International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue5 pp 194-198 August 2012 www.ijsret.org ISSN 2278 – 0882

Congestion Control in Mobile Ad-Hoc Networks

[1]Sandeep Rana, [2]Varun Pundir, [3]Ram Sewak Singh, [4]Deepak Yadav
[1, 2, 3, 4]Shanti Institute of Technology, Meerut
Email: sandeepmietcs@gmail.com
Email: varunpundir@hotmail.com
Email: ramrathopre25@gmail.com
Email: deepakdeshwal87@gmail.com

ABSTRACT
Congestion is the general problem in MANET and it must be overcome to get congestion free network. In this paper we study the problem of jointly performing scheduling and congestion control in mobile ad-hoc networks so that network queues remain bounded and the resulting in congestion free flow rates we present a model for the joint design of congestion control and media access control (MAC) for mobile ad-hoc wireless networks. Mobile Ad Hoc Grid deals with the challenges in resource discovery and job scheduling due to its mobility and power consumption.

I. INTRODUCTION

1. AD-HOC NETWORK
A mobile Ad-Hoc network (MANET) is a group of mobile nodes forming a temporary network without the aid of any fixed infrastructure or centralized administration. The configuration of this network can be static or dynamic. Its life is variable but can be very limited. The specific characteristics of any mobile network:

- The disconnection: voluntary or involuntary, temporary or permanent;
- Insecurity in the storage of data: Is it available at all times for backup operations?
- The low-capacity storage media except some hosts such as laptops;
- Low bandwidth (in the present state of technological progress). This factor is closely linked to technological change;
- The low power mobile sites: Batteries are very far from the stability rather than the energy made available in fixed networks. This factor will play a very important and is closely related to other factors;
- The limited computing power (except for laptops);
- High vulnerability to failures due to the fragility of the environment;
- The high vulnerability to intrusion.

In general, routes between nodes in an ad-hoc network may include multiple hops and, therefore, it is appropriate to call such networks "Ad-Hoc" networks multi-hop. Figure 1 shows an example of mobile Ad-Hoc and communication topology.

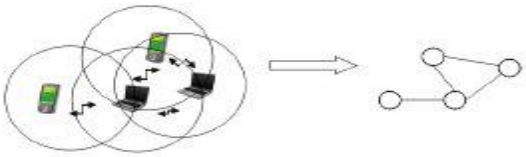

Figure 1 Ad-Hoc network

II. HIGH SPEED NETWORK
For transmitting or receiving high bandwidth data such as video data we need a network with high network capacity and high bandwidth, such type of networks are known as high speed network. In general, any connection to the customer of 256kbit/s (0.25Mbit/s) or greater is more concisely considered as high speed network. High speed network is made up of cables such as fiber optics that support transmission of high speed data. Continuous media applications such as video and audio are sensitive not only to the packet loss probability but also to the correlation of packet losses. For multimedia applications, there is strong need of high speed network based architecture and mechanism

III. CONGESTION
Congestion in a network may occur if the load on the network- the number of packets sent to the network- is greater than the capacity of the network-the number of packets a network can handle. Congestion in a network or internet work occurs because routers and switches

have queues- buffers that hold the packets before and after processing. It degrades quality of service and also can lead to delays, lost data. Congestion can be brought on by several factors. If all of a sudden, streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up. If there is insufficient memory to hold all of them, packet will be lost. This problem cannot be solved by increasing memory, because Nagle discovered that if routers have an infinite memory, congestion gets worse, not better. Slow processor can also cause congestion. If routers' CPUs are slow at performing the bookkeeping tasks required, queues can build up, even though there is excess line capacity. Similarly, low bandwidth lines can also cause congestion.

