A Technical Study of Transport Layer Protocols for Wireless Sensor Network

Monika Sharma
PEC University of Technology
Chandigarh, India

Bhisham Sharma
PEC University of Technology
Chandigarh, India

Trilok C. Aseri, Ph. D
PEC University of Technology
Chandigarh, India

ABSTRACT
A Wireless Sensor Network is made up of self organizing, light weight sensor nodes whose main task is to cooperatively examine environmental conditions like vibration, temperature, pressure etc. and collect the information from the environment and send that information to the sink node. Transport layer protocols offer reliable data delivery as well as congestion control in wireless sensor networks. This paper firstly describes the functions of transport layer protocol. Then it presents the summary of some transport layer protocols on the basis of reliability and congestion control. This paper also presents comparison of these transport layer protocols with design and technical parameters and finally it discuss several research issues of transport layer protocols in wireless sensor network.

General Terms
Transport Layer Protocols; Reliability; Energy Efficiency; Wireless Sensor Network; Congestion Control

1. INTRODUCTION
Wireless sensor network is appealing in various applications such as in environment monitoring, area monitoring, habitat monitoring, security surveillance, medical applications and at home/office applications etc [1]. In wireless sensor network sensor nodes collect the information from environment by sensing and then transmit sensed information to destination node [2] as shown in Figure 1. There are several transport layer protocols which provide services such as reliability, congestion control and energy efficiency. Existing transport protocols over wireline network, TCP [3] (Transmission Control Protocol) and UDP [4] (User Datagram Protocol) are well matured but they have many critical issues in wireless sensor world. TCP does not have good performance in wireless environment in terms of both energy efficiency and throughput. UDP does not provide reliability and congestion control which lead to packet loss and then a lot of energy is wasted in retransmission of lost packets. Therefore TCP and UDP are inappropriate for wireless sensor network.

Reliable data delivery and congestion control are two major functions of transport layer protocols in wireless sensor network. Reliability means data delivered from source node to destination node in an appropriate manner reliably without any packet loss. Due to many unique characteristics and constraints of sensor nodes providing reliability in wireless sensor network can be challenging [5]. As sensor nodes are mainly deployed in non accessible areas, so it's not feasible to change the batteries of sensor nodes periodically, thus in designing of a reliable data transport protocol energy consumption is also main factor that must be considered.

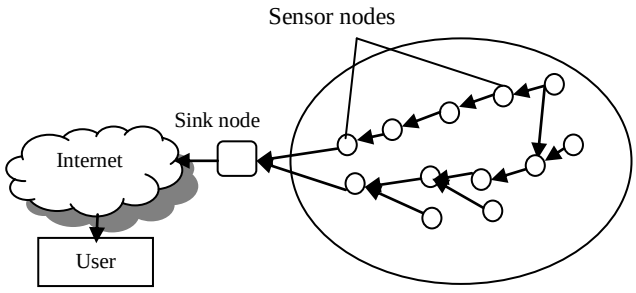

Figure 1: Structure of Wireless Sensor Network

Frequent node failures also a major problem in designing of reliable data transport protocol, node failure causes system crashes, energy consumption and harsh environment in sensor network. [6] Because of multihop nature of wireless sensor network a different degree of congestion occurs, when packet arrival rate is more than the packet service rate then node cannot handle it and starts dropping the packets. As the packet arrival rate increases, congestion is also increases and mainly at nodes near to sink node. Packet loss occurs until congestion is detected or a congestion avoidance technique is adopted and it necessities packet retransmission which causes lot of energy wasted [7].

The rest of this paper is structured as follows: functions of transport layer protocols are described in section 2. Section 3 presents summary of transport layer protocols that provide reliability and both reliability and congestion control in wireless sensor network. Section 4 presents the comparison of transport layer protocols. In section 5 research issues of transport layer protocol is described and at last in section 6 paper is concluded.

2. FUNCTIONS OF TRANSPORT LAYER PROTOCOLS
This section classified the functions of transport layer protocols.

2.1 Reliability Semantics
Reliability level in wireless sensor network is categorized as packet reliability, event reliability and destination reliability [5]. Packet reliability means every packet generated from source node is delivered successfully to the destination node. All protocols provide packet reliability except RETP [8], ESRT [9], DST [10], PORT [11], QERP [12], E^2SRT [13] and LTRES [14]. Event reliability in wireless sensor network refers to successfully detection of the event [15]. Destination reliability refers to all the packets should be delivered successfully to a particular node or to a group of nodes. GARUDA [16] offers both packet reliability and destination reliability.

In transport protocols data flows either in upstream which means data is flow from source nodes to sink node or in downstream which means data flow from sink node to source nodes as sink node sends control and query messages to source nodes for retasking [17]. All transport protocols offer reliability in upstream direction except GARUDA [16] and PSFQ [18].

The loss recovery refers to recovery of packets with retransmission. The loss recovery can be performed in two ways: end-to-end and hop-by-hop [19-21]. In end-to-end loss recovery mechanism only the source node cache packets and it is the responsibility of sink node to detect any packet loss and then send request to source node for retransmission of lost packet. This loss recovery mechanism will cause large delay and low throughput. Some of protocols like DST [10], STCP [22], DTSN [23], ART [24], RCRT [25], ERCTP [26] and RP2PT [27] uses end-to-end loss recovery. In hop-by-hop loss recovery mechanism, all intermediate nodes cache the packets and detect losses and send requests for retransmission, this loss recovery mechanism is more energy efficient. RETP [8], PORT [11], PSFQ [18], DTC [28], RBC [29], ERTP [30], RMST [31], DCDD [32], $(RT)^2$ [33], RTMC [34], TRCCIT [35] offers hop-by-hop loss recovery mechanism.

Transport protocols implement different mechanisms for loss detection and notification; Positive acknowledgements are used when all data packets generated from source nodes are received correctly at destination node. Negative acknowledgements are used if data packet is not received or if packet received incorrectly. The receiver sends selective acknowledgement to inform the sender that all packets are received in order using one control packet. In case of explicit acknowledgement, node explicitly notifies the sink that packet were received correctly. When a node send some packet to neighbor node and after sometime node hears that neighbor node forwards that packet to other nodes then the node assumes that packets were received correctly and assumes it as implicit acknowledgement [17].

2.2 Congestion Semantics

Congestion occurs in wireless sensor network when any node receives more packets than its capacity, then it cannot handle it and starts dropping the packets. So it causes large response time and also it degrades throughput. Congestion control is divided into following three categories: congestion detection, congestion notification and congestion avoidance [36].

