2010 International Conference on Broadband, Wireless Computing, Communication and Applications

Wireless Sensor Networks: Challenges Ahead

[1]A. J. Dinusha Rathnayaka , [2]Vidyasagar M. Potdar
Digital Ecosystems and Business Intelligence Institute
Curtin University of Technology
Perth, Western Australia
[1]abekoon.rathnayaka@postgrad.curtin.edu.au,
[2]v.potdar@curtin.edu.au

[3]Atif Sharif, [4]Saeed Sarencheh, [5]Samitha Kuruppu
Digital Ecosystems and Business Intelligence Institute
Curtin University of Technology
Perth, Western Australia
[3]atif.sharif@postgrad.curtin.edu.au,
[4]sarencheh@gmail.com, [5]kjayamal@gmail.com

***Abstract*— The aim of this paper is to analyze the different Wireless Sensor Network (WSN) transport protocols by identifying various experimental parameters in order to undertake a comparative evaluation. To build the groundwork, we first discuss the generic design for a transport protocol based on three key concepts; congestion control, reliability support and priority support. The basis of this design was developed by assessing several aspects of numerous transport protocols. However they all using different set of parameters and settings and hence it is difficult to benchmark one against the other. In this paper, we discuss the simulation settings like packet size, number of exploited sensors and their distribution in the field, buffer size, coverage area and power levels.**

Keywords- Wireless Sensor Network; Transport protocol; Reliability; Congestion control; Priority

I. INTRODUCTION

Wireless Sensor Network (WSN) [1] is comprised of tiny embedded devices termed as "motes" that has inbuilt features for sensing, processing and communicating information over wireless channels. The Transport layer of WSN is concerned with establishing end-to-end connections over the network. However the proven protocols like User Datagram Protocol (UDP) [2] and Transmission Control Protocol (TCP) [3] are inappropriate for WSN due to many constraints. In present research community, numerous researchers have made significant advancements in developing new transport protocols. These protocols are tested in different experimental environments; hence it is extremely difficult to benchmark one against the other. Study of the generic transport protocol depicts all possible parameters and functions that different protocols may exploit in their operation. Therefore by thoroughly analysing the generic transport protocol design together with different experimental settings of diverse protocols, we tried to come up with a benchmark. Figure 1 illustrates the generic structure of the transport protocol, which is comprised of three main functional modules: (i) congestion module, (ii) reliability module, and (iii) priority module. In next three sections we discuss these modules in detail, while referring relevant existing research contributions.

II. CONGESTION MODULE

Congestion occurs when nodes transmit more combined upstream traffic resulting in packet-arrival rate to exceed the packet processing rate at the node. Congestion also arises when mote's data throughput exceeds the link's available data threshold limit and can also result due to wireless link issues such as contention, interference, and blind mote problem. Congestion causes packet drops and unnecessary packet retransmissions followed by significant network's energy depletion. The congestion module is activated to take corrective actions to reduce congestion, hence to offer the desired reliability. Generally the Congestion module is composed of three sub-modules: (i) congestion detection, (ii) congestion notification, and (iii) congestion avoidance.

A. Congestion Detection

Congestion detection refers to identification of possible events, which may build-up congestion in the network. Generally different protocols identify congestion by utilizing different combinations of the following parameters.

1) Buffer occupancy: The occupied buffer memory locations with respect to the maximum available memory. When the memory of the sensors reaches the maximum threshold due to excessive incoming packets, congestion scenario is forecasted [5, 6, 7, 10, 11, 13, 14, 24, 25, 28].

2) Packet rate: The number of packets received or sent within specified time. If the packet incoming rate exceeds the packet forwarding rate, congestion can occur as the WSN motes have limited storage [4, 5].

3) Packet service time: The time interval between the arrival of the packet at the node and successful transmission of the last bit of the same packet [22, 23, 26].

4) Packet inter-arrival time: The time interval between the two sequential arriving packets from either source or for the transit traffic. If the packet service time exceeds the packet inter-arrival time, it leads to queue build up and packets will suffer from long queue delays [22, 23].

5) Node delay: Node delay at the sensors reveals how busy the surrounding area of sensor node is, and packets get delayed than expected if congestion occurs [7, 11].

