ISSN No. 0976-5697

Volume 2, No. 6, Nov-Dec 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Study of Techniques to Avoid Congestion in Wireless Sensor Networks

Seyed Mojtaba Salari[*]
Department of Computer Science and Engineering
Islamic Azad University of Qazvin
Qazvin, Iran
Salari.sm@gmail.com

Fazlollah Adibniya
Department of Computer Science and Engineering
yazd University
yazd, Iran
fadib@yazduni.ac.ir

Mohammad Javad Fattahi
Department of Computer Science and Engineering,
Islamic Azad University of Qazvin
Qazvin, Iran
mjfattahi@gmail.com

Abstract: In wireless sensor networks (WSNs), congestion may bring about degradation of overall channel quality and increased loss rates, leads to buffer drops and enlarged delays, and tends to be disgustingly unfair toward nodes whose data has to traverse a larger number of hops. Provisioning a WSN so that congestion is an infrequent occasion is quite challenging task. This paper presents a performance comparison study focusing the most relevant congestion control transport protocols for wireless sensor networks.

Keywords: Wireless sensor networks; transport protocols; congestion control protocols; performance.

I. INTRODUCTION

Nowadays, wireless sensor networks (WSNs) are widely used among people and for many situations they provide the facility to collect and process information. These networks were borne in military environment and came to the common every day life environments. WSNs may be composed by thousands of small node devices generally with sensing capabilities. A WSN can congregate are a group of sensors and sinks that are deployed for a wide range of geographical areas, from small areas (as offices) to a large area as natural parks. These networks can be used in human body (called body sensor networks), inaccessible environments, in catastrophe situation as big storms, hurricanes, and in war scenarios. Sensors are the most important components in these networks. This small device senses physical information, and reports to the sink for processing and storage it. The main features that it is desired to make attention in WSNs are network topology, traffic over the network, small message size, external variants and the sensor energy.

In WSNs it is necessary to use several types of protocols [1]. Physical layer protocols is responsible for collecting data, while Data Link Layer specifically a MAC (Medium Access Control) layer for transferring data between network entities as well as detecting and possibly correcting errors occurred in the lower layer. Network Layer is responsible for transferring variable length data sequences from a source to a destination, and finally Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.

In WSNs, congestion may cause degradation of overall channel quality and increased loss rates, leads to buffer drops and enlarged delays, and tends to be disgustingly unfair toward nodes whose data has to traverse a larger number of hops. Provisioning a WSN such that congestion is an infrequent occasion is quite challenging task.

This paper focuses on congestion control transport protocols for WSNs. These protocols are responsible for keep a smooth communication and without interruptions that can be caused by a congestion problem. The congestion can occur in many ways like inoperability of a node and a very high rate transmission. The rest of paper is organized as follows. Section II reviews Architecture of Wireless Sensor Network while Section III presents a list of several protocols that was study. Section IV evaluates the protocols referred. Section V presents network layer protocols and Finally, Section VI concludes the paper and point directions for further research works.

II. ARCHITECTURE OF WIRELESS SENSOR NETWORK

Figure1 gives the architecture of a two-tier cluster-based sensor network. There are three types of nodes in the network, namely, micro-sensor nodes (MSNs), aggregation and forwarding nodes (AFNs), and a base-station (BS). The MSNs can be application specific (e.g., temperature sensors, pressure sensors, video sensors, etc.). They are deployed in groups (or clusters) at strategic locations for surveillance or monitoring applications. For each cluster of MSNs, there is one AFN, which serves as clusterhead.

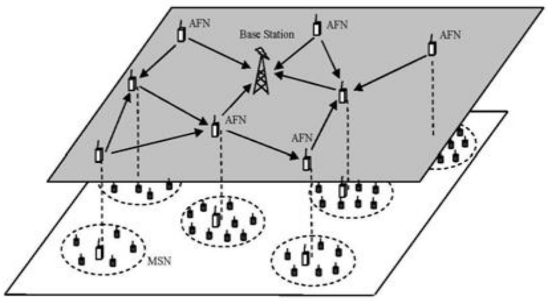


Figure.1 Architecture of a hierarchical sensor network

The MSNs are responsible for sending the collected data to the local AFNs. We assume that each MSN communicates directly with the AFN in its cluster. So MSNs do not have the responsibilities of relaying data. An AFN processes the data streams it receives from the MSNs within the cluster. Data aggregation (or "fusion") is necessary in sensor networks to reduce the amount of data transmitted to the base station. This is possible because a sensor network is data centric.[3]

III. TECHNIQUES FOR DETECTING AND CONTROLLING CONGESTION

This section covers the various congestion techniques the provide reliable data delivery from destination to source or source to destination or base communication and providing congestion control to reduce the packet loss at intermediate nodes.

