TRANSPORT LAYER PROTOCOL FOR URGENT DATA TRANSMISSION IN WSN

AshwiniD.Karanjawane[1], Atul W. Rohankar[2], S. D. Mali[3], A. A. Agarkar[4]

[1, 3]*Department of E&TC, Sinhgad College of Engineering, Maharashtra, India,* ***ashwini_karanjawane@yahoo.co.in***
[2, 4]*Department of IT, Sinhgad College of Engineering, Maharashtra, India****, rohankar@sinhgad.edu***

Abstract

wireless sensor networks is a growing class of highly dynamic, complex network environment on top of which a wide range of applications, such as habitat monitoring, object tracking, precision agriculture, building monitoring and military systems are built. The real time applications often generate urgent data and one-time event notifications that need to be communicated reliably. The successful delivery of such information has a direct effect on the overall performance of the system. Reliable communication is important for sensor networks. Urgent data transmission has been a serious problem for Wireless sensor networks. WSN face difficulties in handling urgent data like congestion and reliability due to their unique requirements and constraints. Various protocols for congestion avoidance and reliability achievement for WSN have been proposed recently. Few of them have also worked on congestion elimination. These protocols try to minimize the problem using different mechanism. This paper explores these mechanisms and tries to find their features and limitations which directed us for our research.

Keywords: *Congestion, Reliability, Transport layer Protocol, Urgent data transmission, Wireless Sensor Network.*

--***--

1. INTRODUCTION

A WSN as a social infrastructure must transmit urgent information faster and more reliable than other information[1]. This sort of WSNs would carry both urgent and non-urgent information, which apparently should not be handled equally. The urgent information, in areas like security, disaster, environmental, and vital conditions monitoring applications, has to be carried through a WSN with higher reliability and lower delay than other non-urgent information such that for regular monitoring for living and working space control. It means that a WSN must be capable of differentiating and prioritizing packets depending on their urgency and importance according to requests from the application layer. Main motivating scenario for this concept is the realization of quality-enabled networks for environmental monitoring in disaster prevention and emergency response scenarios such as underground mines.

The traditional transport protocols are not directly useful for wireless sensor network. There is a need to synthesize the WSN characteristics and transport layer requirement for the same. In this paper, we present survey of transport layer work cited in the literature. Classification and relevance to the WSN scenario is discussed to formulate the specification and guidelines for our protocol. Further we discuss the core functionalities of the transport layer protocol and its implementation issues.

Rest of the paper is organized as follows: WSNs transport layer requirements are discussed in Section2. In section 3 we will briefly summarize Transport layer design issues. Section 4 provides brief overview of the related work on transport protocols and urgent information transmission Section 5 provides comparative summary of the surveyed protocols and finally we conclude in section 6

2. TRANSPORT LAYER REQUIREMENT

The transport layer protocols for wireless sensor networks should support:

2.1 Reliability

For Wireless Sensor Networks[2] 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. Reliability in wireless sensor networks can be realized by different characteristics such as,

a) Reliability Level : Packet Reliability and Event Reliability

b) Loss Detection and Notification :
Acknowledgment (ACK)
 Negative Acknowledgment (NACK)
 Selective Acknowledgment (SACK)

c) Error Recovery: End-to-End and Hop-by-Hop

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 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. Congestion control can be perform in following ways,

1) **Congestion Detection:** Protocols employ a mechanism whether or not a congestion occurred and at what location. Combinations of parameters like Buffer Occupancy, Packet rate, Packet Service Time/Packet Inter-Arrival Time, Node Delay, Channel Status can be used to detect congestion.
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.
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. There are three different techniques for congestion avoidance as rate adjustment, traffic redirection and polite gossip policy.

2.3 Energy Efficiency

In wireless sensor networks, transport layer protocols should avoid packet loss as much as possible since loss translates to energy waste. 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. 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.

3. TRANSPORT PROTOCOL DESIGN ISSUES

Following are major issues in transport protocol design.

