Comparison of Technical Features of Transport Protocols For Wireless Sensor Networks

By

Raheleh Hashemzehi
Reza Noormandipour
Research Article

Comparison of Technical Features of Transport Protocols for Wireless Sensor Networks

Raheleh Hashemzehi, Reza Noormandipour

Department of computer, Science and Research branch, Islamic Azad University, Sirjan, Iran.

Corresponding Author’s Email: rahelehhashemzehi@yahoo.com

ABSTRACT

Transport protocols for Wireless Sensor Networks are used to eliminate congestion and reduce packet loss, to provide fairness in bandwidth allocation, and to guarantee end-to-end reliability. The transport protocols in WSN should support Congestion control, Reliable data delivery, Energy efficiency. The researchers working in this area have to compare the performance of the new protocol with the existing protocols to prove that new protocol is better. In this article we provide review technical characteristics of existing transport protocol design in WSNs and we then compared them.

Keywords: Wireless Sensor Network (WSN), Transport protocols, Reliability, Congestion cont.

INTRODUCTION

A wireless Sensor network is realized as a collection of sensor nodes that are capable of sensing physical phenomena, locally processing the sensed data, and finally route the raw or aggregated data to a remote base station called sink. The sensors are small, with limited processing and computing resources, and sense physical information, process crude information, and report required information to the sink. The unique characteristics of WSN such as coherent nature of traffic to base station that occurs through its many-to-one topology and collision in physical channel are main reasons of congestion in wireless sensor networks. Also when sensor nodes inject sensory data into network the congestion is possible. There are two major functions in the transport protocol of WSNs, that are reliable data delivery and congestion control. Reliable data delivery is required when packets are lost in a multi-hop WSN, some or all of the lost packets can be detected and the lost information recovered by appropriate mechanisms (Quang, 2006). Congestion occurs when many sensor nodes send data to the sinks and the amount of the data traffic exceeds the network capacity. The two most widely known protocols used at the transport layer for wired networks are Transmission Control Protocol (TCP) (Postel 1981) and User Datagram Protocol (UDP) Postel,1980. TCP is a connection-oriented protocol. Before data transmission, there is a three-way handshake interactive process; it is after the TCP connection has been established that TCP sender can begin to transmit data only. UDP contains no ACK mechanism, no reliability mechanism, but behaves faster than TCP due to reduced overhead.

Characteristics of Transport Protocols for WSNs:

Transport protocols have been designed for WSNs into three categories: (Fig. 1)

- protocols that support reliability only
- protocols that support congestion control only
- protocols that support congestion control and reliability
Congestion Control

One of the major challenges in wireless sensor network (WSN) research is to curb down congestion in the network's traffic, without compromising with the energy of the sensor nodes. Congestion affects the continuous flow of data, loss of information, delay in the arrival of data to the destination and unwanted consumption of significant amount of the very limited energy in the nodes. Generally the Congestion control is composed of three mechanisms:

1-congestion detection, 2-congestion notification, 3-rate adjustment

Congestion detection:

Congestion detection refers to identification of possible events, which may build-up congestion in the network. A common mechanism is to use the queue length packet service time (Teczan 2007), or the ratio between packet service time and packet inter-arrival time at an intermediate node (Wang et al., 2006).

Congestion notification

Once congestion has been detected, congestion information should be propagated from the congested node to upstream traffic nodes and source node. The approaches to notify congestion usually can be categorized into explicit congestion notification, and implicit congestion notification.

Implicit congestion notification

The congestion warning is embedded in the header of the normal data packets and the child nodes listen to their parent node to get the congestion information.
Explicit congestion notification:

The source node uses special control messages to notify the involved sensor nodes of congestion.

Rate adjustment

After receiving congestion notification, a sensor node can adjust its sending rate upon receiving a congestion indication. Rate adjustment can be hop-by-hop or end-to-end. If congestion is notified by setting single CN bit then in order to adjust the rate, AIMD (additive increase multiplicative decrease) scheme or its variants are used. Apart from that, if additional information about congestion, it could be piggybacked with the data packet then exact rate adjustment can be done.

Proposed Transport Protocols for congestion control

Congestion Avoidance and Detection (CODA)

CODA (Wan et al.2003) is energy efficient congestion control mechanism designed for WSNs, that introduces three schemes, which are congestion detection, open loop hop-by-hop backpressure and end-to-end multi-source regulation. CODA senses congestion by taking a look at each sensor node’s buffer occupancy and wireless sensor load.

Priority Based Congestion Control Protocol (PCCP)

PCCP (Tezcan 2007) calculates a congestion degree as the ratio of packet inter-arrival time and packet service time which is used to achieve exact rate adjustment with priority-based fairness. PCCP uses implicit congestion notification by piggybacking the congestion information in the header of data packets, thus avoiding additional control packets.

