Review Article

A Comparative Analysis of Reliable and Congestion-Aware Transport Layer Protocols for Wireless Sensor Networks

Bhisham Sharma and Trilok C. Aseri

Department of Computer Science and Engineering, PEC University of Technology (Formerly Punjab Engineering College), Sector 12, Chandigarh 160012, India

Correspondence should be addressed to Bhisham Sharma, bhisham.tiet@gmail.com

Design and implementation of wireless sensor Networks have gathered increased attention in recent years due to vast potential of sensor networks consisting of spatially distributed devices (motes) to cooperatively monitor physical or environmental conditions at different locations. Wireless sensor networks are built upon low cost nodes with limited battery (power), CPU clock (processing capacity), and memory modules (storage). Transport layer protocols applied to wireless sensor networks can handle the communications between the sink node and sensor nodes in upstream (sensor-to-sink) or downstream (sink-to-sensor) direction. In this paper, we present a comparative analysis of reliable and congestion aware transport layer protocols for wireless sensor networks and number of open issues that have to be carefully realized to make use of the wireless sensor networks more efficiently and to enhance their performance. We first list the characteristics of transport layer protocols. We then provide a summary of reliable and congestion aware transport layer protocols with their respective pros and cons and comparison of different protocols based on reliability, congestion control, and energy efficiency. Finally, we point out open research issues of transport layer protocols for wireless sensor networks, which need further attention to overcome the earlier mentioned challenges.

1. Introduction

Wireless sensor networks (WSN) are formed by collection of hundreds or thousands of sensor nodes and are used to monitor events in a region. Sensor nodes are composed of processor, memory, transceiver, one or more sensors, and a battery [1]. The data collected from the region are sent to the Access Point (AP) that connects the sensor network with one or more observers. The observer is end user wishing to receive information from the observed area [2]. Our major focus in this paper is on the comparison of transport layer protocols for wireless sensor networks. Transport protocols are used to decrease congestion and reduce packet loss, to provide fairness in bandwidth allocation, and to guarantee end-to-end reliability [3]. However, the Transmission Control Protocol (TCP) [4] and User Datagram Protocol (UDP) [5] are popular transport protocols and deployed widely in the Internet, neither may be a good choice for wireless sensor networks. There is no interaction between TCP or UDP and the lower-layer protocols such as routing and Media Access Control (MAC) algorithm. In wireless sensor networks, the lower layers can provide generalized information to the transport layer and optimize the badly needed system performance [6]. Both of these protocols are not suitable for wireless sensor networks due to many constraints in terms of throughput and energy efficiency. One of the major drawbacks of TCP is that it uses end-to-end retransmission-based error control and the window-based Additive-Increase Multiplicative-Decrease (AIMD) [7] congestion control mechanisms that may not be feasible for the wireless sensor networks domain and hence, may lead to waste of scarce resources [8]. In contrast, UDP is connectionless transport control protocol and is not suitable for wireless sensor networks due to lack of flow and congestion control mechanisms. UDP contains no ACK mechanism; therefore, the lost datagrams can be recovered only by lower or upper layers, including the application layer [9].

In wireless sensor networks, transport layer protocols should support reliable message delivery, congestion control, and energy efficiency. The reliability feature and congestion control of transport layer in wireless sensor networks can be either hop-by-hop or end-to-end. In wireless sensor networks, reliability can be classified into two categories which are packet reliability and event reliability. Packet reliability requires successful transmission of all packets or at a certain success ratio. On the other hand, the task of event reliability is to report an event to the base station in efficient manner [28].

In wireless sensor networks, sensor nodes at each end of a particular connection have different characteristics, such as capacity of communication and computation. When the sender node transmits segment with a higher rate than the receiver node is able to handle and process, the buffers at the receiver node may result to overflow and congestion occurs. These results in degrading the performance of network, system throughput, loss of packets, increased packet delay, and wasted node energy. To address this challenge, congestion detection and avoidance mechanism in wireless sensor networks is used [29].

In wireless sensor networks, it is much more important that sensor network operation is energy-efficient, which defines network lifetime, and high level Quality of Service (QoS), or fidelity that is met over the course of the network lifetime. Furthermore, one of the greatest challenges in wireless sensor networks is to increase network lifetime by reducing energy consumption because congestion control may involve only in transport layer but the energy conservation may be related to physical layer, data link layer, network layer, and higher layers [6].

The rest of the paper is organized as follows. We introduce characteristics of transport layer protocols for wireless sensor networks in Section 2. In Sections 3 and 4, we present a summary and comparison of reliable and congestion aware transport layer protocols for wireless sensor networks. In Section 5, we point out open research issues in transport layer protocols of wireless sensor networks. Finally, the paper is concluded in Section 6.

2. Characteristics of Transport Layer Protocols

The transport layer protocols for wireless sensor networks should support:

  (i) reliable message delivery;

 (ii) congestion control;

(iii) energy efficiency.

2.1. Reliability for Wireless Sensor Networks. Packet loss in wireless sensor networks is usually due to the quality of the wireless channel, sensor failure, and congestion. Most of the applications need reliable transmission of each packet, and thus packet-level reliability is required. Almost every transport layer protocol for wireless sensor networks offers unidirectional reliable message delivery, but bidirectional reliability is also required in certain applications. Reliability

in wireless sensor networks [10–27, 30, 31] can be realized as packet reliability, event reliability, end-to-end reliability, hop-by-hop reliability, upstream reliability and downstream reliability.

2.1.1. Reliability Level. Data reliability can be defined as follows.

Packet Reliability. Packet reliability refers to the successful delivery of all the packets to the destination. In case of packet reliability, it is required that all the packets from the sensor nodes reach the sink node that can results in wastage of sensors limited energy resources [32]. Due to noisy communication channels, packet loss may occur and thus, it is the requirement of packet reliability that every packet is to be acknowledged and each lost packet is to be retransmitted. This results in increase of communication overhead with high packet loss rates and creates network congestion.

Event Reliability. Event reliability refers to the successful event detection. This requires the reliable transfer of event data from each sensing region in a sensor network. However, in case of event reliability, loss of packet can be tolerated as long as the sink receives at least one packet from the sensor nodes containing the sensed data of an event [32]. As compared to packet reliability, it does not require the retransmissions of every lost packet. This reduces the communication overhead and unnecessary retransmissions of packets.

2.1.2. Reliability Direction. The reliability direction can be classified as follows.

Upstream Reliability. Upstream reliability refers to the communication between the sensor nodes and sink node, which is mostly unicast/convergecast transmission. All the protocols except PSFQ [33] and GARUDA [34] offer upstream reliability.

Downstream Reliability. Downstream reliability refers to the communication between the sink node and sensor nodes, since there is only a single sender (the sink); the data transmission usually uses broadcasting rather than unicasting. It provides successful delivery of control packets and queries from sink to sources. Only PSFQ [33] and GARUDA [34] offer downstream reliability.

Bidirectional Reliability. Bidirectional reliability provides both sensor-to-sink and sink-to-sensor transport mechanism for wireless sensor networks. It is much more important to use a single bidirectional protocol, instead of using two unidirectional protocols for the following reasons: (i) it reduces the complexity and heterogeneity of the network; (ii) it reduces the energy consumption; (iii) it makes use of piggybacking, for example, the sensors piggyback the ACK of query messages on their subsequent messages. None

of the protocols except ART [16] protocol satisfies bidirectional reliability [35].

2.1.3. Loss Detection and Notification.

The loss detection and notification stage of the reliability algorithm is used to detect when a packet has been lost and is thus responsible for initiating any action to recover the loss. In order to perform this task, one of the following methods may be used.

Acknowledgment (ACK). Types of ACK can be as follows.

Explicit. Upon receiving a packet, the node sends back a confirmation on it. The node explicitly notifies the sink which packets were received correctly. An explicit ACK can confirm the reception of a single or multiple packets.