A. CODA (Congestion Detection and Avoidance):

Among the many transport protocols based on congestion control detection, CODA [4] as the name suggests is protocols that continuously detect any kind of congestion and how to avoid it. This protocol is composed by three mechanisms:

Receiver-based congestion detection, a mechanism that plays an important role in the work done by this protocol because it is the mechanism responsible for detecting congestion.

Open-loop, hop-by-hop backpressure, which permits from all previous nodes to know if there is still congestion. This mechanism works with a looping message that only finishes when the congestion ends.

Close-loop, multi-source regulation is the mechanism that regulates the congestion. Like all protocols, CODA also needs a good mechanism to detect congestion, because the process of congestion control needs much energy for the energy-aware sensors and they need to use a method of this type only that is necessary.

For these there are several techniques that are used to detect congestion, the queue length is one of the mechanisms. The load of the transmission channel is another method used to detect congestion. There is always the approximate information of the availability of the transmission channel to receive more data. When there is an overload a message of congestion notification is sent. This mechanism has a limitation in WSNs because each node is always listening when the channel is overloaded and causing a very large spent of energy.

The congestion detection method most used in WSNs is the report of reception data rate. This mechanism works as follows, the base station expects to receive packets with a certain range if the value is below the know value means that a package was lost; otherwise it sends a warning message to indicate that transmission rate is very high. For this there are measures as the waiting time between sending packets from the source to the destination.The backpressure mechanism is a fast and effective method when congestion occurs. When congestion is detected the receiver node where congestion occurred sends a message to all neighboring nodes to indicate that no more blocks of data to send until they receive an indication to resend more data. The nodes send the message to next nodes to stop sending of data packets. *Depth of congestion* indicates the number of nodes that the backpressure message has traversed before a non-congested node is encountered.

B. ESRT (Event-to-Sink Reliable Transport):

ESRT protocol [5] is developed for reliable event detection with minimum energy expenditure. ESRT uses a congestion control mechanism to reduce energy consumption while maintaining the desired reliability level at the sink. ESRT algorithm is run mainly at the sink. The sink computes the reliability factor and reporting frequency at each interval. The reliability factor is a measure of the data packets received from the source nodes to the sink. The computed reliability factor is compared against an application-defined desired reliability. If the computed reliability is greater than the desired reliability, ESRT would reduce the reporting frequency of the source nodes. If the computed reliability is lower than the desired reliability, ESRT would increase the reporting frequency of the source nodes to achieve the desired reliability. At each interval, the sink broadcasts the new reporting frequency to source nodes in the network. Upon receiving the information, source nodes adjust their reporting rate. In ESRT, the congestion control mechanismis based on monitoring the routing buffer of each sensor nodes. A sensor node whose buffer overflows is an indication of congestion. Upon experiencing congestion, the sensor node sets the congestion notification bit flag in its outgoing packets. The sink receiving these packets along with the computed reliability factor determines the state of the network and acts accordingly. Simulation results show that ESRT is able to attain the desired reliability level with minimum energy expenditure under different network states with random and dynamic topologies.

C. PSFQ (Pump Slowly, Fetch Quickly):

PSFQ [6] is a reliable transport protocol that is scalable and robust. The goals of PSFQ are to guarantee data segment delivery, minimize the number of transmission for lost detection and data recovery operation, to operate in harsh environments, and to provide a loose delay bound for data delivery. PSFQ operates in three functions: pump operation, fetch operation, and report operation. The pump operation controls the rate at which data packets are passed along into the network.