Fusion

In Fusion (Tezcan 2007) hop by hop flow control mechanism is used for congestion detection as well as congestion mitigation. Congestion is detected through queue occupancy and channel sampling technique at each intermediate node. Congestion notification (CN) bit will set in the header of every outgoing packet when the node detects congestion. Once the CN bit is set, neighboring node can overhear it and stop forwarding packet to the congested node.

Siphon

Siphon (Wan et al.2005) aims at controlling congestion as well as handling funneling effect. Funneling effect is where events generated under various work load moves quickly towards one or more sink nodes, which increases traffic to sink which leads to packet loss. Virtual sinks are randomly distributed across the sensor network which takes the traffic load off the already loaded sensor node. In siphon initially VS discovery is done. Virtual sink discovery is initiated by the physical sink by as explained in . Node initiated congestion detection is based on past and present channel condition and buffer occupancy as in CODA (Wan et al.2003). After congestion detection traffic is redirected from overloaded physical sink to virtual sinks. It is done by setting redirection bit in network layer header.

Fairness Aware Congestion Control (FACC)

FACC (Xiaoyan et al., 2009) is a congestion control mechanism, which controls the congestion and achieves fair bandwidth allocation for each flow of data. FACC detects the congestion based on packet drop rate at the sink node. In FACC nodes are divided into two categories near sink node and near source node based on their location in WSNs. When a packet is lost, then the near sink nodes send a Warning Message (WM) to the near source node. After receiving WM the near source nodes send a Control Message (CM) to the source node. The source nodes adjust their sending rate based on the current traffic on the channel and the current sending rate. After receiving CM, flow rate would be adjusted based on newly calculated sending rate.
Table 1: Congestion Control protocols for WSN

<table>
<thead>
<tr>
<th>Features Protocols</th>
<th>Congestion Detection</th>
<th>Congestion notification</th>
<th>Rate Adjustment</th>
<th>Energy Efficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>CODA</td>
<td>Buffer size &amp; Channel condition</td>
<td>Explicit</td>
<td>AIMD-like end-to-end rate adjustment</td>
<td>Good</td>
</tr>
<tr>
<td>PCCP</td>
<td>packet inter-arrival time &amp; packet service time</td>
<td>Implicit</td>
<td>Exact hop-by-hop rate adjustment</td>
<td>No</td>
</tr>
<tr>
<td>Fusion</td>
<td>Buffer size</td>
<td>Implicit</td>
<td>Stop-and-start hop-by-hop rate adjustment</td>
<td>No</td>
</tr>
<tr>
<td>Siphon</td>
<td>Buffer size &amp; application fidelity</td>
<td>-</td>
<td>Traffic redirection</td>
<td>No</td>
</tr>
<tr>
<td>FACC</td>
<td>Packet Drop At the Sink node</td>
<td>Explicit</td>
<td>Hop-by-Hop rate adjustment</td>
<td>No</td>
</tr>
</tbody>
</table>

Reliability

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

Upstream reliability

Upstream reliability refers to the successful delivery of dataflow traffic from sources to sink, which is mostly unicast/converge cast transmission.

Downstream reliability

Downstream reliability refers to the successful delivery of control packets and queries from sink to sources, which is mostly multicast/broadcast transfer.

Loss recovery

The loss recovery refers to repairing the packet drops by means of packet retransmission. The loss recovery can be addressed in two ways which are hop-by-hop and end-to-end. In hop-by-hop loss recovery method, the intermediate nodes cache packet information and perform loss detection and notification. End-to-end recovery is refers to reliable data transfer of sensed data from source to destination node.

Loss detection and notification

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

- ACK (positive acknowledgements)
- NACK (negative acknowledgements)
- IACK (Implicit ACK)

Both ACK and NACK rely on special control messages, while Implicit ACK (IACK) just piggybacks ACK information in the header of data packets. In IACK, if a packet is overheard being forwarded again, it implies that the packet has been successfully received and acknowledged simultaneously.

**Proposed Transport Protocols for Reliability**

**Reliable multisegment transport (RMST)**

The RMST (Stan 2003) scheme is mainly used in the sensorstosink direction and it provides guaranteed reliability of packet delivery. It is designed to complement directed diffusion by including a reliable data transport service on top of it. Directed diffusion is used to discover paths from sensors to the sink. RMST is a NACK-based protocol, which employs primarily timer-driven loss detection and repair mechanisms.

**Reliable Bursty Convergecast (RBC)**

The aim of RBC (Zhang et al, 2005) protocol is to improve channel utilization and to reduce acknowledgement loss. It is designed with a window-less block acknowledgement scheme that guarantees continuous packet forwarding and replicates the acknowledgement for packet.

**Pump Slowly Fetch Quickly (PSFQ)**

PSFQ (Wan et al, 2002) transport protocol, suitable for constrained devices. It includes three main functions: message relaying, relay-initiated error recovery and selective reporting. Main drawbacks of this approach are: it is not compatible with IP (minimal requirements on the routing infrastructure) and needs precise time synchronization between sensor nodes. PSFQ is designed with the assumption that sensors application generates light traffic.