3.1 Congestion Control and Reliability

Transport layer is responsible for congestion control and reliable delivery of data[2]. Since most data are from the sensor nodes to the sink, congestion might occur around the sink. Although MAC protocol can recover packets loss as a result of bit error, it has no way handling packet loss as a result of buffer overflow. WSNs need a mechanism for packet loss recovery, such as ACK and selective ACK used in TCP. Furthermore, reliable delivery in WSNs may have a different meaning than that in traditional networks; correct transmission of every packet is guaranteed. For certain sensor applications, WSNs only need to receive packets correctly from a fraction of sensors in that area, not from every sensor node in that area. This observation can result in an important input for the design of WSN transport protocols. Energy efficiency can be improved by reducing packet loss. For this purpose we should use hop-by-hop congestion control and packet loss recovery mechanism. The hop-by- hop approach can also reduce the buffer requirement at the central nodes.

3.2 Quality of Service (QoS)

Transport 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[2]. Most applications in WSNs are reactive, which means that they monitor passively and wait for events to occur before sending data to the sink. These applications may have only a few packets to send as the result of an event.

3.3 Packets Dropping Rate

Transport protocols for WSNs should avoid packet loss as much as possible since loss translates to energy waste[2]. To avoid packet loss, the transport protocol should use an active congestion control (ACC) at the cost of slightly lower link utilization. ACC triggers congestion avoidance before congestion actually occurs. As an example of ACC, the sender (or intermediate nodes) may reduce its sending (or forwarding) rate when the buffer size of the downstream neighbors exceeds a certain threshold.

3.4 Throughput

The transport control protocols should guarantee fairness for different nodes in order that each node can achieve fair throughput.

3.5 Cross-Layer Optimization

If possible, a transport protocol should be designed with cross-layer optimization in mind. For example, if a routing algorithm informs the transport protocol of route failure, the protocol will be able to deduce that packet loss is not from congestion but from route failure. In this case, the sender may maintain its current rate.

4. LITERATURE SURVEY

A larger number of wireless sensor network applications require urgent data delivery. However, due to the nature of sensor networks, designing a data transport protocol for urgent transmission faces many challenges, such reliability and congestion. This section presents an overview of general reliability and congestion control issues in the data transport protocol for wireless sensor networks and discusses some recently proposed data transport protocols.

There are several transport protocols that have been designed for wireless sensor networks. The existing transport protocols are distinguished by three different categories which are protocol providing only reliability, few provides only congestion control and protocol that provides both reliability and congestion control. Followings are few protocols which we have studied and summarized in Table 1.

4.1 Protocol with Reliability Guarantee

Wan et al. proposed PSFQ (Pump Slowly Fetch Quickly) [3]protocol . It provides reliable communication in downstream direction (i.e. from sink to sensor nodes). It is designed to be scalable and energy efficient. It uses multiple local timers and minimizes the number of signaling messages. It transmit data from sink to sensors at comparatively slow-speed, and allow nodes experiencing data loss to recover any missing segments from immediate neighbors very aggressively. It operates in three steps: Pump operation, Fetch operation, and Report operation. It makes use of NACK for data recovery. Sensors will send data delivery status information to sink using a simple and scalable hop-by-hop report mechanism.

F. Stann et. al. proposed RMST [4](Reliable Multi-segment Transport Protocol) which provides reliability for upstream direction. RMST implements a cross layer between network layer and MAC layer to provide guaranteed hop-by-hop reliability. It is also designed to run above Directed diffusion (to use its discovered path from sensors to sink) in order to provide guaranteed reliability from sensors to sink (delivery and fragmentation/reassembly) for applications.