978-0-7695-4236-2/10 $26.00 © 2010 IEEE
DOI 10.1109/BWCCA.2010.179

6) Channel status: The channel condition gives an idea about how busy the channel is, and the interference of surroundings, which eventually reveals whether the channel is ready to transmit and receive data without resulting in congestion. Intra-path interference occurs when transmissions of the nodes interfere with the successor's reception, which prevents the reception of the following packet from a predecessor node [10, 28].

7) Application fidelity: The concept of quality represents a range of operational measures including packet latency, number of successful event detections, data quality, and redundancy. If the fidelity of received data is below the perceived performance, the congestion is assumed [24].

8) Reliability parameters: In congested networks, packets are dropped often and delayed retransmissions occur. Some protocols detect the congestion based on reliability related factors such as, the time to recover packet loss, transmission error loss rate, number of transmission attempts made before a packet is delivered, and reception of acknowledgements within time-out [6, 8, 9, 12, 29].

B. Congestion Notification

To initiate the congestion mitigation, the communication of the congestion to the neighboring motes is essential. The congestion can be notified either explicitly or implicitly.

*1) Explicit notification:*This is a special control packet that warns the congestion to its neighbouring nodes [6,28].

2) Implicit notification: Here the congestion warning is embedded in the header of the normal data packets [4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 22, 23, 25, 26, 29].

C. Congestion Avoidance

Congestion avoidance means to alleviate the network congestion, hence to increase the smooth data transfer in wireless link. Once the congestion notification is received at the nodes, the control loop for congestion avoidance is initiated and the sensors are updated to ease down the congestion. The main congestion avoidance techniques are rate adjustment and traffic redirection.

1) Rate adjustment: Rate adjustment refers to regulating the transmission rate of the congested sensors upon the reception of the congestion notification [4, 5, 6, 7, 9, 10, 11, 12, 14, 22, 23, 25, 26, 28, 29].

Based on the location at which the rate adjustment plans are implemented, the rate adjustment schemes are categorized as either centralized or distributed. In centralized rate adjustment, the control decisions are made centrally, usually at the sink [5, 9, 11, 14]. In distributed rate adjustment, the control decisions are made at each hop of the network [4, 7, 8, 10, 13, 22, 23, 25, 26, 28, 29].

Generally different transport protocols use different rate control algorithms, which can be broadly categorized in to two; *simple rate adjustment like AIMD* (Additive Increase Multiplicative Decrease) and *exact rate adjustment*. In *simple rate adjustment*, merely a single congestion notification bit is used to notify the congestion. The congestion bit is enabled and cleared based on the congestion level. Such protocols use AIMD policy or its variants for rate adjustment, which increases the reporting rate in additive manner if successful data transmissions