The pump operation is based on a simple scheduling scheme which used two timers, Tmin and Tmax. A node must wait at least Tmin before transmitting a packet. By waiting at least Tmin, a node is given the opportunity to recover missing packets and reduce redundant broadcasts. Tmax is used as a loose upper delay bound for when all packets should be received. The fetch operation is called when there is a gap in the sequence number between the packets received. The fetch operation requests a retransmission of the lost packet from the neighboring nodes. If multiple packets are lost in a bursty event, a single fetch would be sent to retrieve the packets. Lastly, the report operation provides a feedback status to the users. A status report message travels from the farthest target node in the network to the requesting user. Along the path, each node appends its report message in an aggregated manner into the original message. Results show that PSFQ outperforms the idealized scalable reliable multi-cast (SRM-I) [5] in terms of tolerance, communication overhead, and delivery latency.

D. GARUDA:

GARUDA [2] is a reliable downstream data delivery transport protocol for WSNs. It addresses the problem of reliable data transfer from the sink to the sensors. Reliability is defined in four categories: (1) guarantee delivery to the entire field, (2) guarantee delivery to a subregion of sensors, (3) guarantee delivery to a minimal set of sensors to cover the sensing region, and (4) guarantee delivery to a probabilistic subset of sensors. GARUDA’s design is a loss-recovery core infrastructure and a two-stage NACK-based recovery process. The core infrastructure is constructed using the first packet delivery method. The first packet delivery method guarantees first packet delivery using a Wait-for-First-Packet (WFP) pulse. WFP pulse is a small finite series of short duration pulses sent periodically by the sink. Sensor nodes within the transmission range of the sink will receive this pulse and wait for the transmission of the first packet. The first packet delivery determines the hop-count from the sink to the node. Nodes along the path can become candidates for the core. A core candidate elects itself to be a core node if it has not heard from neighboring core nodes. In this manner, all core nodes are elected in the network. An elected core node must then connect itself to at least one upstream core node.

GARUDA uses an out-of-order forwarding strategy to overcome the problem of under-utilization in the event of packet losses. Out-of-order forwarding allows subsequent packet to be forwarded even when a packet is lost. GARUDA uses a two-stage loss-recovery process. The first stage involves core nodes recovering the packet. When a core node receives an out-of-sequence packet, it sends a request to an upstream core node notifying that there are missing packets. The upstream core node receiving that message will respond with a unicast retransmission of the available requested packet. The second stage is the non-core recovery phase, which involves non-core nodes requesting retransmission from the core nodes. A non-core node listens on all retransmissions from its core node and waits for completion before sending its own retransmission request.

E. SenTCP:

SenTCP [8] is an open-loop hop-by-hop congestion control with few special features. It jointly uses average local packet service time and average local packet inter-arrival time to estimate current local congestion degree in each intermediate node. In SenTCP, nodes avoid congestion by issuing periodic feedback signals to adjust the reporting rate of their upstream nodes depending on local buffer status. The use of hop-by-hop feedback control can remove congestion quickly and reduce packet dropping, which in turn conserves energy.

F. Price-oriented reliable transport protocol (PORT):

PORT [9] minimizes energy consumption, achieves the necessary level of reliability, and provides a congestion-avoidance mechanism. PORT minimizes energy consumed by avoiding high communication cost. End-to-end communication cost is the measure of the amount of energy consumed to deliver a packet from the source to the base station (sink). To achieve the necessary level of reliability and minimize energy, the source’s reporting rate is dynamically adjusted in a bias manner. PORT provides an in-network congestion mechanism to alleviate traffic dynamically. PORT differs from other transport protocols in that its view of reliability is not a ratio of the total incoming packet rate to the desire incoming rate, but the assurance that the sink obtains enough information on the phenomenon of interest. When a phenomenon of interest occurs, nodes closer to the phenomenon will contain more information and less error. PORT adapts bias packet reporting rate of the sensor nodes to increase the sink’s information regarding the phenomenon. PORT provides two mechanisms that ensure this reliability.

The first is a dynamic source report rate feedback mechanism to allow the sink to adjust the reporting rate of each data source. Each packet sent by the source is encapsulated with its node price. Node price is the total number of transmission attempts made before a successful packet is delivered from the source to the sink. It is a metric used to evaluate the energy cost of the communication.

The sink adjusts the reporting rate of each source based on the source’s node price and the information provided about the physical phenomenon. Feedback from the sink is sent to the sources along the reverse path. The second mechanism provides the sink with end-to-end communication cost information from the source to the sink End-to-end communication cost is used to alleviate congestion. When congestion occurs, communication cost increases with respect to packet loss. The sink uses the communication cost information to slow down the reporting rate of the appropriate source and increase the reporting rate of other sources that have lower communication cost since reliability must be maintained.

