 

# Signal Strength Based Congestion Control in In MANET

Prof. Shitalkumar Jain[1*], Miss.Sunita I. Usturge[2]

1. Dept. of Computer Egg. M.A.E. Alandi (D), Pune, India.
2. Dept. of Computer Egg. M.A.E. Alandi (D), Pune, India.

* sajain@maecomp.ac.in

**Abstract**

All nodes in MANET (Mobile Ad-hoc Network) are mobile and dynamically connected in an arbitrary manner. Mobility causes frequent link failure which results in packet losses. TCP assumes that these packet losses are due to congestion only. This wrong assumption requires packet retransmissions till packet arrives successfully at the receiver. Goal is to improve TCP performance by using signal strength based cross layer approach which obviously resolves the congestion. We are reviewing a signal strength based measurements to improve such packet losses and no need to retransmit packets. Node based and link based signal strength can be measured. If a link fails due to mobility, then signal strength measurement provides temporary higher transmission power to keep link alive. When a route is likely to fail due to weak signal strength of a node, it will find alternate path. consequently avoids congestion. We will make changes at MAC routing and routing layer to predict link failure. MANET hits the protocol's strength due to its highly dynamic features, thus in testing a protocol suitable for MANET implementation we have selected two routing protocols AODV and DSR. Packet Delivery Ratio, Packet Drop, Throughput and end to end delay are the metrics used for performance analysis of the AODV routing protocols.

**Keywords-**Congestion control, Signal strength, TCP performance ,Cross layer interaction, Route discovery

## 1. Introduction

MANET represents complex distributed systems that contain wireless mobile nodes that can freely and dynamically self-organize into temporary, ad-hoc network topologies [1]. Mobility causes route failure. They require robust, adaptive communication protocols that can handle the unique challenges of these multi-hop networks smoothly. The TCP has been widely deployed as transport layer protocol on a multitude of internet works including the Internet, for providing reliable end-to-end data delivery [2]. Several routing protocols are used in MANET. Reactive routing protocol AODV is used. Signal strength based metric produces better results compared with other protocols. Routing protocols are classified on different basis, routing protocols can be classified on the basis of topology.

Reactive protocol establish route when needed. Proactive routing protocols continuously learn topology of network by exchanging topological information among the nodes. Second, based on method of data delivery from source to destination routing protocols are uncast and multicast. Uncast routing protocols sends information packets to a single destination from a single source, Multicast routing protocols delivers information to a group of destinations simultaneously[6][8]. One of the challenge of MANET is varying nature of radio link fluctuates end-to-end communication quality. Objective of congestion control is to prevent saturation of network resources also ensures degree of fairness in the allocation of resources. Traffic resources are of two types first is window based and second is rate based resources. To provide an end to end congestion control a sender side variation of TCP Reno, called as TCP Venom was developed. A threshold value β is used to make the decision. If the estimated congestion level in the network exceeds the value of β, packet loss is detected as congestion loss. Otherwise loss is due to random errors.

## 2. Signal strength based proposed Algorithms

In Mobile Ad Hoc Network (MANET) nodes are not fixed they are moving. With congestion control and improving TCP using cross layer approach, we also have to consider some problems such as a route failure and other similar aspects. Many routing algorithms in mobile ad-hoc network for routing and congestion free networks are explained below.

### *2.1 TCP venoplus A cross layer approach*

TCP cannot distinguish between congestion losses from random losses caused due to channel noise and interference. TCP veno has some drawbacks. TCP venom's packet loss identification causes under utilization of bandwidth in lightly loaded network. TCP venoplus is a cross layer approach to improve TCP performance in a wireless network. The cross layer approach uses one of parameter i.e. signal strength. TCP venoplus has two refinements. First refinement is a new variable congestion loss window used in TCP veno and is useful for light loaded network. Second refinement is taking into account power level of received packet from the MAC Layer for better detection of random losses. Packet loss identification is also correct in TCP Venoplus. TCP veno provides a Packet loss identification scheme. To provide an end to end congestion control a sender side variation of TCP Reno, TCP Venom was developed [2]. A threshold value β is used to make the decision. If the estimated congestion level in the network exceeds the value of β, packet loss is detected as congestion loss. Otherwise loss is due to random errors.