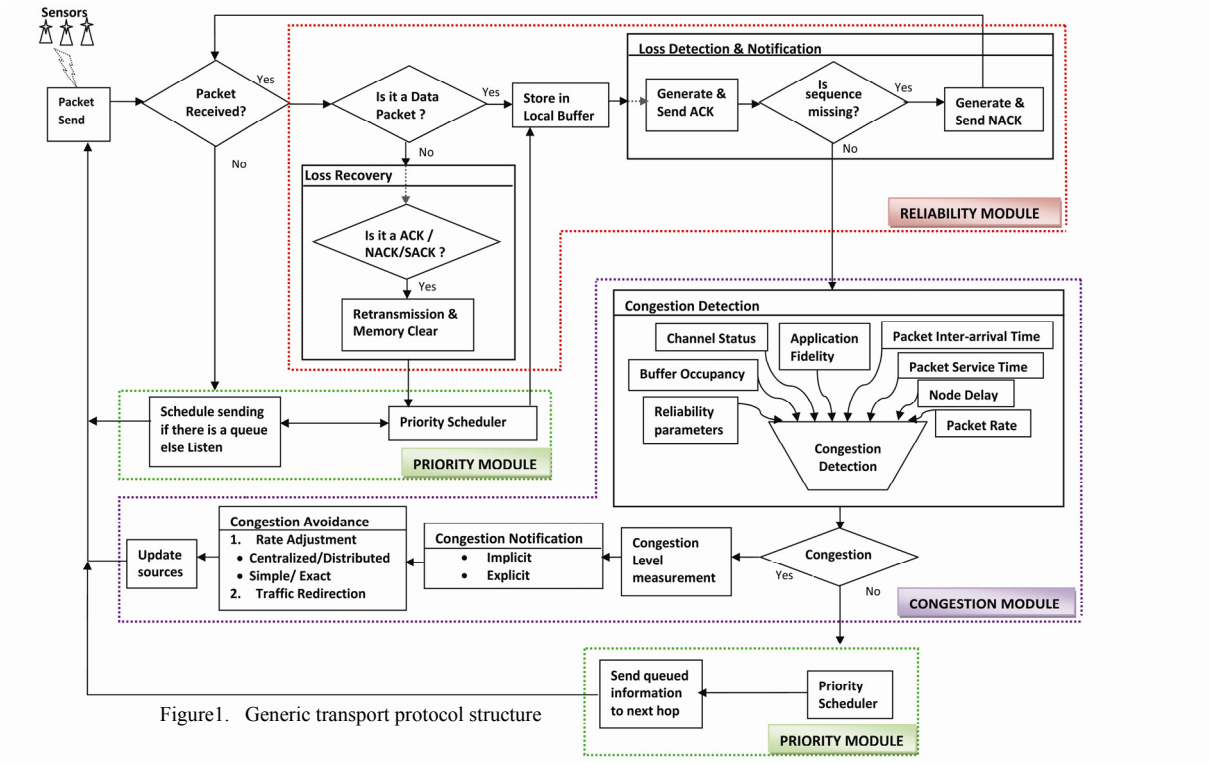

Figure1. Generic transport protocol structure

occur, and reduces the rate in multiplicative style if congestion occurs. AIAD (additive increase additive decrease) is another such notion, in which the rate is reduced in additive manner in congested scenarios [5, 8, 9, 10, 13, 14, 25, 28, 29]. In *exact rate adjustment*, the rate is adjusted based on the information feedback obtained from the neighbours, implementing more accurate rate adjustment plan. These estimated parameters include congestion degree, acceptable data rate and delay parameters etc [4, 7, 11, 22, 23, 26].

2) Traffic Redirection: In traffic redirection, the nodes dynamically allocate its outgoing traffic to the uncongested paths. The congested paths are avoided using the feedback information obtained from the neighbours such as high loss rates of those links[12,13,24].

III. RELIABILITY MODULE

Reliability in the context of transport protocols refers to the successful delivery of each segment that the sources generate to the ultimate destination. The reliability module must efficiently detect the packet drops and retransmit these packets to relevant sources.

A. Reliability Direction

In WSN, data transfers occur in two directions. When sensors detect an event, they inform their sensed information to the sink node. Sink also sends control packets or query messages to the sources. To satisfy the reliability for these scenarios, transport protocols offer upstream reliability and downstream reliability respectively.

Upstream Reliability refers to the successful delivery of dataflow traffic from sources to sink [4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20]. *Downstream Reliability* refers to the successful delivery of control packets and queries from sink to sources [16, 21]. *Bidirectional Reliability* means satisfying reliability in both directions, upstream and downstream [8].

B. Reliability Level

The level of reliability means the extent of reliability supported by the protocol. Three levels of data reliability can be defined as follows;

1) Packet level reliability: Successful delivery of all the packets to the destination. This is necessary in certain control driven application scenarios, where every sensed information is of pivotal nature and any loss of information may result in process malfunction. [4, 5, 6, 7, 9, 10, 13, 15, 16, 17, 18, 19, 20, 21]

2) Event level reliability: Successful event detection. For example, if more than one sensor in the field senses the same information and reports to the sink, it is expected that at least one packet will be delivered [8, 11, 12, 14].

3) Destination reliability: Successful delivery of packets only to the selected cluster in the entire WSN [16].

C. Loss Detection and Notification

In reliable data transport, every packet loss should be identified by the receiver and the receiver should inform to the corresponding data storage mote or to the relevant source for retransmission. When a packet is dropped, a common mechanism for the packet loss detection would be to use packet sequence numbers in identifying packet drops. This is done in such a way that the source embeds packet header with two fields; source identifier and sequence number. Upon the reception of packets, the destination checks the sequence number and once a gap is detected in the sequence numbers, it determines that the packet corresponding to the missing sequence number is lost. The protocols notify the packet losses, using following types of feedbacks;

1) Positive acknowledgements: Positive acknowledgements are sent explicitly as special control packets (ACK)[4, 6, 8, 13, 15, 17, 19, 28] or implicitly (iACK)[4, 15, 18] in order to confirm the successful reception. The node generates ACK control packets for all the packets received or single ACK packet for multiple fragments received (Cumulative ACK)[9]. Implicit acknowledgement (iACK) is the interpretation for the transmitter's ability to overhear the forwarding transmissions in physical wireless links, which iACK piggybacks ACK in the packet header.

