusters and so on.

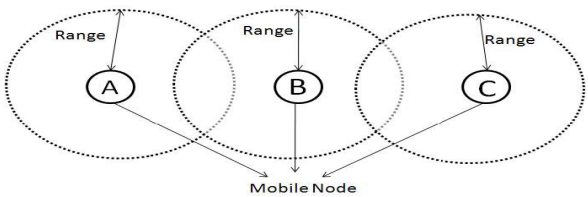

Figure 1 : MANET

A Mobile ad hoc network is illustrated in Figure 1 consists of three wireless mobile nodes A, B and C. Transmission range of a node represented by dotted circle. Mobile node A is not within the transmission range of C and vice versa. If A wants to establish communication with C. Node B which in the transmission range of A and C forwards the packets so that A and C are able to communicate each other successfully. The fundamental difference between fixed networks and MANET is that the computers in a MANET are mobile. Due to the mobility of these nodes there are some characteristics that are only applicable to MANET.

In [3] MANET congestion occurs when the amount of data sent to the network exceeds the available capacity. Such situation leads to increased buffer space usage in intermediate nodes, leading to data losses. Periodic Hello messages in AODV denote the presence or absence of neighbors. Congestion is detected at transport layer. One of the challenges of TCP is unable to differentiate congestion losses from other losses. TCP assumes that all packet losses are due to congestion [5]. Congestion is main reason for performance degradation of TCP. The objective of congestion control is to limit the delay and buffer overflow caused by network congestion and provide better performance of the network. Packet loss reasons are node mobility and link layer congestion. Cross layer approach is used to improve TCP performance and is used to solve route failures. Cross-layer design allows us to make better use of network resources by optimizing across the boundaries of traditional network layers. It is based on information exchange and joint optimization over two or more layers.

The rest of the paper is organized asfollows. Limitations of MANET are described in Section II. Descriptions of routing protocols are given in Section III. Section IV describes all the cross-layer design proposals in detail with relevant mentioning of related work. We study performance evaluation in Section V and finally Section VI summarizes conclusion.

2.LIMITATIONS OF MANETs

Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security and other issues in Manets-

- ***Packet loss due to transmission errors***- There are many reasons of packet loss problem in Manets. Packet loss may happen due to mobility of nodes, bit rate error, due to interference[4].
- ***Variable capacity links***- Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications--after accounting for the effects of multiple access, fading, noise, and interference conditions etc. is often much less than a radio's maximum transmission rate. One effect is congestion is typically the norm rather than the exception.*Frequent disconnections/partitions*- As the host movement and topology change is frequent so links gets fail easily causes network disconnected.
- ***Limited communication bandwidth***- The bandwidth available for wireless networks is generally low than that of wired networks. The throughput of these networks is generally low due various noises, fading effects.
- ***Dynamically changing topologies/routes***- Nodes are free to move arbitrarily in any direction thus the topology of the network change unpredictably.
- ***Lack of mobility awareness by system/applications*** - At times the mobile nature of nodes may even create network error. Since nodes can freely join or leave a network so it is easy for nodes to behave maliciously
- ***Short battery lifetime***- The nodes are portable devices and are dependent on batteries. This is the most important design consideration of the MANET.
- ***Co-operativeness*** - Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications[5].
- ***Limited power supply*** - The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply[5].
- ***Lack of Centralized Management*** - Since Manets form a random network and even the nodes are mobile so there is no centre management. Due to lack of centralized management the detection of attacks is very difficult[4].
- ***Infrastructure less*** - Manets infrastructure less nature brings difficulty in detecting any malicious node or faults in the network
- ***No network boundary*** – Since Manets have no network boundary because the nodes are movable this may lead to increase in number of attacks on them. Any node may enter the network and may hinder the network communication.
- ***Adversary inside the Network*** - The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes [6].
- ***Scalability*** – Due to mobility of network the scale of the network is changing all the time.
- ***Variation in nodes*** – Each node has different transmission and receiving capabilities. In addition each mobile node has different software/hardware configurations which cause trouble in operating in a network. [1]

- ***Hidden problem-*** Hidden node means two nodes[2] out of each other's radio range,simultaneously try to transmit data to an intermediate node, which is in radio range of both the sending nodes. None of the sending nodes will be aware of the other node's transmission, causing a collision to occur at the intermediate node. Hidden node interference problem can be solved by using the RTS/CTS (Request To Send/Clear To Send) handshake method.
- ***Security*** - It is one of the major issue in mantes. All major networking tasks such as routing and packet formatting are done by nodes itself which are mobile [9]. Any attacker can easily attack on the network and can acquire the data.
- ***Resource Availability*** – For manets providing secure communication in such a challenging environment where the network is mobile and is vulnerable to attacks requires various resources and architectures[4].