In congestion detection, firstly congested events are identified and then identified the locations where congestion occurred. Congestion detection has various parameters such as packet rate, buffer occupancy, packet service time, node delay and channel status etc. are used to detect congestion [37-40]. After congestion detection, congested nodes send notification of congestion to their neighbors or to source nodes or to destination nodes. Congestion notification is of two types: implicit congestion notification and explicit congestion notification. The method of sending congestion notification to other nodes is designed very carefully because sending messages to the network which is already congested could violent the situation. To send congestion notification, congestion bit is set in packet header either 0 or 1. To avoid the congestion, it is simple to stop sending packets into network or to send packets at lower rate. Congestion avoidance techniques are further divided into three categories: rate adjustment, polite gossip policy and traffic redirection [17].

Figure 2 shows the flow chart of working of reliability and congestion control module in wireless sensor network. Sensor nodes firstly sensing the environment conditions and then finally route the aggregated data to next hop. If next node receives the data then it store it in cache otherwise loss recovery mechanism is used to recover the data. Intermediate nodes buffer data in their local cache for future processing. Nodes that received data generate a positive acknowledgement and send it to source from where data comes. If data is not received according to sequence, it means data is lost so that node generates negative acknowledgement and send it to source and requests for retransmission of data. Otherwise if data is receives properly congestion is checked, if there is no is congestion then data is send to next hop. Otherwise if congestion is detected then congestion notification information from congested node is send to source node or to neighbor nodes. Then they used congestion avoidance techniques such as, traffic redirection in which traffic is redirected to different paths to avoid congestion and rate adjustment in which transmission rate of packets is adjusted to avoid the congestion and then information is updated, and that information is send to sensor nodes.

3. TRANSPORT LAYER PROTOCOLS

Some of transport layer protocols of wireless sensor network support reliability, some support congestion control and some protocols support both reliability and congestion control. This paper summarizes the protocols that offers reliability and both reliability and congestion control.

3.1 Reliability based protocols

Transport layer protocols that provide reliability are presented in this section

PSFQ: Pump Slowly Fetch Quickly [18] is a hop-by-hop downstream transport protocol. In this protocol firstly user node slowly inject messages into network and if there is any packet loss occurs then it uses aggressive hop by hop error recovery. As it uses hop-by-hop loss recovery so all intermediate nodes buffer data in their cache and forwards packet with proper schedule. PSFQ exploits the loss aggregation concept in which when any packet loss occur, it combine all the message losses into one single fetch operation. It also uses a report operation which gives data delivery information to users. PSFQ has several limitations such as PSFQ forward messages in sequence order that means any node does not forward packets until it does not receive all the packets so it increases the latency. As PSFQ uses NACK based loss detection and notification, so it does not provide reliability for every single packet. There is difficulty in adjusting the timers (T_{min}, T_{max}, T_r).

RMST: Reliable Multi Segment Transport [31] offers data segmentation/reassembly and guaranteed delivery. In RMST large data is fragmented at source node, and then transmitted through network and reassembles at base station. Cached mode and non cached mode are two modes of RMST to achieve reliability. In cached mode, every intermediate node cache the data and if base station detect any loss of fragment then it send NACK to source node through intermediate node. Then Intermediate nodes check there cache, if they have lost fragments then send it to sink node and, if not then forward NACK to next node. In non cached mode only source nodes and sink node is keeping the fragments. RMST has limitation such as it needs every intermediate nodes cache all the data in their cache spaces that they received, so RMST is not scalable.

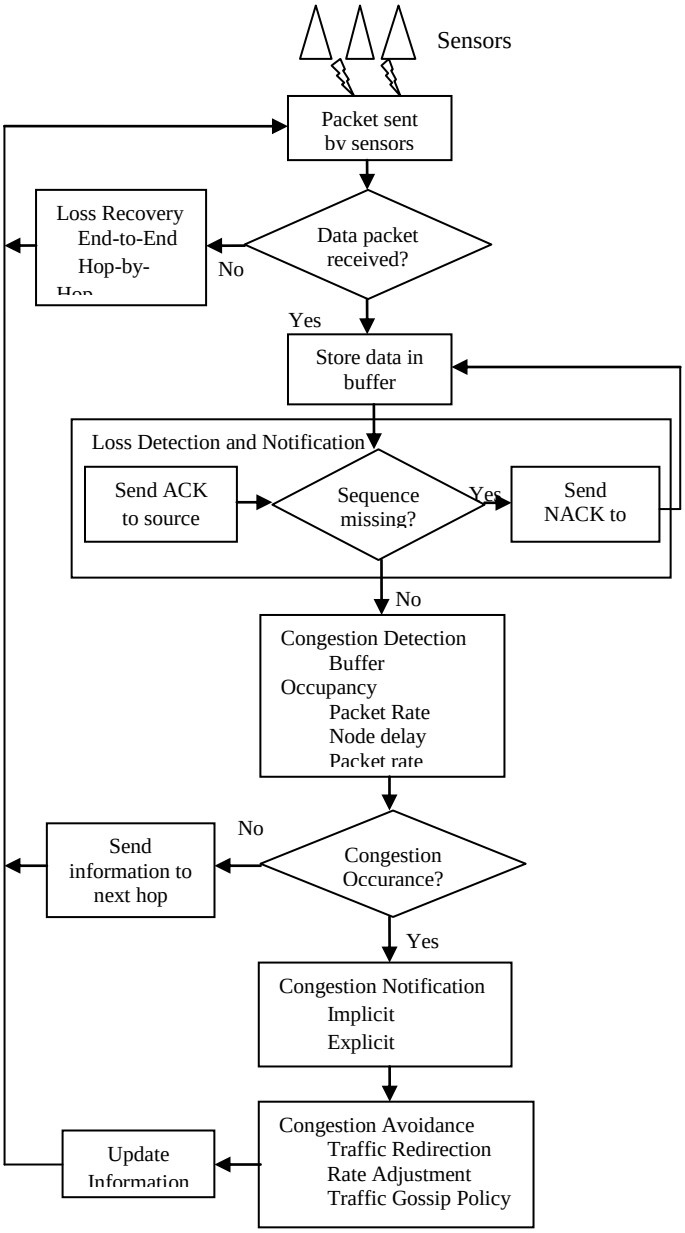

Figure 2: Flow chart of function of transport protocol

DTC: Distributed TCP Caching [28] increases the performance of TCP in wireless sensor network. In DTC sensor nodes help each other in caching the data segments, or if any segment is lost because of any link error or failure, then neighboring node retransmit the lost segments. Segment from cache is deleted only when they get acknowledgement of that segment or when segment times out. Nodes that are close to sink node, DTC shifts the load on that nodes. Selective acknowledgement used by DTC, it improves efficiency of loss recovery process. DTC uses a technique called flying start that provides a good estimate of round trip time (RTT), and it attains 10-25% of improvement over slow start mechanism that is used by TCP.