4.2 Protocol with Congestion Control

Wan et. al proposed CODA[5] (Congestion Detection and Avoidance) protocol. In this protocol they have introduced three schemes as congestion detection, open loop hop-by-hop backpressure and end-to-end multi-source regulation. It improves energy efficiency by controlling congestion. It uses parameters like current buffer occupancy and wireless channel load to detect congestion. Node detecting congestion will notify its upstream nodes to decrease rate accordingly those nodes will trigger to decrease output rate like AIMD. In this way this protocol can regulate multi-source rate using closed-loop end-to-end approach. When a sensor rate value reaches beyond theoretical throughput, it will set regulation bit in event packet. If the event packet received by sink has “regulation” bit, sink should send ACK control message to sensors to inform them to decrease their rate. If congestion is cleared, sink will actively send ACK control message to sensors to inform them to increase their rate.

Wang at el. proposed SenTCP[6] an open-loop hop-by-hop congestion control protocol for upstream traffic with two special features. This protocol uses packet arrival time and packet inter-arrival time to calculate the congestion degree in every intermediate sensor node. For congestion regulation it uses hop-by-hop feedback control. This process also reduces packet dropping, which in turn save energy and increases the throughput. Neighboring sensor nodes will adjust their sending rate in response to the feedback signal, carrying information like local congestion degree and the buffer occupancy ratio. Wang et. al. have proposed PCCP [7] (Priority-based Congestion Control Protocol) provides congestion control in upward direction. Ratio of mean packet arrival time to the mean packet service time is used to calculate a congestion degree. It uses implicit congestion notification by piggybacking the congestion information in the header of data packets. This will avoid additional control packets. PCCP uses priority-based rate adjustment (PRA), a hop-by-hop rate adjustment scheme. It provides three priorities which are source traffic priority, transit traffic priority and global priority based on node priority index.

4.3 Protocol with both Reliability &Congestion Control Guarantee

Currently, there are many protocols that provides both reliability and congestion control. But each protocol still has some drawbacks. Further we will categorize these protocols based on congestion detection technique.

4.3.1 Congestion Control with Queue Occupancy Detection Technique

Akan et al. proposed ESRT [8] an Event to Sink Reliable Transport Protocol for End to End reliability. This protocol achieves reliable event detection in WSN with minimum energy expenditure. For reliable detection of an event and congestion avoidance sink will control the transmission rate of each source. It provides reliability for applications. by controlling sensor report frequency ESRT improves energy efficiency.

Sundaresanat.el. had proposed ATP[9](Ad-hoc Transport protocol), it 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.

Yogesh et al. proposed STCP [10] Sensor Transmission Control Protocol is a generic, scalable and reliable transport layer protocol in which base station is responsible for all major functionalities STCP controls variable reliability, congestion detection and avoidance, and supports multiple flows in the network. Congestion information is carried by data packets. Base station will store all the information from received session initiation packet. Accordingly initiate the timers and other parameters for each flow, and provide acknowledgment of this packet. . STCP supports two types of data flow traffics: continuous for which reliability is measured as the fraction of packets successfully received and event-driven flows where the base station calculates reliability as a ratio of packets received to the highest sequence numbered packet received. Every sensor node maintains two thresholds in its buffer and on the basis of buffer value node will set the congestion notification bit in every packet it forwards. On receiving this packet, the base station informs the source of the congested path by setting the congestion bit in the acknowledgment packet. Accordingly the source will either route successive packets along a different path or slow down the transmission rate.

Kim et al. proposed Flush [11] a reliable transport protocol for Radio network designed for transferring bulk data across a multi-hop path from a source to a sink. Flush uses a sink-initiated control protocol to coordinate transfers, with E2E selective NACK and retransmissions to provide reliability. Flush moves through four phases: topology query, data transfer, acknowledgment, and integrity check. The sink uses an estimate of the Round Trip Time (RTT) to decide when to send a request for packet loss. On long paths, flush pipelines packets over multiple hops. To minimize the transfer time, Flush proposed a distributed rate control algorithm, which dynamically estimates the sending rate that maximizes the pipeline utilization. The sink also needs to keep track of packets it received. In the acknowledgment phase, the sink sends the sequence numbers of the lost packets back to the data source. Flush is designed for bulk data transfer. This protocols aim to achieve 100 % reliability and high throughput.