Implicit. When a node overhears his neighbor forwarding a packet sent by the node; it can assume that the delivery of the packet to that neighbor was successful. This method can only confirm the delivery of a single packet.

Negative Acknowledgment (NACK). The node explicitly notifies the sender which packets were received incorrectly and thus may need to be retransmitted. A NACK can also refer to a single or multiple requested packets. In multiple NACK schemes, the notion of loss window refers to a range of lost packets.

Selective Acknowledgment (SACK). It is a combination of an explicit single or multiple ACK used for the last packets received in-order and multiple ACKs for other packets that were also received, but which are out of order [36, 37].

2.1.4. Error Recovery.

The error recovery can be classified as follows.

End-to-End Error Recovery. Like TCP [4], in end-to-end error recovery mechanisms only the final destination node is responsible for detecting loss and requesting for retransmission. This approach will cause large delay and low throughput. In wireless sensor networks, the end points (a sensor and a base-station) are responsible in loss detection and notification. Some of the protocols like ATP [11], Tiny TCP/IP [12], STCP [14], DST [15], ART [16], Flush [17], RCRT [18], TSS [19], CTCP [20], CRRT [23], and ERCTP [27] offer end-to-end error recovery [30, 38, 39].

Hop-by-Hop Error Recovery. Hop-by-hop error recovery is widely accepted recovery mechanism in sensor networks. The basic design idea of hop-by-hop error recovery is that the intermediate nodes, rather than just the final node, perform loss detection and recovery. In hop-by-hop error recovery, pair of neighboring nodes is responsible for loss detection and can enable local retransmission that is more energy efficient, as compared to the end-to-end approach. The biggest advantages of hop-by-hop error recovery are that recovery from packet loss can occur quickly, and progress made in early hops is not lost if a failure occurs in a later hop. Most of the protocols like Tiny TCP/IP [12], RT^2 [21], RTMC [22], CRRT [23], TRCCIT [26] offer hop-by-hop error recovery [3, 40, 41].

2.2. Congestion Control for Wireless Sensor Networks.

In wireless sensor networks, the main sources of congestion are interference between concurrent data transmissions, the addition or removal of sensor nodes in the network, high data rates, many-to-one network topology, huge bursts of event data, and collision in the physical channel [29, 42–44]. The traditional UDP [5] protocol does not offer any congestion control mechanism, whereas TCP [4] employs window based approaches to avoid the congestion scenario. The congestion pattern is different for upstream, downstream and bidirectional data flow. Congestion generally occurs due to the packet-arrival rate exceeding the packet-service rate. This is more likely to occur at sensor nodes close to the sink, as they usually carry more combined upstream traffic. Congestion also arises on the wireless link due to noise, interference, contention, or bit synchronization errors [3]. Congestion control can be classified as follows.

2.2.1. Congestion Detection.

Congestion detection protocols employ a mechanism whether or not a congestion occurred and at what location. Combinations of parameters are used by different protocols to detect congestion.

Buffer Occupancy. Buffer occupancy refers to the occupied buffer memory locations against the total available memory. A sensor node consists of limited sized buffers in wireless sensor networks due to memory limitation. As the network load increases, the packets are dropped due to excessive incoming traffic. In wireless sensor networks, contention level is controlled by network buffer size because if the number of source nodes is increased, contention level is also increased [45, 46].

Packet Rate. Packet rate refers to number of packets sent or received within specific time interval. If the packet receiving rate is higher than the packet forwarding rate, the buffer overflow is possible as the wireless sensor network motes have limited memory storage.

Packet Service Time/Packet Inter-Arrival Time. The time required to process one packet at the node is known as packet service time. It actually refers to the time interval between the arrival of the packet at the node and successful transmission of the last bit of the same packet [43]. The packet inter-arrival time is the time interval between the two sequential arriving packets from either source or for the transit traffic [44].

Node Delay. Node delay refers to the delay expected by each packet at each node. Node delay at the sensors reveals how busy the surrounding area of sensor node is, and packets get delayed than expected if the congestion occurs [47].

Channel Status. The channel status provides the information about how busy the channel is, and the interference of surroundings, which helps to detect whether the channel is ready to transmit and receive data without resulting in congestion [47].

2.2.2. Congestion Notification. After detecting congestion, the congestion notification information needs to be conveyed from the congested nodes to their neighbors or to the source nodes or destination nodes in wireless sensor networks. The congestion information can be sent in the form of a Congestion Notification (CN) bit in packet header as defined in [29, 48] or in complete format that includes the congestion degree [44] or allowable data rate [43]. Congestion notification information can be further categorized as follows.

Implicit Congestion Notification. In Implicit Congestion Notification, the congestion information piggybacks in normal data packets. By receiving or overhearing such packets, sensor nodes can access the piggybacked information.

Explicit Congestion Notification. In Explicit Congestion Notification, the congestion information can be sent in an explicit control message to notify the relevant nodes [3].

2.2.3. Congestion Avoidance. A direct way of avoiding congestion is to simply stop sending packets into the network, or to send at a lower rate. It also requires that sensor nodes limit their flow to their next-hop neighbors and help them to deal with congestion. Congestion avoidance techniques are of three different types.

Rate Adjustment. The rate adjustment decision can be made by the congested nodes themselves, by a node outside the congested area (sink node), or by a predetermined policy. The rate adjustment schemes are classified as either centralized or distributed. In centralized rate adjustment, the control decisions are made at the sink node only. In distributed rate adjustment, the control decisions are made at each hop of the network [49].

Traffic Redirection. The task of traffic redirection technique is to forward the excess traffic to a secondary high speed network, if available, that has a long communication range and is able to forward the traffic to the base station quickly.

Polite Gossip Policy. This technique is only used by Trickle [50] to control congestion in wireless sensor networks. In Polite Gossip policy, each node tries to broadcast a summary of its data to all the nodes periodically, but if nodes hear identical data from neighbors it "politely" suppress its own broadcasting. On the other hand, if any sensor node receives any new code from its neighbors, it broadcasts its own code, which in turn makes the receiving sensor node with the new code to broadcast that code.

2.3. Energy Efficiency for Wireless Sensor Networks. In wireless sensor networks, transport layer protocols should avoid packet loss as much as possible since loss translates to energy waste. The key attribute of wireless sensor network is defined in the literature is energy efficiency. A sensor node consists of one or more integrated sensors, embedded processors with limited capability, and short-range radio communication ability. These sensor nodes are powered using batteries and have limited energy. Since the nodes in the wireless sensor networks are battery powered, the energy consumed during their operation equates directly to the overall network life-time. In case of large-scale wireless sensor network deployments, it is commonly impractical or more expensive to change the batteries after deployment [3, 28]. A packet loss in wireless sensor networks can be common due to bit error and/or congestion. In case of congestion, significant amount of packet loss takes place due to lack of huge buffer space for the overwhelming number of packets. This results in packet retransmission and causes a significant amount of energy loss and delivery delay [51, 52].

3. Reliability-Based and Congestion Aware Protocols for Wireless Sensor Networks

Some of the transport layer protocols can support both reliability metrics as well as congestion control metrics in wireless sensor networks. In wireless sensor networks, some protocols use end-to-end congestion control while other uses hop-by-hop congestion control method. Some protocols claims event reliability and others provide packet reliability. As shown in Table 1, some transport layer protocols [10, 12–16, 19–25, 27] are energy efficient while, others such as [11, 17, 18, 26], are not energy efficient. Reliability and congestion control based protocols in wireless sensor networks are described as follows.

