

# A Survey on Reliable and Congestion Control Transport Protocols of WSN

Kanchan Kaushal  
CTIEMT  
Shahpur  
Jalandhar, India

Taranvir Kaur  
CTIEMT  
Shahpur  
Jalandhar, India

Jaspinder Kaur  
CTIEMT  
Shahpur  
Jalandhar, India

## ABSTRACT

Transport layer protocols of Wireless sensor networks, plays an important role in the achievement of high performance and the long life time of the network. This layer is specifically needed when a system is organized to access other networks. Two functions provided by this layer are; reliability and the congestion control. Many numbers of protocols are designed to achieve these two functions. This paper gives you a review of reliable transport layer protocols and congestion control transport layer protocols. First, it gives an introduction to the wireless sensor networks. Second, gives an idea about the various services provided by transport layer and the disadvantages of using traditional TCP (Transport control protocol) and UDP (User datagram protocol) of transport layer. Third are some existing transport layer protocols. Further is the conclusion of this review.

## General Terms

Transport layer protocols, Congestion control, Reliability, Wireless sensor networks.

## Keywords

Transport layer protocols, Congestion control protocols, Reliability protocols, Protocol stack of Wireless sensor networks.

## 1. INTRODUCTION

In 1999 it was one of the “21 ideas for the 21st Century” and in 2003 was presented as one of “10 new technologies that will change the world”. This revolutionary technology is known as WSNs. A Wireless Sensor Network [1] is formed of spatially dispersed unmonitored sensor nodes connected via a transmission infrastructure, which is wireless, to cooperatively monitor, record and save physical or atmospheric conditions like temperature, pollutants, sound or motion.”

Wireless Sensor Networks (WSNs) are the rapidly sprout research area, awning both an extensive variety of devices and applications. WSN is an auto composing network of tiny low power sensor nodes which communicate between each other and use radio signals for communication and deployed to sense, monitor and analyze the physical world. Wireless sensor nodes are called “motes”. The motes have very restricted physical size, memory, CPU power and bandwidth.

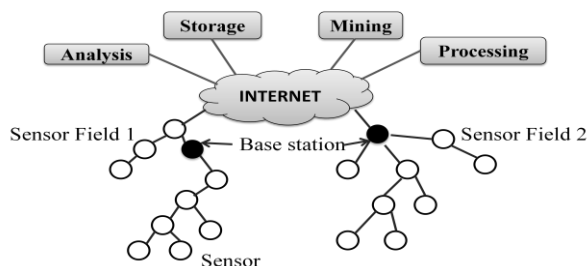


Fig. 1: Architecture of Wireless Sensor Networks.

The protocol stack of WSN consists of five standard protocol layers; application layer, transport layer, network layer, data link layer and physical layer and three cross layers. The five layers of protocol stack are shown in figure 2.

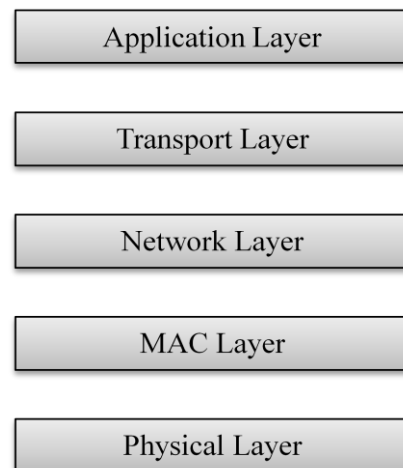


Fig. 2: Protocol stack of WSN.

Transport layer protocols have gained fundamental importance in WSN because it establishes end to end connections in the network. Transport layer ensures the reliability and quantity of data at the source and the sink. Basic services provided by transport layer protocols are:

### 1.1 Reliability

Reliability is the delivering each segment successfully from source mote to destination mote. Reliability can be described in two ways, in WSNs: Packet reliability or event reliability and Hop by Hop reliability or End to End reliability.

### 1.2 Congestion Control

Congestion arises in a network when bandwidth is inadequate and network data traffic run over capacity. The overall quality of the channel degrades due to congestion and congestion also leads to increase in loss rates, enlarge the delays and cause buffer drops.