 

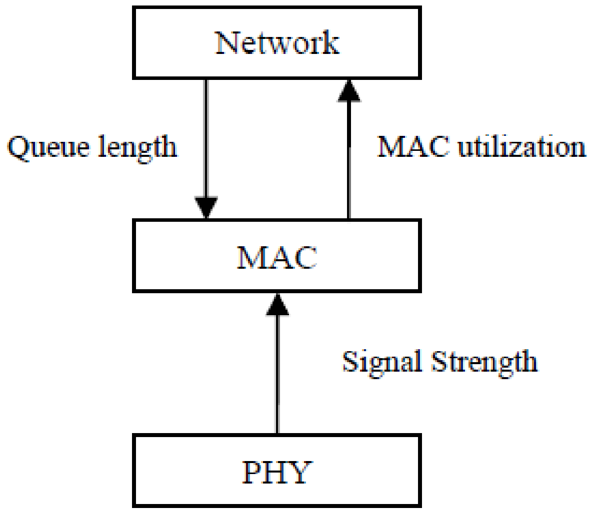


Fig. 1 Cross layer communication in wireless network.

Cross-layer approaches have gained significant attention, due to their ability to allow critical information of the wireless medium in the MAC and physical layers to be shared with higher layers as shown in Fig.1, in order to provide efficient methods of allocating network resources and applications over the Internet [19].

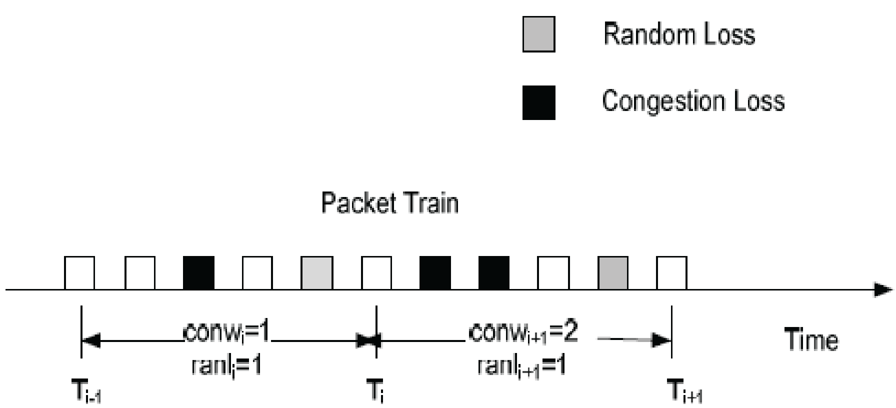

Fig. 2 Computation of congestion loss window and random loss rate.

As shown in Fig. 2, the congestion loss window $coni_c$ can be calculated as follows:

$$coni_c = C_{hi} / (T_i - T_i\text{-}1) \quad (1)$$

TCP Venoplus utilizes the received signal strength information (RSSI) for a packet to calculate random losses due to noise and interference.

The packets whose RSSI is less than the RXThresh or CSThresh are dropped by the MAC layer. But Venoplus procures the number of dropped packets ($R_{ib}$) from the MAC layer and computes the random loss rate ($rank_{le}$). $R_{ib}$ is calculated at the MAC layer by keeping track of the received signal strength (RSS) of each packet. If the RSS value falls below a certain threshold the packet is dropped.

$$rank_{le} = R_{ib} / (T_i - T_i - 1) \quad (2)$$

The packet identification scheme has four different scenarios which are as follows: 1) If $coni_c > conw_i$-1 and $rank_{le} > ranl_i$-1, the network suffers from losses due to congestion and random errors in the link simultaneously. This situation requires slowing down the transmission of packets which is reflected by the reduction of the congestion window by half. 2) If $coni_c < conw_i$-1 and $rank_{le} > ranl_i$-1, the packet losses can be attributed to random errors in the link only. The congestion window is cut down by 1/5. 3) If $coni_c > conw_i$-1 and $rank_{le} < ranl_i$-1, the packet losses can be attributed to congestion losses in the network. The congestion window is now cut down by 1/2. 4) Finally, if $coni_c < conw_i$-1 and $rank_{le} < ranl_i$-1, the congestion in the network and the random errors in the link are not getting worse, which means that the congestion window remains unchanged.

2.2 The impact of wireless channel on TCP

Generally packet loss is due to link layer contention, and it is caused by hidden terminals. To increase TCP performance over multihop wireless network two link layer techniques are proposed [12]. First is a link-RED algorithm to tune the wireless link's drop probability. Second is an adaptive link-layer spacing scheme to increase the spatial channel reuse.

2.2.1 Link-RED algorithm

In LRED, the link layer maintains the average number of the retries for recent packet retransmissions. The head-of-line packet is dropped/marked from the buffer with a probability based on this average number. At each node, if the average number of retries is small, for E.g. 'month', which means that the node is rarely hidden, packets in the buffer are not dropped/marked. When it gets larger, the dropping/marking probability is computed, and the minimum value of the computed drop probability and a maximum bound max P is used.