2) Negative acknowledgements (NACK): NACKs are sent for the missing sequence numbers in received stream. NACK can be generated as single [5, 8, 9, 10, 13, 16, 17, 20, 21] or a range of lost fragments[21], which is referred as notion of loss window.

3) Selective acknowledgements (SACK): The receiver sends SACK [7, 19] to inform the sender about all segments that have arrived successfully, effectively this notifies the last fragment received in-order. So the sender needs to retransmit only the segments that have actually been lost.

D. Loss Recovery

The loss recovery means repairing the packet drops by means of packet retransmission. Loss recovery can be categorized into two as follows;

1) End-to-end loss recovery: Here the end points are responsible in loss detection and notification. Only the source caches the packet information and the generation of repair requests occurs only at sinks. Relevant source retransmits the packet upon the reception of repair request [5, 8, 9, 10, 11, 13, 17].

2) Hop-by-hop loss recovery: Here the intermediate nodes cache packet information and perform loss detection and notification. The lost packet recovery requests are initiated at each hop. Once the caching node obtains the repair request, it initiates the retransmission [4, 5, 6, 7, 15, 18, 19, 20, 21].

IV. PRIORITY MODULE

Source prioritization is to differentiate diverse sensors by means of introducing precedence levels to different sensors or assigning flows or applications identifiers to reflect the importance of each sensor. For example; it is important to assign higher priority to the event driven information compared to synchronous information sensing. Data prioritization is critical in WSN that supports heterogeneous applications having mixed traffic flows. This enables to obtain the application specific QoS objectives and also the weighted fairness, which assigns more bandwidth for more critical applications.

A. Priority Scheduler

The prioritization scheduler differentiates the source information based on the nature of the flow or the application [6, 13, 4], the precedence level of the source [22, 23] and information of time to live or the remaining time to deadline [7, 11] of the packets etc. The intermediate nodes arrange the received packets based on the importance and forward the scheduled queued data to the next hop.

V. DESIGN SPACE

If we investigate the WSN research base, numerous research contributions in designing transport protocols can be found. The uniqueness of each new protocol more or less lies in one of the components or attributes discussed in Figure 1. However for the new researchers working in this area, the fundamental challenge is in evaluating all these existing protocols, since there is no well defined benchmark. Hence to prove one's protocol is better than the rest is challenging. So we decided to study the experimental design space of different protocols, so that we can get some kind of benchmark to compare our protocol.

Here we first categorized these protocols based on their capability to support congestion control and reliability (Table I) and a detailed evaluation of these protocols based on the congestion control, reliability support and priority support is available in [30]. The readers also should refer the corresponding references for further information. In this section, we highlight their experimental attributes like number of sensors, sensor deployment, packet size, simulation area, buffer size and power levels (Table II). Most of the performance overhead in WSN transport layer depends on these parameters.

The *number of sensor nodes* distributed in network is mainly determined by the factors like the nature and the size of the area of interest. For example, in indoor network applications like home automation, not many sensors are required to cover a small area with fewer obstacles. If it is an outdoor network like rainforest or an agricultural field, the size of the region as well as the amount of disturbances may be higher. Therefore it may require more sensors. As illustrated in the Table I, most protocols [4, 7, 8, 11, 13, 14, 15, 16, 22, 26] have attempted to perform their simulations using higher number of sensors, which is equal or more than 100 sensors. The ability to perform successfully in huge network proves the scalability of the design.

Sensor node deployment must be carefully done, mostly when dealing with a large number of sensors. Sensor nodes may be deployed in physical environment either in random locations [5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 22, 26, 28] or in deliberately selected locations based on pre defined plans (e.g. tree, grid)[4, 9, 16, 18, 20, 21, 23, 24, 25]. The ad hoc distribution, which is utilized by many protocols here, is used in most practical scenarios, mostly for the establishments where human interaction is low.

The *coverage area* is referred to the area covered by the effective communication range of the sensors. Based on the coverage area presented by different protocols, we can deduce the suitability of the protocol for different physical locations. For example we can assume that the protocols [4, 5, 6, 7, 8, 11, 13, 14, 15, 21, 22, 25], which show lesser covering area (let's take the area less than 300x300m^2) may be suitable for the applications with small and medium size establishments like buildings and bridges etc. The protocols [12, 16] that exhibit higher area may be suitable for larger regions like forests and agricultural fields.