### 1.3 Flow Control

Rate of data transmission [11] among two motes is managed by flow control. Flow control should be distinguished from congestion control, because congestion control is used to control the flow of data when congestion actually occurred.

### 1.4 Fair Allocation of Bandwidth [11]

Transport protocols provide the service of fair allocation of bandwidth [11] that is allocating unbiased bandwidth to each node.

## 1.5 Packet Loss Recovery [13]

The service provided is repairing the packet drops by means of packet retransmission.

## 1.6 Energy Efficiency

The nodes in WSNs have limited amount of energy and they make use of that energy for the purpose of computation, sensing and communication. Therefore the energy consumption is a major issue need to be considered in Wireless Sensor Networks.

## 2. WHY NOT TCP and UDP

Generally, UDP (User datagram protocol) and TCP (Transmission control protocol) [13], are well known protocols widely used in the internet. But neither TCP nor UDP are appropriate for WSN's because of many reasons one of which is throughput and another is energy consumption.

One of the major limitations in TCP is that it involves with end to end reliability model and exhibits low throughput. This is due to the reason that TCP believes that every packet drop occurs due to congestion only and it reduces the rate of transmission of data. On the other hand, UDP does not provide flow control, reliability and congestion control because it is a connectionless protocol. So, different protocols of transport layer have been designed for the WSNs. These transport layer protocols are divided into three categories:

- Protocol that support reliability only
- Protocol that support congestion control only
- Protocol that support both reliability and congestion control

## 3. Reliability Protocols

In transport protocols, reliability is delivering each segment successfully that is generated at source to the eventual destination. Reliability could be attained by detecting the dropped packets and retransmit packets to significant sources.

### 3.1 Reliability Direction

In WSN, data is transferred in two directions. When node detect an event, they send all the sensed information to the node at the sink. Sink then send the control packets to the sources. The transport protocols offer two directions of reliability; upstream reliability and downstream reliability.

#### 3.1.1 Upstream Reliability

Upstream reliability is when data flow traffic is successfully delivered from source nodes to the sink; mostly it is unicast type of transmission. All the protocols except the GARUDA and PSFQ have upstream reliability.

#### 3.1.2 Downstream Reliability

Downstream reliability is the delivery of control packets and queries successfully from sink to the source nodes, which is a multicast or the broadcast transfer. Only GARUDA and PSFQ have downstream reliability.

#### 3.1.3 Bidirectional Reliability

Bidirectional reliability can be explained as a satisfying reliability in both of the directions, downstream and upstream. Reliability can be more perfect if it is achieved bidirectional. But only ART protocol provides bidirectional reliability.

## 3.2 Reliability Level

The level of reliability means the extent of reliability supported by the protocol. Three levels of reliability can be given as follows: \_

### 3.2.1 Packet Reliability

Packet reliability is the delivery of all the packets successfully to the destination. It is necessary in certain control driven application scenarios, e.g. continuous humidity monitoring for a control process, etc. Every sensed information is of pivotal nature and any loss of information may result in process malfunction.

### 3.2.2 Event Reliability

Event reliability refers the successful event detection. For example, if more than one sensor in the field senses the temperature and reports to the sink, it is expected that at least one packet will be delivered and the successful delivery of each and every packet is not necessary. Only PORT, ART, ESRT, and DST offer event level reliability.

### 3.2.3 Destination Reliability

This concerns to send the message successfully only to the specific nodes or a selected cluster in entire WSN network. GARUDA offers destination reliability in addition to the packet reliability. As a whole, the packet reliability is much more trust worthy than the event reliability as it guarantees the delivery of each and every bit of information. But on the other hand, packet level reliability involves more energy utilization. Therefore the protocol design should be more flexible to adapt both event and packet reliability depending on the targeted application. Some Reliability protocols are described as follows:

## 3.3 PSFQ

PSFQ (Pump Slowly Fetch Quickly) [1] is a transport layer protocol that supports reliability only. PSFQ assures downstream reliability that is from sink mote to the source. PSFQ is a scalable, reliable and robust protocol. PSFQ is designed:

- to assure that all the data segments are delivered to all the deliberate receivers with min. support from the fundamental transport basis;
- to minimize the number of transmissions for detecting the lost and For the recovery operations with minimal signaling;
- to work correctly even in conditions where the radio link quality is not good at all; and
- to supply loose delay bounds for the delivery of data to all the deliberate receivers.

