DETECTION AND AVOIDANCE OF CONGESTION CONTROL USING AD-HOC NETWORK

Mrs. Sonal Beniwal, Jyoti Kaushik

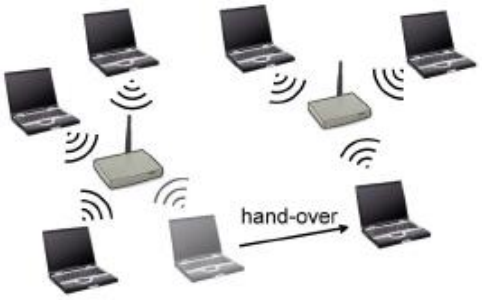
Computer Science and Engineering, (Network Security), BPSMV KHANPUR KALN SONIPAT, INDIA

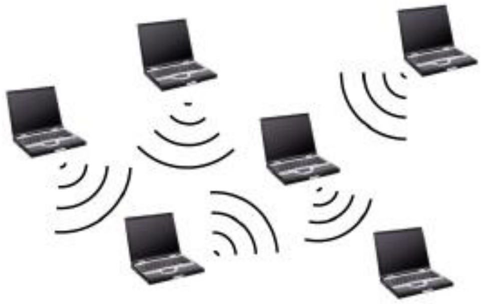
ABSTRACT

Recent advances in Wireless Sensor Networks (WSNs) lead to applications with increased traffic demands. There are many cases in the fields of automation, health, and disaster response that demand WSNs with strict performance assurances. Congestion occurrence is a key factor that can negatively affect the performance of WSNs. The overwhelming majority of approaches that deal with congestion control in WSNs attempt to control congestion, by reducing the rate with which sources inject packets in the network. This method is called traffic control. Although traffic control seems to be an effective method for controlling congestion, it presents a number of drawbacks which are not easy to ignore. By controlling the rate with which packets are injected in the network, the amount of information that reaches the data sinks reduces. This fact can jeopardize the purpose of the network. Thus, in case of heavy data load, this path of nodes can easily become power exhausted. This leads to the creation of routing "holes" in the network. In this paper we approach congestion control and avoidance in WSNs with a different perspective.

1. MANET

A mobile ad hoc network (MANET) is formed by a group of mobile nodes connected by wireless.





1.1 An infrastructure network with two base stations. 1.2 A mobile ad-hoc networks.

The nodes can talk to each other by direct peer-to-peer wireless communication when they are close to each other .When the sender and receiver are far away, their packets can be forwarded by the intermediate nodes along a multi-hop path.

1.2 Application areas of MANET

Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective. There are many uses of mobile ad-hoc networks such as:

1. **Business Environments:** In e-business applications, more and correct information might lead to better deals including e learning and in e-learning applications is only possible if the needed information is available at time.
2. **Crisis Management Services:** Such as in disaster recovery, where the entire communication infrastructure is destroyed and resorting communication quickly is crucial. By using a mobile ad-hoc network, an infrastructure could be set up in hours instead of weeks, as is required in the case of wired line communication.

3. **Private Area Network (PANs):** Bluetooth designed to support a personal area network by eliminating the need of wires between various devices, such as printers, digital cameras and personal digital assistants.
4. **Industrial and Commercial applications:** Some applications of MANET technology could include industrial and commercial applications involving cooperative [6] mobile data exchange. And also mesh-based mobile networks can be operated as robust, inexpensive alternatives or enhancements to cell-based mobile network infrastructures.
5. **Military Networking requirements:** Existing and future military networking requirements for robust, IP compliant data services within mobile wireless communication networks. Many of these networks consist of highly dynamic autonomous topology segments.
6. **Communication Operations:** When properly combined with satellite-based information delivery, MANET technology can provide an extremely flexible method for establishing communications for fire/safety/rescue operations or other scenarios requiring rapidly deployable communications with survivable, efficient dynamic networking.
7. **Environmental Application:** In an environmental network, the temperature, atmospheric pressure, amount of sunlight, and the relative humidity.

2. Security Goals:

I)Availability: Ensures survivability despite Denial Of Service (DOS) attacks. [1] On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel.

II) Confidentiality: Ensures certain information is never disclosed to unauthorized entities.

III)Integrity: Message being transmitted is never corrupted.

IV)Authentication: Enables a node to ensure the identity [1] of the peer node it is communicating with.

V)Non-repudiation: Ensures that the origin of a message cannot deny having sent the message.