3.1. ESRT (Sankarasubramaniam et al., 2003). ESRT [10] (Event-to-Sink Reliable Transport) provides upstream event reliability and congestion control while avoiding the dropping of packets and minimum energy consumption. In case of the traditional concept of packet reliability, where single packet is retransmitted, until the Acknowledgment (ACK) is received from the sink node, whereas ESRT protocol defines event reliability as the received packet rate associated to the particular sensing process. The term event reliability implies that collective information of sensor nodes within the event radius are reliably received at the base station. The base station implements the ESRT algorithm to decide that the event is reliably detected or not. The reliability can be classified as observed reliability and desired reliability. (1) The observed event reliability, r_i, is the number of received data packets in decision interval i at the sink. (2) The desired event reliability, R, is the number of data packets required for reliable event detection. This reliability is determined by the particular application.

ESRT periodically computes a reliability figure (r), representing the rate of packets received successfully in a given time interval. It then deduces the required sensor

TABLE 1: Comparison of technical features of reliable and congestion aware transport layer protocols.

Category	Transport Layer Protocols in Wireless Sensor Network	Rel. Lvl.	Rel. Dir.	Rel. Type	Ack.	Delay	Caching	Seq. No. Out-of-Order	Cgst. Det.	Cgst. Noti.	Cgst. Miti.	AIMD	Fair.	Exp. Testbed/Simulation	Egy Effnt.
Both reliable and congestion aware transport layer protocols	ESRT [10]	Evt.	Up	Evt.-to-Sink	—	Large	No	No	Queue Occupancy	Imp	Rate Adj.	No	No	Simulation	Yes
	ATP [11]	Pkt.	Up	E-to-E	NACK	Med.	No	Yes	Queue Occupancy	Exp	Rate Adj.	No	Yes	Simulation	No
	Tiny TCP/IP [12]	Pkt.	Up	E-to-E H-by-H	iACK, eACK	Small	Yes	Yes	Pkt. Rate	Imp	Rate Adj.	No	No	Both	Yes
	PORT [13]	Evt.	Up	—	—	—	No	No	Node Price, Link-Loss Rates	Imp	Rate Adj., Traffic Red.	No	No	Simulation	Yes
	STCP [14]	Pkt.	Up	E-to-E	NACK, eACK	Large	Yes	No	Queue Occupancy	Imp	Rate Adj., Traffic Red.	Yes	No	Simulation	Yes
	DST [15]	Evt.	Up	E-to-E	—	Med.	No	No	Node Delay, Queue Occupancy	Imp	Rate Adj.	No	No	Simulation	Yes
	ART [16]	Evt.	Both	E-to-E	eACK, NACK	Small	No	Yes	ACK received to core nodes	Imp	Reduce Traffic of non-core nodes	No	No	Simulation	Yes
	Flush [17]	Pkt.	Up	E-to-E	NACK	Small	No	No	Queue Occupancy, Link Interference	Imp	Rate Adj.	No	No	Exp. Testbed	No
	RCRT [18]	Pkt.	Up	E-to-E	NACK, cumm.ACK	—	No	Yes	Time to recover loss	Imp	Rate Adj.	Yes	No	Exp. Testbed	No
	TSS [19]	Pkt.	Up	E-to-E	iACK	Large	Yes	Yes	Pkt. Rate	Imp	Rate Adj.	No	Yes	Simulation	Yes
	CTCP [20]	Pkt.	Up	E-to-E	eACK, Double eACK	Med.	No	No	Queue Occupancy, Transmission error loss	Exp	Rate Adj.	No	No	Simulation	Yes
	(RT)[2] [21]	Pkt.	Up	H-by-H	SACK	Med.	No	No	Queue Occupancy, Node Delay	Imp	Rate Adj.	No	No	Simulation	Yes

TABLE 1: Continued.

Category	Transport Layer Protocols in Wireless Sensor Network	Rel. Lvl.	Rel. Dir.	Rel. Type	Ack.	Delay	Caching	Seq. No. Out-of-Order	Cgst. Det.	Cgst. Noti.	Cgst. Miti.	AIMD	Fair.	Exp. Testbed/Simulation	Egy Effnt.
	RTMC [22]	Pkt.	Up	H-by-H	—	Large	No	No	Memory Overflow	Imp	Header Memory Info.	No	No	Both	Yes
	CRRT [23]	Pkt.	Up	E-to-E H-by-H	NACK, MAC	Med.	No	Yes	Queue Occupancy, Pkt. Rate	Imp	Rate Adj.	Yes	Yes	Simulation	Yes
	E^{2}SRT [24]	Evt.	Up	Evt.-to-Sink	—	Large	No	No	Queue Occupancy	Imp	Rate Adj.	No	No	Simulation	Yes
	LTRES [25]	Evt.	Up	Evt.-to-Sink	SIP_ACK, GNP_ACK	Med.	No	Yes	Link-Loss Rates	Imp	Rate Adj.	Yes	Yes	Simulation	Yes
	TRCCIT [26]	Pkt.	Up	H-by-H	iACK, eACK	Large	No	No	Pkt. Rate	Imp	Rate Adj.	No	No	Simulation	No
	ERCTP [27]	Pkt.	Up	E-to-E	NACK	Med.	No	Yes	Buffer Occupancy	Imp	Rate Adj.	No	Yes	Simulation	Yes

reporting frequency (f) from the reliability figure (r) using an expression such as $f = G(r)$. Finally, the base station broadcasts the newly calculated value of (f) to the whole sensor network. After receiving the event reporting frequency, every sensor node scans the buffer level at the end of every reporting interval to find out the possible congestion and compute its event reporting duration. If sensor node detects the congestion, it enables the congestion bit in the event report packet. When these packets arrive at the base station, the base station gets an overall view of the congestion level of the network.

ESRT still have the limitations, such as power and processing if the source node produce data too much slowly than the required reliability is not achieved, but if data produced by source node is very fast, high reliability may occur and this may lead to loss of packets and network congestion.

3.2. ATP (Sundaresan et al., 2003). ATP [11] (Ad-hoc Transport Protocol) is designed to improve TCP's performance over wireless network. Lack of fixed infrastructure, mobility, shared channel and limited bandwidth features of Ad-hoc network differentiate them from traditional computer network. This protocol solves multiple problems that TCP has traditionally met over wireless Ad-hoc network. ATP decouples congestion control and uses feedback from intermediate forwarding nodes to judge precise estimate of the network state. ATP is designed on the basis of receiver-based and network-assisted end-to-end feedback control algorithm. The transmission delay (D) is calculated by the intermediate network nodes. The value of delay is calculated over the entire packet traversing the node and used to update the value piggybacked in every outgoing packet, if the current calculated value of D is higher than the older value. After that receiver calculates the required end-to-end rate (Inverse of D) and sends it back to the sender. Finally, the sender can adjust the sending rate according to the value received from the receiver. To achieve reliability, ATP uses a selective ACK that allows the receiver to state number of packets it has received and the remaining number of packets to be received in the future. To accomplish congestion control, the intermediate nodes in the network provide congestion information in terms of the available rate to the sink node. This protocol is not optimized to minimize energy consumption and its end-to-end approach is not suitable for wireless sensor networks.

3.3. Tiny TCP/IP (Dunkels et al., 2004). Tiny TCP/IP [12, 53] is designed to modify TCP/IP protocol suite for wireless sensor networks and provides combination of end-to-end and hop-by-hop reliability. TCP/IP protocol is not well suited for wireless sensor networks due to many constraints in terms of throughput and energy efficiency. Tiny TCP/IP provides four mechanisms: spatial IP address assignment, shared context header compression, application overlay routing, and Distributed TCP Caching (DTC) to use TCP/IP protocol for wireless sensor networks. With spatial IP address assignment, each sensor node uses its spatial location to construct an IP address. If sensor nodes are part of the same IP subnet, there is no need to transmit full IP addresses in the headers of packets. Hence, the IP header can be compressed and shared among the sensor nodes of the same subnet. For implementing an application overlay routing mechanism, Tiny TCP/IP broadcast UDP datagrams using link local IP broadcast. Finally, DTC provides the packet reliability using a distributed approach. In case of packet loss, it uses TCP packet caching within the in-network sensor nodes to reduce the burden of the end-to-end retransmission of fragments.