IV. CONGESTION CONTROL

Congestion control refers to the mechanism and techniques to control the congestion and keep the load below the capacity. It is a mechanism that can either prevent congestion, before it happens, or remove congestion, after it has happened. The objective of congestion control is to maintain the number of packets within the network below the level at which performance falls off dramatically. Due to the unpredictable fluctuations and burstiness of traffic flows within high speed network congestion can occur frequently. So we need efficient congestion control technique. There are many mechanisms developed for congestion control:

IV.1 Adaptive Congestion Control:

Adaptive congestion control is a mechanism with learning capability. This learning capability enables the mechanism to adapt to dynamically changing network conditions to maintain stability and good performance. In this a feedback is send to the sender to change sending rate, according to the current network conditions. It is scalable with respect to changing delays, bandwidth and number of users utilizing the network. ACP is characterized by its learning capability which enables the protocol to adapt to the highly dynamic network environment to maintain stability and good performance. This learning capability is materialized by a novel estimation algorithm, which 'learns' about the number of flows utilizing each link in the network. Previous experience in the design of congestion control algorithms has shown that at each link, the number of flows utilizing the link is necessary in order to maintain stability in the presence of delays.

IV.2 Rate Control Protocol:

Rate Control Protocol (RCP) is a congestion control algorithm designed for fast download times. RCP is designed for the typical flows of typical users in the Internet today. RCP has two components:

(1) End-host congestion control layer that sits between IP and TCP/UDP. During introduction, the end-host could adapt by testing for RCP at each end and along the path, falling back to TCP if need-be

(2) Each router maintains a single fair-share rate per link

IV.3 Explicit Congestion Control Protocol:

XCP is a window based congestion control protocol intended for best effort traffic. Senders maintain their congestion window and RTT and communicate this to routers via a congestion header in every packet. Sender uses the feedback field in the congestion header to request its desired window increase. Routers monitor the input traffic rates to each of their output queues. Based on the difference between the link bandwidth and its input traffic, router tells the flows sharing that link to increase or decrease their congestion window.

V. COMPETITIVE AND CONSIDERATE CONGESTION CONTROL PROTOCOL (4CP)

4CP is a new congestion controller that implements the farsighted strategy. The controller has the following features:

(i) It chooses an additive-increase and inverse-decrease window adjustment in congestion avoidance;

(ii) The inverse-decrease parameter is adapted very slowly targeting verification of a given loss-throughput formula over large timescale;

(iii) The window is used as a bad phase detector and can assume negative values: it indicates bad (respectively, good) phase when it is negative (respectively, positive) and it is used as the congestion window in good phases;

(iv) It is sender-only change of standard TCP, and thus it can communicate to any standard TCP receiver (easing the deployment);

(v) No change to network routers or other network infrastructure is required.

VI. FLOW CONTROL

Flow control limits the amount of data transmitted by the sending transport entity to a level, or rate that the receiver can manage. At the transport level flow control will allow the transport protocol entity in a host to restrict the flow of data over a logical connection from

the transport protocol entity in another host. TCP uses an end-to-end flow control protocol to avoid having the sender send data too fast for the TCP receiver to receive and process it reliably. Having a mechanism for flow control is essential in an environment where machines of diverse network speeds communicate.

VII. RELATED WORK

In this chapter we will explain briefly problems and their solution that is related to congestion control in high speed network. We have studied so many papers. From all of them we only discuss some important issues related to our proposed model. The problems occur in several protocols that were previously used for congestion control. TCP, a widely used protocol, work efficiently in low speed data network but in the case of high speed network, it gives poor performance. Previous protocols were fail to satisfy key design requirements of congestion control protocols, such as max-min fairness, high utilization, small queue sizes and no observable packet drops. To fix that problem they design a new adaptive protocol that has a learning capability.

In this a new packet header is defined that contains three fields: Sender's RTT estimate, desired sending rate and Congestion bit. When an acknowledgment is sent by the user, appropriate values are set in these three fields. In realistic traffic scenarios comprising of a small number of long flows and a large number of short flows, ACP outperforms both TCP and XCP, even in the presence of random packet losses. ACP does not require maintenance of per flow states within the network and utilizes an explicit multi-bit feedback signaling scheme. To maintain stability it implements at each link a novel estimation algorithm which estimates the number of flows utilizing the link.