WISDEN: Wisden [41] provides reliability for structural monitoring applications in wireless sensor network. To achieve data reliability, it uses a hybrid of end-to-end loss recovery and hop-by-hop loss recovery mechanism. It is based on a data time stamping scheme in which base station have enough knowledge of timings of packets like when that packets are generated by sending nodes and when they are received at base station, so it decreases overhead. There is no need of global clock synchronization. Widen compress periods of structural responses by using a run length encoding scheme. Widen implementation is performed on Mica 2 motes.

GARUDA: GARUDA [16] works in three steps: In first step WFP wait for first packet pulse transmission is used, it guaranteed the successful delivery of a single or first packet to all sensor nodes. In second step it chooses core sensor nodes and noncore sensor nodes, nodes that have a hop count multiple of 3 from sink node is elected as core nodes and other nodes are elected as noncore nodes. In third step a two stage NACK based loss recovery process is used to recover losses, it uses out of order sequencing for forwarding the data and it also minimizes overhead of retransmission process. It is only evaluated through ns2 simulator not performed on experimental testbed.

RBC: Reliable Bursty Convergecast [29] is a hop-by-hop upstream reliable transport protocol which is designed to reliably deliver the large quantity of data from different locations to a sink node. Sensor nodes divide large data into small fragments and sending to sink node through different paths and at sink node all the fragments are reassembled. It uses a window less block acknowledgement scheme that ensures reliability and reduces unnecessary retransmissions. It uses a differentiated contention control mechanism in which sensor nodes uses virtual queues and priority is given to nodes according to their queuing conditions, packets that have high rank in virtual queue has to access the channel first. It uses performance metrics event reliability, packet reliability, event good put and node reliability. RBC does not have any energy model so it does not support some applications that need more energy utilization.

DTSN: Distributed Transport for Sensor Network [23] is end-to-end upstream protocol which provides different grades of reliability. It uses Selective Repeat Automatic Repeat Request (ARQ) mechanism to ensure full reliability service, uses both positive acknowledgement and negative acknowledgement, as it consumes less of energy so it increases the lifetime of network. In differentiated reliability service, enhancement flow and forward error correction are used; in enhancement flow at source node only a fraction of data is buffered and then transmitted with full reliability. Differentiated reliability uses forward error correction which increases throughput.

ERTP: Energy Efficient and Reliable Transport Protocol [30] upstream transport layer protocol. It is mainly used by data streaming applications where more than one sensor node senses the data and sends data to sink node. It employs a statistical reliability metric which assures that the number of data packets received at sink node is exceeding from a threshold or not. For loss recovery of packets, it uses stop and wait hop-by-hop implicit acknowledgement and explicit acknowledgement is send to source node when a packet successfully reaches at sink node.

RP2PT: Reliable Point to Point Transport protocol [27] firstly establishes a virtual circuit between sensor nodes and sink node. All data is fragmented at source nodes and send to sink node through virtual circuit and reassembly of data packets is performed at sink node. All intermediate nodes contain the information of virtual circuit such as address of source, address of destination, next hop and previous hop. It uses two type of transmissions upload and download transmission. It has better performance in case of number of transmitted packets, energy efficiency and number of acknowledgements.

DCDD: Diversity Coded Directed Diffusion [32] uses the prongs for energy efficiency. It uses formats of query packet, answer packet, interest packet and observation packets. In DCDD firstly large observation is fragmented into small parts and each fragment take different optimal path to reach to sink node and at sink node reassembly of fragments is performed.

Here reliability is achieved by encoding and decoding. Encoding and decoding is performed using TWOFISH algorithm. In DCDD sink node firstly send query packet to sensor nodes, after receiving query packet sensor nodes increments hop count and compare the energy level if energy of sensor nodes is lower than the energy mark then it drops the packet or if energy of sensor is greater than energy mark then it processes the packet. Then sensor nodes firstly make a neighboring table and send answer packet to sink node.

A New Reliable Data Delivery Protocol in wireless sensor network: The aim of this protocol [42] is to provide high reliability and, minimizing overhead and network delay. It uses a new queue pattern which gives priority to packets. Each node has a queue whose main task is to temporary store packets and manages their retransmission. Ready bit is used by every packet, it indicates its status. If ready bit is 1 then it means that packet is ready to send or if ready bit is 0 it means that the packet has been already sent and now no need to resend that packet. After receiving ACK or NACK, node checks packet ID set in the ACK then node compares packet ID with packets in its queue, if it matches then that packet and other packets which are older than these packets are deleted from queue. It is performed on experimental testbed using single line topology. Limitation of a new reliable data delivery protocol is that it is not scalable.

RETP: Reliable Event Transmission Protocol [8] consists of two procedures accurate event detection and real time reliable transmission. In accurate event detection, whenever an event is occurred nodes which are nearer to event forms a cluster which saves energy. To ensure event detection every node checks sensed value and threshold value. If sensed value is greater than threshold value then it ensures that the event has been occurred. Each node after individual sensing broadcast a packet which contains sensed value, then the nodes take a combined cooperate decision and final decision is made among clusters. To achieve real time and reliable transmission, more than one sensor nodes called decision nodes send event packet to sink node to improve the event reliability. In this protocol, number of event forwarding nodes is restricted by n/2 for even number of nodes and (n-1)/2 for odd number of nodes. It uses greedy approach for routing. RETP is performed on ns2 simulator and it has good results in terms of delivery ratio and energy efficiency.

3.2 Reliability and Congestion based Protocols

This section presents transport layer protocols that provide both reliability and congestion control.

ESRT: Event to Sink Reliable Transport protocol [9] provides upstream event-to-sink reliability, energy efficiency and congestion control. The base station implements the algorithm to take the decision that the event is detected reliably or not. Observed reliability and desired reliability are two categories of ESRT reliability. The observed reliability r_i is the number of packets that are received at sink node in decision interval i. The desired reliability R is the number of packets needed which ensures the event detection reliably. If event to sink reliability is smaller than required then it increase the reporting frequency to get the required reliability or if event to sink reliability is greater than required, then reporting frequency is decreases to avoid the congestion and it saves energy consumption. ESRT has several limitations such as it does not guarantee reliable delivery of every packet, it only guarantees reliable detection of individual event to sink node. As in wireless sensor network multiple events occur at same time so there is difficulty in adjusting the reporting frequency.

