



Flow Deviation Congestion Control in Wireless Sensor Networks

Mohammed Ashraf.A¹
M.Sc. Computer Science,
VIT University, India

Sirajul Ameen.C²
M.Sc. Computer Science,
VIT University, India

Prabakaran.N³
Assistant Professor
VIT University, India

Abstract— *Wireless sensor network is an emerging area which is used in various application. As the nature of node its sense and send the data to the sink. This wireless sensor node leads to unpredictable load and congestion that collects an additional data then the forward which causes power devastate, throughput decrease and packet drop. Our proposal suggests a scheme called Flow Deviation Congestion Control which efficiently controls the congestion in the network. If any flow gets busy or leads to packet loss then Control message is created which consist of flow id, node id and destination id. It is forwarded further to the destination node which created the packet using the available free path in the network.*

Keywords- *Flow Deviation; Congestion Control; Control message; sink;*

I. INTRODUCTION

Wireless sensors nodes are widely used in variety of applications to observe physical and environmental conditions, node can be deployed anywhere in the sensing field. Some of the applications are battlefield surveillance, healthcare, object tracking and environment monitoring. Nodes are spatially scattered self-governing sensors that corporately pass their data to the sink. Nodes are accomplished for sensing, data forward and communicating components. Sensor nodes consist of built-in onboard processor that computes and broadcast only their necessary and partly processed data, sensor operate under idle to a detect event. When the event is detected then it is converted as information and passed to sink node then forwarded to base station, Node generalized as source and destination, source node send data to destination node through hop by hop infrastructure. Data flow leads to unpredictable load it causes congestion. Avoiding congestion in the network is bit difficult, but we can control them with various methods that proposed to control the congestion in wireless sensor network and some of them do not provide fairness among sensors to control the congestion. Our proposal called flow Deviation congestion control in Wireless Sensor Network which creates Control message when packet is dropped and sends control message to destination node using available free flow.

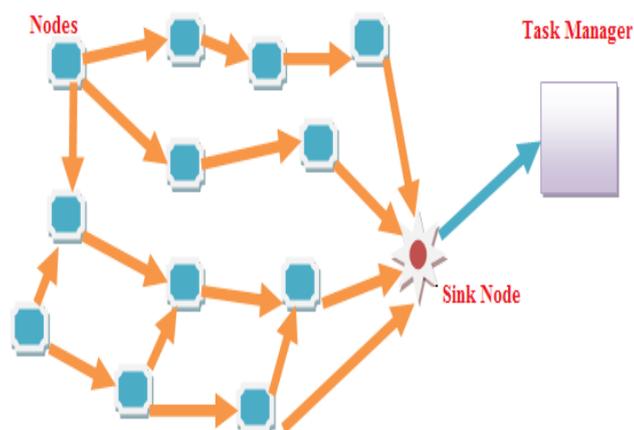


Figure 1 Wireless Sensor Network Model

II. RELATED WORKS

For congestion control many methods are proposed. F.stann and herdemann uses transport protocol which offer end to end reliability and use the method RMST (Reliable Multi segment transport protocol) it's a hop by hop delivery mechanism which recover lost packet by using cache in-between nodes using direct diffusion algorithm [4]. RMST give consistency but it is designed for advance nodes and also transmission rate is manually defined by the administrator.