3. ROUTING PROTOCOLS

A fundamental challenge in MANET is the design of scalable and robust routing protocols[7]. The routing protocol needs to have following qualities in order to be effective: distributed operation, loop-freedom, demand-based operation, proactive operation, security, "sleep" period operation, unidirectional link support. Distributed operation means that any host can enter or leave the network whenever it wants. Loop-freedom is needed to prevent that host will be sending information uselessly creating overhead. Demand-based operation will let the protocol adapt to the traffic pattern to decrease traffic and use bandwidth resources more efficiently, but this will increase route discovery delay.

Routing protocols in adhoc networks are typically divided in two categories: proactive and reactive protocols[8]. Proactive protocols attempt to monitor the topology of the network in order to have route information between any source and destination available at all time. It performs well in low mobility environment. The DSDV and OLSR are well-known proactive routing protocols. On the other hand, reactive protocols find a route only when it is needed, upon the start of a connection. It is better suited to networks of more mobile nodes. The AODV and DSR are representatives of on-demand routing protocols.

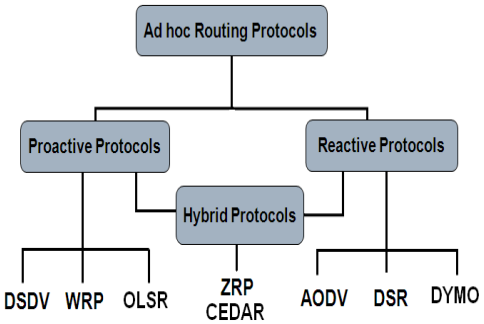

Figure 2 Classification of Routing Protocols

4. LITERATURE SURVEY

In Mobile Ad Hoc Network (MANET) nodes are not fixed they are moving. MANET performance degrades due to two main reasons. First, when a node moves out of its transmission range, node starts dropping the packets. Second reason is congestion, when too many nodes trying to access the channel at the same time obviously packet losses occur. In [9] congestion decreases the performance of TCP. To increase performance of TCP signal strength measurements are done at physical layer. Using cross layer approach signal strength information is given to upper layers i.e. MAC layer based on signal strength information it predict the possible link failure. Routing protocol AODV is considered in this approach since in AODV the received signal strength can be used to predict link status. A large number of cross layer designs have been proposed for mobile ad hoc networks for routing and congestion free networks which uses AODV as routing protocol are explained below:

4.1. AODV(ADHOC ON DEMAND DISTANCE VECTOR PROTOCOL)

AODV is a reactive protocol[2],[8] that determines routes solely on-demand. It is based on the distance vector technology. AODV is based on DSR and DSDV routing protocol. It use periodic sequence numbering procedure of DSDV and route discovery as DSR. The hosts only know the next hop to every destination. AODV[8] has better congestion avoidance mechanisms, as only the first route received is kept in the routing table and any routes that have a bigger delay are discarded. AODV is a pure on-demand route acquisition system, since node that are not on a selected path do not maintain routing information or participate in routing table exchanges.

AODV works as follows:

- When a source node desires to send a message to some destination and does not already have a valid route to that destination, it initiates a "route discovery" process to locate the destination.
- It broadcasts a route request packet to its neighbor's, which then forward to their neighbors and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located.

- During the process of forwarding the RREQ, the intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received thereby establishing a reverse path.
- If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route.
- The destination /intermediate node responds by a unicast route reply (RREP) packet back to the neighbor from which it first received the RREQ[2].

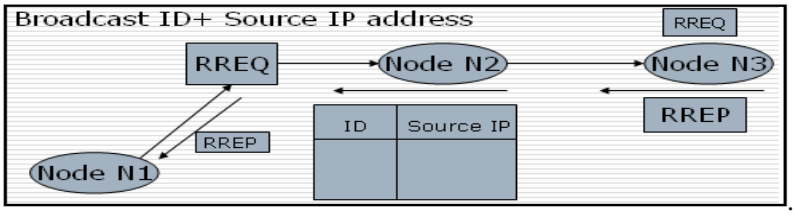

Figure 3 Overview of AODV Protocol

Advantages of AODV Protocol

1. AODV [8] greatly reduced the number of routing messages in the network.
2. Since it is bandwidth efficient so it consumes less battery power.
3. The main advantage of AODV protocol is that routes are established only when one node raises a demand to communicate with another node.
4. To overcome the counting to infinity problem like in other distance vector routing protocols AODV uses sequence numbers to find the fresh route to the destination.

Disadvantages of AODV Protocol

1. Overhead on the bandwidth, because RREQ & RREP packets needs to carry a lot information to validate a route.
2. If the intermediate node does not have the latest destination sequence number it can lead to stale entries.
3. Multiple RREP packets in response to a single RREQ packet can lead to large control overhead.
4. The hello messages add a significant amount of overhead to the protocol.
5. The messages can be misused for insider attacks including route disruption, route invasion and resource consumption.
6. AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.
7. AODV does not discover a route until route discovery process is not initiated. Route discovery latency result can be high in large-scale hybrid and mesh networks.