Alam and Hong have designed CRRT [12] protocol (Congestion-Aware and Rate-Controlled Reliable Transport) 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. It uses congestion Sensor Networks 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.

Giancoliet. al. proposed CTCP [13] (Collaborative Transport Control Protocol). It 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 Fraction of packets successfully received and Energy Consumption. 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.

4.3.2 Congestion Control with Decentralized Parameters

Previous researchers mainly utilize queue occupancy to predict the congestion in a single sensor node. Few researches point out that the queue length alone is not enough to reflect the congestion level in the sensor node accurately, as the essential damage of congestion is the packet drop caused by queue overflows so they have proposed few scheme, in which congestion is detected by not only the queue length but also the queue length change rate or some other decentralized parameters.

Zhou et al. proposed PORT [14] a Price-Oriented Reliable Transport protocol. PORT employs node price to measure the congestion. Node price is defined as the total number of transmissions attempts across the network from a source to a sink for achieving successful packet delivery. To ensure the fidelity of the collected events, PORT estimates the optimal reporting rate for each source. To improve the data reliability from a sensor source to a sink, each node in the network dynamically allocates its outgoing traffic based on the neighboring nodes' feedback of their node prices and the link loss rates between the neighbors. This approach can alleviate network congestion. PORT also employs a source reporting rate control mechanism which controls the source reporting rates based on the node prices of the source. The in-network congestion-avoidance mechanism and the E2E reporting-rate adjustment mechanism can provide fidelity of interested events while minimizing energy consumption.

Tezcan and Wang proposed ART [15] (Asymmetric and Reliable Transport) which is designed as upstream end to- end event reliability, upstream congestion control and downstream end-to-end query reliability. ART consist of three main operations, reliable query transfer, reliable event transfer and distributed congestion control. ART classify nodes as essential node (E-nodes) which is a subset of sensor nodes and nonessential node (N-nodes) .in congestion less network , both E-node and N-node will transmit message to the sink. For upstream and downstream reliability, ART uses both ACK and NACK mechanisms.

Paek and Govindan proposed RCRT [16] (Rate-Controlled Reliable Transport). It 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. (2) to sustain network efficiency by avoiding congestion collapse. In congestion collapse, sources are sending data faster than the network can transport them to the base station. (3) Provides flexibility to choose capacity allocation policies by different applications. (4) be robust to routing dynamics and to nodes entering and leaving the system.

Zhou et. al. have proposed RTMC[17] (Reliable Transport with Memory Consideration). 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. It also results in maximization of throughput and reduces the transport time. It is much more energy-effective, and has less memory cost and less transport time.

4.4 Protocol with Congestion Elimination Mechanism

The urgent information produced in event driven applications has some special characteristics compared with the traditional periodic collecting scenarios.

1. When an emergency happens, a large amount of traffic are injected into the network simultaneously and in a very short time
2. In emergent situations, it is urgent to get the information about the event as quickly as possible

There are various types of traffic with different priorities, which should be handled with different qualities of service. Various protocols are designed for communication in WSN. But, it is observed that very few of them describe the assured transmission of urgent data. The methods which are developed till dates are application specific. Most of them detect congestion in a sensor node by a metric such as the queue length or the ratio between packet service time and packet arrival time. They also assume that the congestion occurs just on the moment which is inconsistent with the real environment. Meanwhile, all of their rate adjustment schemes do not take the urgent information's reliable transmission into consideration. There are few protocols which try to eliminate congestion and provide reliable transmission of urgent data. Few of them are summarized in table 2.

Lulu Liang et al. proposed (RETP-UI)[18]a reliable transmission protocol for urgent information in wireless sensor networks. This protocol classifies the traffic into three classes and correspondingly maintains three kinds of priority queues in each sensor node. To predict the congestion more accurately, it detects congestion by combining the queue length and its fluctuation together. Furthermore, state machine is also introduced in evaluating the congestion level to alleviate congestion; they have design a multistage rate adjustment scheme. Finally, conduct the detail simulations by comparing the performance of RETPUI with PCCP. The simulation results show that proposed RETP-UI can provide a reliable transmission service for urgent information with lower packet loss probability, shorter delay, and higher throughput.