O.Akan et al uses the method ESRT which is centralized congestion control scheme ESRT (Event sink reliable transport) allocates transmission rates for particular applications and receive their readings in base station which avoid congestion in a network [5]. Transmission rate is centrally computed which counts amount of gain sensor readings and reallocate the transmission rate for the sensor, this method is not sufficient for finest rate allotment. B.Hull et al proposed a method disturbed congestion control scheme which uses queue size to calculate the congestion level and integrate three methods hop by hop flow control, rate control and prioritized MAC [3]. This technique provide same transmission rate for all nodes in the network. Xiayon Yin et al proposed method FACC (Fairness aware congestion control) this method splits in-between node as near sink and near source node [2]. Near source node maintain a pre flow and near sink node uses Probabilistic dropping algorithm by calculating hit frequency. As we see near source node if congestion occur in an intermediate node this scheme force to slow down the generating rates of source nodes by using available bandwidth [2]. But existing bandwidth and traffic weight are time varying so they uses busyness ratio, threshold value and also estimating the existing bandwidth, comparison of received flow rate, estimation of the number of active flow and transmission control [2]. The disadvantage is difficult to calculate every flow for every time because the data generated frequently when event is detected so this is difficult to implement in real time. Another one we have near sink node it uses stateless Fair Queue Management mechanism this mechanism uses two threshold value Q_l and Q_h [2]. The hit frequency $h(t)$ is calculated by identifying the packet which belongs to same flow of one of the randomly chosen packet in the buffer. If arrived packet and randomly taken packet are belonging to same flow the hit frequency increased by one using this we can assume that huge amount of data exist in the particular flow [2]. The disadvantage of this is it only checks for a particular flow and also generate rate and bandwidth are time varying. Another method is hop by hop backpressure which creates a WM message where packet is drop and send this message back to the nearest source node the message contain flow id and node id and the near source node compute and assign the approximately fair rate share for every passing path by using the threshold value Q_h and Q_l [2]. The disadvantage in this while sending warning message back to the near source at the time also it leads to congestion because they flow is busy. Another Technique is fairness of the stateless queue management mechanism this mechanism makes comparison whether they arrived packets have to admit or dropped and the comparison can be done using threshold values Q_l and Q_h [2]. If the buffer occupancy is smaller than Q_l incoming data is admitted if the buffer use is among Q_l and Q_h each arrived packet is evaluate with randomly selected packet form buffer where the dropping probability depend on the calculated hit frequency if the buffer occupancy is greater than Q_h then arriving packet is drop [2]. This mechanism is suitable for more capable sensor nodes.

III. PROBLEM AND MODEL COMMUNICATION

In sensing environment, nodes are used to detect various events like temperature monitoring, army surveillance, habitant monitoring etc. Normally the sensor nodes are idle as the event detected the nodes generate data and the generated data frequently transmitted to the main node called sink. Depend on the transmission rate many nodes send data to the sink, at the same time increases the network load and it leads to congestion which decreases the performance of the network which includes packet loss throughput reduction.

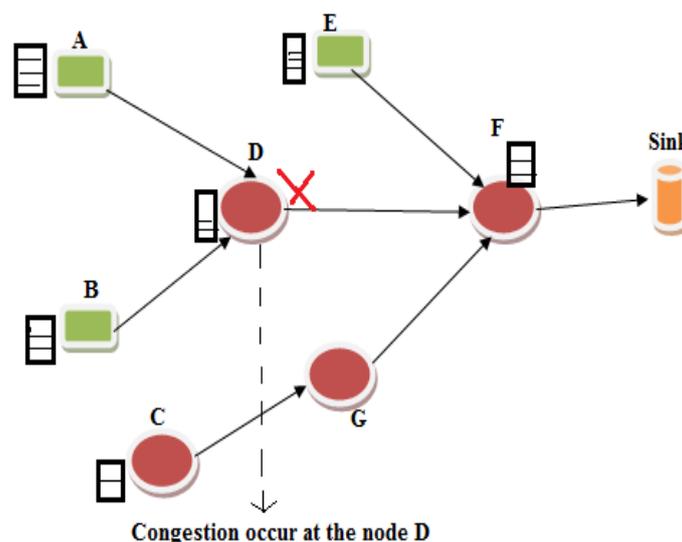


Figure 2 Congestion model for node level

In the Figure 2 the Nodes are deployed in the sensing field to detect an event the node A,B and E are source node .The data generated by this node have to pass through the neighbouring nodes to sent the data to base station that is sink node. Whenever the data is generated it store in the temporary buffer in queue format. Basically the traffic will be high near the sink and it's depending on Bandwidth and transmission rate. The node A, B, and E are idle when they sense an event data are generated and starts to transmit through the neighbouring to pass sink node. In the Fig.2 Node A node B has to pass through node D which is a neighbour node. Basically the nodes have limited storage capacity if the both nodes send

simultaneously to the node D the traffic will increase. For example the node A detect an event and generate data of size 3kb and the node B generate data of 3kb and the capacity of node D is 3 kb while receiving the data from those nodes it will store in its temporary buffer and if the node D caring huge data in the queue then its lead to packet loss and decrease the quality of service.