A feature of this algorithm is that it can integrate with Explicit Congestion Notification (ECN) enabled TCP flows. Instead of blindly dropping packets, we can simply mark them at the link layer, and thus allow ECN enhanced TCP flows to adapt their offered load without losing any packets. TCP performance is further improved, by paying the moderate cost of a slightly more complex link-layer design. LRED is a simple mechanism which monitors a single parameter i.e. average number of retries.

2.2.3. Adaptive pacing

Second technique takes an adaptive pacing approach at the link-layer. The goal is to improve spatial channel reuse, by distributing traffic among intermediate nodes in a more balanced way, while enhancing the coordination of forwarding nodes along the data path. This design works in concern with the 802.11 MAC.

This algorithm works together with LRED as follows. Adaptive pacing is enabled by LRED. When a node finds its average number of retries to be less than month, it calculates its back off time as usual. When the average number of retries goes beyond month, adaptive pacing is enabled and the back off period is increased by an interval equal to the transmission time of the previous data packet. This way, a better coordination among nodes is achieved under different network load.

2.3 Route stability in wireless mesh

Route stability algorithm is given. Reactive routing protocol is used. It has two phases First is Route discovery and second is route maintenance. Author has given disadvantages of reactive routing approaches: Collisions and hidden node problem exists due to use of shared medium. Second is these are dependent on intermediate nodes. And problem is that these intermediate node can mistakenly considers temporary transmissions problem as actual link breakage and source is frequently notified of route breakages, which causes burden on network decrease performance, throughput decrease and end-to-end delay is increased.

2.4 Received signal strength based minimization of broadcast storm

MANET cannot control broadcast packet since nodes are mobile. Optimal Reliability Broadcast Mechanism (ORBM) is given in [14]. ORBM is area based broadcast protocol and relies on signal strength of a broadcast packet to assign rebroadcast priorities for every node in the network. It controls temporal congestion (arising out of broadcast storm), and reduces rebroadcast. ORBM is scalable and adjust with neighbor as well as mobility.

ORBM uses two data structures

Zone Marker Table: The purpose of this table is to associate a Zone Identifier with the received signal power, as indicated by the Zone Signal Threshold.

Zone Entry Table: Each node also maintains a Zone Entry Table, which is updated every time a packet is received. Its characteristic fields include a Sequence Number for the currently received packet, a pointer to the Zone Table to associate the received packet with a Zone Identifier and a corresponding Zone Contention Window.

2.4.1 ORBM operation:

ORBM has two phases, First is differentiation of immediate neighbors into zones, such that nodes with a lower zone identifier get a priority to rebroadcast. It is achieved by received signal power. Second phase is there can be multiple nodes in a zone itself resulting contention. To resolve contention each node selects a random back off. Selected back off should be greater than contention window of previous zone Selected back off should be less than contention window of previous zone. Advantage of ORBM is that nodes which receive the weakest signal are given a priority in rebroadcasting. In this ORBM algorithm If new broadcast packet is received then it will Calculate Zoned m from received signal strength and will Set a back off timer as random [CW(m - 1), CW(m)]. It will also Set self to forwarding node. Otherwise if duplicate broadcast packet is received and If back off timer < CW(m - 1) then algorithm will cancel the associated timer and will reset 'forwarding node' status and reject the packet. Continue countdown of backup timer. If back off timer expires, then it will rebroadcast the packet.

2.5 ARL: Adapting MAC 802.11 for performance optimization of MANET

ARL (Adaptive Retransmission Limit) algorithm reduces the false link failure and predict the node mobility [15]. False link failure occurs when the MAC protocol declares that the link to a neighbor node is broken, even though neighbor node is within its transmission range. Objective of this algorithm is to differentiate the false link failures caused by interference from true link failures due to mobility. Key challenge of this algorithm is to distinguish between false and true link failure.

ARL works in two phases: in first phase each node overhears packet without regard to their destinations and look at their source address (node ID) and gets the received signal strength (RSS) corresponding to the overheard packet from physical layer. Then it stores this information into a table called neighbor table with the receiving time of packet. Second phase is the adaptive MAC reports a link failures only if the retransmissions limit deduced using the ARL algorithm.

2.6 Gray Zone Prediction Algorithm

Cross Layer Stability based routing mechanism (CLS_AODV). 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.