STCP: Sensor Transmission Control Protocol [22] is end-to-end upstream transport protocol that provides controllable variable reliability and congestion control. For event driven flows ACK based end-to-end-retransmission is used in which positive acknowledgement is send to source nodes. Source node does not delete the packet from its buffer until it gets acknowledgement from sink node. For continuous flows, NACK based end-to-end retransmission process is used in which base station sets a timer, if node does not received packet until timer expires it sends negative acknowledgement to source node. In STCP sensor nodes uses a session initiation packet which helps in making the association of source node with sink node. When base station gets the session initiation packet, it sends ACK to sensor nodes which inform the source nodes that the connection is established and after getting ACK sensor nodes starts transmitting the data to sink node. In STCP sensor nodes always wait for ACK so it causes long latency in large scale of multi hop wireless sensor network.

PORT: Price Oriented Reliable Transport [11] provides upstream event reliability, congestion control and energy efficiency. PORT uses node prices which are defined as the total number of attempt transmission in between sensor node and sink node. To ensure energy efficiency it uses two schemes: In first scheme sink sends feedback of the exact reporting rate of each source nodes and also sends their energy consumption. In second scheme source nodes sends feedback to sink node which is about the congestion and because of congestion nodes cost increases. PORT is based on three assumptions: first is source nodes would keep reporting data for a long period of time based on interest, second is sink node has the knowledge about the sources of data from where it originates and third is sink node is aware about the information of that carries a data packet.

DST: Delay sensitive Transport [10] provides both reliability and congestion control, a end-to-end upstream transport protocol and also it is energy efficient. To ensure reliable event detection it uses observed delay constraint reliability and desired delay event reliability. In congestion control mechanism, any sensor node whose buffer is overflow because of in excessive data packets is called congested and then source node sends a congestion notification to sink node. In real time event transport mechanism, two main components are used event transport delay which is time between detection of any event and reliably delivery of that event to sink node and; event processing delay which is processing delay estimated by sink node. It is essential that event to sink delay should be greater than of sum of event transport delay and event processing delay for reliable event detection. The limitation of DST is that there is difficulty in adjusting the reporting frequency.

ART: Asymmetric and Reliable Transport [24] use end-to-end bidirectional reliability in wireless sensor network. It offers reliability in two directions: upstream end-to-end event reliability and downstream end-to-end query reliability. ART uses an energy aware node classification scheme in which nodes are categorized as essential nodes and non essential nodes, a group of sensor nodes that are choose on the basis of

residual energy are called essential nodes. It is a type of weighted greedy algorithm. The algorithm gets the information of sensor nodes that have limited battery and then there is less chances to become that nodes essential. Thus, this algorithm balances the available energy and increases the network lifetime. ACK mechanism is used for transferring the events and for reliable query delivery NACK is used. It uses upstream congestion control mechanism. The limitation of ART is that it does not provide congestion control for non essential nodes. In ART congestion control mechanism is centralized so there is large load on network as traffic passes through the network.

RCRT: Rate Controlled Reliable Transport is [25] is a multipoint to point transport protocol, in RCRT all functionalities like congestion detection, rate allocation and rate adaption are performed at sink node. RCRT has main six goals. The first goal is that data packets send from source nodes are reliably delivered at sink node. Second goal is to sustain network efficiency at an optimal operating point. Third goal is to support multiple different concurrent applications. The fourth goal is to provide flexibility to different applications by choosing capacity allocation policies. The fifth goal is that main functionalities are performed at sink node not at sensor nodes. The sixth goal is that RCRT is robust for nodes that are entering and leaving system as because of congestion, traffic route dynamically changes so RCRT adjust itself according to these changes.

$(RT)^2$: Real Time and Reliable Transport [33] provides reliability, timely event detection, and congestion control and energy efficiency. It is based on event to action delay bound which is sum of event processing delay, event transport delay and event action delay. This protocol is based on two states start up state and steady state: In startup state, to capture the transmission rate of packets the source node sends a probe packet to receiver; in steady state, it consists of further four sub states such as increase, decrease, hold and probe states. In increase state when the source node gets the feedback from sink node, it increases the transmission rate. In decrease state after getting the feedback from sink node, it decreases the transmission rate if desired. It uses a combined congestion detection method which uses a local buffer level monitoring and an average node delay calculation. The limitation of $(RT)^2$ is that because of its configuration adjustment nature it causes large delay in wireless sensor network

RTMC: Reliable Transport with Memory Consideration [34] provides 100% reliability and ensures that all the data packets received at sink node reliably. RTMC is motivated from a pipe flow method. Four types of packets are used in RTMC: initiation packet, data packet, requiring packet and end packet. In header of packet, RTMC contains entire information of memory and exchanged that information between neighbors and by using that method it helps in preventing memory overflow. From experimental results it was clear that it provides 100% reliability and effective channel utilization. It has good performance in terms of energy cost, memory cost and transport time etc.

E^2SRT: Enhanced Event to Sink Reliable Transport [13] is a modified version of ESRT which provides reliability, congestion control and energy efficiency. In ESRT there is a problem called 'over demanding' event reliability problem. This protocol solves this problem. It works same as that of ESRT, it checks the event to sink reliability if it is greater than desired reliability it decreases transmission rate of packets which avoid congestion and minimizes the consumption of energy. And if event to sink reliability is lesser than that desired reliability, it increases the transmission rate of packets to get the desired reliability. E^2SRT has good performance in terms of throughput, latency and loss rate in comparison to ESRT.

LTRES: Loss Tolerant and Reliable Event Sensing [14] provides both reliability and congestion control. For congestion control it uses a source rate adaption mechanism. In this mechanism firstly sink node measures the event sensing fidelity level and then sends that information of measure to enodes. To ensure the congestion control the sink node updates their source rate on the basis of enodes. Overhead minimizes because of light weight congestion detection mechanism. The limitation of LTRES is that as it uses the source rate adaption mechanism and in it lot of energy is wasted.

ERCTP: End-to-End Reliable and Congestion Aware Transport layer Protocol [26] provides both reliability and congestion control. ERCTP has two modules congestion module and reliability module. To achieve the reliability ERCTP uses Distributed Memory Storage (DMS) in which designated intermediate nodes stores temporary packet information, and if data is lost and not reached to sink node then sink node can get the packet information from designated intermediate nodes. Congestion control mechanism is further divided into three sub parts: congestion detection, congestion notification and congestion avoidance. In congestion detection, buffer occupancy and link capacity are checked to detect the congestion. In congestion notification, nodes place a congestion notification bit either 0 or 1 in the packet and send it to source node and notifies source nodes about the congestion. In congestion avoidance, to reduce source rate value is adjusted.