Tetsuya Kawai et al. had proposed a [19]fast and reliable transmission mechanism for urgent information in sensor networks. An emergency packet first establishes an assured corridor from the origin node to the BS. In the corridor, all nodes keep awake for fast transmission of emergency packets. Along the corridor, all nodes refrain from the emission of normal packets to avoid disturbing transmission of emergency packets in the corridor. The other nodes stay in normal operation. They also introduced a retransmission scheme to achieve reliable transmission of the first emergency packets. Their experiments showed that the corridor was quickly established and then emergency packets are transmitted to the BS with a high reliability of more than 90 % delivery ratio and a low latency of less than 90 ms. In this protocol congestion has been eliminated by suppressing normal data transmission and establishing assured path for emergency data.

Manikanden Balakrishnan et al. have introduced Channel Preemptive EDCA[20] (CP-EDCA) scheme, an in-channel emergency preemption methodology for the EDCA framework. In CP-EDCA, the emergency traffic preempted the services of other routine traffic in the network for achieving deterministic MAC delay bounds. The simulation results of emergency frames depicted up to 50% uniform decrease in MAC delays and insensitivity to routine traffic competition, even under network overloads. CP-EDCA will retain all the advantages of random MAC, while still guaranteeing deterministic QoS bounds for sporadic emergencies. The initial work aimed at validating the CP-EDCA method and the importance of preemptions to expand the applicability of 802.11e standards to distributed emergency reporting.

Rachid Haji et. al. have proposed a framework for [21]Adaptive Management of QoS in different situations (Ad-M-QoS-DS) that guarantees a level of QoS using the following parameters. The situation, the degree of importance of information and QoS parameters Under normal circumstances, the Framework focuses on the efficiency of energy consumption. Upon detection of an event of emergency, the proposed framework adapts its behavior to minimize delay and ensure reliability. And if that requires the intervention of operators, the framework ensures mobility management, collaboration, and security. Upon detection of an event, sensors transmit the information on multi-hop to the base station which is responsible for transmitting them to the Coordination Committee. The latter analyzes the information received. If the event is safe, the data will be stored in a database and if the event presents a danger the Committee takes appropriate decisions and informs the operators on the appropriate actions. Authors have proposed different modules of Framework that are necessary for the proper management of rescue operations and cooperation during a disaster. 1) Message Classification and Prioritization Module 2) Aggregation Management Module3) Adaptive Energy Management Module4)Adaptive Load Management Module5) Mobility Management Module6)Routing Security Module 7)MAC Filter Module 8) Two security modules need to be taken into account Routing Security module and MAC Filter module.

S. Sharma and D. Kumar [22] presents a Framework for adaptive routing protocol. It makes use of priority for data routing. According to data priority the framework describes two paths for transmission. It discovers and maintains the shortest path by using their routing protocol which is an enhanced version of Ad hoc On-Demand Distance Vector Routing (AODV). This will also improve transmission delay. For improving energy efficiency they have used an ant-based protocol. The WSN present much essential liabilities that increases the security risk. Deny Of service attack will reduce energy efficiency for which WNS requires efficient and effective security mechanism.

Koichi Ishibashiet. al. proposed [23] a forwarding method for urgent messages on the ubiquitous wireless sensor network. The proposed method provides a reliable forwarding method for urgent messages, even if packet loss on the wireless links exists. Evaluated the effect of traffic and message's loss rate for an urgent message by computer simulation and confirmed that the proposed method achieves the lower message's loss rate than the existing routing protocol in the region where the packet loss probability on the wireless links are higher. The urgent messages are sent from a monitoring node, appreciating the detected event as emergency situation, to a specific node such as the network management node. To meet specified requirements, they have invented a new design scheme of the ad hoc routing protocol to overcome poor quality of error-prone wireless channel, in order to support the reliable forwarding method for the urgent messages on the UWSN.