2.6.1 CLS_AODV has three main parts:

1. Route Discovery
2. Route monitoring
3. 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.

After detecting communication gray zone preemptive route repair procedure should be initiated. And this route repair process is given in below Fig. 3

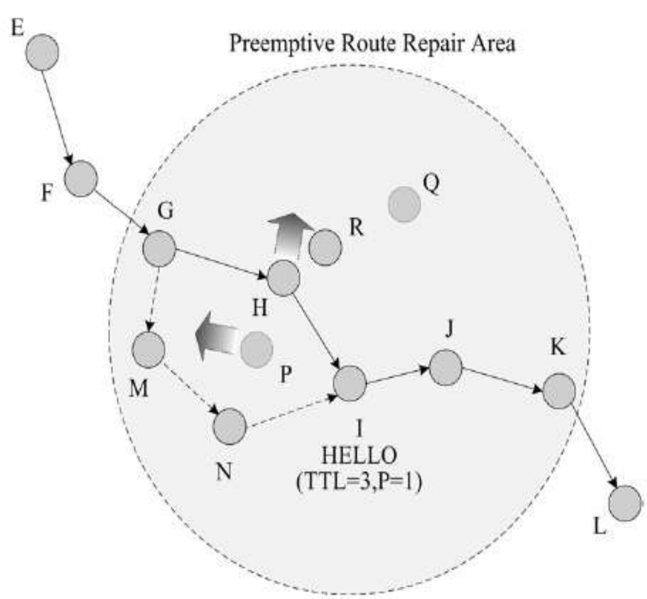


Fig. 3. Preemptive route repair procedure.

Fig. 3 shows the procedure of preemptive route repair. preemptive local route repair zone, is denoted by the dotted line, which is decided by 3-hop HELLO messages broadcasted by node I. Supposing that node H is the moving node detected by position location scheme [4], node G should be informed to execute preemptive local route repair, and node I is the destination of local route repair. The value of TTL is set to 3. SNF_Thresh and Link_Length_Thresh are assumed to set to 8 and 15 m respectively. In short this route repair process finds the moving node which is responsible for the occurrence of communication gray zone. In above Fig.3 such a node is Node I is responsible for predicting the occurrence of gray zone and starts preemptive route repair scheme. Thus in this way CLS_AODV react to link breakages using route state monitoring and gray zone prediction. 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.

2.7 MultiAgent based Adaptive DSR (MA-DSR)

MADSR is a multihop routing algorithm. It uses signal strength as routing metric to predict link break before they actually occurs. MADSR algorithm deletes routes that contain mobile or low power node from cache and specific policies for future use of this node in routing algorithm [16]. MA-DSR algorithm focus on four principles: First, Determination of congestion in level of each node. Second is Prediction of links statuses by considering the received signal power in intermediate and destination nodes to prevent the effects due to breakages. Third is energy level of each node. Fourth is final status of each node (NSV). A new cross layer approach and some modifications in the MAC layer for Route Error (RERR) are given.

MA-DSR algorithm checks link break is due to mobility of nodes. But, when this problem don't occur, this algorithm will check possibility of congestion problem. This can be found from queue length. Therefore, queue is tested to check fullness percentage of queue and its value is used in decision. If this value is higher than threshold, congestion occurred. Because existence of many packets in node's queue can result long latency for packets or even packets dropping [8]. In this case, algorithm don't delete route from cache but reduce its selection probability by changing its Row Optimality Weight ROW parameter. Finally, if sender received RERR packet and protocol don't detect low power, mobility and/or congestion problem, this may be an attack from malicious nodes which do not cooperate with other nodes and try to disrupt the network. Black list is introduced for dangerous nodes and change ROW of routes that containing them for better performance three lists are given and we can keep some nodes in them according to below rules. Each list has constant length (Table 1). Rules that implied in new routing mechanism: Rule1: Set very escaped or congested nodes in yellow list after 5 times and in red list after 8 times. Rule 2: If a node declare RERR more than 10 times without any reason, it's may be malicious node and It should set in black list. Rule 3: Nodes whose battery is low(less than 20%) are set in red list. By this way nodes that their battery lower than other, act as a router seldom. Rule 4: If routes contain nodes that redound any problem previous, their ROW multiply in 1.25, but if these nodes in one of the three lists, algorithm can act based on coefficients in Table 1.

Table 1. Lists and their properties

| List | Size | ROW Coefficient |
|---|---|---|
| Yellow | (Number of Nodes)/5 | 1.5 |
| Red | (Number of Nodes)/10 | 1.75 |
| Black | (Number of Nodes)/10 | 2 |

MA-DSR algorithm acquires some properties such as signal strength, shortest-path metrics, congestion measurement and energy level in each node, these are used in route selection decision. By using this information the cause of route breakage can be determined and changes can be applied in the routing decision policies of MA-DSR protocol.