3. TCP Congestion control:

On the Internet, Congestion control is in the responsibility of the transport layer, more precisely of the Transmission Control Protocol (TCP). TCP combines congestion control and reliability mechanisms. This combination allows to perform congestion control without the need for explicit feedback about the congestion state of the network, and without direct participation of the intermediate nodes. [15] To detect network congestion TCP simply observes occurring packet losses. Since on the Internet missing packets are almost always caused by congestion, a missing packet is interpreted as a sign for network congestion. In other words, TCP is a protocol that can exhibit complex behavior, especially when considered in the context of the current Internet, where the traffic conditions themselves can be quite complicated and subtle. The attention on the congestion avoidance behavior of TCP and its impact on throughput, taking into account the dependence of congestion avoidance on ACK behavior, the manner in which packet loss is inferred (e.g., whether by duplicate ACK detection and fast retransmit, or by timeout), limited receiver window size, and average round trip time (RTT).

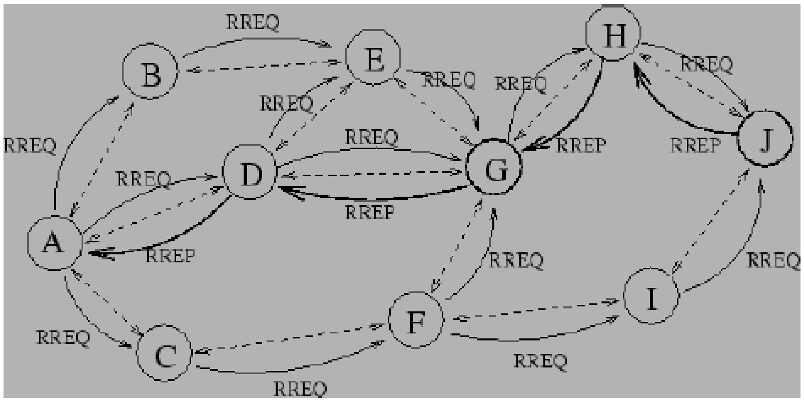


Figure 3.1. Possible path for route reply if A wishes to find route to J

4.4 Characteristics of AODV Routing Protocol

A few characteristics of the AODV protocol are discussed in this section. On-demand routing is responsible for discovering hops, either in broadcast mode or in non-broadcast mode. Unlike link-state routing protocols, the distance vector protocol supports all three- unicast, multicast, and broadcast. It is not necessary to have an additional protocol in the AODV protocol environment to obtain a loop free network. The AODV routing protocol itself has an added feature of including a topology database table to ensure that no redundant paths are formed. Quick aging is one of the characteristics of the AODV protocol and is responsible for the timeout of route entries in the database. The AODV protocol is deterministic in nature, that is, in a given AODV protocol environment, the routes between a pair of nodes are preprogrammed or determined in advance to transmission. These protocols are incapable of load balancing traffic. Singlepath interconnected networks are not fault tolerant.

4.5 Advantages of AODV Routing Protocol

The AODV protocol does not require a central administrative system for handling the routing process. It is a flat routing protocol, whereby routes are constituted on demand. The sequence numbers are utilized for finding the latest route to destination. The AODV protocol reduces the overhead of control traffic messages at the cost of an increase in latency in routediscovery. This has a relatively low connection setup delay. The AODV protocol is loop free and avoids the count-to-infinity problem by utilizing sequence numbers.

4.6 Disadvantages of AODV Routing Protocol

Inconsistent routes may occur due to the source sequence number. If the value of the source sequence number is stale at the source and the intermediate routes contain a higher (but old) destination sequence number, then heavy control overhead may be caused if multiple RREP packets are sent in response to a single RREQ packet. The periodic beaconing leads to unnecessary bandwidth consumption which leads to congestion and packet drops in the network

5. PROPOSED WORK

5.1 The Congestion Problem

In computer networks, mismatch of incoming and outgoing data rates results in congestion. For wired networks like INTERNET, there are mixed links with different bandwidths. The node with the lowest bandwidth along a path from the source to the destination is called the bottleneck. Usually, congestion occurs in the bottleneck since it receives more data than it is capable of sending out. In this situation, packets will be queued and sometimes get dropped. As a consequence, response time will increase and throughput will also degrade. Figure 3.1 illustrates network performance as a function of the load. When the load is light, throughput is linearly proportional to the load and response time is almost unchanged. After the load reaches the network capacity (the knee point), throughput won't increase much with the load. Instead, packets will be queued and the response time will become longer in this period. The throughput may suddenly drop if packets get discarded due to buffer overflow, which is called the cliff point as shown in Figure 4.1. Congestion can be realized in many ways, but in simple terms one may say that, if, for any time interval, the total sum of demands on a source is more than its available capacity, the source is said to be congested for that interval. Mathematically speaking:

$\sum$Demand > Available Resources (4.1)

Congestion in wireless networks is different from that of wired networks. Due to the memory restrictions of the sensor nodes and limited capacity of shared wireless medium, network congestion may be experienced during the network operation. In wireless networks congestion happens due to contention caused by concurrent transmissions, buffer overflows and dynamically time varying wireless channel condition

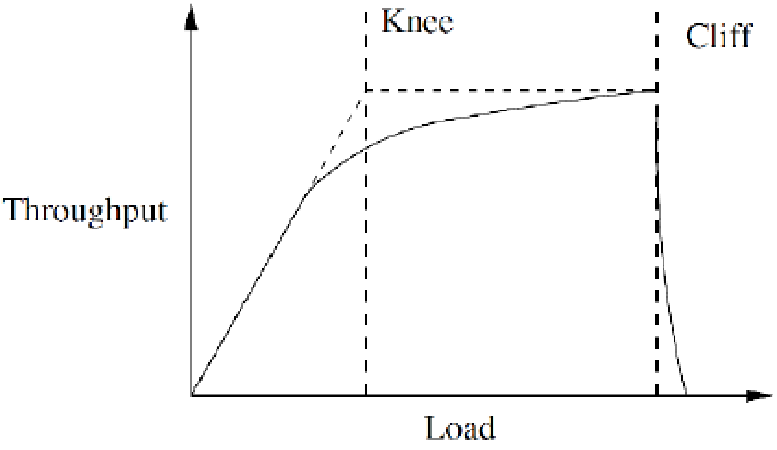


Figure 4.1: Effect of congestion on throughput

5.2Effects of Congestion

As WSN is a multi-hop network, congestion taking place at a single node may diffuse to the whole network and degrade its performance drastically. Congestion causes many folds of drawbacks:

1. Increases energy dissipation rates of sensor nodes,

2. Causes a lot of packet loss, which in turn diminish the network throughput and

3. Hinders fair event detections and reliable data transmission.

4. Large queuing delays are experienced as the packet arrival rate nears the link capacity.

5. The sender must perform retransmissions in order to compensate for dropped packets due to buffer overflow.

6. Unneeded retransmissions by the sender in the face of large delays may cause a router to use its link bandwidth to forward unneeded copies of a packet.

5.3 Objective

Our objective in this thesis is to provide efficient data rate throughout the network operation, handling varying traffic rates. Congestion is main factor in degrading network throughput. To satisfy this objective we propose techniques to detect congestion, and take action to maintain a constant traffic rate. Our aim is to try and maintain network in an ideal state in which it will deliver maximum packets allowed by network bandwidth consistently. Initial step towards achieving this goal is to categorize packet loss and congestion types in wireless networks.

5.4 Congestion Detection

In our work we have proposed a congestion control technique. But accurate congestion detection is also equally important. AODV routing protocol is used to make a route from source to destination. To show congestion multiple sources to single destination are used, which results in path of common nodes and congestion may occur in that path. Before discussing the detail of congestion detection mechanism a light has been put on AODV protocol.

5.5.1 AODV

It is on demand protocol, when any node needs to send a message to sink then it broadcasts request to all nearby nodes which is broadcasted further if no destination node is found. At the destination acknowledgement message in form RREP is sent back following the same route from which it gets route request from source and source selects the minimum hopes path to send the message. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hopcount, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

5.5.2 Congestion detection algorithm

The congestion in path occurs only when a common path is shared by others. Figure 4.2 shows the single active source path to sink without congestion. Since those path is not shared by others so no congestion will occur until the data transmitted crosses the bandwidth limit of channel. This can be case of 'HELLO' message flood, a attack by intruders in the network.