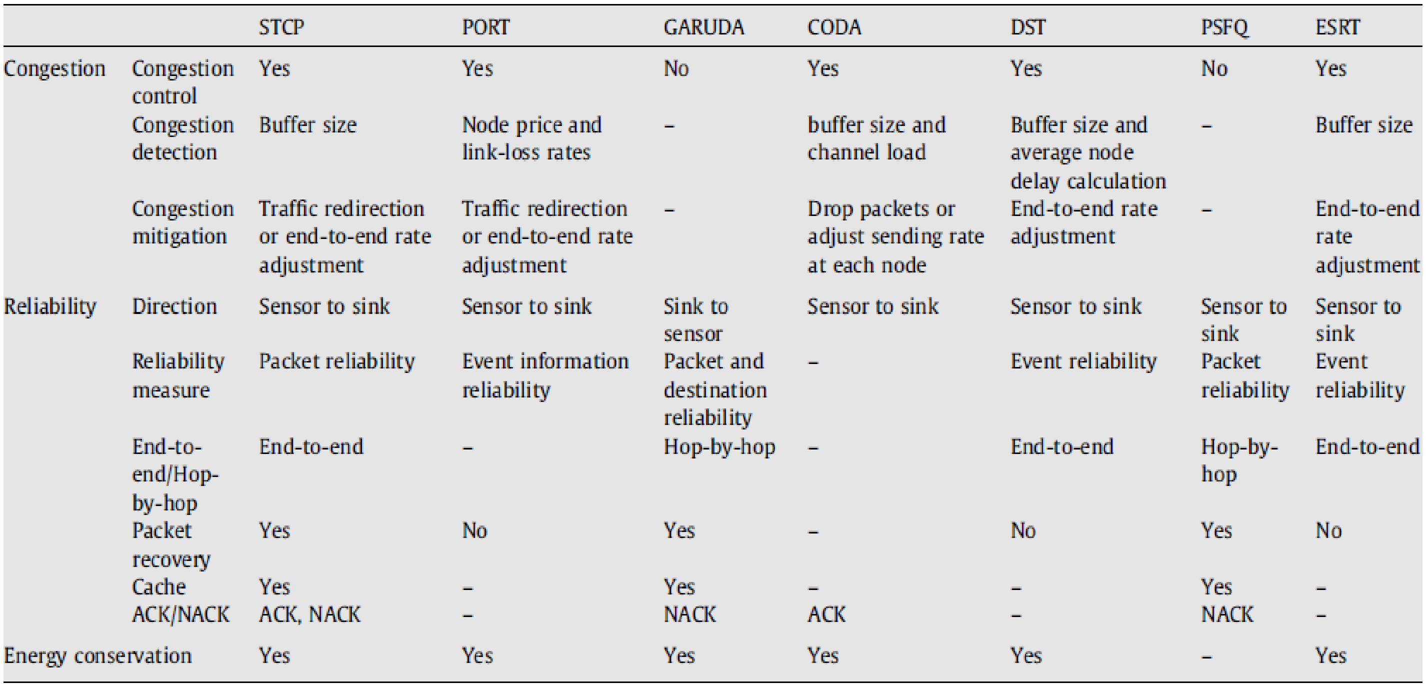
G. Delay sensitive transport (DST):

DST protocol [10] addresses the issue of congestion control, reliability, and timely packet delivery. DST has two components: a reliable event transport mechanism and a real-time event transport mechanism. Reliable event transport mechanism measures the observed delay-constrained event reliability against the desired delay-constrained event reliability to determine if appropriate action is needed to ensure the desire reliability level for event-to-sink communication. The observed delay-constrained event reliability is defined as the number of packet received within a certain delay bound at the sink over a specified interval. The desired delay- constrained event reliability is the minimum number of data packets required for the event to be a reliable detection. If the observed delay-constrained event reliability is greater than the desire delay-constrained event reliability, the event is considered to be reliable. Otherwise, the report rate of the sensors must be increased to assure that the desired reliability level is met. DST also assures reliable and timely event detection within the event-tosink delay bound. The real-time event transport mechanism uses this event-to-sink delay bound delay to achieve the application specific objectives. The event-to-sink delay is a measure of the event transport delay and event process delay. Event transport delay is the time between the event occurring and when the sink receives it. Event process delay is the processing delay at the sink. For congestion detection, DST measures buffer overflow at each node and computes the average node delay. Upon congestion, sensor nodes inform the sink of the congestion situation. The sink in response would adjust the reporting rate of the sensors. Simulation experiments show that DST achieves reliability and timely event detection with minimum energy consumption and latency.

