Reliable and Congestion Control Protocols for Wireless Sensor Networks

Kirti Kharb*, Bhisham Sharma, Dr. Trilok C. Aseri

Department of Computer Science Engineering, PEC University of Technology, Chandigarh, India

Received 05 November 2015; received in revised form 13 November 2015; accepted 20 November 2015

Abstract

The objective of this paper is to analyze review and different congestion control protocols that are employed at the transport layer and some of them working at the medium access control layer in wireless sensor networks. Firstly, a brief introduction is given about wireless sensor networks and how congestion occurs in such networks. Secondly, the concept of congestion is discussed. Thirdly, the reason of occurrence of congestion in wireless sensor networks is analyzed. After that, congestion control and why it is needed in the wireless sensor networks is discussed. Then, a brief review of different congestion control and reliable data transport mechanisms are discussed. Finally, a comparative analysis of different protocols is made depending on their performance on various parameters such as - traffic direction, energy conservation characteristic, efficiency etc. and the paper is concluded.

Keywords: wireless sensor networks, reliability, congestion avoidance, transport layer protocols

1. Introduction

Wireless sensor networks are a group of heterogeneous nodes called sensor nodes, spread over a large field with a central processing node called as sink. Basically, wireless sensor networks perform two main actions – wireless sensing and data networking. They provide a bridge between the real physical and virtual worlds. Wireless sensor networks have diversified arena of applications, some of them being in health care, animal care monitoring and surveillance, logistics & transportation, soil health maintenance for agriculture, real time security and surveillance, infrastructure etc. However, there are also some concern issues pertaining to wireless sensor networks. The main concern areas related to wireless sensor networks are - resources, energy wastage, memory utilization, and computational power. [1] Most discussed issue is that of energy consumption and battery usage problems. Next issue in wireless sensor networks is the issue of the occurrence of congestion in the networks. Another issue is that of the security. In this paper, we aim to review and compare different reliable and congestion control algorithms working at the transport layer in wireless sensor networks. How and why it is important to address, detect and control the congestion, and the many mechanisms/ algorithms which help us in doing so is also discussed. Section II provides the study that motivates why it is inadvertent to go for congestion control, the section III deals with the problem of congestion, congestion avoidance and congestion control. Section IV reviews different schemes employed to control congestion in wireless sensor networks. A comparative analysis of different congestion control algorithms is done in the concluding section.

2. Congestion in Wireless Sensor Networks

This section makes a brief explanation about congestion, the congestion process and the different types of congestion happening in wireless sensor networks.

* Corresponding author. E-mail address: kharb.kirti46@gmail.com

2.1 Brief Overview

Traffic flows in sensor networks is shaped according to the physical structure of the fields that they work in. Wireless sensor networks generally operate under light load conditions and become active whenever an event occurs. If the corresponding application load is high, it may result in the generation of huge continuous data flows leading to disrupted performance of the network, which may lead to congestion. In such condition, collision occurs in the network, due to which data packets start getting dropped, buffer overflows start happening at the nodes in the network.

Therefore, we can say that the congestion is said to occur in a network, if the speed of the incoming traffic is larger than the data processing rate of the network it. Following are some of the probable causes due to which congestion happens in wireless sensor networks:

- processing speed of nodes is low
- incoming traffic arrives at faster rate than it can handle
- if packet collisions happen on data links, leading to alternate routing of packets & excessive re-transmission of packets

2.2 The Congestion Process

The Congestion happens in a network either due to buffer overflow (when packets are getting stored at the source because the previous packets have not been delivered) or/and link collisions (which results into packet losses and large number of re-transmissions) [2]. Depending on physical topology of the network, both types of above situation may occur. In Buffer overflow situation, data packets get dropped which negatively impacts the application, since the throughput is restricted to the maximum data sending rate of node. As a result continuously packets get dropped; a lot of power is wasted in re-transmissions. To counter this, a congestion control algorithm is to be used which either reduces the data rate of the transmitting nodes or reroutes the excess data packets through alternative paths.

If link collisions occur, all the nodes in the network receive limited number of packets and the reliability of the application running on the network is badly affected. For mitigating this, a congestion control algorithm that focuses on the MAC layer may be used, that maintains optimum and collision free access to the medium.