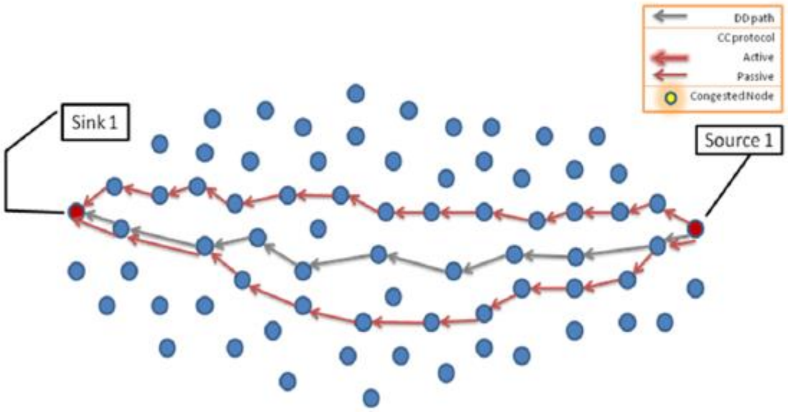


Figure 4.2: Scenario with a single source - single sink showing paths formed by AODV

Figure 4.3 shows the path shared by two sources. At node number 34 sharing of paths started as indicated by a blue circle in the figure. The channel bandwidth in WSN is always fixed and can't be altered so nodes have to transmit message within that limit. When message from source 1 is transmitted to destination and after same time source 2 transmits then it senses the path is already acquired by other and no space to transmit the new message to destination. It will wait for some moment at node 34, if this waiting time is high then source node may consider the loss of packets as no feedback from sink node is received within expected time and again new packet will be lost if path is still engaged.

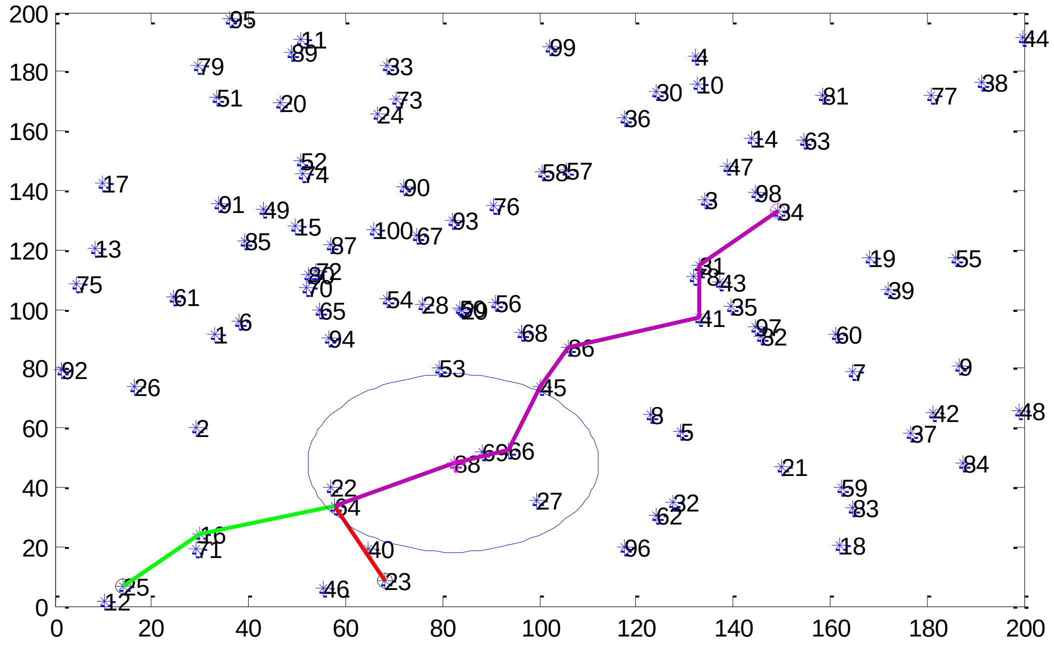


Figure 4.3: Common path for two sources to destination

So our algorithm will work on common node, in above case at node 34. Common node will keep a track of bandwidth usage of channel, when it receives message from other source then it will check for the space in the channel, if there is space to transmit the partial packets or all packets, then it will transmit otherwise hold the message upto a specified time, that time is called waiting time. The time of process is calculated by the following formula:

- $T_{min}= T_R + T_C + 3T_S + T_A$ (4.2)

- Where T_R = Time consumed on RTS
- T_C = time consumed on CTS
- T_S = SIFS period
- T_A = time consumed on data acknowledgement

6. RESULTS & DISCUSSION

We have considered two sources selected randomly and one common destination to show congestion in the path. Their two different paths are shown by green and red colored lines. We have taken care of no congestion condition too. It’s not mandatory that every time congestion occurs in the path. The condition for congestion is either data sent by source should exceed the channel bandwidth or waiting time should be more than threshold

7. CONCLUSION & FUTURE SCOPE

7.1 Conclusion

Initially in this thesis we prove that traffic bottlenecks is a major issue in WSNs and that queue formation starts very early when bottlenecks appear in the network. Thus, in order to avoid queue formation the data rate of the incoming flow must be severely reduced. In case that this action is omitted, buffer fill-up is going to happen, while the time that passes until the nodes’ buffers fill-up depends on the difference between incoming and outgoing flows. In order to solve this issue congestion control algorithms needs to be applied. These algorithms can be based either on traffic or resource control. According to the results of this paper, the traffic control method is an effective method for transient congestion occurrences but can be proven inappropriate when application needs all data to be transferred to sink. For this reason we base our proposed algorithms to the resource control method, a method that has not attracted a lot of interest due to the overhead that it creates. In this paper we addressed all possible problems that resource control methods may face and presented a novel algorithm.