Tiny TCP/IP has following limitations: (1) it does not provide explicit congestion control mechanism. (2) The assumption of static spatial subnet IP makes is unsuitable for many of the mobility-supported wireless sensor networks applications.

3.4. PORT (Zhou and Lyu, 2005). PORT [13] (Price-Oriented Reliable Transport) is designed as upstream reliable, congestion control and energy efficient transport layer protocol. It is based on three assumptions: (1) source nodes would keep reporting data to the sink on the phenomenon of interest for a long period of time. (2) The sink is aware of the sources of the data packets from where the packet originates. (3) The sink is aware about the information a data packet carries.

PORT defines node price, which is measured as the total number of transmission attempts between the sensor node and sink, across the network. PORT minimizes energy consumed by avoiding links with high communication cost. It also minimizes energy consumption with two schemes: the first scheme is based on the sink's application-based optimization approach that sends as feedback the optimal reporting rate of each source as well as energy consumption of the sensor-to-sink communication from each source to the sink. The second is locally optimal routing scheme based on feedbacks from source node to the sink to inform it about congestion and increase the nodes costs. PORT provides an in-network congestion mechanism to alleviate traffic dynamically. PORT uses two mechanisms that ensure reliability. The first is a dynamic source report rate feedback mechanism to allow the sink to adjust the reporting rate of each data source. The second mechanism provides the sink with end-to-end communication cost information from the source to the sink.

3.5. STCP (Iyer et al., 2005). STCP [14] (Sensor Transmission Control Protocol) is a flexible, end-to-end upstream transport layer protocol that provides both end-to-end reliability and congestion control mechanism. In terms of reliability, STCP allows the application to specify how many packets, within a fixed window size, must be delivered reliably and if the data is to be transferred continuously at a specific rate, the receiving base station uses a time-out mechanism to find out a packet loss and recovers the lost packets by sending the NACK message to the sensor node. For unpredictable event-driven packets, source node uses Acknowledgment (ACK) message to make sure that the base station has successfully received the packets.

Each packet resides in the source nodes cache until and unless it receives an ACK from the base station. In case of congestion control mechanism, STCP uses a simple, end-to-end, closed loop, congestion detection method based on packet queue occupancy monitoring. STCP assumes that all the sensor nodes within the wireless sensor networks have strict clock synchronization with the base station, which might be a cause of performance problem with STCP. Sensing nodes waiting for the ACK reply from the base station will cause long latency in large scale multi-hop wireless sensor networks.

3.6. DST (Gungor and Akan, 2006). DST [15] (Delay Sensitive Transport) is designed as reliable, congestion control, and timely packet delivery transport layer protocol for wireless sensor networks. It integrates the Time Critical Event First (TCEF) scheduling mechanism to meet the application-specific delay bounds at the sink node. DST consists of 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 real-time event transport mechanism uses this event-to-sink delay bound to achieve the application specific objectives. For congestion detection, DST measures buffer overflow at each node and computes the average node delay. In DST protocol, a node is said to be congested whose buffer overflows due to excessive incoming packets or average node delay is above a certain delay threshold value. After detecting the congested node, it then informs the congestion information to the sink node by setting the Congestion Notification (CN) bit in the header of the event packet.

3.7. ART (Tezcan and Wang, 2007). ART [16] (Asymmetric and Reliable Transport) is designed as upstream end-to-end event reliability, upstream congestion control and downstream end-to-end query reliability. The important functions of ART are reliable query transfer, reliable event transfer and distributed congestion control. It selects a subset of sensor nodes called essential node (E-node) and the nonessential node (N-node) that cover the whole area to be sensed in an energy efficient way. ART creates sub network consisting of E-nodes that take part in reliable data transfer between the base station and sensor nodes in upstream and downstream direction including the recovery of lost fragments. For upstream and downstream reliability, ART uses both ACK and NACK mechanisms. The four different characteristics of ART protocol are: (1) (N-node) nonessential nodes do not face end-to-end communication overhead. (2) To regulate traffic flow effectively congestion control methods can be decentralized. (3) Few number of nodes can participate in lost message recovery. (4) ART uses distributed energy aware congestion control. The drawback of ART is that it only guaranteed congestion control, two-way

reliability for E-node (essential node) but not for N-node (nonessential node).

3.8. Flush (Kim et al., 2007). Flush [17] is designed as reliable, single-flow bulk transport protocol for wireless sensor networks. It provides end-to-end reliability, reduces transfer time, and adapts to time-varying network conditions. It uses sink-initiated control protocol to coordinate transfers, with end-to-end selective Negative Acknowledgments (NACK) and retransmissions to provide reliability. In Flush, large data is divided into packets and sends in its entirety using a pipelined transmission scheme to the sink. The sink sends the selective (NACK) requests repeatedly to the source for missing packets until it receives all packets successfully. The second goal of Flush is to minimize transfer time. To accomplish this, Flush proposes a rate allocation scheme for adapting dynamically the sending rate of the sensor nodes. Flush try to send packets at the maximum rate that will avoid intra-path interference [54]. The rate allocation algorithm follows two basic rules: (1) Rule 1: A node should only transmit when its successor is free from interference. (2) Rule 2: A node's sending rate cannot exceed the sending rate of its successor. These rules reduce intra-path interference in the wireless sensor networks and minimize losses due to the queue overflows for all nodes.

3.9. RCRT (Paek and Govindan, 2007). RCRT [18] (Rate-Controlled Reliable Transport) is designed as multipoint-to-point reliable transport layer protocol. It provides end-to-end explicit loss recovery and places all the congestion detection, rate adaptation and rate allocation functionality in the sinks. The different goals of RCRT protocol are: (1) reliable end-to-end transmission of all data transmitted by each sensor to a sink. This goal is required by high data rate applications which are loss intolerant like networked imaging [55], acoustic source localization and structural health monitoring [56]. (2) The second goal is to sustain network efficiency by avoiding congestion collapse [57]. In congestion collapse, sources are sending data faster than the network can transport them to the base station. (3) The third goal provides flexibility to choose capacity allocation policies by different applications. A capacity allocation policy determines how the overall network capacity is divided up among the different sources. (4) The last goal requires the RCRT be robust to routing dynamics and to nodes entering and leaving the system.

3.10. TSS (Braun et al., 2007). TSS [19] (TCP Support for Sensor Nodes) is designed to support energy-efficient operation of TCP in wireless sensor networks. TSS allows intermediate sensor nodes to cache TCP segments and to perform local retransmissions in case of errors. To avoid congestion, it does not forward a cached segment until it knows that the previous segment has been successfully received by the next hop node. It uses Implicit ACK (iACK) mechanism for loss recovery. In TSS, local retransmissions are performed by intermediate nodes, when they assume that a cached segment has not been received by the child node

towards the destination. The retransmissions are mainly triggered by timeouts, which requires careful setting of timeout values. Like DTC [58], the retransmission timeout is set to $1.5 * RTT$. The major drawback of TSS is that if a message transmission of one sensor node fails, it leads to stop the transmission of all its previous sensor nodes. According to the result produced by authors, TSS improves TCP performance both in terms of the overall number of transmitted TCP segments and throughput. The result shows that TSS importantly reduces the number of TCP segment and acknowledgment transmissions compared to TCP without TSS.