2.3 Different types of Congestion in Wireless Sensor Networks

The congestion in WSNs can be stratified in two major classes depending upon

- how data packets are lost, and
- where in the network congestion is taking place

2.3.1 How data packets are lost

Due to congestion, packets can be lost in the following two ways in the wireless sensor networks:

1) Packet Collisions in the Medium: At a particular instant of time in a geographical area, many nodes within vicinity of one another attempt to transmit data simultaneously, resulting in data losses due to interference and thereby reduce the throughput of all nodes in the area. [3] Proper local synchronization among neighbor nodes can reduce this type of loss, however, we cannot eliminate it completely because non-neighboring nodes may still interfere in the data transmission.

2) Packet Drops Due to Buffer Overflow: Within a particular sensor node, if the queue or buffer used to hold data packets that are to be transmitted, overflows then congestion occurs. In this case, nodes receive packets with a rate higher than that they can transmit or process. This kind of congestion usually occurs in wired networks.

2.3.2 Where in the network packets are lost

After congestion occurs, there are three possible sites for the data packets to get lost. These three sites are:

1) Hotspot Near Source—Source Congestion: The hotspot referred in this paper means the area in the network where congestion occurs and packets start getting dropped. Whenever the sensors are deployed densely, the data packets which are generated during a crucial event will create hotspots very close to the sources. In this scenario, localized and quick time-scale mechanisms which are capable of providing backpressure messages from the nodes that cause congestion, back to the sources would be helpful for immediate traffic controlling until the congestion is removed by other means.

2) Hotspot Near the Sink-Sink Congestion: Even sparsely deployed sensors that generate data at comparatively low data rates may create hotspots in the sensor network, but likely farther away from the sources, near the sink. In such a scenario, combined use of localized back-pressure and packet dropping methods would be more effective. Another way of removing the sink congestion is to employ multiple sinks that are uniformly distributed across the sensor network and, therefore, traffic is balanced among these sinks.

3) Forwarder Congestion: A sensor network usually has more than one flow (sink-source pair), and these flows will intersect with one another. The area around such points of intersection is likely to become a hot spot for congestion. In a tree-like communication network, every intermediate node may suffer from the problem of forwarder congestion. [4] Compared to the other congestion scenarios, forwarder congestion is way more challenging because it is very difficult to predict the intersection points due to the highly dynamic nature of the network. In this case, even sparsely situated sensor nodes generating data will create both transient as well as persistent hotspots distributed throughout the sensor field.

3. Congestion Control Methods

In this section, firstly the congestion control process is discussed, then the different congestion control schemes are analyzed and finally the congestion control mechanism is discussed.

3.1 Congestion Control

Congestion control is the mechanism through which congestion is prevented from being occurring in a wireless sensor network, and if congestion has already happened then to detect where it has occurred, to monitor its status and controlling its aftermath. . In buffer overflow scenario, reduction of data sending rate is done on the nodes whose buffer is overflowing or re-transmissions are done through some alternative paths. To overcome congestion in link collisions, a congestion control algorithm that focuses on the MAC layer may be used to help co-ordinate the network access among the nodes.

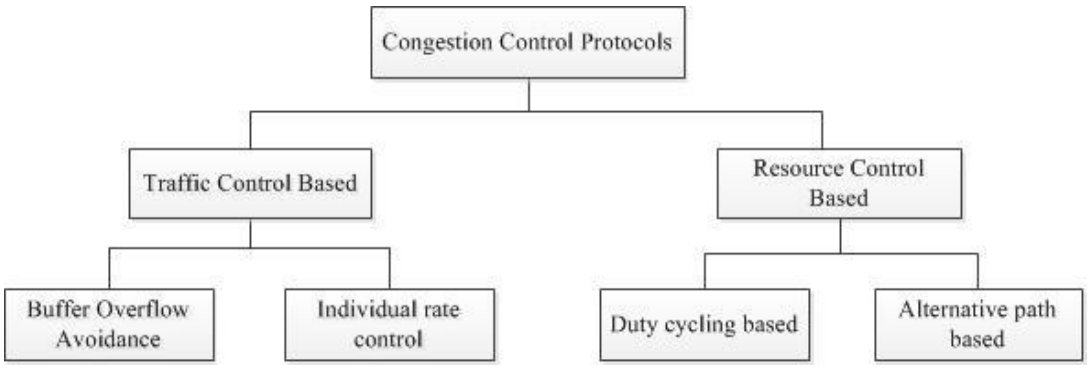

Fig. 1 Different categories of congestion control protocols

3.2 Congestion Control Schemes

Generally, protocols that deal with congestion control in WSNs can be basically classified in three major categories. These categories are: Congestion Control, Congestion Avoidance, and Reliable Data Transmission protocols.