Three functions of PSFQ are:

### 3.3.1 Pump

Pump uses two timers  $T_{min}$  and  $T_{max}$ , where the node waits for  $T_{min}$  before transmission, to recover [1] off track packets and eliminate lay off in broadcast. Node stays for time  $T_{max}$  if some packets or the multiple packets are vanished.

### 3.3.2 Fetch

Fetch operation request to retransmit the missing packets from neighbor.

### 3.3.3 Report

The third operation report provides evaluation to the user.

### 3.4 GARUDA

GARUDA is a mythological bird that transported gods reliably. GARUDA provides data delivery from a single point to the multiple points from sink mote to the sources. Hence we can say that GARUDA assures downstream reliability. Reliability can be classified into four parts:

- assures delivery to the whole field,
- assures delivery to a sub region of the sensors,
- assures delivery to a minimal set of sensors and
- assures delivery to a anticipate subset of sensors.

GARUDA make use of an out-of-order forwarding approach to conquer the problem of less utilization in the act of packet losses. Out-of-order forwarding allows consecutive packet to be forwarded even when the packet is lost.

GARUDA uses two stage loss recovery processes. [1] In first stage, packet recovery is done by the core nodes [11]. When a packet arrives at central node which is not according the sequence, it notifies to a central node in upstream direction that some packet is missing. Another is called noncore recovery [1] phase in which non central nodes requests to transmit packets again from core nodes.

### 3.5 RBC

RBC is Reliable Bursty Convergent protocol. In RBC, intermediate nodes cache every fragment they receive. If a fragment is acknowledged, it is deleted from the cache, otherwise it is repeated  $n$  times. RBC implements a special cache queuing model capable of efficiently delivering unordered fragments, which is useful for bursty communication. The protocol uses multiple (block) ACKs.

### 3.6 RMST

RMST is Reliable Multi-Segment Transport [6] was presented to traverse reliability at the transport layer [11]. RMST is a protocol based on selective NACK which may be configuring for innetwork caching & repair. RMST was designed to work in synchronicity with directed diffusion. RMST i.e. Reliable Multi-Segment Transport [11] was designed to comprehend the action of innetwork processing for the reliably transfer the data. RMST is beneficial over diffusion routing, because it adds minimal additional control traffic. More so while multiple hops show higher rates of error the RMST guarantees the delivery. Delivery order is transparent to the clients of RMST but order is not guaranteed. RMST does not ensure any guarantees at real time.

In RMST, receivers are responsible for detecting if a fragment needs to be re-sent or not. Here the “receiver” does not necessarily mean sink. In the non-caching mode, only sinks monitor the integrity of an RMST entity regarding received fragments. In caching mode, an RMST node collects fragments and is capable of initiating recovery for missing fragments to the next node along the path toward the source.

## 4. CONGESTION CONTROL PROTOCOLS

Congestion arises when motes transmit more upstream traffic which results in exceeding the packet-arrival rate more than the packet processing rate at the mote. Congestion also occurs when data throughput of mote becomes more than the available data threshold limit of the link and may also result because of wireless link issues like contention, interference, and blind mote problem. Congestion can be the reason of

drops of packets and packet retransmissions unnecessarily and energy depletion. The congestion module takes corrective actions to mitigate the congestion, which leads to offer the reliability. There are five transport protocols that provides only congestion control mechanism which are Congestion Detection and Avoidance (CODA), SenTCP, Fusion, Congestion Control and Fairness (CCF) and Priority-based Congestion Control Protocol (PCCP). [14] But, all of these protocols do not have any reliability mechanism. Some congestion control protocols are described as:

### 4.1 CCF

Congestion Control and Fairness (CCF) provides congestion control and fairness. In CCF congestion is detected on the basis of packet service time at MAC layer and control congestion based on hop-by-hop manner with simple fairness. CCF makes use of packets service time to conclude the available service rate and detect the congestion in each intermediate node. When the congestion arises, it sends the information to the downstream nodes to mitigate their data transmission rate and vice versa.