3.11. CTCP (Giancoli et al., 2008).

CTCP [20] (Collaborative Transport Control Protocol) is designed as upstream end-to-end reliability and congestion control transport layer protocol for wireless sensor network. The performance of CTCP is evaluated by using the following metrics: (1) Fraction of packets successfully received: in CTCP, reliability is quantified as the fraction of transmitted packets successfully received in case of packet error rates, node's failure and frequent disconnections. (2) Energy Consumption: CTCP calculates the energy consumed by individual node and the total of individual consumption is the network consumption. Energy consumed by the total number of sensor nodes in the network is much higher than the total energy consumed by transport and application layers. Thus, the CTCP energy consumption represents a small part of the total energy consumption and its use is applicable for applications that require reliable delivery of data.

The different features of CTCP are: (1) reliable delivery of all packets to base station, even in the case of nodes failures and frequent disconnections. (2) To accomplish energy efficiency, it defines two reliability profiles. (3) It is capable to distinguish congestion loss from transmission error loss. (4) It controls congestion through the interruption of packets forwards, if their buffer is up the threshold.

3.12. $(RT)^2$ (Gungor et al., 2008).

$(RT)^2$ [21] (Real-time and Reliable Transport) is designed as reliable and timely event detection with congestion control and energy efficient transport layer protocol for wireless sensor networks. In $(RT)^2$, communication can be classified as follows.

(1) *Sensor-Actor Communication.* The process of transmission of event features from the sensor nodes to the actor nodes is referred as sensor-actor communication.

(2) *Actor-Actor Communication.* Actor-actor communication is referred as communication between the actors to make a decision on the most appropriate way to collaboratively perform the action.

In $(RT)^2$, reliable event transport is needed to fulfill the heterogeneous requirements of both sensor-actor and actor-actor communication. The important characteristics of reliability functionalities are as follows.

(1) *Sensor-Actor Transport Reliability.* Sensor-actor transport is characterized by the dense deployment of sensors that collects data from the physical environment and forwarded to the corresponding actor nodes.

(2) *Actor-Actor Transport Reliability.* Actor-actor ad-hoc communication is also needed to collaboratively perform the right action upon the sensed phenomena in reliable and timely manner. The $(RT)^2$ protocol provides SACK (Selective Acknowledgment) based reliability mechanism to achieve 100% packet reliability.

$(RT)^2$ provides a combined congestion detection mechanism based on both local buffer level monitoring of the sensor nodes and average node delay calculation. The average node delay provides information about how busy the surrounding neighborhood of the sensor node.

3.13. RTMC (Zhou et al., 2008).

RTMC [22] (Reliable Transport with Memory Consideration) is designed as hop-by-hop reliable and congestion control transport layer protocol for wireless sensor networks. It is inspired from pipe-flow method. RTMC provides hop-by-hop retransmission of data packets to make sure all of the packets can be received by the sink with 100% reliability. In wireless sensor networks, the technique of rate adjustment is not suitable to adapt the rapid change of the traffic. Wireless sensor networks with lossy links and rapid changing traffic, results in loss of the control messages. This protocol includes memory information in the header of the packets and exchange information between the neighbors and in this way it allows preventing memory overflow. RTMC is implemented on MICA2 motes and achieve 100% reliability for each segment if the links are not broken. It also results in maximization of throughput and reduces the transport time. Authors also compared the performance of RTMC with other protocols and it is much more energy-effective, and has less memory cost and less transport time.

3.14. CRRT (Alam and Hong, 2009).

CRRT [23] (Congestion-Aware and Rate-Controlled Reliable Transport) is designed as hop-by-hop and end-to-end upstream reliable and congestion control transport layer protocol for wireless sensor networks. CRRT provides an efficient MAC layer retransmission method to increase the hop-by-hop reliability. CRRT is based on reservation-based retransmission mechanism, in which the sender reserves the medium to retransmit a packet to the receiver. In CRRT, packet is only retransmitted when the packet is dropped due to collision or wireless link error and if the sender does not receive the ACK. CRRT requires end-to-end acknowledgment of the sent packets in order to provide 100% reliability and in-order delivery of packets. This can be achieved by using either the positive Acknowledgment (ACK) or the Negative Acknowledgment (NACK). In CRRT, packet loss is detected by observing the sequence number of the received packets. CRRT uses NACK to inform a packet loss and the source retransmits the requested packet. It uses congestion

avoidance technique to avoid unnecessary packet dropping and thus tries to detect the incipient congestion. The level of congestion is measured by using both buffer occupancy and the forwarding rate of the node. Sink node is responsible for controlling the congestion and the rate of every source node based on the Congestion Notification (CN) of the intermediate nodes.

3.15. E^2SRT (Kumar et al., 2009). E^2SRT [24] (Enhanced Event-to-Sink Reliable Transport) is designed to resolve the "overdemanding" event reliability problem in ESRT [10] protocol and to stabilize the network. It is modified version of ESRT protocol and provides better performance in terms of both reliability and energy consumption. E^2SRT addresses the following two issues. (1) How to detect an overdemanding desired event reliability (R_{od}) situation? and (2) How to quickly converge to a maximum achievable reliability without requiring the full knowledge of network conditions? As compared to ESRT protocol, E^2SRT scheme successfully avoids the fluctuations and recursively converges to it best achievable reliability values in a few decision intervals. E^2SRT works in the similar fashion as the ESRT scheme, if the desired reliability can be satisfied by the network. It is designed as robust and more adaptive to the changing event and network environment. E^2SRT simulation results show that it performs very well in the presence of "Overdemanding Event Reliability" (OR). E^2SRT enhances the network performance by around 20–25% in terms of throughput with lower latency and loss rate as compared to the ESRT scheme.

3.16. LTRES (Xue et al., 2009). LTRES [25] (Loss-Tolerant Reliable Event Sensing) is designed as reliable transport layer protocol for dynamic event observation in wireless sensor networks. The level of reliable event sensing for a particular application is determined by the sink at the transport layer. As compared to Loss-Sensitive Reliable (LSR) transport layer protocols, LTRES provides adaptive end-to-end reliable data transport based on the dynamic event sensing requirements, which results in minimized packet transmission with less energy consumption. It is designed as light-weight loss rate based congestion detection and mitigation mechanism and used to reduce the control overhead. The sink node is responsible for early congestion detection and adjusts the source rates at the aggressive sensor nodes. It is based on event-to-sink reliability, where the end-to-end transport reliability requirement is guaranteed for an event area instead of from each source node. LTRES uses a distributed steady-state throughput estimation approach to enforce the fare rate control while providing LTR guarantee with higher bandwidth utilization and fast convergence time. Authors have implemented LTRES protocol in wireless network simulator GloMoSim [59] using different application scenarios with different sensing reliability requirements.

3.17. TRCCIT (Shaikh et al., 2010). TRCCIT [26] (Tunable Reliability with Congestion Control for Information Transport) is designed as hop-by-hop upstream tunable reliable and congestion control transport layer protocol for wireless sensor networks. To accomplish the tunable reliability, it implements probabilistic adaptive retransmissions, Hybrid Acknowledgment (HACK) and retransmission timer management. On the other hand, it reduces the network congestion by transporting the information on multiple paths. Retransmission timers directly impact the number of transmissions. In TRCCIT, large Retransmission Timeout (RTO) values increase information transport delay, whereas small Retransmission Timeout (RTO) values results in unnecessary retransmissions. To achieve reliable information transport, TRCCIT provides a simple and localized mechanism to manage the retransmission timers.

The performance metrics of TRCCIT are classified as follows. (1) Information transport reliability: it is the ratio of amount of information received by the sink to the total amount of the information generated by the sensor nodes. (2) Timeliness: it is defined as the time elapsed from the creation of the first information packet to the arrival of the first information packet at the sink. (3) Efficiency: it is determined in terms of message complexity, as the total number of message transmissions required for the information transport reliability. To reduce congestion, it efficiently monitors the information flow and adapts between single path and multiple paths.