3.2.1 Congestion 'Control' Protocols

These protocols can be classified on the way they detect congestion, the way they notify the other nodes for the occurrence of congestion, as well as how the congestion countering mechanisms are performed. Congestion detection by these protocols is done by: checking the level of buffer occupancy at the nodes in the network, measuring the load level of the channel, and by counting the packet service timings and packet inter-arrival time. [5] Congestion notification is done by either using additional notification packets that are sent across the network or by overhearing the data packets that are being transmitted across. Congestion counter mechanisms can be performed either through reduction of traffic or through the creation of alternative paths from the source node(s) to the sink node(s).

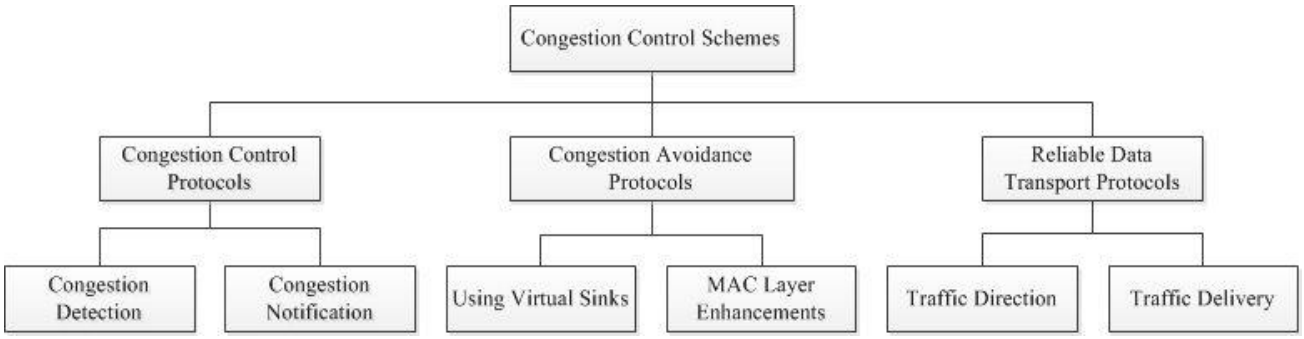

Fig. 2 Different types of Congestion Control Schemes

3.2.2 Congestion 'Avoidance' Protocols

These protocols are classified on the basis of how congestion is going to occur and on what mechanisms will be used avoid the congestion from even occurring in a network. Congestion detection is done same as in congestion mitigation protocols. Congestion can be avoided by using virtual sinks for those sinks which are getting highly congested and by using MAC layer enhancements.

3.2.3 Reliable Data Transport Protocols

The reliable data transmission protocols are the protocols that, not only put effort to control congestion in a network, but also attempt to recover all or part of the information which is lost. These are normally employed when all of the information in network is critical for the application and is using some transport layer mechanisms. These protocols are divided on the basis of three attributes: their traffic direction (whether downstream or upstream), whether they provide hop-to-hop or end-to-end delivery, and the parameter on which reliability focuses (packet or event).

4. Different Congestion Control, Avoidance and Reliable Data Transport Protocols

The different protocols employed for congestion control in wireless sensor networks, basically deal with three core functions- controlling the congestion, avoiding the congestion and providing for reliable data transportation. Following sections deal with this concept in detail.

4.1 Congestion Control Protocols

These protocols mainly perform three functions - congestion detection, congestion notification (notifying the nodes in the network that congestion has occurred) and the congestion mitigation strategy.

4.1.1 Adaptive Rate Control (ARC) Algorithm

The ARC scheme was proposed by J. Zhao et al. in 2001 [6]. This algorithm does not involve any congestion detection or notification mechanisms. It uses an AIMD-like traffic control mechanism for congestion mitigation, which works as follows: an intermediate node increases its sending rate by a constant *a* if it senses a successful packet forwarding by its

parent node. Otherwise, the intermediate node multiplies its sending rate by a factor *b*, where $0 < b < 1$. In order to guarantee fairness, ARC basically maintains two independent sets of these two factors: *a* and *b*, for source and transit traffic respectively. Studies done by authors have shown that ARC is not only effective in achieving fairness but it also maintains good bandwidth along with reasonable energy efficiency, especially during low traffic situations that are the common case in wireless sensor networks.