TABLE I. TRANSPORT PROTOCOLS CLASSIFICATION

Reliability support only	Congestion control only
• ERTP: Energy-efficient and Reliable Transport Protocol [15] • GARUDA [16] • DTSN: Distributed Transport for Sensor Networks [17] • RBC: Reliable Bursty Convergecast [18] • DTC: Distributed TCP Caching [19] • RMST: Reliable Multi-Segment Transport [20] • PSFQ: Pump Slowly Fetch Quickly [21]	• PHTCCP : Prioritized Heterogeneous Traffic-oriented Congestion Control Protocol [22] • PCCP : Priority-based Congestion Control Protocol [23] • Siphon [24] • Fusion [25] • CCF: Congestion Control and Fairness [26] • Trickle [27] • CODA: Congestion Detection and Avoidance[28] • ARC: Adaptive Rate Control [29]

Both congestion control and reliability support
• TRCCIT: Tunable Reliability with Congestion Control for Information Transport [4] • CRRT: Congestion aware and Rate controlled Reliable Transport[5] • CTCP: Collaborative Transport Control Protocol [6] • RT^2: Real-Time and Reliable Transport [7] • ART: Asymmetric and Reliable Transport [8] • RCRT: Rate-Controlled Reliable Transport [9] • Flush [10] • DST: Delay Sensitive transport [11] • PORT: Price-Oriented Reliable Transport[12] • STCP: Sensor Transmission Control Protocol [13] • ESRT: Event-to-Sink Reliable Transport [14]

TABLE II. TRANSPORT PROTOCOLS EXPERIMENTAL SETTINGS

	Protocols	Applications	Sensor deployment	Number of Sensors	Packet Size	Coverage Area (m^2)	Buffer size	Tx Power/ current	Rx Power
Both Reliability and Congestion control	TRCCIT (2010)	Heterogeneous concurrent multiple applications	Grid	100	29bytes	60 x 60	36	-	-
	CRRT (2009)	High-rate applications: imaging, acoustic localization	Ad-hoc	80	32 bytes	100x100	40	-	-
	CTCP (2008)	Heterogeneous concurrent multiple applications	Ad-hoc	25	216 bits	50 x 50	-	-	-
	RT^2 (2008)	Heterogeneous concurrent real-time applications: Target tracking, chemical attack detection	Ad-hoc	200 / sources:41, 62,81, 102	30 bytes	200x200	65	0.660W	0.39W
	ART (2007)	Mission critical applications like country border security	Ad-hoc	100	100 bytes	300x300	50	24 mW	13 mW
	RCRT (2007)	High-rate applications: imaging, acoustic localization	Tree	40	64 bytes	-	-	-	-
	FLUSH(2007)	Bulk data collection applications: volcanic activity monitoring	Ad-hoc	79 sensors	35 bytes	-	-	-	-
	DST (2006)	Heterogeneous real-time applications : Border surveillance and intrusion detection	Ad-hoc	200/ sources:41, 62,81, 102	30 bytes	200x200	65	0.660W	0.39W
	PORT (2005)	General Sensing application	Ad-hoc	100	36 bytes	1350x1350	50	0.66 W	0.39 W
	ESRT (2005)	Event detection applications: signal estimation/tracking	Ad-hoc	200/sources 41, 52, 62	30 bytes	100x100	65	0.66 W	0.39 W
	STCP (2005)	Heterogeneous concurrent multiple applications	Ad-hoc	50,100	-	100x100	-	-	-
Reliability only	ERTP (2009)	Data streaming applications: whether and habitant monitoring	Ad-hoc	200	40 bytes	180xl80	-	31.8 mA	13.4 mA
	GARUDA (2008)	Downstream reliability applications	grid	100	1Kbytes	650x650	-	-	-
	RBC (2005)	High-volume bursty traffic applications	Grid	49	-	-	-	-	-
	RMST (2003)	Applications require fragmentation /reassembly like multimedia	Grid	21	50-100 bytes	-	-	-	-
	PSFQ (2002)	Downstream slow fetch reliability applications	Linear	13	50 bytes	100x100	-	-	-
Congestion control only	PHTCCP (2008)	Heterogeneous concurrent multiple applications	Ad-hoc	100	29,33,41, 64 bytes	100x100	10	-	-
	PCCP (2006)	Heterogeneous concurrent multiple applications	Tree, Linear	7	-	-	-	-	-
	Siphon (2005)	Generic data dissemination application	grid	48	-	-	-	-	-
	Fusion (2004)	High-volume bursty traffic applications and fairness	tree	55	-	1493 (sqm)	-	–10 dBM	-
	CCF (2004)	Fairness in applications: large area temperature monitoring	Ad-hoc	116	30 bytes	-	10	-	-
	CODA(2003)	General Sensing application	Ad-hoc	30	64 bytes	-	-	-	-