TRCCIT: Tunable Reliability with Congestion Control for Information Transport [35] uses some localized techniques to ensure tunable reliability such as hybrid acknowledgement, probabilistic adaptive transmissions and retransmission timer management. In TRCCIT for congestion control data is transformed from multiple different paths. The performance metrics in TRCCIT are information transport reliability, timeliness and efficiency. Information transport reliability is the ratio of number of data packets obtained by sink nodes to the total number of data packets produced by source nodes. Timeliness is the time between generations of first information data packet at source node to receiving of that data packet at sink node. Efficiency is the amount of transmitted messages which are required for reliability.

QERP: Quality Based Event Reliability Protocol [12] uses a property which means according to environmental conditions for event detection; data reported from every sensor nodes is different in contribution degree. It uses two interdependent processes one is selection process and other is transport process. A selection process is used for electing source nodes which send data to sink node on the basis of contribution degree. The transport process successfully delivers the data even in case of congestion. Selection process uses two fields one is CD field that contains contribution degree of data packet and other is Full Selection field, if FS field is set that means all sensor nodes send event information to sink node. These two fields are placed in selection process and utilized by transport process. It provides better reliability and energy efficiency as compare to ESRT. It handles congestion with the help of buffer management.

4. COMPARISION OF EXISTING TRANSPORT LAYER PROTOCOLS

Table 1, 2, 3 and 4 shows the comparison of various transport layer protocols in wireless sensor network using design and technical parameters. In table 1 comparison has been made between the transport protocols that provides only reliability and comparison is based on parameters reliability level, reliability direction, loss recovery type, loss notification, throughput, delay, simulation environment and energy efficiency. In Table 2 comparison has been made between transport protocols that provides both reliability as well as congestion control by using following parameters like reliability level, reliability direction, loss recovery type, loss notification, congestion detection, congestion notification, congestion avoidance, throughput, delay, simulation environment and energy efficiency.

Reliability is an important function of transport layer; it ensures that packets are delivered successful from source to destination or not. In wireless sensor network, packet drop occurs due to several reasons such as poor channel conditions, node failure and congestion etc. then reliability must detect the packet drop and retransmit the dropped packet. Packet reliability means all the packets generated at source nodes should be delivered at destination node reliably [43]. From Table 1 and Table 2, all the protocols provide packet reliability, except RETP [8], ESRT [9], DST [10], PORT [11], QERP [12], E^2SRT [13] and LTRES [14] which provide event reliability. Event reliability means successfully detection of event. Data is flow in two directions in wireless sensor network upstream and downstream. Upstream means data transmission from source nodes to sink node, downstream means data transmission from sink node to source nodes. Except GARUDA [16] and PSFQ [18] all the protocols in Table 1 and Table 2 offers upstream reliability.

To recover packet loss either end-to-end loss recovery or hop-by-hop loss recovery is used. In end-to-end loss recovery mechanism only source node caches the data, and it is responsibility of sink node to detect the loss and requesting for retransmission. As shown in Table 1 and 2 DST [10], STCP [22], DTSN [23], ART [24], RCRT [25], ERCTP [26] and RP2PT [27] offers end-to-end loss recovery. In hop-by-hop loss recovery, all intermediate nodes cache the data, detect packet loss and send requests for retransmissions. Hop-by-hop loss recovery is very faster and more energy efficient than end-to-end loss recovery, but it needs extra memory at intermediate nodes to cache the data. End-to-End loss recovery mechanism causes large delay and low throughput. Protocols like RETP [8], PORT [11], PSFQ [18], DTC [28], RBC [29], ERTP [30], RMST [31], DCDD [32], $(RT)^2$ [33], RTMC [34], TRCCIT [35] and A new reliable delivery protocol [42] offers hop-by-hop loss recovery. ESRT [9], E^2SRT [13] and LTRES [14] provides event to sink reliability where event information is send to sink node. WISDEN [41] protocol provides a hybrid of end-to-end loss recovery and hop-by-hop loss recovery mechanisms. Transport protocols use different loss notification techniques for loss recovery such as implicit acknowledgement, explicit acknowledgement, selective acknowledgement and negative acknowledgement. Table 1 and 2 shows the loss recovery notifications which are used by transport protocols to recover the losses.

Congestion occurs when any node receives more packets as compare to packets that it forwards and process to other nodes so it cannot handle that packets and starts dropping the packet. It causes unnecessary packet retransmissions, consumes lot of energy and also increases network latency. ESRT [9], E^2SRT [13], STCP [22] and RCRT [25] detects the congestion when the queue length go beyond a predefined threshold value. ART [24] uses a timer to detect congestion; if node does not receive any acknowledgment packet until timer expires, then congestion is detected. QERP [12] and ERCTP [26] detect congestion when buffer capacity is higher than a predefined threshold value. Node delay means delay supposed at each node by each packet to reach at destination node. DST [10] and $(RT)^2$ [33] detect congestion in case of node delay and buffer occupancy. After congestion detection, notification of congestion is send to other nodes by either explicitly sending control messages to other nodes or implicitly that includes control information in ordinary packet. In Table 2 all reliability and congestion aware protocols uses implicit congestion notification except STCP [22] and ART [24]. To avoid the congestion, there are two techniques rate adjustment and traffic redirection used. Rate adjustment means send the packets with lower rate. Rate adjustment decisions are taken by the nodes that are in congestion themselves, or by sink node. ESRT [9], DST [10], QERP [12], E^2SRT [13], LTRES [14], RCRT [25], ERCTP [26], $(RT)^2$ [33] and TRCCIT [35] uses rate adjustment. Traffic redirection refers to redirect the traffic to different path. PORT [11] and STCP [22] uses rate adjustment and traffic redirection to avoid the traffic.

As show in Table 1 and 2 some of protocols implemented in simulator or in experimental testbed, and some protocols are implemented in both. All the protocols are energy efficient except GARUDA [16], PSFQ [18], RCRT [25], RBC [29], TRCCIT [35], WISDEN [41] and A New reliable data delivery protocol [42]. Comparison of protocols on the basis of design parameters such as number of sensor nodes, type of topology used, Size of packet, size of buffer, traffic load, simulation time and coverage area are shown in Table 3 and 4.