4.1.2 Congestion Detection and Avoidance algorithm (CODA)

This algorithm [7] deals with both - congestion control and avoidance in wireless sensor networks. Present and past channel load conditions are used by CODA as the congestion indication parameters. The channel load is listened by each node before it starts transmitting data i.e. carrier sensing is pro-active here, this is done to avoid congestion. If congestion is detected, the receiver node broadcasts an explicit back-pressure message to its neighbors signaling that congestion has happened and correspondingly neighbor nodes reduce their local data sending rates. If congestion persists for a longer time, this back-pressure is sent all the way to the sink node. A constant feedback in the form of ACK packet is maintained from the source to the sink nodes. If the source node does not receive ACK, then it reduces its data transmission rate. The CODA algorithm does not ensure fairness in the network and the bandwidth is not utilized efficiently.

4.1.3 Congestion Control and Fairness (CCF)

Saima Zafar [8] proposed this scalable algorithm for many to-one routing in wireless sensor networks. Here, congestion detection is performed on the basis of packet servicing time which is the time period taken in sending the data packet form the transport layer to the network layer and reception of the successful data transmission. Traffic control is used to carry out congestion mitigation. Congestion control is performed in hop-by-hop fashion and each node uses exact rate adjustment based on its available packet servicing rate. Each child node divides its data sending rate by the number of children nodes it has, compares this newly arrived data rate with its parent data rate. If the defined threshold congestion level is reached in the network, then the algorithm requests the child nodes to reduce their data transmission rate. Since a separate queue is maintained for every child node, a considerable amount of bandwidth is exhausted in this algorithm.

4.1.4 Fusion Algorithm

Proposed by Mohamed Amine Kafi et al., [9] this scheme is used for mitigating the congestion in wireless networks. This algorithm uses explicit congestion detection method i.e. a congestion bit in the header of every data packet. Whenever, congestion occurs it is notified to all the nodes in the neighborhood by setting the value of congestion bit to 1 in every outgoing packet from a node. Congestion detection can also be done by checking upon the queue size of each sensor node. If the queue length crosses a specified threshold limit, the congestion bit is set, else it is reset. If congestion lasts for longer, then hop-by-hop back pressure message is sent to the source notifying it to reduce the data transmission rate. A prioritized MAC scheme is used to provide access to channel medium when the nodes are congested.

4.1.5 Biased Geographical Routing (BGR) Algorithm

Proposed by Dashkova et al. [10], in this protocol whenever congestion is detected the nodes reactively split traffic. Detection of congestion is done depending on the level of buffer occupancy and wireless usage of the network. The wireless usage is calculated by taking periodic samples of wireless medium. An implicit congestion bit added to each data packet is used for congestion notification. Each node listens to the packets sent by its neighbors to detect the congestion status of the network. Congestion is resolved using two algorithms: In-Network Packet Scatter (IPS) and End-to-End Packet Scatter (EPS). IPS removes short term congestion in the network by splitting the traffic immediately before the congested areas. Whereas, EPS removes long term congestion by splitting the data flow at source node and then performs rate control by the Additive Increase Multiplicative Decrease (AIMD) strategy.

4.1.6 Hierarchical Tree Alternative Path Algorithm (HTAP)

Hierarchical Tree Alternative Path algorithm is proposed for event-based sensor applications. Propounded by Charalambos Sergiou et al., [11] it tries ensuring application reliability during overload periods without reducing the source node's data rate while sending information during critical events. HTAP works on a combination of two algorithms, Alternative Path Creation (APC) and Hierarchical Tree Creation (HTC), and it uses the network density to choose between them. When congestion takes place or a node's battery is about to draining, APC and HTC form alternative paths to the sink by unused nodes. APC uses these nodes by randomly exploiting neighboring table, while in HTC these nodes are placed in a hierarchical levelled tree starting from 0 for the leaves nodes. Every node piggybacks its buffer occupancy, reflecting its congestion state, when sending packets and the neighbors refresh their neighboring state tables when overhearing packets. A congested receiver sends a back-pressure packet to the sender in the purpose to remove congestion. The sender stops transmitting to this node and searches for a less congested receiver which leads to alternative paths creation.

4.2 Congestion Avoidance Protocols

These protocols are more focused on the 'avoidance part' of the congestion control process. Basically involve two strategies- congestion detection methodology and congestion avoidance mechanism.