VIII. PROPOSED WORK

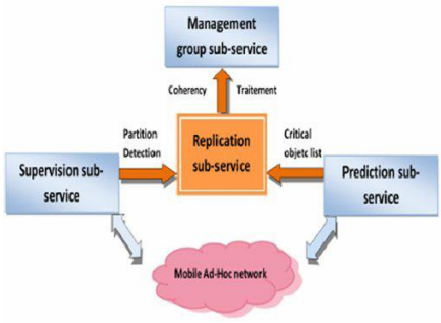

Figure 2: Architecture of fault tolerance service

 the sub-service prediction predicts a possible failure or disconnection of the network by establishing a list of critical object. Each leader can know the current status of all nodes of its group. To assess the criticality, the sub-service can detect several types of items critical energy point and frequent failure or shutdown.
 if an energy level of a node reaches "low energy" the prediction as the class critic node.
 the sub-service prediction predicts a possible failure or disconnection of the network by establishing a list of critical object. Each leader can know the current status of all nodes of its group. To assess the criticality, the sub-service can detect several types of items critical energy point and frequent failure or shutdown.

IX. RESULT

 the sub-service prediction predicts a possible failure or disconnection of the network by establishing a list of critical object. Each leader can know the current status of all nodes of its group. To assess the criticality, the sub-service can detect several types of items critical energy point and frequent failure or shutdown.
 if an energy level of a node reaches "low energy" the prediction as the class critic node.

a. Impact of the range

 in the first simulation, we wanted to determine the impact of the range on the number of requests accepted/lost. The simulated networks are composed of 50 nodes, 200 requests (reading), 20 data, simulation time 60 seconds, time pause 1 second and mobility speed 3 m/s. We considered the range from 50 to 200 m in steps of 50. The result of this experiment is shown in Figure 3.

 With a range of 100 m the network is completely connected (no partition), which
is why the number of lost motion whether with or without our approach is zero.
Above 150 m there is a significant increase in the number of lost motion.
However with our approach the number of lost motion is reduced.

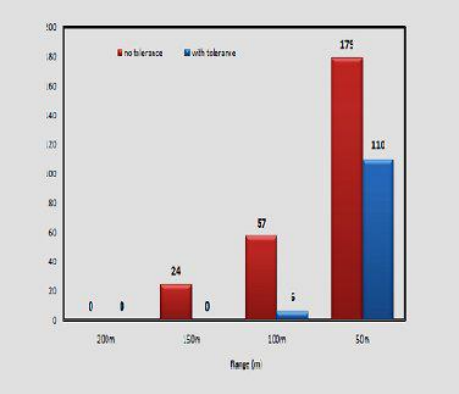

Figure 3: Impact of the range

 We proposed a series of simulation with the same parameters of the previous experiment except that this time, we vary the number of stops volunteer in the network from 0 to 8 stops in steps of two.
 The Figure 4 shows the contribution of our approach with fault tolerance to compare to the number of voluntary stops in the network. We note that the number of requests lost with our approach is always zero even increase stops volunteers. This is due to the replication before the nodes stops. While no tolerance, the number of lost requests increases exponentially

b. Impact of voluntary fault

We proposed a series of simulation with the same parameters of the previous experiment except that this time, we vary the number of stops volunteer in the network from 0 to 8 stops in steps of two.
 The Figure 5 shows the contribution of our approach with fault tolerance to compare to the number of voluntary stops in the network. We note that the number of requests lost with our approach is always zero even increase stops volunteers. This is due to the replication before the nodes stops. While no tolerance, the number of lost requests increases exponentially

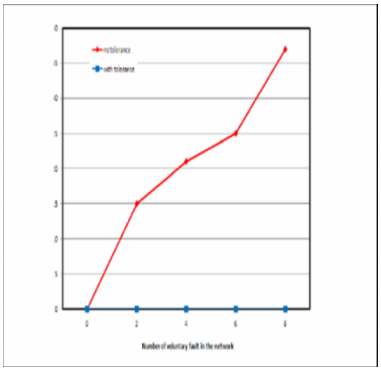
Figure 4: Impact of voluntary fault

c. Impact of number of nodes

 A network is unstable when the pause time is low (less than one second). After several rounds of simulations we found that the network is more stable our service will save more energy.
 We conducted a simulation with the same parameters of the previous simulation by varying the number of nodes from 100 to 700 nodes in steps of 100. The simulation results are expressed in Figure 8.
 It can be seen in Figure 6 that energy consumption with our approach is still low compared to an approach without fault tolerance. This is due to the reduction of long distance communications, which are very costly in energy.