It is necessary to ensure that transport layer protocol is capable of handling large *packet size*, while maintaining desired performance. The simulation with large packet size evidences its capability to handle complex application packets like multimedia without loss of the quality of output, which can be resulted due to fragmentation. From these protocols, very few offer higher packet size [8, 16], and all other protocol simulations have been done with packet sizes less than 100 bytes.

Buffer size in a WSN mote means the maximum available storage locations in memory. The buffer motes use to store the incoming packets and initiate retransmission in loss recovery process. When the buffer level is low, the possibility of congestion occurrence is high. Since the prac-tical WSN motes contain limited storage, the transport protocol simulation done in software environment also should utilize low buffer lengths to match with the actual environment.

In WSN, it is essential to minimize energy wastage, hence to maximize the lifetime of motes. Sensor mote power consumption is strongly dependent on the operating mode power levels, i.e. *transmit (Tx) and receive (Rx) power levels.*

VI. CONCLUSIONS

In this paper, we analyzed the design space of different WSN transport protocols. Thus we tried to obtain some sort of benchmark to evaluate the protocol performance. To

accomplish this, we comprehensively investigated the functional components of the generic transport protocol, which is built using the attributes and functions of existing research contributions. This article may give broad understanding of the settings of existing protocols which may offer support in future transport protocol developments.

REFERENCES

[1] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks", *IEEE Computer*, 37(8), pp. 41-49, 2004.

[2] TCP. Retrieved August 2008: http://www.ibiblio.org/pub/docs/rfc/rfc793.txt.

[3] UDP. Retrieved August 2008: http://tools.ietf.org/html/rfc768.

[4] F. K. Shaikh, A. Khelil, A. Ali, and N. Suri, "TRCCIT: Tunable Reliability with Congestion Control for Information Transport in Wireless Sensor Networks," in *the Proceedings of the International Wireless Internet Conference (WICON)*, Singapore, 2010.

[5] M. Alam and C. S. Hong, "CRRT: Congestion-Aware and Rate-Controlled Reliable Transport in Wireless Sensor Networks," *IEICE Trans. Commun,* vol. E92-B, pp. 184-189, January 2009.

[6] E. Giancoli, F. Jabour, and A. Pedroza, "CTCP: Reliable Transport Control Protocol for Sensor Networks," in *the Proceedings of Fourth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Sydney,Australia, 2008, pp. 493-498.

[7] V. Cagri, Gungor, Ö. B. Akan, and I. F. Akyildiz, "A real-time and reliable transport $(RT)^2$ protocol for wireless sensor and actor networks," in *the IEEE/ACM Transactions on Networking (TON)*, Piscataway, NJ, USA, 2008, pp. 359-370.

[8] N. Tezcan and W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," *International Journal of Sensor Networks,* vol. 2, pp. 188-200, June 2007

[9] J. Paek and R. Govindan, "RCRT: rate-controlled reliable transport for wireless sensor networks," in *the Proceedings of the 5th international conference on Embedded networked sensor systems*, Sydney, Australia, 2007, pp. 305 - 319.

[10] S. Kim, R. Fonseca, P. Dutta, A. Tavakoli, D. Culler, P. Levis, S. Shenker, and I. Stoica, "Flush: a reliable bulk transport protocol for multihop wireless networks," in *Proceedings of the 5th international conference on Embedded networked sensor systems* Sydney, Australia, 2007, pp. 351 - 365.

[11] V. C. Gungor and O. B. Akan, "DST: Delay sensitive transport in wireless sensor networks," in *the Proceedings of Seventh IEEE International Symposium on Computer Networks*, Istanbul, Turkey, 2006, pp. 116–122.

[12] Y. Zhou and M. R. Lyu, "PORT: a price-oriented reliable transport protocol for wireless sensor network," in *the proceedings of 16th IEEE International Symposium on Software Reliability Engineering* Chicago, 2005, pp. 117-126.