### 4.2 PCCP

Priority-based Congestion Control Protocol (PCCP) calculates the degree of congestion as a ratio of inter arrival time of packet and service time of packet. CODA adjusts the sending rate similarly to AIMD, while and PCCP use an exact rate adjustment algorithm. PCCP provides priority-based fairness and overcomes the drawbacks from the use of nonwork conservative scheduling. Priority-based Congestion Control Protocol (PCCP) provides congestion control and fairness. PCCP calculates the degree of congestion as the ratio of inter-arrival time of packet and service time of packet which is used to achieve exact rate adjustment with priority-based fairness. PCCP uses absolute congestion notification by caching the congestion information in the header of data packets, thus avoiding additional control packets.

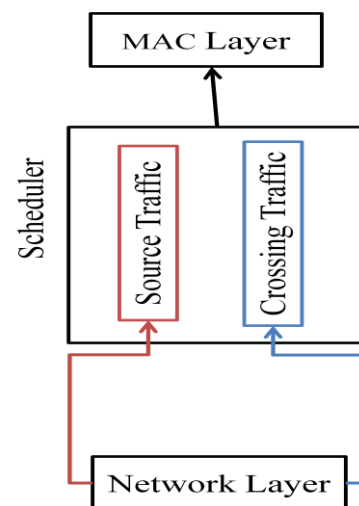


Fig. 3: A model of PCCP

### 4.3 FUSION

Fusion controls congestion in a stop-and-start non smooth manner. In Fusion, neighboring nodes stop forwarding packets to the congested node immediately when congestion is detected and notified. The Fusion protocol provides congestion control and fairness. Each sensor node performs congestion detection based on measurement of packet queue length. Congestion notification (CN) bit will set in the header of every outgoing packet when the node detects congestion.

Once the CN bit is adjusted, the node in the neighbor can over listen it and will stop forwarding packets to the congested node.

#### 4.4 ARC

Adaptive Rate Control (ARC) [12], there is no congestion detection or notification; congestion control works as follows: an intermediate node increases its sending rate by a constant  $\alpha$  if it overhears successful packet forwarding by its parent node. Otherwise, the intermediate node multiplies its sending rate by a factor  $\beta$ , where  $0 < \beta < 1$ . ARC maintains two independent sets of  $\alpha$  and  $\beta$ , respectively, for source traffic and transit traffic in order to guarantee fairness.

#### 4.5 Siphon

There is no rate adjustment in Siphon. When congestion arises, Siphon changes the direction of traffic to virtual sinks (VSs) that, beside the primary mote radio with low-power, have another long-range radio used as an alternative or “siphon” to reduce congestion. This protocol has four processes, as in CODA and has an additional process that restraint the congestion in a secondary network that is made by the virtual sinks (VSs) as shown in Figure 4.

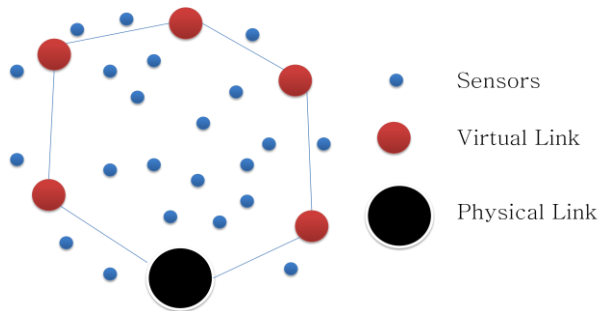


Fig. 4: A Network with Siphon protocol uses a secondary network

### 5. CONCLUSION

In this paper, we have presented a study of some existing transport layer protocols of WSN.