Table 1: Comparison of reliability based protocols (Technical Parameters)

Protocol	Reliability Level	Reliability Direction	Loss Recovery	Loss Notification	Throughput	Delay	Energy Efficient	Simulation Environment
PSFQ	Packet	Down	Hop-by-Hop	ACK	Low	Small	No	NS2 Simulator, Experimental Testbed
RMST	Packet	Up	Hop-by-Hop	NACK	Low	Large	Yes	NS2 Simulator
DTC	Packet	Up	Hop-by-Hop	eACK, SACK	Low	Medium	Yes	OMNET++
WISDEN	Packet	Up	Hop-by-Hop, End-to-End	iACK, NACK	Medium	Large	No	Experimental Testbed
GARUDA	Packet	Down	Two tier loss recovery	NACK	High	Small	No	NS2 Simulator
RBC	Packet	Up	Hop-by-Hop	iACK	Low	Small	No	Experimental Testbed
DTSN	Packet	Up	End-to-End	iACK, eACK	Medium	Large	Yes	OMNET++
ERTP	Packet	Up	Hop-by-Hop	iACK, eACK	Medium	Small	Yes	NS2 Simulator
RP2PT	Packet	Up	End-to-End	ACK	Low	Large	Yes	C++
DCDD	Packet	Up	Hop-by-Hop	ACK, NACK	Low	Small	Yes	NS2 Simulator
A New Reliable Data Delivery Protocol	Packet	Up	Hop-by-Hop	eACK, NACK	High	Medium	No	Experimental Testbed
RETP	Event	Up	Hop-by-Hop	iACK	High	Medium	Yes	NS2 Simulator

Table 2: Comparison of both reliability and congestion based protocols (Technical Parameters)

Protocol	Rel. Lvl.	Rel. Dir.	Loss Recovery	Loss Notif.	Congestion Detection	Cgst. Notif.	Cgst. Avod.	Thghpt.	Delay	Egy. Effnt	Simulation Envi.
ESRT	Event	Up	Event to Sink	iACK	Queue Occupancy	Implicit	Rate Adjust.	High	Large	Yes	NS2 Simulator
STCP	Packet	Up	End-to-End	eACK, NACK	Queue Occupancy	Explicit	Rate Adjust., Traffic Redirn.	Low	Large	Yes	TOSSIM
PORT	Event	Up	Hop-by-Hop	eACK	Node Price	Implicit	Rate Adjust., Traffic Redirn .	Low	Large	Yes	NS2 Simulator
DST	Event	Up	End-to-End	-	Queue Occupancy, Node Delay	Implicit	Rate Adjust.	High	Medium	Yes	NS2 Simulator
ART	Packet	Both	End-to-End	eACK, NACK	Core nodes received ACK	Explicit	Reduce traffic of noncore nodes	Low	Small	Yes	NS2 Simulator
RCRT	Packet	Up	End-to-End	Cumm.ACK, NACK	Queue Occupancy	Implicit	Rate Adjust.	High	Medium	No	TinyOS, Experimental Testbed
$(RT)^2$	Packet	Up	Hop-by-Hop	SACK	Queue Occupancy, Node Delay	Implicit	Rate Adjust.	Medium	Medium	Yes	NS2 Simulator

Protocol	Rel. Lvl.	Rel. Dir.	Loss Recovery	Loss Notif.	Congestion Detection	Cgst. Notif.	Cgst. Avod.	Thghpt.	Delay	Egy. Effnt	Simulation Envi.
RTMC	Packet	Up	Hop-by-Hop	iACK	Memory Overflow	Implicit	Header Memory	High	Large	Yes	Simulator, Experimental Testbed
E^2SRT	Event	Up	Event to Sink	iACK	Queue Occupancy	Implicit	Rate Adjust.	High	Small	Yes	NS2 Simulator
LTRES	Event	Up	Event to Sink	ACK	Link Loss Rates	Implicit	Rate Adjust.	Medium	Medium	Yes	GloMoSim Simulator
ERCTP	Packet	Up	End-to-End	NACK	Buffer Occupancy	Implicit	Rate Adjust.	High	Medium	Yes	NS2 Simulator
TRCCIT	Packet	Up	Hop-by-Hop	iACK, eACK	Packet Rate	Implicit	Rate Adjust.	Low	Large	No	TOSSIM
QERP	Event	Up	-	-	Buffer Occupancy	Implicit	Rate Adjustment	High	Large	Yes	QualNet Simulator

Table 3: Design parameters for reliability based protocols

Protocols	Topology	No. of sensors	Size of packet (bytes)	Coverage area (mt^2)	Traffic Load	Simulation Time
PSFQ	Linear	13	50	100*100	100 pkts./sec.	100ms
RMST	Grid	21	50-100	100 *100	-	-
DTC	Chain	11	100	-	500 pkts./sec.	30s
WISDEN	Tree	10	80	40*20	0.1,0.2,0.25.0.5,1 pkts./sec.	142s
GARUDA	Grid	100	1kb	650*650	25 pkts./sec.	-
RBC	Grid	49	-	-	Upto 14 pkts./sec.	40s
ERTP	Ad-hoc	200	40	180*180	1/60 pkts./sec.	200s
RETP	Adhoc	35	100	500*500	-	200ms

Table 4: Design parameters for both reliability and congestion based protocols

Protocols	Topology	No. of sensors	Size of packet (bytes)	Coverage area (mt^2)	Buffer size	Traffic Load	Simulation time
ESRT	Ad-Hoc	200	30	100*100	65	10, 0.1, 0.01, 0.01 pkts./sec.	60s
STCP	Ad-hoc	50,100	-	100*100	-	1/50 pkts./sec.	5000s
PORT	Ad-hoc	100	36	1350*1350	50	50 pkts./sec.	500s
DST	Ad-hoc	200	30	200*200	65	1, 0.1, 0.01, 0.001 pkts./sec.	-
ART	Ad-hoc	100	100	300*300	50	Query frq.2-10 sec. Event freq. 0.1-1 sec.	150s
RCRT	Tree	40	64	1125*1125	-	1.2 pkts./sec.	1800-3600s
RT^2	Ad-hoc	200	30	200*200	65	1, 5, 10, 15, 20	1000s

						msg./sec.	
Protocols	**Topology**	**No. of sensors**	**Size of packet** (bytes)	**Coverage area** (mt^2)	**Buffer size**	**Traffic Load**	**Simulation time**
E^2SRT	Ad-Hoc	200	30	100*100	65	4000-4500 pkts./10 sec.	60s
LTRES	Grid	50	32	100*200	-	50, 90, 150 pkts./sec.	-
TRCCIT	Grid	100	29	60*60	36	20 msg./sec.	-
QERP	Ad-hoc	500	-	1000*1000	-	50 pkts./sec.	20s

5. RESEARCH ISSUES IN TRANSPORT LAYER PROTOCOLS

This section presents various research issues of transport layer protocols in wireless sensor networks.