[13] H. Zhang, A. Arora, Y.R.Choi, Y.G.Iyer, S.Gandham, and S.Venkatesan, "STCP: a Generic Transport Layer Protocol for Wireless Sensor Networks," in *the Proceedings of the 14th IEEE International Conference on Computer Communications and Networks (ICCCN)*, USA, 2005, pp. 449–454.

[14] Y.Sankarasubramaniam, O.B.Akan, and I.F.Akyildiz, "ESRT: Event-to-Sink Reliable Transport in Wireless Sensor Networks," in *the Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM Mobihoc)*, USA, 2003, pp. 177–188.

[15] T. Le, W. Hu, Peter, Corke, and S. Jha, "ERTP: Energy-efficient and Reliable Transport Protocol for data streaming in Wireless Sensor Networks," *Computer Communications,* vol. Volume 32, pp. 1154-1171, May 2009.

[16] S.J.Park, R.Vedantham, R.Sivakumar, and I.F.Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *the Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM Mobihoc),* Japan, 2004, pp. 78-79.

[17] B.Marchi, A.Grilo, and M.Nunes, "DTSN – Distributed Transport for Sensor Networks," in *the Proceedings of IEEE Symposium on Computers and Communications (ISCC)*, Aveiro, Portugal, 2007.

[18] M.G.Gouda, "Reliable Bursty Convergecast in Wireless Sensor Networks," in *the Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM Mobihoc),* USA, 2005, pp. 266-276.

[19] A.Dunkels, T.Voigt, H.Ritter, and J.Alonso, "Distributed TCP Caching for Wireless Sensor Networks," in *the Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop*, Turkey, 2004.

[20] F.Stann and J.Heideman, "RMST: Reliable Data Transport in Sensor Networks," in t*he Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA)*, USA, 2003, pp. 102–113.

[21] C.Y.Wan, A.T.Campbell, and L.Krishnamurthy, "PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks," in *the Proceedings of ACM International Workshop on WSN and Applications (WSNA),* USA, 2002, pp. 1–11.

[22] M. M. Monowar, M. O. Rahman, A.-S. K. Pathan, and C. S. Hong, "Congestion control protocol for wireless sensor networks handling prioritized heterogeneous traffic," in *the Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, Dublin, Ireland, 2008.

[23] C. Wang, K. Sohraby, V. Lawrence, B. Li, and Y. Hu, "Priority-based Congestion Control in Wireless Sensor Networks," *Trustworthy Computing,* vol. 1, pp. 22-31, 2006

[24] C. Y. Wan, S. B. Eisenman, A. T. Campbell, and J. Crowcroft, "Siphon: overload traffic management using multi-radio virtual sinks in sensor networks," in *3rd international conference on Embedded networked sensor systems*, San Diego, California, USA, 2005, pp. 116 -129

[25] B.Hull, K.Jamieson, and H.Balakrishnan, "Mitigating Congestion in Wireless Sensor Networks," in *the Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (ACM SenSys)*, USA, 2004, pp. 134-147

[26] C. T. Ee and R. Bajcsy, "Congestion control and fairness for many-to-one routing in sensor networks," in *the Proceedings of 2nd international conference on Embedded networked sensor systems*, Baltimore, MD, USA, 2004, pp. 148 - 161

[27] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks," in *the Proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation - Volume 1 table of contents*, San Francisco, California, 2004, pp. 29-31.

[28] C.Y.Wan, S.B.Eisenman, and A.T.Campbell, "CODA: Congestion detection and avoidance in sensor networks," in *the Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems (ACM SenSys)*, USA, 2003, pp. 266–279.

[29] A. Woo and D. E. Culler, "A transmission control scheme for media access in sensor networks," in *the Proceedings of the 7th annual international conference on Mobile computing and networking*, Rome, Italy, 2001, pp. 221 - 235.

[30] A. J. D. Rathnayaka, V. M. Potdar, and A. Sharif, "Wireless Sensor Network Transport Protocol – A State of the Art," accepted by *Fifth International Conference on Broadband and Wireless Computing, Communication and Applications*, Fukuoka, Japan, 2010.

[31] A. Sharif, V. Potdar, and A. J. D. Rathnayaka, "Prioritizing Information for Achieving QoS Control in WSN," in *the Proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications*, Australia, 2010, pp. 835-842.