A D Karanjawaneet. al [24] proposed the path assured data transfer protocol(PAT) which operates in three stages. In the first stage the ED node desiring to transfer urgent information initiates blocking operation for rest of the devices to assure clear path for urgent data packets. In the second stage, the urgent data packets are transferred with software acknowledgment from the receiver towards the destination master node. When all the packets are transferred, the master initiates release message for the network. The assured path guarantees collision less data transfer towards the destination devices and avoid delays due to retry transmissions. The PAT is designed for reliable transfer of single as well blocks of urgent packets. The PAT protocol improves the data transfer reliability over normal data transfer protocols by 20-40%.

5. COMPARATIVE ANALYSIS

This section presents comparative analysis of the above cited transport protocols based on reliability, congestion control and energy efficiency. Table 5.1resents the comparison based on congestion detection technique and reliability support.

Reliability is the main function at transport layer which ensure the proper delivery information from source to destination or sink node. There are difference reliability mechanisms for different proposed protocols because most of the protocols were designed to solve problem based on the application. Protocols like ATP, STCP, ART, Flush, RCRT, CTCP, CRRT, offer end-to-end error recovery in which only the final destination node is responsible for detecting loss and requesting for retransmission. This approach will cause large delay and low throughput. Other protocols like RTMC, CRRT, PSFQ, RMST offer hop-by-hop error recovery which is widely accepted recovery mechanism in sensor networks. In this method intermediate nodes, rather than just the final node, perform loss detection and recovery. Pair of neighboring nodes is responsible for loss detection and can enable local retransmission that is more energy efficient. The biggest advantages is that recovery from packet loss can occur quickly, and progress made in early hops is not lost if a failure occurs in later hop.

Among these RMST and PSFQ do not provide any congestion control scheme. PSFQ can't detect the loss of single packet since it used only NACK not ACK. It uses statically and slowly pump that result in large delay. Besides that, most of the protocols used negative acknowledgement (NACK) and time out for loss detection and notification stage and used packet retransmission for loss recovery stage. Each proposed method has advantages and disadvantage that appropriate with the application itself.

Protocols like CODA, PCCP and SenTCP do not provide any reliability mechanism and have only congestion control mechanism. In PCCP, the priority is defined from a node viewpoint instead of the traffic flow viewpoint. Thus, the traffic flows from a node cannot be differentiated.

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, ATP, Flush and ESRT solely detect the congestion when the buffer usage is higher than the predefined threshold, whereas CRRT and SenTCP use packet rate addition to the buffer occupancy. CTCP uses both transmission error loss rates and the buffer usage. CODA uses channel status with QO. In CODA the delay or response time of closed-loop multi-source regulation will be increased under heavy congestion since the ACK issued from sink would loss with high probability at this time. ESRT have the drawbacks, such as this protocol may not applicable to many of the WSN application because ESRT assume that the base station is one-hop away from all sensor nodes. STCP and ESRT are not as energy efficient as HBH loss recovery schemes since the rate decision is controlled centrally. ESRT also has some performance problem i.e. it assumes that all the sensor nodes within the WSN have a clock synchronization. Flush is not designed for data streaming applications in which energy efficiency is highly concern but not throughput. ART have the disadvantages where any packet loss due to congestion at non-essential nodes will unnoticed and their recovery is not guaranteed because congestion control and the two-way reliability is maintained by only E-node. Rest of the protocols detects the congestion based on feedback parameters of the reliability module.

Table-1: Transport protocols for congestion control and reliability.