Transport layer protocols have gained a fundamental importance in WSN. Basic services provided by transport layer protocols are; Reliability, Flow control, Congestion control, Fair allocation of bandwidth, packet loss recovery and energy efficiency. TCP and UDP, the standard transport layer protocols, are not suitable for WSN Because of many reasons like; TCP has low throughput and on the other hand UDP is not reliable. There are three types of existing transport layer protocols; the protocols that provide reliability only, protocols that provides congestion control only and the protocols that provides both of the reliability and congestion control. Two types of which are presented in this paper. Protocols that provides reliability are PSFQ, RBC, RMST, GARUDA and the protocols that provides only congestion control are CCF, PCCP, ARC and Fusion.

### 6. ACKNOWLEDGMENTS

The authors wish to thank the faculty from the computer science department at CTIEMT, Jalandhar for their continued support and feedback.

### 7. REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, and Deepak Ghosal, “Wireless sensor network survey,” Computer

Networks, vol. 52, pp. 2292-2330, Elsevier, April 2008. Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

- [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, pp. 393–422, 2002.
- [3] Ahmad Abed, Alhameed Alkhatib, and Gurdinder Singh Baicher “Wireless Sensor Network Architecture,” International Conference on Computer Networks and Communication Systems, IPCSIT, vol. 35, 2012.
- [4] A.J.Dinusha Rathnayaka n, VidyasagarM.Potdar “Wireless Sensor Network transport protocol: A critical review,” Journal of Network and Computer Applications, vol. 36, pp. 134–146, Elsevier, December 2011.
- [5] Hongwei Zhang, Anish Arora, Young-ri Choi, and Mohamed G. Gouda, “Reliable bursty convergecast in wireless sensor networks,” Computer Communications, vol. 30, pp. 2560–2576, Elsevier, June 2007.
- [6] Faisal Karim Shaikh, Abdelmajid Khelil, Neeraj Suri, “A Comparative Study of Data Transport Protocols in Wireless Sensor Networks,” IEEE Networks, 2008.
- [7] Ahmed Ayadi, “Energy-Efficient and Reliable Transport Protocols for Wireless Sensor Networks: State-of-Art,” Wireless Sensor Network, vol. 3, pp. 116-113, Scientific research, March 2011.
- [8] Chieh-Yih Wan, Andrew T. Campbell, and Lakshman Krishnamurthy, “PSFQ: A Reliable Transport Protocol for Wireless Sensor Networks,” ACM, September 2008.
- [9] Raheleh Hashemzahi, Reza Noormandipour, “Comparison of Technical Features of Transport Protocols for Wireless Sensor Networks,” Greener Journal of Internet, Information and Communication Systems, vol. 1, pp. 033-039, ISSN: 2354-2373, January 2013.
- [10] Praveen Budhwar<sup>1</sup>, Bhisham Sharma<sup>2</sup> & Dr. Trilok C. Aseri, “Congestion Detection and Avoidance based Transport Layer Protocols for Wireless Sensor Networks,” International Journal of Engineering Research and Development, Vol. 10, pp. 56-69, Issue 5, May 2014.
- [11] Chonggang Wang, Mahmoud Daneshmand, Bo Li, and Kazem Sohraby, “A Survey of Transport Protocols for Wireless Sensor Networks,” IEEE Network Magazine Special Issue on Wireless Sensor Networking.
- [12] Debnath Bhattacharyya, Tai-hoon Kim, and Subhajit Pal, “A Comparative Study of Wireless Sensor Networks and Their Routing Protocols,” Sensors, vol. 10, ISSN: 1424-8220, pp. 10506-10523, 2010.
- [13] Chonggang Wang, Kazem Sohraby<sup>1</sup>, Bo Li, and Weiwen Tang, “Issues of Transport Control Protocols for Wireless Sensor Networks,” unpublished.
- [14] Rubal Bambra, Ruchika sharma “Multipath Routing metrics and QoS in Wireless Sensor Networks: Survey and Research Challenges,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, issue 7, ISSN: 2277 128X, July 2014.