1. Protocols presented above provide reliability either in downstream direction or in upstream direction. There is no protocol except ART [24] which provides reliability and congestion control in both directions.
2. Another issue is that there are two types of loss recovery is used end-to-end and hop-by-hop, in hop-by-hop loss recovery mechanism intermediate nodes takes responsibility for loss recovery and involvement of intermediate nodes needs more cache spaces which results higher cost. End-to-end loss recovery mechanism has large delay and it is not energy efficient. So in existing protocols there is need of better cache placement at intermediate nodes.
3. Transport protocols provide two types of reliability either application reliability or packet reliability not provide

   both of reliability packet and application. If two applications are used by wireless sensor network in which one application requires application reliability and other application requires packet reliability, so its faces difficulty. There is need of mechanism that provides packet reliability and application reliability both.
4. In STCP [22] protocol, sensor nodes generated data with different priorities. Except STCP other protocols which are discussed above are not use priority. The protocol must use the priority as it provides better QoS.
5. Existing transport layer protocols use cross layer optimization very rarely [44]. It solves the issues of scalability, network lifetime, limited resources etc. So cross layer optimization is more important in wireless sensor network.
6. Sensor nodes have limited power and it is charged with external batteries and it's difficult to replace the battery if more energy is consumed. So there is requirement to design transport layer protocols that consumes less energy.
7. Sensor nodes distributed in field firstly make a network by using a topology which provides energy efficiency and reliability. To make such a topology that conserves energy and provides reliability is very challenging.
8. Wireless sensor networks are vulnerable to attacks because of their broadcast nature so they have need of security. Sensor nodes contain critical important information in some applications. If there is no security, a malicious node intercept with data and then send infected data in network, thus security in sensor networks is very important. There are various types of attacks on sensor networks such as denial of service attack, sinkhole attack, hello flood attack, selective forwarding attack, spoofing, desynchronization, acknowledgement spoofing and wormhole attack as discussed in Table 5. To provide security in wireless sensor network cryptography, stegnography should be used [45-48].

6. CONCLUSION

This paper presented a technical study of transport layer protocols in wireless sensor network. The main functions of transport layer are reliable data delivery and effective congestion control mechanism. Firstly this paper described functions of transport layer protocols for wireless sensor networks and then presented a summary of existing transport layer protocols that provides reliability and both reliability and congestion control in wireless sensor networks. Then it discussed the comparison of transport layer protocols on the basis of technical parameters and design parameters; technical parameters such as reliability level, reliability direction, loss recover, loss notification, congestion detection, congestion notification, congestion avoidance, throughput, delay, experiment testbed/simulation and energy efficiency; and design parameters such as topology used, number of sensors, size of data packet, traffic load, buffer size, coverage area and simulation time. This paper also discussed some research issues in transport layer protocols for future research.

Table 5: Threats on Wireless Sensor Network

Threat	Threat Description
Denial of service attack	Malicious node sends unnecessary packets and legitimate user does not access services and resources. Environment conditions, software bugs, hardware failures causes denial of service attacks.
The SinkHole attack	A malicious node inserts itself between two communicating nodes for e.g. sensor nodes and sink node; and attracts all data to itself and can do anything with data.
Hello Floods	Malicious node that have high transmission power, broadcast hello message to other nodes by using false route, when nodes send information to base station it passed through attacker. It increases delay in network
Selective Forwarding attack	Malicious node inserts itself between flow path and it forwards some selected messages and dropped other packets.
Spoofing	Malicious node successfully disguise as another node and gain illegitimate advantages
Desynchronization	Disrupting transmission of packets between two nodes by attacker that stuck in synchronization and wastes lot of energy
Acknowledgement spoofing	Attacker spoof acknowledgment and disguise the sender
WormHole attack	Malicious node records messages at one location and tunnels that packet at another location by a hidden route

7. REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_sensor_network. Last seen on: Jan. 14, 2014.

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

[3] J. Postel, "Transmission Control Protocol", Information Sciences Institute,1981,RFC-793.

[4] J.Postel, "User Datagram Protocol",August 1980, pp. 161-164.

[5] M.A.Rahman, A.E.Saddik and W.Gueeaieb, "Wireless Sensor Network: State of Art" , Springer, Heigelberg, Germany,2008, pp.221-245.

[6] I.F.Akyildiz,W.Su,Y. Sankarasubranmaniam and E.Cayirci, "A Survey on Sensor Networks", IEEE Communication Magzine,November 2008, pp.102-114.

[7] C. Wang, B. Li,K.Sohraby, M.Daneshmand and Y. Hu, "A Survey of transport protocols for Wireless Sensor Network", IEEE Network,May/June 2006, pp. 34-40.

[8] K.C.Terence, "RETP: Reliable Event Transmission Protocol in Wireless Sensor Network", IEEE International Conference on Emerging trends in Computing, Communication and Nanotechnology,2013.PP.181-188.

[9] Y. Sankarasubramaniam, O. B. Akan and I. F. Akyildiz, "ESRT: Event to Sink Reliable Transport in Wireless Sensor Network" , ACM MobiHoc,2003, pp. 177-188.

[10] V. C. Gungor and O. B. Akan, "DST: Delay Sensitivr Transport in Wireless Sensor Networks", 7th IEEE International Symposium on Computer Networks,2006,pp. 116-122.

[11] Y. Zhou and M.R.Lyu, "PORT: A Price Oriented Reliable Transport for Wireless Sensor Network", 16th IEEE International Symposium on Software Reliability Engineering,2005, pp. 117-126.

[12] H.Park,J.Lee , S.Oh, Y.Yim and S.H. Kim, "QERP: Quality Based Event Reliable Transport", 8th IEEE consumer Communication and Networking Conference,2011,PP.730-734.

[13] 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 issue 10,2009,pp. 1301-1311.

[14] Y. Xue, B. Ramamurthy and Y. Wang, "LTRES: A Loss Tolerant Reliable Event Sensing Protocol for Wireless Sensor Networks", Computer Communications,Vol 32 Issue 15,ELSEVIER ,2009,pp. 1666-1676.

[15] M. A. Mahmood and W. K. G. Seah, "Event reliability in wireless sensor networks", 7th international conference on intelligent sensors, sensor networks and information processing, 2011, pp. 377-387.

[16] S. J. Park, R. Vedantham, R.Sivakumar and I.F. Akyildiz, "A Scalable approach for Reliable downstream data delivery in Wireless Sensor Networks", ACM MobiHoc,May 2004, pp. 78-89.

[17] A.J.D.Rathnayaka and V.M.Potdar, "Wireless Sensor Network transport Protocol: A critical review", Journal of Network and Computer Applications ELSEVIER,2011, PP. 1-13.