Protocol Name	Congestion Detection	Congestion Avoidance	Reliability level	Type	Reliability Confirmation
PSFQ	-	-	Packet	H-B-H	NACK
RMST	-	-	Packet	H-B-H	NACK
CODA	QO ,Chan. Status	RateAdjs.	-	-	-
Sen TCP	QO , Packet rate	Rate Adjs.	-	-	-
PCCP	Metric ratio	Rate adjs.	-	-	-
ESRT	QO	Rate Adjs.	Event	E-to-E	-
ATP	QO	Rate Adjs.	Packet	E-to-E	SACK
STCP	QO	Rate Adjs.	Packet	E-to-E	NACK
Flush	QO	Rate Adjs.	Packet	E-to-E	NACK
CRRT	QO, pkt. Rate	Rate Adjs.	Packet	E-to-E H-B-H	NACK,Ack
CTCP	QO, Trans error loss	Rate Adjs.	Packet	E-to-E	eAck
PORT	Node price	Rate Adjs.	Event	E-to-E	-
ART	Ack to core node	Reduce Traffic of Noncore node	Packet	E-to-E	NACK
RCRT	Time to recover loss	RateAdjs.	Packet	E-to-E	NACK Cumm. Ack
RTMC	Memory overflow	HeaderMemoryInfo	Packet	H-B-H	-

The congestion warning is notified to other nodes explicitly or implicitly. 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, most of them follow centralized rate adjustment scheme, whereas STCP, Flush, ART and RTMC use decentralized scheme. Exact rate adjustment is a popular method because the node simply schedules the sending of its packet using specific timings in order to fulfill that calculated rate in order to implement accurate rate adjustment.

Energy conservation can be divided into three categories, which are good, fair and no energy efficient. Most of the existing transport protocol do not concern about the energy efficient. The energy conservation for protocols that provide both reliability and congestion control mechanism is low compared with the protocols that provide only reliability or congestion control. Energy efficient need to be emphasized in future transport protocol for WSN. This is due to sensor nodes have a limited operating system lifetime. Thus, mechanism for energy efficient is very crucial in WSN.

Reliable routing is more difficult to achieve in wireless networks than in wired networks, because the wireless bandwidth is shared among no. of nodes and the network topology changes unpredictably as the node move. Also to achieve Quality of services in wireless sensor networks, limitation in power, computational capacities, and memory space should be taken into consideration. This requires extensive collaboration between the nodes, both to establish the route and to guarantee the resources necessary to provide the reliability.

Wireless Sensor Network would carry both urgent and non-urgent information, which apparently should not be handled equally. Previous protocols basically aim at providing a best-effort packet delivery, so that all messages including urgent messages are processed equally. Therefore, when the network is congested, packets with high priority experiences large delay, and possibly could be discarded. It means that a WSN must be capable of differentiating and prioritizing packets depending on their urgency and importance.

Table-2: Congestion elimination in urgent protocol.

Protocol Name	Congestion Detection	Congestion Avoidance	Reliability level	Type	Reliability Confirmation
RETPUI	QO and Fluctuation	Multistage Rate Adjs.	Event	H-B-H	ACK
FARTM	Urgent data Occurrence	Establishing assured path by suspension of normal data transmission	Event	H-B-H	ACK
CP-EDCA	Emergency detection	Normal data preemption	Event	H-B-H	ACK
ADMQOS	Event detection	Priority wise categorization	Event	H-B-H	ACK
OD-AODV	Event classification	Priority wise shortest path transmission	Event	H-B-H	ACK
FMUMUWSN	Event classification	Multipath transmission	Event	H-B-H	ACK
PAT	Urgent event	Blocking of normal data	Event	H-B-H	ACK

There is need to design such a protocol which assure about the reliable and fast transmission of urgent data.

For congestion control, a proper rate adjustment schemes should be implemented to mitigate congestion. Many mechanisms have been proposed in recent years. However, most of the proposed rate adjustment mechanisms decrease the source rate at the cost of event reliability. PAT protocol implies simple mechanism to provide assured path for urgent data transmission. When WSN is used for urgent message transmission, its important purpose is to inform its user about the urgency reliably and timely without loss of fidelity.

CONCLUSIONS

In this paper, we have presented a comparative analysis of the various existing protocol providing reliable & congestion free transmission and also protocols provided for urgent data transmission. In this work first we elaborate problems of using existing protocols for urgent data transmission. We have discussed requirement and design issues of transport layer protocol. We briefly review several existing reliable and congestion control protocols for wireless sensor networks, and list out several problems of the existing protocols. This survey directed us to explore transport layer issues in urgent data transmission.