IV. COMPARISON BETWEEN VARIOUS CONGESTION CONTROL TECHNIQUES

In this section we make a comparison between the performances of the various congestion control techniques.

Table 1:Comparison of transport layer protocols for WSNs



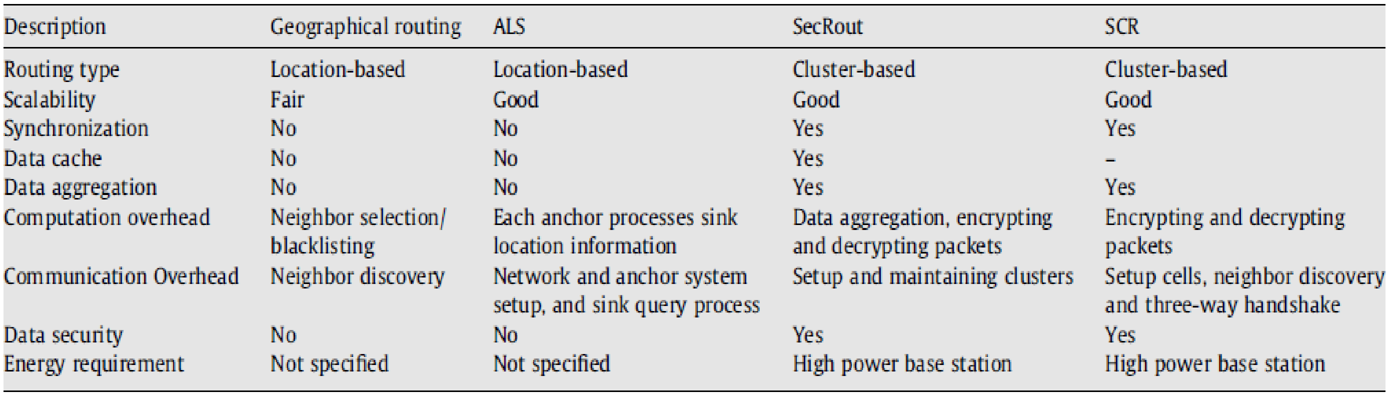
		STCP	PORT	GARUDA	CODA	DST	PSFQ	ESRT
Congestion	Congestion control	Yes	Yes	No	Yes	Yes	No	Yes
	Congestion detection	Buffer size	Node price and link-loss rates	–	buffer size and channel load	Buffer size and average node delay calculation	–	Buffer size
	Congestion mitigation	Traffic redirection or end-to-end rate adjustment	Traffic redirection or end-to-end rate adjustment	–	Drop packets or adjust sending rate at each node	End-to-end rate adjustment	–	End-to-end rate adjustment
Reliability	Direction	Sensor to sink	Sensor to sink	Sink to sensor	Sensor to sink	Sensor to sink	Sensor to sink	Sensor to sink
	Reliability measure	Packet reliability	Event information reliability	Packet and destination reliability	–	Event reliability	Packet reliability	Event reliability
	End-to-end/Hop-by-hop	End-to-end	–	Hop-by-hop	–	End-to-end	Hop-by-hop	End-to-end
	Packet recovery	Yes	No	Yes	–	No	Yes	No
	Cache	Yes	–	Yes	–	–	Yes	–
	ACK/NACK	ACK, NACK	–	NACK	ACK	–	NACK	–
Energy conservation		Yes	Yes	Yes	Yes	Yes	–	Yes

V. NETWORK LAYER PROTOCOLS

Many routing protocols have been proposed for routing data in sensor networks. Table 2 summaries the characteristics of routing protocols covered in this survey. Important considerations for these routing protocols are energy efficiency and traffic flows. In this review, two categories of routing approaches are explored: location-based routing and cluster-based routing. Location-based routing considers node location to route data. Cluster-based routing employs cluster heads to do data aggregation and relay the information to the base station. A comparison of security routing protocol is also included in the table. A security routing protocol strives to meet security requirements to guarantee secure delivery of the data from the source to the destination.