7.2 Future Work

This research area is never ending area as due to sensor nodes battery constraint, researcher always try to develop algorithm which may consumes very less energy during transmission and reception as well as in detection mechanism executed on that. In our work we have not considered the energy concept at nodes, but in actual the congestion detection is done at node which takes energy of node in processing, decreasing the alive time of node. In future work, energy can be considered as a constraint in the algorithm as it may happen as with our case, after 50n seconds congestion detection, energy residual are not enough to send an alarm to source node about congestion in the path. That will increase the packet drop ratio.

REFERENCES

[1] S. Yin, and X. Lin, "MALB: MANET adaptive load balancing", In Vehicular Technology Conf. IEEE, Beijing, China, vol. 4, pp. 2843-2847, 2004.

[2] Heena Gupta, Deepak Goyal,"A Review On Congestion Control In Ad-Hoc Network" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014.

[3] S. Floyd and K. Fall, "Promoting the use of end-to-end congestion control in the internet" IEEE/ACM Transactions on Networking, 7(4), August 1999..

[4] BarkhaShakya,Deepak Kulhare," Investigation of TCP Congestion Control with Reliable Communication Technique in MANET",International Journal of Computer Applications,Volume 65– No.14, March 2013

[5] S.Sheeja, RamachandraV.Pujeri,"Cross Layer based Congestion Control Scheme for Mobile Ad hoc Networks" International Journal of Computer Applications, Volume 67– No.9, April 2013

[6] S.Sheeja, Dr.Ramachandra.V.Pujer,"Effective Congestion Avoidance Scheme for Mobile Ad Hoc Networks" I. J. Computer Network and Information Security, 2013

[7] L. Xia, Z. Liu, Y. Chang, P. Sun, "An Improved AODV Routing Protocol Based on the Congestion Control and Routing Repair Mechanism", Int. Conf. Communications and Mobile Computing, IEEE, China, 2009, vol. 2, pp. 259-262.

[8] AmandeepKaur, AashdeepSingh,"A Review on Ant Based Routing Protocols for Manet" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015

[9] H. M. El-Sayed, O. Bazan, U. Qureshi, M. Jaseemuddin" Performance Evaluation of TCP in Mobile Ad hoc Networks", Second International Conference on Innovation in Information Technology (IIT'05).

[10] V.Elamathi, D.Dhivya "To Avoid Congestion by Using Flooding Approach in Wireless Ad Hoc Networks", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[11] S. Floyd and K. Fall, "Promoting the use of end-to-end congestion control in the internet" IEEE/ACM Transactions on Networking, 7(4), August 1999.

[12] NishuGarg, R.P.Mahapatra "MANET Security Issues ", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[13] Anup W. Burange, PRMIT &R,Badnera,Dr. Vijay T. Ingole "Minimization of Congestion in Mobile Ad-Hoc Network ",International Journal of Advance Research

in Computer Science and Management Studies Research Paper Volume 1, Issue 7, December 2013.

[14] NaziaZaman, KaziChandrimaRahman, Syed Faisal Hasan " Explicit Rate-based Congestion Control for Multimedia Streaming over Mobile Ad hoc Networks", International Journal of Electrical & Computer Sciences IJECS -IJENS Vol:10 No: 04.

[15] S.Karunakaran&P.Thangaraj, "A Cluster Based Congestion Control Protocol For Mobile Ad hoc Networks", International Journal of Information Technology and Knowledge Management, July-December 2010, Volume 2, No. 2, pp. 471-474.

[16] ".GasimAlandjani and Eric E. Johnson, "Fuzzy Routing in Ad Hoc Networks" IEEE 2003

[17] S.Sheeja and Ramachandra.V.Pujeri, "Efficient Energy Based Congestion Control Scheme for Mobile Ad Hoc Networks", Journal of Theoretical and Applied Information Technology 10th June 2014. Vol. 64 No.1.