Although a number of research works on transport layer has been done so far, many of them assume that all of the information transmitted in a WSN is of the same type, which means the network handles all packets equally. Some researchers have provided the reliable and congestion free transmission considering urgent data transmission over WSN by using different mechanisms and modules. However, they involve some complicated communication and calculation and this could be a burden for a resource-constrained sensor node. Our aim is to provide simple mechanism where the transmission of urgent information to controlling device is guaranteed with high reliability and low transmission delay.

REFERENCES

[1] I. Khemapech, et al., "A survey of wireless sensor networks technology," in 6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, 2005.

[2] K. S. Chonggang Wang1, Bo Li, and Weiwen Tang, "Issues of Transport Control Protocols for Wireless Sensor Networks," University of Arkansas, Fayetteville, AR, USA,.

[3] C.-Y. Wan, et al., "PSFQ: a reliable transport protocol for wireless sensor networks," in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, 2002, pp. 1-11.

[4] F. Stann and J. Heidemann, "RMST: reliable data transport in sensor networks," in Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, 2003, pp. 102-112.

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

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

[7] K. S. C. Wang, V. Lawrence, B. Li, and Y. Hu, "Priority-based congestion control in wireless sensor networks," in in Proc. IEEE International Conference on Sensor Networks,Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 22–31.

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

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

[10] Y. G. Iyer, et al., "STCP: a generic transport layer protocol for wireless sensor networks," in Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on, 2005, pp. 449-454.

[11] S. Kim, et al., "Flush: a reliable bulk transport protocol for multihop wireless networks," in Proceedings of the 5th international conference on Embedded networked sensor systems, Sydney, Australia, 2007, pp. 351-365.

[12] M. M. A. a. C. S. Hong, "CRRT: congestion-aware and rate-controlled reliable transport in wireless sensor networks," in IEICE Transactions on Communications, pp. 184–199.

[13] F. J. E. Giancoli, 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.

[14] Y. Z. a. 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, 2005.

[15] N. T. a. W. Wang, "ART: an asymmetric and reliable transport mechanism for wireless sensor networks," International Journal of Sensor Networks, vol. vol. 2, pp. 188–200, 2007.

[16] J. P. a. 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, 2007.

[17] X. G. H. Zhou, 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.

[18] L. Lulu, et al., "A Novel Reliable Transmission Protocol for Urgent Information in Wireless Sensor Networks," in Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, 2010, pp. 1-6.

[19] T. Kawai, et al., "A fast and reliable transmission mechanism of urgent information in sensor networks," Proceedings of the 3rd International Conference on Networked Sensing Systems (INSS 2006), 2006.

[20] M. Balakrishnan, et al., "Service preemptions for guaranteed emergency medium access in Wireless Sensor Networks," in Military Communications Conference, 2008. MILCOM 2008. IEEE, 2008, pp. 1-7.

[21] R. Haji, et al., "Towards an adaptive QoS-oriented and secure framework for wireless sensor networks in emergency situations," in Multimedia Computing and Systems (ICMCS), 2012 International Conference on, 2012, pp. 1007-1011.

[22] S. S. a. D. Kumar, "An approach to optimize adaptive Routing Framework to provide QOS in Wireless Sensor Networks," in proceeding of International Journal of wireless Networks and Communication, vol. 1(1), pp. 55-692009.

[23] K. Ishibashi and M. Yano, "A Proposal of Forwarding Method for Urgent Messages on an Ubiquitous Wireless Sensor Network," in Information and Telecommunication Technologies, 2005. APSITT 2005 Proceedings. 6th Asia-Pacific Symposium on, 2005, pp. 293-298.

[24] A. W. R. A D Karanjawane, S D Mali, A A Agarkar, "Designing Path Assured Data Transfer Protocol for Wireless Sensor Network," In proceeding of International Journal of Engineering Research and Technology(IJERT), vol. 2, pp. 1151-1160, 2013.