Future research issues should address security, QoS, and node mobility. Experimental studies regarding security applied to different routing protocols in WSNs should be examined. There is little research in QoS routing in sensor networks. QoS guarantees end-to-end delay and energyefficient routing. In applications where sensor nodes are mobile, new routing protocols are needed to handle frequent topology changes and reliable delivery.

Table 2 :Comparison of network layer protocols for WSNs



Description	Geographical routing	ALS	SecRout	SCR
Routing type	Location-based	Location-based	Cluster-based	Cluster-based
Scalability	Fair	Good	Good	Good
Synchronization	No	No	Yes	Yes
Data cache	No	No	Yes	–
Data aggregation	No	No	Yes	Yes
Computation overhead	Neighbor selection/ blacklisting	Each anchor processes sink location information	Data aggregation, encrypting and decrypting packets	Encrypting and decrypting packets
Communication Overhead	Neighbor discovery	Network and anchor system setup, and sink query process	Setup and maintaining clusters	Setup cells, neighbor discovery and three-way handshake
Data security	No	No	Yes	Yes
Energy requirement	Not specified	Not specified	High power base station	High power base station

VI. CONCLUSION

Wireless sensor networking is an emerging technology that promises a wide range of potential applications in both civilian and military areas, and has therefore received tremendous attention from both academia and industry in recent years. Depending on the application, the large amount of correlated synchronized impulses of data sends to a small number of nodes. This high generation of data packets is usually uncontrolled and results in network congestion. In this paper, we presented a comprehensive survey of congestion control technique in wireless sensor network.

They have the common objective of trying to prolong the lifetime of the wireless sensor networks. We also show the comparison between the performances of the various congestion control techniques .

VII. REFERENCES

[1]. C. Mallanda, A. Suri, V. Kunchakarra, S. S. Iyengar, R. Kannan, and A. Durresi, "Simulating Wireless Sensor Networks with OMNeT++," LSU Simulator, 2005.

[2]. Performance Assessment of Congestion Control transport Protocols for Wireless Sensor Networks, David M. Monteiro, Binod Vaidya, Joel J. P. C. Rodrigues,Conference of Wireless sensor network, 2010

[3]. A Study on Prolong the Lifetime of Wireless Sensor Network by Congestion Avoidance Techniques Pooja Sharma, Deepak Tyagi, Pawan Bhadana,International Journal of Engineering and Technology Vol. 2(9), 2010, 4844-4849

[4]. C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, CODA: Congestion detection and avoidance in sensor networks," in Proceedings of ACM Sensys'03, November 5-7, 2003, Los Angeles, USA.

[5]. Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyidiz, "ESRT: Event-to-sink reliable transport in wireless sensor networks," in Proceedings of ACM Mobihoc'03, June 1-3, 2003, Annapolis, USA.

[6]. C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, "PSFQ: A reliable transport protocol for wireless sensor networks," Proc. First ACM Intl. Workshop on Wireless Sensor Networks and Applications (WSNA '02), Atlanta, GA, 2002, pp. 1–11

[7]. S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," Proc. of ACM MobiHoc '04, May 24-26, 2004, Roppongi, Japan.

[8]. C. Wang, K. Sohraby, and B. Li, "SenTCP: A hop-by-hop congestion control protocol for wireless sensor networks," in Proceedings of IEEE INFOCOM 2005 (Poster Paper), Miami, Florida, USA, Mar. 2005.

[9]. Y. Zhou, M.R. Lyu, PORT: a price-oriented reliable transport protocol for wireless sensor network, in: Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (ISSRE),Chicago, IL,2005.

[10]. V.C.Gungor,O.B. Akan, DST: Delay sensitive transport in wireless sensor networks, in: Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN), 2006, pp. 116–122.

[11]. Wireless sensor network survey, Jennifer Yick , Biswanath Mukherjee, Dipak Ghosal, journal of Computer Networks, Elsevier 2008

[12]. Wireless Sensor Network Simulators: A Survey and Comparisons, Harsh Sundani, Haoyue Li, Vijay Devabhaktuni, Mansoor Alam, Prabir Bhattacharya, International Journal Of Computer Networks (IJCN), 2011