4.2. RELIABLE AODV

In[10] a homogenous network, the AODV routing protocol uses the shortest path algorithm that prefers long hops and results in routes with weak links.Hence, route failure becomes frequent; even in case of low mobility which leads to increased routing overheads due to frequent re-route discovery processes. In order to minimize control overheads and to save resources. In this proposed cross-layer design, the received signal strength of RREQ packets are used to decide whether to forward the RREQ or not. In [11]the network layer the signal strength is compared with a predefined threshold value. If the signal strength is above the threshold, the network layer continues the route discovery process. Otherwise the reliable AODV drops the RREQ packet. This forms the routes with strong links where adjacent nodes are within the transmission range of each other[2]. So even when the nodes are moving, the probability of route failure due to link breakages would be less with Reliable AODV. The threshold value is set according to nodes transmission power.

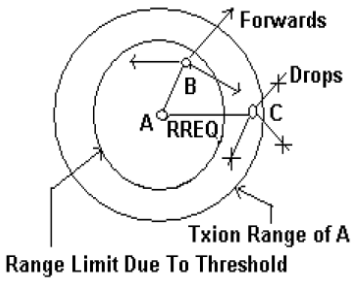

Figure 4 Reliable AODV

Fig. 4 shows Reliable AODV where the node A sends a RREQ which is received by its neighbors B and C. As the received received signal strength at node B exceeds the threshold, it forwards the RREQ but the node C drops the RREQ because it is close to the transmission range boundary of node A and hence has a weak link to node A. In[9]The received signal

strength(RSS) of RREQ is stored/updated in Neighbor Table (NT) of routing protocol, against the address of the neighboring node from which the RREQ is received.

4.3. MAODV

There are two mechanism based on signal strength for link management, is implemented at MAC layer. First is Proactive link management and second is Reactive link management. Reactive LM does not use the signal strength to estimate a distance of a neighbor node. Proactive LM informs the routing protocol that a link is going to break before the link actually breaks. The link break prediction mechanism uses the information from neighbor table.

Advantage of this scheme is that it can improve the TCP good put by upto 75% when the network is lightly loaded and 14—30% when network is heavily loaded. Its drawback is while shorter connection TCP good put is less significant.

4.4. MULTI-RATE AODV

In [12], the focus was on the multi-rate communications handling problem of the traditional AODV protocol. The authors proposed a protocol called Multi-Rate AODV (MRAODV) that establishes more efficient routes in wireless multi-rate environments. This protocol uses the path gain as a routing metric to select the best path between the source and the destination. As the number of nodes or the distance increases, the protocol shows better performance compared to AODV, this is due to the efficient route selection algorithm implemented. In contrast, the route discovery process takes more time than that of the traditional AODV.

4.5. MOBILITY ADAPTIVE CROSS-LAYER

In [13], the authors developed mobility adaptive cross layer design that improves the performance of AODV by coupling the route discovery process, the RSS information, and the mobile node speed to establish stable and optimum routes. The design allows better network resource utilization by decreasing the routing failures and overheads, leads to better results in dense networks, and reduces the route failures and routing overhead.

4.6. CLS_AODV (Cross Layer Stability Based Routing Mechanism)

In [2] Cross Layer Stability based routing mechanism (CLS_AODV) is given. Where received signal strength can be used to make known the link state information for unstable zone prediction and route state monitoring. A gray zone prediction algorithm is used to find out unstable paths. A HELLO-based preemptive local route repair algorithm is used to prevent the occurrence of link breakages. CLS_AODV has three main parts:

- Route Discovery
- Route monitoring
- Route repair

In Route discovery AOMDV is used to find multiple path between source to destination. For finding stable route route discovery two things are necessary. One is erasing the unstable paths and another is to calculate route stability metric. The calculation of route stability metric involves both forward and reverse path. In the route monitoring process stable and unstable path are decided by checking whether received power is always greater than threshold, then link between the current node and upstream node is considered to be stable otherwise it detects communication gray zone i.e. unstable paths. The route repair process finds the moving node which is responsible for the occurrence of communication gray zone. Thus in this way CLS_AODV react to link breakages using route state monitoring and gray zone prediction.

Advantages:-

- CLS_AODV over performs than Ad-hoc On Demand Distance Vector AODV.
- CLS_AODV is more stable and find reliable path than AODV.
- Another advantage of CLS_AODV is that it achieves better packet loss ratio than AODV.