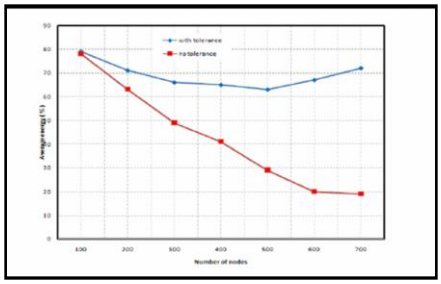
Figure 5: impact of the number of nodes

d. Impact on the life of the network

 Figure 7 shows the lifetime of nodes in the network. We took the same parameters as the previous simulation but with a number of nodes equal to 300 and a simulation time of 240 s.
 From this figure, we can see that our proposed with fault tolerance, can conserve energy better than the standard approach, increasing the overall lifetime of the network.

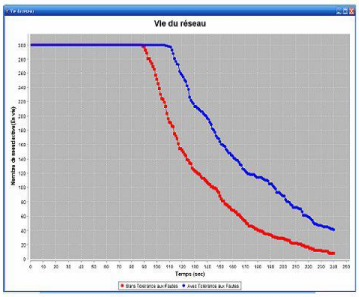

Figure 6: Evolution of life the network

V. CONCLUSION

 So a solution has been given for the management of fault tolerance in the Ad-Hoc networks, combining the functions needed to better availability of data. Our

contribution takes into account the characteristics of mobile terminals in order to reduce the consumption of resource is critical (energy), and to minimize the loss of information.

- The experimental results obtained have shown that our solution allows reducing the number of lost requests, reducing response times to queries, better conserve energy which increases the lifetime of the network and supporting the scalability.
- In the future, we can extend this work by taking into account firstly the consistency of replicas in such a highly dynamic environment, and secondly by incorporating a model of energy to reduce by advantage in energy consumption.

REFERENCES

[1] Buttyan, L. and Hubaux, J.-P. (2000) 'Enforcing service availability in mobile ad-hoc WANs'. In Proc. of the 1st ACM International Symposium on Mobile Ad Hoc Networking (MobiHoc 2000). Boston, Massachusetts: ACM, 2000, pp. 87–96.

[2] Goncalves, B., Mitton, N. and Guérin-Lassous, I. (2006) 'Comparison of two Self-Organization and Hierarchical Routing Protocols for Ad Hoc Networks'. In Second International Conference on Mobile Ad Hoc and Sensor Networks (MSN), Hong-Kong, China, December.

[3] Hamdy, M. and Konig-Ries, B. (2008), 'A service distribution protocol for mobile ad hoc networks', ICPS '08: Proceedings of the 5th international conference on Pervasive services, Sorrento, Italy, pages. 141-146.

[4] Hauspie, M. and Simplot, D. and Carle, J. (2003),'Partition Detection in Mobile Ad-hoc Networks', In Proceeding of the 2nd Mediterranean Workshop on Ad Hoc Networks (Med- Hoc-Net 2003), Mahdia, Tunisia.

[5] Ito, S. and Yoshigoe, K. (2009), 'Performance Evaluation of Consumed Energy-Type-Aware Routing (CETAR) For Wireless Sensor Networks', International Journal of Wireless & Mobile Networks (IJWMN), Vol. 1, No. 2, November 2009, pp. 90-101.

[6] Jorgic, M. and Stojmenovic, I. and Hauspie M. and Simplot-Ryl, D. (2004), 'Localized algorithms for detection of critical nodes and links for connectivity in ad hoc networks'. In Proceeding of the Third Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net, June, Bodrum, Turkey.

[7] Michiardi, P. and Molva, R. (2004), 'Mobile Ad Hoc Network', Wiley-IEEE Press, ch.12: Ad Hoc Network Security, pp. 329–354