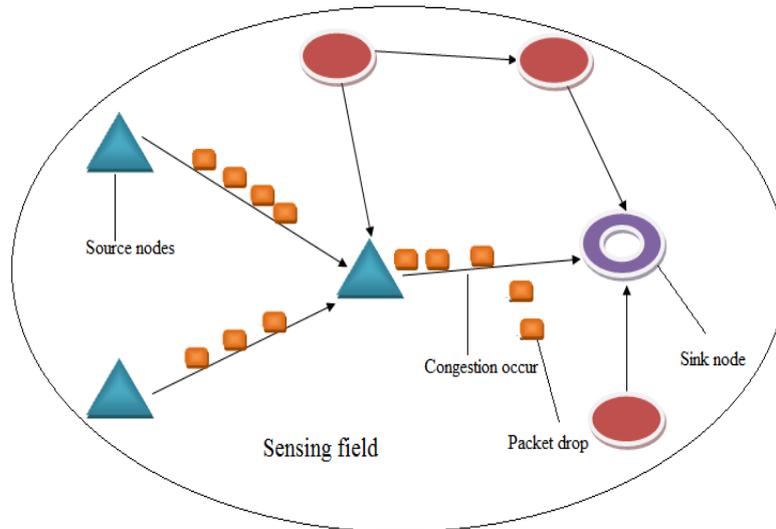


Figure 3 Congestion Model for Flow level

In the Figure 3 source nodes generate the packets and send to the nearest node .In the triangle shapes are source node and circle is a sink node. Each node generate at particular transmission rate. If the transmission rate is less then are equal to the bandwidth of the Network then no congestion will occur. If the transmission rate increases then the bandwidth congestion will occur and hence it will leads to packet loss are throughput reduction which decreases the quality of service. So we have to find that flow and have to control that both Transmission rate and bandwidth are time varying so it's difficult manage the transmission rate

IV. FLOW DEVIATION CONGESTION CONTROL

A. Logical Design

In this proposed design sensing nodes are deployed in field which includes base station called sink node. The red colour nodes are source node, blue colour nodes are sensor node which is in idle position and violet colour node is sink node which is base station. As the event detected by the particular node, it generates data and passes it to the neighbouring node. This neighbour node forward the data to the next neighbour node like that it pass until it reach to the sink node while passing if any of flow is busy then it will start dropping the packets.

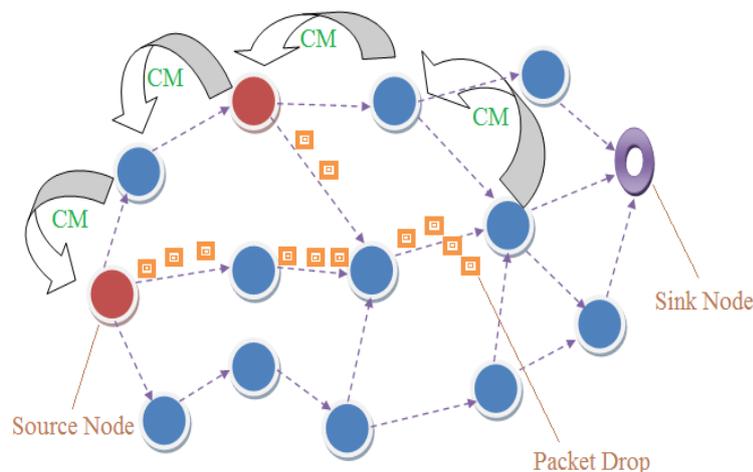


Figure 4 Flow Deviation Congestion Control Model

To avoid this we proposed scheme called Flow deviation congestion control this creates a control message in the node where packet is drop. This control message contains three fields Flow id, node id and destination id. Flow id is the id of busy flow and node id is an id where packet is drop.