3.18. ERCTP (Sharif et al., 2010). ERCTP [27] (End-to-End Reliable and Congestion Aware Transport Layer Protocol) is designed as end-to-end reliable and congestion aware protocol that aims to achieve high data reliability by the usage of distributed memory concept and minimum packet drop by the implementation of congestion detection and rate adjustment scheme for heterogeneous wireless sensor networks. Packet drop in wireless sensor network is generally due to congestion, poor link quality, mote failure, collisions due to hidden motes. ERCTP consists of congestion control module and reliability module. Congestion control module is divided into three sub-modules that is congestion detection module, congestion notification module and congestion avoidance module. In congestion detection module, congestion can be detected through congestion state of the network based on the link capacity and intermediate nodes buffer occupancy. In congestion notification module, it is necessary to notify the neighboring nodes about the occurrence of the congestion in order to avoid extreme congestion scenarios. In congestion avoidance module, source rate value is adjusted for child nodes in order to reduce congestion. ERCTP also helps sink node to explicitly and periodically send the estimated value of rate adjustment to source nodes. The task of the reliability module is to resend the sensed information upon receipt of Negative Acknowledgment (NACK) packet that is when packet loss occurs. To achieve data reliability, ERCTP has introduced the concept of Distributed Memory Storage (DMS) in which the designated intermediate nodes are used to temporarily store packet information, which can then be used for retransmission in case the sink fails to receive the designated packet information.

4. Comparative Analysis of Protocols

In Sections 2 and 3, we have provided a brief overview of characteristics of transport layer protocols and existing reliable and congestion control protocols proposed for WSNs. Their major features are summarized in Table 1.

In Table 1, comparison has been made on reliable and congestion aware protocols for wireless sensor networks by using different parameters like reliability level, reliability direction, reliability type, acknowledgment, delay, caching, sequence number out-of-order, congestion detection, congestion notification, congestion mitigation, AIMD, fairness, experimental testbed/simulation, and energy efficiency.

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. Packet reliability refers to the successful delivery of all the packets to the destination. All the protocols discussed in Table 1, concern on packet reliability except PORT, ART, ESRT, and DST, E^2SRT, and LTRES. Event reliability refers to the successful event detection. This requires the reliable transfer of event data from each sensing region in a sensor network. As compared to packet reliability, it does not require the retransmissions of every lost packet. Only PORT, ART, ESRT, DST, E^2SRT, and LTRES offer event level reliability.

In WSN, data transfers occur in two directions. Upstream reliability refers to the successful delivery of dataflow traffic from sensor nodes to the sink node. All the protocols in Table 1 offer upstream reliability. Downstream reliability refers to the successful delivery of control packets and queries from sink to sensor nodes, which is mostly multicast/broadcast transfer. None of the protocols in Table 1 offer downstream reliability. Bidirectional reliability provides both sensor-to-sink and sink-to-sensor transport mechanism for wireless sensor networks. None of the protocols except ART protocol in Table 1 satisfies bidirectional reliability.

End-to-end reliability refers to reliable data delivery of sensed data from the source to the destination node or vice versa. Most of the protocols like ATP, Tiny TCP/IP, STCP, DST, ART, Flush, RCRT, TSS, CTCP, CRRT, and ERCTP in Table 1 offer end-to-end reliability. On the other hand, hop-by-hop reliability needs the intermediate nodes to participate in the control process, which may increase the workload and power consumption on these resource-limited nodes. Some of the protocols like Tiny TCP/IP, RT^2, RTMC, CRRT, and TRCCIT in Table 1 offer hop-by-hop reliability. ESRT, E^2SRT, LTRES addresses event-to-sink reliability in Table 1, where the end-to-end transport reliability requirement is guaranteed for an event area instead of from each source node.

In reliable data transport, every packet loss should be identified by the receiver and should inform to the corresponding data storage mote or to the relevant source for retransmission. Positive acknowledgments are sent as explicit control packets (eACK) or as implicitly (iACK) in order to confirm the successful reception. Another variant of ACK is SACK and NACK. In case of NACK, node explicitly notifies the sender which packets were received incorrectly and thus may need to be retransmitted. In case of SACK, receiver sends SACK 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.

Node delay refers to the delay expected by each packet at each node. Node delay at the sensors reveals how busy the surrounding area of sensor node is, and packets get delayed than expected if the congestion occurs. ESRT, STCP, TSS, RTMC, E^2SRT, and TRCCIT offer large delay, ATP, DST, CTCP, $(RT)^2$, CRRT, LTRES, and ERCTP offer medium delay, Tiny TCP/IP, ART, and Flush offer small delay defined in Table 1. In order to optimize retransmission efficiency, possible approach is to cache packets at the intermediate node that is closer to the potential congested node where packet loss more likely arises. In Table 1 some of the protocols like Tiny TCP/IP, STCP, and TSS cache packets at the intermediate node.

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 the packet corresponding to the missing sequence number is lost. Most of the protocols like ATP, Tiny TCP/IP, ART, Flush, RCRT, TSS, CTCP, CRRT, LTRES, and ERCTP follow out-of-order sequence number.

Congestion detection refers to identification of possible events, which may build-up congestion in the network. Combinations of parameters like queue occupancy, packet rate, node price, link-loss rates, node delay, link interference, ACK received to core nodes, time to recover loss, transmission error loss, and memory overflow are used by different protocols to detect congestion. Now we discuss how different protocols use these parameters to detect congestion. STCP and ESRT solely detect the congestion when the buffer usage is higher than the predefined threshold, whereas $(RT)^2$ and DST monitor the node delay threshold in addition to the buffer occupancy. CTCP uses both transmission error loss rates and the buffer usage. ART, PORT, and RCRT detect the congestion based on feedback parameters of the reliability module. TRCCIT identifies congestion when the packet incoming rate is higher than the packet outgoing rate and CRRT assumes congestion when nodes experience the reduced packet forwarding rate and excessive buffer usage.

The congestion warning is notified to other nodes explicitly or implicitly. Most of the existing transport protocols defined in Table 1 implicitly notifies the congestion, whereas CTCP send explicit notification. CTCP generates control messages when congestion occurs as well as when congestion is resolved. A direct way of avoiding congestion is to simply stop sending packets into the network, or to send at a lower rate. Transport protocols are designed with three different congestion avoidance techniques, with two common techniques; rate adjustment and traffic redirection,

and one rarely used mechanism; polite gossip policy. From existing protocols, CRRT, RCRT, ESRT, and DST follow centralized rate adjustment scheme, whereas STCP, Flush, ART, $(RT)^2$, and TRCCIT use decentralized scheme.

AIMD is used to regulate the rates at which data is locally generated or forwarded for other nodes. This parameter is used by some of the protocols like STCP, RCRT, CRRT, and LTRES defined in Table 1. Sensor nodes are usually scattered in a geographical area. Due to the many-to-one convergent nature of upstream traffic, it is more difficult for sensor nodes far away from the sink to transmit the data. Transport protocols need to provide fair bandwidth allocation among all sensor nodes so that the sink can obtain a fair amount of sensory data from all sensor nodes. Fairness is only achieved by ATP, RCRT, CRRT, LTRES, and ERCTP protocols. Authors have implemented some of the protocols in simulator, or in experimental testbed, or in both environments. Energy efficiency is measured in terms of energy consumed per unit of successful communication or packets received by the base station from the sensor nodes. All the protocols except ATP, Flush, RCRT, and TRCCIT are energy efficient.