4.7 TURBO AODV (T-AODV)

In [14] Turbo AODV "TAODV" is a modified cross layer design version of the well-known AODV routing protocol. The modification considers route selection engineering process. The cross layer design relies on information (remaining energy, RSS and remaining queue length) that can be obtained from lower layers as illustrated in Fig.6. On the other hand, routing packets headers are changed by adding new fields; routing packets forwarding algorithms are modified and the route selection algorithm at the destination is completely enhanced.

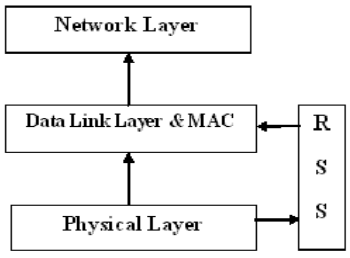

Figure 6 Cross Layer Design

- ***Route request and route reply modifications-***

First, the route request packet (RREQ) in the routing protocol is modified. There are two reserved fields in the RREQ packet of the traditional AODV protocol. These fields are used in TAODV; one is used to store the remaining queue length and the other is used to store the remaining energy value at the current node. Also the Route Reply packet (RREP) is modified. There are two reserved fields in the RREP packet of the traditional AODV protocol. Only one of these fields is used in TAODV to store the weight of the weakest hop across the selected route.

Table 1 :COMPARISON OF AODV,CLS_AODV AND TAODV

PARAMETERS	CLS_AODV	AODV	TAODV
Packet Loss Ratio	More	Less	Less
End to End Delay	Less	More	Less
Reliable Path	More reliable path can be found	Less reliable path	More reliable path as compared to AODV
Stability	More stable routes	Less stable routes	More stable routes
Routing Overhead	Less	More	Less
MAC Overhead	Less	More	Less

5. CONCLUSION

As a result of our study, it can be said that we can enhance the performance of MANET. Cross layer approach and signal strength these parameters can be used to avoid a route failure which clearly improves congestion control. AODV is best suitable for signal signal strength based congestion control. We observed that the cross-layer approach for reliable AODV benefitted with stable route formation, but it suffers with improved delay. Also, it is suitable for high-density mesh networks, as it affects network connectivity to definite extent. Cross layer Stability based routing CLS_AODV performs good but it is well suited for highly dense networks. TAODV may reduce the routing overhead, the normalized routing load and the dropped packets at the interface queue. It may increase the end-to-end delay for FTP traffic which is not a significant parameter for this type of traffic.

References

[1] Huaming Wu and Alhussein A. Abouzeid Cluster-based Routing Overhead in Networks with Unreliable Nodes.

[2] Mrs. Sunita Nandgave-Usturge Study of congestion control using AODV and signal strength by avoiding link failure in MANET 978-1-4577-2078-9/12/$26.00©2011 IEEE

[3] C.E. Perkins, E.M. Belding -Royer, and I. Chokers, "Ad Hoc on demand distance vector (AODV) routing," IETF Internet draft, Oct. 2003.

[4] Saloni Sharma, Anuj Kumar Gupta A Comprehensive Review of Security Issues in Manets International Journal of Computer Applications (0975 – 8887) Volume 69– No.21, May 2013

[5] Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3 MANET: Vulnerabilities, Challenges, Attacks, Application IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893

[6] Kakapo Oaken, Manure Lertwatechakul "An improvement of Ad Hoc route maintenance" International Symposium on Communications and Information Technologies (ISCIT 2008)

[7] B.Praveen Kumar, P.Chandra Sekhar, N.Papanna, B.Bharath Bhushan, A SURVEY ON MANET SECURITY CHALLENGES AND ROUTING PROTOCOLS ISSN:2229-6093

[8] Zhan Huawei, Zhou Yun Comparison and Analysis AODV and OLSR Routing Protocols in Ad Hoc Network 978-1-4244-2108-4/08/$25.00 © 2008 IEEE

[9] M. Abolhasan, T. Winsock, E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Elsevier Ad Hoc Networks Journal 2 (1) (2004) 1–22.

[10] B.Ramachandran and S.Shanmugavel Received Signal Strength –based Cross-layer Designs for Mobile Adhoc Networks IETE TECHNICAL REVIEW VOL 25 JUL-AUG 2008

[11] B. Ramachandran S. Shanmugavel "Impact of Node Density on Cross Layer Design for Reliable Route Discovery in Mobile Ad-hoc Networks"

[12] M.Rahman et al., "A Routing Protocol for Multi-Rate Wireless Ad Hoc Networks: Cross Layer Approach," IEEE, p. 5, 2008.

[13] B.Ramachandran et al., "Mobility Adaptive Cross Layer Design for Reliable Route Discovery in Ad Hoc Networks," IEEE, p. 5, 2008

[14] Zouhair El-Bazzal, Khaldoun El-Ahmadieh*, Zaher Merhi, Michel Nahas and Amin Haj-Ali A Cross Layered Routing Protocol for Ad hoc Networks 978-1-4673-1166-3/12/$31.00 ©2012 IEEE.