Algorithm:

- Step 1: Identify the usual routing flows available and let it be α .
- Step 2: Based on hop and node ID available in the dropped packet, pick up the busy paths $k*\alpha$.
- Step 3: select an alternative path or traffic free path (μ) to send warning message for a particular source node from the available α -($k*\alpha$).
- Step 4: Identify the number of nodes available from $n*\mu$.
- Step 5: Compare and find minimal number of nodes existing path from $n*\mu$.
- Step 6: set the destination address and forward the warning messages through the identified new traffic free flow.

This Control message has to pass back to the source node where packet is generated. If we send control message back through the busy flow then it meaningless, because again it increases the congestion. So we have to send the control message through available free routing flow. We can find this available free routing flow using busy flow and overall available routing flow. Using this information source node gets aware of busy path so that it can divert forwarding data in some other flow.

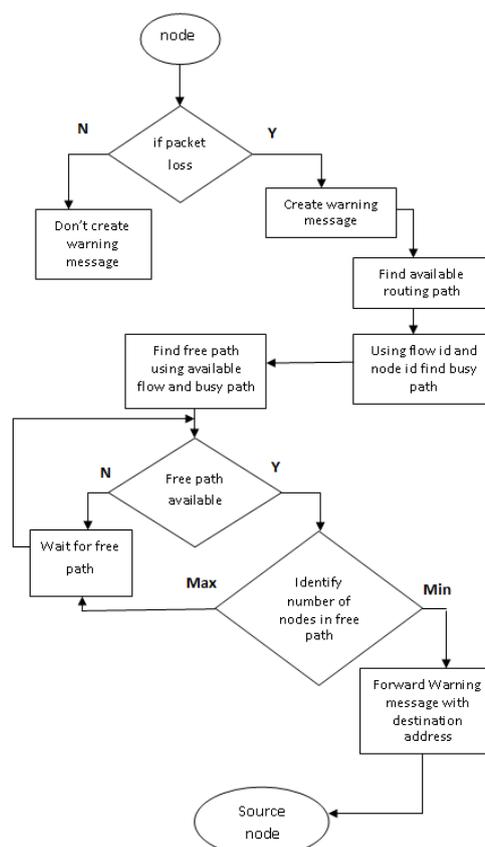


Figure 5 Flow Chart for Flow Deviation Congestion Control

If the packet is dropped by the node, create a control message and find the available routing flow using this available routing flow we can identify the busy flow and free flow. Next we have to find minimal number node in a particular free flow to send this control message to the source node. By getting this information the source node get aware of busy path flows and it pass packet to neighbour nodes by using control message.

V. PERFORMANCE VALUATION

A. Performance metrics

Control message is propagated when congestion is occurred. This message consists of information about node id and flow id. It creates a control message and passes through the node with three fields such as node id, flow id and destination id to the source node. To do this so, find the available free path and identify them. The queue is preserve if the received packets contain larger number of packets, it is specify as

$$\mu n = \begin{cases} n\mu, & n < s \\ s\mu, & n > s \end{cases}$$

Identify the number of packets in the flow or the busy flow path (M/M/1) is

$$P_n = \left(\frac{\lambda_0}{\mu_0}\right)^n \cdot P_0 \quad \text{where } P_0 = (1 - \rho)$$

P_0 indicates the free path which means fewer packets in that flow.

$$P_n = \begin{cases} \frac{1}{n!} \left(\frac{\lambda}{\mu}\right)^n P_0, & n < s \\ \frac{1}{s!} (s)^{n-s} \left(\frac{\lambda}{\mu}\right)^s P_0, & n \geq s \end{cases}$$

Where,

$$P_0 = \left[\sum_{n=0}^{s-1} \frac{1}{n!} \left(\frac{\lambda}{\mu}\right)^n + \frac{1}{s!} \left(\frac{\lambda}{\mu}\right)^s \frac{s\mu}{s\mu - \lambda} \right]^{-1}$$