5. Research Issues of Transport Layer Protocols for Wireless Sensor Networks

In wireless sensor networks, transport layer protocols are designed to provide congestion control, reliability guarantee, and energy efficiency but the existing transport layer protocols are unidirectional (Upstream or Downstream) provides either congestion control or reliability guarantee and none of them provides congestion control and reliability simultaneously in both the direction. We have seen examples of transport protocols assuring reliability in one direction such as PORT, STCP, ESRT in the upstream and PSFQ, GARUDA in the downstream direction, but there is still no attempt made to provide bidirectional reliable transport possible in one protocol. However most of the applications require both functions in both directions simultaneously in wireless sensor networks. Another serious problem in transport layer protocols, that they can control congestion either in end-to-end or hop-by-hop method and guarantee reliability either in packet-level or application level not both of them. If a sensor network supports two applications (one of them needs only packet-level reliability, and another needs only application-level reliability), the existing transport control protocols will face difficulty and will be not the optimal choices. Therefore, an adaptive recovery mechanism is required to support packet-level and application-level reliability, and to be helpful for energy-conservation. Sensor nodes in a WSN might have different priorities since sensor nodes could be installed with different kinds of sensors and deployed in different geographical locations. Therefore sensor nodes can generate sensory data with different characteristics and have different priorities in reliability and bandwidth requirement. However, most existing protocols do not consider node priority, although recent approach PCCP provides a priority-based congestion control protocol. Transport layer protocols should be designed with cross-layer optimization because if

the routing algorithm informs the transport layer protocol of route failure, then the protocol will be able to decide that packet loss is due to route failure at network layer but not congestion failure. Though sensor networks are applicable in wide range of applications, their usage is not efficient due to design constraints like presence of limited power sensor nodes, changing topology, connectivity, clustering, data gathering, scheduling, service discovery, security, query processing, QoS (Quality of Service), and reliability. Sensor nodes are powered by external batteries and it can be difficult to replace them when consumed, so it is critical to design algorithms and protocols that utilize minimal energy.

The common research issues in transport protocols are classified as follows.

(1) A reliable transport layer protocol must be capable of isolating applications from the unreliable nature of wireless sensor networks in an efficient and robust manner.

(2) Transport layer protocols for wireless sensor networks should simplify the initial connection establishment process or use a connectionless protocol to speed up the connection process, improve throughput, and lower transmission delay.

(3) Transport layer protocols for wireless sensor networks should avoid packet loss as much as possible since loss translates to energy waste.

(4) The transport control protocols should guarantee fairness for a variety of sensor nodes [8, 9].

6. Conclusion

In this paper, we have presented a comparative analysis of the transport layer protocols for wireless sensor networks. Firstly, we have described characteristics of transport layer protocols in wireless sensor networks. Secondly, we have described several existing reliable and congestion aware transport layer protocols for wireless sensor networks along with their pros and cons and made comparison of different protocols by using different parameters like reliability direction, level, type, acknowledgment, delay, caching, sequence number out-of-order, congestion detection, notification, mitigation, AIMD, fairness, experimental testbed/simulation, and energy efficiency. Finally, we have discussed various current research issues in transport layer protocols for wireless sensor networks.
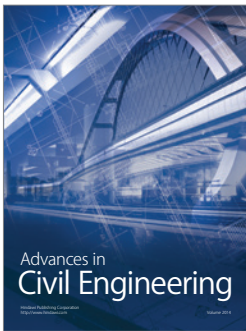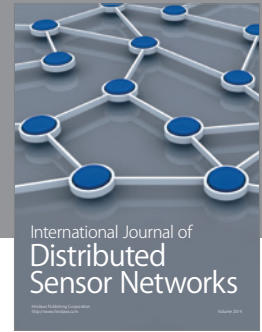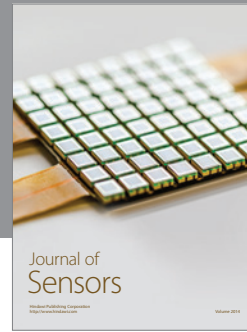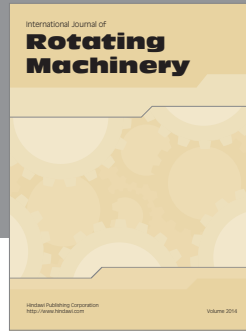
Acknowledgments

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks," in *Proceeding of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 139–150, July 2001.

[3] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *IEEE Network*, vol. 20, no. 3, pp. 34–40, 2006.

[4] J. Postel, "Transmission control protocol," Tech. Rep. RFC-793, Information Sciences Institute, 1981.

[5] J. Postel, "User datagram protocol," Tech. Rep. RFC-768, Information Sciences Institute, 1980.

[6] C. Wang, K. Sohraby, Y. Hu, B. Li, and W. Tang, "Issues of transport control protocols for wireless sensor networks," in *Proceedings of the International Conference on Communications, Circuits and Systems (ICCCAS '05)*, pp. 422–426, May 2005.

[7] D. M. Chiu and R. Jain, "Analysis of the increase and decrease algorithms for congestion avoidance in computer networks," *Computer Networks and ISDN Systems*, vol. 17, no. 1, pp. 1–14, 1989.

[8] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless Sensor Networks*, Kluwer Academic Publishers, Boston, Mass, USA, 2004.

[9] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks Technology, Protocols, and Applications*, John Wiley & Sons, New Jersey, NJ, USA, 2007.

[10] Y. Sankarasubramaniam, O. B. Akan, and I. F. Akyildiz, "ESRT: event-to-sink reliable transport in wireless sensor networks," in *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM Mobihoc '03)*, pp. 177–188, June 2003.

[11] K. Sundaresan, V. Anantharaman, H. Y. Hseeh, and R. Sivakumar, "ATP: a reliable transport protocol for ad-hoc networks," in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, pp. 64–75, Annapolis, Md, USA, June 2003.

[12] A. Dunkels, J. Alonso, and T. Voight, "Making TCP/IP Viable for wireless sensor networks," in *Proceedings of European Workshop on Wireless Sensor Networks (EWSN 04)*, pp. 1–4, Berlin, Germany, 2004.

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

[14] Y. G. Iyer, S. Gandham, and S. Venkatesan, "STCP: a generic transport layer protocol for wireless sensor networks," in *Proceedings of the 14th International Conference on Computer Communications and Networks (ICCCN '05)*, pp. 449–454, October 2005.

[15] V. C. Gungor and O. B. Akan, "DST: delay sensitive transport in wireless sensor networks," in *Proceedings of 7th IEEEInternational Symposium on Computer Networks*, pp. 116–122, Istanbul, Turkey, 2006.

[16] N. Tezcan and W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," *International Journal of Sensor Networks*, vol. 2, no. 3-4, pp. 188–200, 2007.

[17] S. Kim, R. Fonseca, P. Dutta et al., "Flush: a reliable bulk transport protocol for multihop wireless networks," in *Proceedings of the 5th ACM International Conference on Embedded Networked Sensor Systems (SenSys '07)*, pp. 351–365, Sydney, Australia, November 2007.

[18] J. Paek and R. Govindan, "RCRT: rate-controlled reliable transport for wireless sensor networks," in *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems*, pp. 305–319, Sydney, Australia, 2007.

[19] T. Braun, T. Voigt, and A. Dunkels, "TCP support for sensor networks," in *Proceedings of the 4th Annual Conference on Wireless on Demand Network Systems and Services (WONS '07)*, pp. 162–169, January 2007.

[20] E. Giancoli, F. Jabour, and A. Pedroza, "CTCP: reliable transport control protocol for Sensor networks," in *Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '08)*, pp. 493–498, December 2008.

[21] V. C. Gungor, O. B. Akan, and I. F. Akyildiz, "A real-time and reliable transport $(rt)^2$ protocol for wireless sensor and actor networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 2, pp. 359–370, 2008.

[22] H. Zhou, X. Guan, and C. Wu, "Reliable transport with memory consideration in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 2819–2824, May 2008.

[23] M. M. Alam and C. S. Hong, "CRRT: congestion-aware and rate-controlled reliable transport in wireless sensor networks," *IEICE Transactions on Communications*, vol. E92-B, no. 1, pp. 184–199, 2009.