**GARUDA**

GARUDA (Park et al, 2004) belongs to downstream reliability guarantee. It has three primary components. Firstly, GARUDA uses WFP (Wait-for First Packet) pulse transmission to guarantee success of single/first packet delivery, in order to choose and construct Core sensors. Secondly, GARUDA performs Core election using such methods-only sensors with HopCount of the form 3*i where i is a positive integer, are allowed to elect themselves as Core sensors. Thirdly, GARUDA begins two phases: Loss recovery for Core sensors and Loss recovery for non-Core sensors using out-of-sequence NACK.

<table>
<thead>
<tr>
<th>Features Protocols</th>
<th>Congestion Detection</th>
<th>Congestion notification</th>
<th>Rate Adjustment</th>
<th>Reliability direction</th>
<th>Loss recovery</th>
<th>Loss detection and notification</th>
<th>Energy Efficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>STCP</td>
<td>Buffer size</td>
<td>Implicit</td>
<td>AIMD</td>
<td>upstream</td>
<td>End-to-End</td>
<td>ACK&amp;NACK</td>
<td>No</td>
</tr>
<tr>
<td>ART</td>
<td>Service time</td>
<td>Implicit</td>
<td>-</td>
<td>Upstream &amp; downstream</td>
<td>End-to-End</td>
<td>ACK&amp;NACK</td>
<td>No</td>
</tr>
<tr>
<td>ESRT</td>
<td>Buffer size</td>
<td>Implicit</td>
<td>Exact rate adjustment</td>
<td>upstream</td>
<td>-</td>
<td>-</td>
<td>fair</td>
</tr>
</tbody>
</table>
Proposed Transport Protocols for Congestion Control and Reliability

Sensor Transmission Control Protocol (STCP)

STCP (Iyer et al., 2005) is a transport layer protocol, which supports heterogeneous applications, such as continuous flow or event-driven applications, and provides reliability and congestion control services for them. To provide reliability for continuous flow applications, it takes advantage of the base station’s knowledge of and the inter-arrival time between packets to implement NACK-based reliability. (Iyer et al., 2005) Data packets take an important role in maintaining the congestion information. STCP also has some performance problem which is SCTP assumes that all the sensor nodes within the WSN have a clock synchronization.

Asymmetric and reliable transport (ART)

In ART (Teczan 2007), a series of nodes which are called essential nodes, are selected. These nodes are selected in a way to be able to cover the whole area, and then a sub-network of these nodes is formed and merely is involved in reliable transmission and congestion control.

Event-to-Sink Reliable Transport (ESRT)

ESRT (Iyer et al., 2005) protocol is a novel transport solution developed to achieve reliable event detection in WSN with minimum energy expenditure. The goal of ESRT is to adjust the reporting frequency of source nodes in order to achieve the end-to-end desired reliability guarantee while keeping energy consumption minima. It provides reliability for applications and not for each single packet. The benefit resulting from ESRT is energy-conservation since it can control sensor report frequency. However, ESRT still have some drawbacks, such as this protocol may not be applicable to many of the WSN application because ESRT assume that the base station is one-hop away from all sensor nodes.

Table 3: Reliable and Congestion Control protocols for WSNs

<table>
<thead>
<tr>
<th>Features Protocols</th>
<th>Reliability direction</th>
<th>Loss recovery</th>
<th>Loss detection and notification</th>
<th>Energy Efficient</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMST</td>
<td>Upstream</td>
<td>Hop-by-Hop</td>
<td>NACK</td>
<td>Good</td>
</tr>
<tr>
<td>RBC</td>
<td>Upstream</td>
<td>Hop-by-Hop</td>
<td>IACK</td>
<td>No</td>
</tr>
<tr>
<td>PSFQ</td>
<td>downstream</td>
<td>Hop-by-Hop</td>
<td>NACK</td>
<td>No</td>
</tr>
<tr>
<td>GARUDA</td>
<td>downstream</td>
<td>Two-tier loss recovery</td>
<td>NACK</td>
<td>No</td>
</tr>
</tbody>
</table>

Energy-Efficiency

Sensor nodes have limited energy and it is important for the transport protocol to maintain the high energy in order to achieve and maximize system lifespan. Packet loss in WSN can be common due to bit error or congestion (Rahman et al., 2008).

CONCLUSIONS

In this article some existing transport control protocols for WSNs are classified and compared. We have focused on the most important Characteristics of the transport protocol. The ideal transport protocol for WSNs should have high energy-efficiency and provide flexible reliability. Both the factors of congestion control and reliability helps in reducing packet loss, which results in an energy efficient operation of the network, which is a important
factor in increasing the lifespan of the sensor network. Another factor to be taken into account by the transport protocols is the limited resources of the node devices.

REFERENCES


Taiwan.