Using the above equation, the network performance can be work out by using the term called waiting time that means lengthy data should be waiting in the flow to get the service. The waiting model can be determined by

$$W_q = \frac{\lambda}{\mu} + L_q$$

Where,

$$L_q = \frac{\lambda^2}{\mu(\mu - \lambda)}$$

L_q refers of data in the flow. The congestion can be considered as L_q , it plays the role for determine the congestion in the sensor network. Likewise the mean waiting time is determined by,

$$W_q = \frac{L_q}{\mu}$$

Where L_q is,

$$L_q = \left(\frac{\left(\frac{\lambda}{\mu}\right)^{s+1}}{s \cdot s! \left(1 - \left(\frac{\lambda}{\mu s}\right)^2\right)} \right) P_0$$

VI. CONCLUSION

This method can be projected to standardize the quantity of packet in between the node and control congestion flow level in Wireless sensor networks. It accomplishes sensible fair packet rate and impresses the results of prior results. This model results gain performance in terms of data transfer, data loss and power saving. The scheme is responsible for reducing data loss when flow load is full. This scheme increases network performance and also gains the speed of packet transmission in between the sensor nodes and source nodes.

REFERENCES

1. Ian F. Akyildiz, W. Su, Y. Sankaransubramaniam, and E. Cayirci, "A Survey on Sensor Networks" *IEEE Communication Magazine*. Vol. 40, no. 8, pp. 102-104, August. 2002.
2. Xiaoyan yin, Xingshe zhou, Rongsheng Huang, Yuguang Fang and Shining Li, "A Fairness aware congestion control scheme in wireless sensor network", *IEEE Transactions on Vehicular Technology*, vol., 58, No 9, November 2009.
3. B. Hull, K. Jamieson, and H. Balakrishnan "Mitigation congestion in wireless sensor networks," in Proc. 5th ACM conference. Embedded network sensys, Baltimore, Md, November. 2004, pp. 134-147
4. F. Stann and J. Herdemann, "RMST: Reliable data transport in sensor networks," in Pro. 1st IEE Workshop SNPA, Anchorage, AK, Nov. 2003, pp. 102-112.

5. Y. Sakarasubramaniam, O. Akan, and I.F. Akyildiz, "ESRT: Event-to Sink reliable transport in wireless sensor networks," in *Proc. 4th ACM Int. Symp. Mobile ad hoc network. Comput. MobiHoc, Annapolis, Md, Jun. 2003*, pp.177-188.
6. N. Prabaharan, k. Geetha and K. Janani, "Data Propelling Scheme for Node level Congestion Control in Wireless Sensor Networks," in *IEEE- International Conference on Advances in Engineering, Science and Management (ICAESM-2012) March 30, 31, 2012*
7. S. Hedetniemi, A. Lies tman, "A Survey of Gossiping and Broadcasting in Communication Networks," *Networks*", vol. 18, 1988.
8. Vievk Deshpande, Prachi Sarode and Sambhaji Sarode,"EDCAM -Early Detection Congestion Avoidance Mechanism "International Jouranl of Computer Application 7(2)11-14, Number 18, Article 6.
9. C.Y. Wan, S. B. Eisenman and A.T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," *IEEE Trans Mobile Comput. Vol 6, no 7. Pp, Jul. 2007*.
10. N.Prabaharan, B.Shanmugaraja, R.Prabaharan, V.R.Sarma Dhulipala "Rate optimization scheme for node level congestion in WSNs", on *JCDeCom. 2011. 5738548, pages (1-5) in IEEE 2011*.
11. J. Kulik, W. Rabiner, and H. Balakrishhan, "Adaptive protocols for information dissemination in wireless sensor networks." In *Proc, ACM MobiCom, Seattle, WA, Aug. 1999*, pp.174-185.
12. S. Kim, R. Fonseca, P.Dutta, and A. Tavakoli, "Flush: A reliable built transport protocol for multihop wireless networks," *proc. 5th Acm Conf. Embedded Network. Sensys, Sydney, Australia, Nov. 2007*, pp. 351-365.
13. N. Prabaharan et.al on, "Fusion Centric Decision Making for Node Level Congestion in Wireless Networks" *Journal on Springer 2014*.