2.8 Improved-ADTCP (Improved Adhoc TCP)

Improved-ADTCP (I-ADTCP) is an improvement on ADTCP [17]. To improve the performance of ADTCP considers following: it ensures sufficient bandwidth utilization of the sender-receiver path; avoid the overloading of network by limiting TCP's congestion window below the Upper Bound of Bandwidth Delay Product (BDP-UB) of the path; it checks for incipient congestion by calculating inter-packet delay difference and short term throughput using Relative Sample Density (RSD) technique. In an incipient congestion condition, we reduce Congestion Window Limit (CWL) to half, which limits the packets send by the sender and does not allow the congestion to build up. Thus the algorithm tries to remain in congestion avoidance phase at all times by detecting and reacting to incipient congestion.

## 3. Conclusion

As a result of our studies, it can be said that we can increase the performance of TCP which automatically improves congestion. Cross layer approach, TCP performance signal strength and mobility these four parameters can be used to improve congestion control. Objective of most of the algorithms is to reduce the packet losses due to mobility in ad hoc networks and thereby improves the performance of TCP. Towards this, some author had proposed a link management framework that helps in improving TCP packets in transit upon the incidence of link failure. The framework consists of various mechanisms. One of it is we can induce a temporary increase in the transmit power level when a node moves out of range to temporarily reestablish the failed link. This would enable the TCP packets that are already in flight to traverse the link. These algorithms can considerably reduce the number of packet losses. Consequently the number of TCP re-transmission time-outs is reduced and the TCP sources send more packets.

**References**

S. Ramanathan, M. E. Steenstrup, "A survey of routing techniques for mobile communications networks, mobile networks and applications," Vol. 1, pp. 98–104, 1996.

Sachin Shetty, Ying Tang, William Colane "TCP venoplus - a cross-layer approach to improve TCP performance in wired-cum-wireless networks using signal strength"

Ming Yang "Congestion-aware Cross-Layer Design for Wireless Ad Hoc Networks"

Li-Na Wing, Jibe Yang "A cross-layer stability-based routing mechanism for ultra wideband networks" Computer Communications 33 (2010) 2185–2194

D. B. Johnson, D. A. Maltz, and J. Broch, "Dynamic source routing for multihop wireless ad hoc networks," in Ad Hoc Networking.("in press")

M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," Proceedings IEEE International Conference Network Protocols (ICNP), pp. 14–23, 2001.

J. Broch, D. Johnson, and D. Maltz, "The Dynamic Source Routing protocol for Mobile Ad Hoc Networks," IETF Internet draft, Oct.1999.

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

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.

H. Lundgren, E. Nordstrom, C. Tschudin, "The gray zone problem in IEEE 802.11b based ad hoc networks", ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002) 49–55.

Went Song, Fuming Fang "Routing with Congestion Control Using Cross-layer Design in Wireless Mesh Network" ICWMMN2006

Zhengzhou Fu, Petro's Zeros, Haiku Lou, Songhua Lu, Lidia Zhang, Mario Gela "The impact of multihop wireless channel on TCP throughput and loss", UCLA Computer Science Department, Los Angeles, CA 90095-1596

Us man Ashram, Slim Abdellatif and Guy Jangle "Route stability in wireless mesh access networks"

LAAS-CNRS, 7-Avenue du Colonel Roche, 31077 Toulouse University of Toulouse, France. 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

Atanu Roy Chowdhury "Received signal based minimization of broadcast storm in multi-hop MANET" 1-4244-0340-5/06/$20.00 02006 IEEE

Aura Bhatia and Vive Kumar "Adapting MAC 802.11for performance optimization of magnet using cross layer interaction" international journal of wireless & mobile networks (ijwmn) vol.2, no.4, november 2010

M. Rajabzadeha, F. Adibniyab, M. ghasemzadehc "Condition aware robust routing algorithm with cross layer technique for ad hoc situations" Procedia Computer Science 3 (2011) 698–705

Sachin Ajar, "Improving performance of Adhoc TCP in Mobile Adhoc Networks" 978-1-4244-2746-8/08/$25.00 © 2008 IEEE

Y. Lu, W. Wang, Y. Hong, and B. Baraga, "Study of distance vector routing protocols for mobile ad hoc networks," Proceedings IEEE International Conference Pervasive Computing and Comm. (Parco), pp. 187–194, March 2003.

S. Shakkottai, T. S. Rappaport and P. C. Karlsson,"Cross-layer Design for Wireless Networks,", IEEE Communications magazine, October, 2003.

N.C. Wang, Y.F. Huang, J.C. Chen, A stable weight-based on-demand routing protocol for mobile ad hoc networks, Information Sciences 177 (24) (2007) 5522–5537.