[24] S. Kumar, Z. Feng, F. Hu, and Y. Xiao, "E^2SRT: enhanced event-to-sink reliable transport for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 9, no. 10, pp. 1301–1311, 2009.

[25] Y. Xue, B. Ramamurthy, and Y. Wang, "LTRES: a loss-tolerant reliable event sensing protocol for wireless sensor networks," *Computer Communications*, vol. 32, no. 15, pp. 1666–1676, 2009.

[26] F. K. Shaikh, A. Khelil, A. Ali, and N. Suri, "TRCCIT: tunable reliability with congestion control for information transport in wireless sensor networks," in *Proceedings of the 5th Annual International Wireless Internet Conference (WICON '10)*, pp. 1–9, Singapore, March 2010.

[27] A. Sharif, V. M. Potdar, and A. J. D. Rathnayaka, "ERCTP: end-to-end reliable and congestion aware transport layer protocol for heterogeneous WSN," *Scientific International Journal for Parallel and Distributed Computing*, vol. 11, no. 4, pp. 359–371, 2010.

[28] M. A. Rahman, A. E. Saddik, and W. Gueaieb, *Wireless Sensor Network Transport Layer: State of the Art*, Springer, Heidelberg, Germany, 2008.

[29] C. Y. Wan, A. T. Campbell, and S. B. Eisenman, "CODA: congestion detection and avoidance in sensor networks," in *Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems: (SenSys '03)*, pp. 266–279, Los Angeles, Calif, USA, November 2003.

[30] P. R. Pereira, A. Grilo, F. Rocha et al., "End-to-end reliability in wireless sensor networks: survey and research challenges," in *Proceedings of the EuroFGI Workshop on IP QoS and Traffic Control*, pp. 1–8, Lisbon, Portugal, December 2007.

[31] S. Kim, R. Fonseca, and D. Culler, "Reliable transfer on wireless sensor networks," in *Proceedings of the 1st Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, IEEE (SECON '04)*, pp. 449–459, October 2004.

[32] M. A. Mahmood and W. K. G. Seah, "Event reliability in wireless sensor networks," in *Proceedings of the 7th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '11)*, pp. 377–382, 2011.

[33] C. Y. Wan, A. T. Campbell, and L. Krishnamurthy, "PSFQ: a reliable transport protocol for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 862–872, 2005.

[34] S. J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *Proceedings of ACM (MobiHoc '04)*, pp. 7824–8926, Roppongi, Japan, May 2004.

[35] N. Tezcan, W. Wang, and M. Y. Chow, "A bidirectional reliable transport mechanism for wireless sensor networks," in *Proceedings of the Military Communications Conference (MILCOM '05)*, vol. 2, pp. 1193–1199, October 2005.

[36] L. Buttyán and L. Csik, "Security analysis of reliable transport layer protocols for wireless sensor networks," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '10)*, pp. 419–424, April 2010.

[37] M. H. Yaghmaee and D. Adjeroh, "A reliable transport protocol for wireless sensor networks," in *2008 International Symposium on Telecommunications (IST '08)*, pp. 440–445, August 2008.

[38] F. Yunus, N. S. N. Ismail, S. H. S. Ariffin, A. A. Shahidan, N. Fisal, and S. K. Syed-Yusof, "Proposed transport protocol for reliable data transfer in wireless sensor network (WSN)," in *Proceedings of the 4th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO '11)*, pp. 1–7, April 2011.

[39] N. Tezcan, E. Cayirci, and M. U. Caglayan, "End-to-end reliable event transfer in wireless sensor networks," in *Proceedings of the IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC '04)*, pp. 989–994, September 2004.

[40] H. Lee, Y. Ko, and D. Lee, "A hop-by-hop reliability support scheme for wireless sensor networks," in *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications*, pp. 435–440, March 2006.

[41] F. K. Shaikh, A. Khelil, and N. Suri, "A comparative study of data transport protocols in wireless sensor networks," in *Proceedings of the 9th IEEE International Symposium on Wireless, Mobile and Multimedia Networks (WoWMoM '08)*, pp. 1–9, June 2008.

[42] R. Chakravarthi, C. Gomathy, S. K. Sebastian et al., "A Survey on Congestion Control in Wireless Sensor Networks," *International Journal of Computer Science & Communication*, vol. 1, no. 1, pp. 161–164, 2010.

[43] C. T. Ee and R. Bajcsy, "Congestion control and fairness for many-to-one routing in sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, pp. 148–161, Baltimore, Md, USA, November 2004.

[44] C. Wang, K. Sohraby, V. Lawrence, L. Bo, and H. Yueming, "Priority-based congestion control in wireless sensor networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 22–31, June 2006.

[45] M. C. Vuran, V. C. Gungor, and O. B. Akan, "On the interdependence of congestion and contention in wireless sensor networks," in *Proceedings of SenMetrics*, pp. 136–147, San Diego, Calif, USA, July 2005.

[46] M. M. Alam and C. S. Hong, "Buffer and rate control based congestion avoidance in wireless sensor networks," in *Proceedings of Korea Information Processing Society*, pp. 1291–1293, May 2007.

[47] A. J. D. Rathnayaka and V. M. Potdar, "Wireless sensor network transport protocol: a critical review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 134–146, 2013.

[48] B. Hull, K. Jamieson, and H. Balakrishnan, "Mitigating congestion in wireless sensor networks," in *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (ACM SenSys '04)*, pp. 134–147, November 2004.

[49] A. Sridharan and B. Krishnamachari, "Explicit and precise rate control for wireless sensor networks," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys '09)*, pp. 29–42, November 2009.

[50] P. Levis, N. Patel, D. Culler, and S. Shenker, "Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks," in *Proceedings of the 1st USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI '04)*, pp. 1–14, San Francisco, Calif, USA, 2004.

[51] J. Kim and K. H. Park, "An energy-efficient, transport-controlled MAC protocol for wireless sensor networks," *Computer Networks*, vol. 53, no. 11, pp. 1879–1902, 2009.

[52] Y. Wang, C. Y. Want, M. Martonosi, and L. S. Peh, "Transport layer approaches for improving idle energy in challenged sensor networks," in *Proceedings of the SIGCOMM Workshop on Challenged Networks*, pp. 253–260, September 2006.

[53] A. Dunkels, A. T. Voigt, J. Alonso, H. Ritter, and J. Schiller, "Connecting wireless sensornets with TCP/IP networks," in *Proceedings of the 2nd International Conference on Wired/Wireless Internet Communications (WWIC '04)*, pp. 1–10, Springer, Frankfurt, Germany, 2004.

[54] A. K. Vyas and F. A. Tobagi, "Impact of interference on the throughput of a multihop path in a wireless network," in *Proceedings of the 3rd International Conference on Broadband Communications, Networks and Systems (BROADNETS '06)*, pp. 1–10, October 2006.

[55] M. Rahimi, R. Baer et al., "Cyclops: in situ image sensing and interpretation in wireless sensor networks," in *Proceedings of 3rd ACM Conference on Embedded Networked Sensor Systems (SenSys '05)*, pp. 192–204, 2005.

[56] K. Chintalapudi, T. S. Fu, R. Govindan et al., "Structural damage detection and localization using NETSHM," in *Proceedings of the 5th International Conference on Information Processing in Sensor Networks (IPSN '06)*, pp. 475–482, April 2006.

[57] S. Floyd, Congestion control principles, RFC2914, 2000.

[58] A. Dunkels, T. Voigt, H. Ritter, and J. Alonso, "Distributed TCP caching for wireless sensor networks," in *Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop*, pp. 1–10, Istanbul, Turkey, 2004.

[59] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," in *Proceedings of the 12th Workshop on Parallel and Distributed Simulation*, pp. 154–161, May 1998.