[18] C.Y.Wan, A. T. Campbell and L. Krishnamurthy, "PSFQ: A Reliable Transport Protocol for Wireless Sensor Network", ACM international workshop on WSN and applications (WSNA), September 2002,pp. 1-11.

[19] P. R. Pereira, A. Grilo, F. Rocha et al., " End-to-End reliability in wireless sensor network: survey and

research challenges", EuroFGI workshop on IP QoS and traffic control,December 2007,pp. 1-8.

[20] F.K.Shaikh, A. Khelil and N.Suri, "A comparative study of data transport protocols in wireless sensor networks", 9th IEEE International Symposium on wireless mobile and multimedia network", June 2008, pp. 1-9.

[21] H.Lee, Y. Ko and D. Lee, " A Hop-by-Hop reliability support scheme for wireless sensor networks", 4th Annual IEEE International Conference on Pervasive Computing and Communications, March 2006, pp. 435-440.

[22] Y.g.Iyer, S.Gandham and S. Venkatesan, "STCP: A Generic Transport layer Protocol for Wireless Sensor Network", IEEE International Confrence on Computer Communications and Networks,2005,pp. 449-454.

[23] M. Marchi, A. Grilo and M. Nunes, "DTSN: Distributed Transport for Sensor Networks", IEEE Symposium on Computers and Communications(ISCC),2007, PP. 165-172.

[24] N.Tezcan and W. Wang, "ART: An Asymmetric and Reliable Transport mechanism for Wireless sensor Network", International Journal of Sensor Networks, vol.2, June2007, pp. 188-200.

[25] J. Paek and R. Govindan, "RCRT: Rate Controlled Reliable Transport for Wireless Sensor Networks", international conference on embedded networked sensor systeams,2007, pp. 305-319.

[26] A.Sharif, V. M. Potdar and A. J. D. Rathnayaka, "ERCTP: End-to-End Reliable and Congestion aware Transport Protocol for hetrogeneous WSN", Scientific International journal for parallel and Distributed Computing, November 2010, pp. 359-371.

[27] X. Chan, D.Fang, Na An, T.Xing,F.Chan and B. Gao, "RP2PT: Reliable Point to Point Transport Protocol", IEEE,2011, pp. 490-496.

[28] A.Dunkels, T.Voigt, H. Ritter and Alonso J, "Distributed TCP Caching for Wireless Sensor Network", Annual Mediterranean Adhoc networking workshop,2004,pp. 1-10.

[29] M.G.Gouda, "Reliable Bursty Convergecast in Wireless Sensor Network", ACM international symposium on mobile adhoc networking and computing,2005, pp. 266-276.

[30] T.Le, W. Hu, P. Corke and S.Jha, "ERTP: Energy Efficient and Reliablr Transport Protocol for data streaming applications in Wireless Sensor Network", ELSEVIER Computer Communications,2009, pp. 1154-1171.

[31] F.Stann and J. Heidemann, "RMST: Reliable Multisegment Transport in Wireless Sensor Network", IEEE international workshop on sensor network protocols and applications, May 2003, pp. 102-112.

[32] G. Shinde,S. Joshi and Shami, "DCDD: Diversity Coded Directed Diffusion for Wireless Sensor Network", ICCACCI,ACM,2012.

[33] V. C.Gungor, O.B.Akan and I. F. Akyildiz, "A Realtime and Reliable Transport Protocol sor Wireless Sensor and Actor Networks", IEEE/ACM transactions on networking, 2008, pp. 359-370.

[34] H.Zhou, X. Guan and C. Wu, " Reliable Transport with Memory Consideration in Wireless Sensor Networks", International Conference on Communication(ICC) IEEE, May 2008, pp. 2819-2824.

[35] F.K. Shaikh, A. Ali and N. Suri, "TRCCIT: Tunnable reliability with Congestion Control fot Information Transport in Wireless Sensor Networks" , International Wireless Internet Conference(WICON), 2010, pp. 1-9.

[36] S.SriDevi and M. Usa, "Taxonomoy of Transport Protocols for Wireless Sensor Networks", IEEE International Conference on Recent Trends in Information Technology,June 2011, pp. 467-472.

[37] B. Hull, K. Jamieson and H. Balakrishnan, " Mitigating congestion in wireless sensor networks", 2nd ACM International ACM Conference on Embedded Networked Sensor Systems Sensys, Nov 2004, pp.134-147.

[38] C. T. Ee and R. Bajcsy, "Congestion control and fairness for many to one routing in sensor networks", 2nd ACM International Conference on Embedded Networked Sensor Systems Sensys, Nov 2004, pp. 148-161.

[39] C. Y. Wan, S. B. Eisenman and A. T. Cambell, "CODA: Congestion Detection and Avoidance in sensor networks", 1st ACM conference on Embedded Networked Sensor Systems, Nov 2003, pp. 266-279.

[40] C. Wang, K. Sohraby, V. Lawrence, L. Bo and H. Yueming, "Priority Based Congestion Control in wireless sensor network", IEEE International Conference on Sensor Networks, June 2006, pp.22-31.

[41] N.Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan and D. Estrin, "A Wireless Sensor Network for Structural Monitiring," in Proc. International Conference on Embedded Networked Sensor Systems,2004,pp. 13-24.

[42] M.Pajouhesha, A.M. Bidgoli and M.H. Yektaie, "A New Reliable Data Delivery Protocol in Wireless Sensor Network," in Proc. Journal of Basic and Applied Scientific Research,2012,pp. 132-137.

[43] F.Yunus, N. N. Ismail,S. H. S. Ariffin, A.A.Shahidan, N. Fisal and S. K.Syed-Yuof, "Propose Transport Protocol for Reliable Data Transfer in Wireless Sensor Network", International Conference on Modeling, Simulation and Applied Optimization (ICMSAO), April 2011, pp. 1-7.

[44] C.Wang, K. Sohrby, Y. Hu, B. Li and W. Tang, "Issues of Transport Control Protocols for Wireless Sensor Network", International Conference on Communications, Ciruits and systems, May 2005, pp. 422-426.

[45] H.Sarma and A. Kar, "Security Threats in WSN", IEEE,2006, pp.243-251.

[46] S. Ranson, D. Pfisterer and S. Fischer, "Comprehensive security synthesis for wireless sensor networks", ACM, Dec 2008, pp. 19-24.

[47] A. Tayebi, S. Berber and A. Swain, "WSN Attacks: An overview and critical analysis", 7th IEEE International conference on sensing technologies, pp. 97-102.

[48] L.Buttyan and L.Csik, "Security analysis of reliable transport protocol for wireless sensor network", IEEE,2010. pp. 419-423.