4.2.1 Siphon

This scheme was proposed by G. Srinivasan *et al.* [12]. It is a source to-sink congestion control protocol. Congestion detection is done through – buffer occupancy level, sink load level and wireless channel load conditions. Congestion notification method involved is implicit in nature. Congestion mitigation is performed by traffic redirection through virtual sinks (VSs). These virtual sinks form a dynamic adhoc network and split traffic when nodes get congested, thereby preventing the data packets from getting deleted. This algorithm comprises mainly these steps – first being the discovery of virtual sinks that will be selected for congestion control in particular congested areas. For this every sensor node maintains a table of VS it has in its vicinity. The second step is to use the service of a VS, a congested node enables a redirection bit which signals a VS to re-route the traffic out of the congested neighborhood, for this every VS has dual radio interfaces maintained on it – a long range interface to communicate with other VSs and a short range interface to communicate with the sensor nodes in the network. Finally, when the VS detect the value of redirection bit as set, it re-routes the packets using a combination of hop-by-hop and end-to-end transmission.

4.2.2 Buffer and Rate Control Based Congestion Avoidance Algorithm

M. M. Alam *et al.* [13] proposed the "Buffer and Rate Control Based Congestion Avoidance" protocol. There are three main steps involved in this algorithm. These are: the Upstream Source Counting, the Buffer Occupancy based rate control, and the Snoop based MAC level ACK. The first two steps are used to control the rate of upstream nodes. It actually provides two advantages. The first is that congestion is reduced by media access contention, as the upstream nodes proactively decrease their data transmission rate, while the second advantage is that the congestion due to buffer overflow is avoided as the upstream nodes delay the transmission of packets whenever the buffer capacity of the downstream nodes is full. In the third step, explicit ACK packets are avoided. Instead, each node may overhear its own transmitted packet while forwarded by its downstream node, hence eliminating the need for ACK packets. To accomplish this overhearing task, the upstream node MAC address and a sequence number need to be appended into the MAC frame of the node. Many advantages of this protocol are that this can reduce collision drop Rate, increase delivery ratio and improve the network's energy efficiency.

4.2.3 Priority Based Medium Access Protocol

The Priority Based Medium Access Protocol for Congestion Avoidance was proposed by Patil et al [14]. This is a MAC layer protocol that helps in avoiding congestion by giving proportional access to the nodes based on their source count

values. For example, a node carrying a higher load of data traffic gets more access time than others. Each sensor node then calculates its contention window on a provided equation. This contention window has different size for different node data conditions. Simulation series that have been performed by scholars in MATLAB resulted that there is an optimal contention window size through which the collision in the MAC layer can be minimized and enables all the sensor nodes to transmit their data packets without delays.

4.2.4 LACAS

The concept of "Learning Automata-Based Congestion Avoidance Algorithm in Sensor Networks" (LACAS) was propounded by Vrisha Tickoo *et al.* [15] which is actually an adaptive learning solution for avoiding the congestion in wireless sensor networks. The target of this algorithm is to control the data rate of intermediate nodes in order to avoid congestion before it reaches to the sink in the network. To monitor the data rates, automatas are developed at each of the network's nodes that are capable of controlling the rate of flow of data at the intermediate nodes. These states are based on probabilistically how many packets are likely to get dropped if a particular flow rate is maintained. In this case, an "automaton" "learns" from past behaviors, will increase data rate if packets are not being dropped or else will reduce the data rate from the previous level of data rate in order to avoid congestion. This algorithm actually works on the reinforcement learning strategy and keeps on optimizing the data rate depending upon its past performance achieved.

4.3 Reliable Data Transport Protocols

These protocols mainly aim at providing reliable data transmission and traffic control in the wireless sensor networks.

4.3.1 Event to Sink Reliability (ESRT) Protocol

Sankarasubramaniam *et al.* [16] proposed this protocol. ESRT aims for reliability at the application level and provides reliable delivery of packets from sensors to the sink. By regulating sensor frequency, this protocol tries to guarantee end-to-end reliability. However, reliability is maintained for the whole application and not for each single data packet. Congestion feedback from sensor nodes is broadcasted, notifying to adjust the reporting rate in the network so that the sensor nodes are able to receive sufficient number of packets but only as much as packets necessary in order to avoid congestion and save energy. ESRT runs on the sink, with negligible functionality needed at the sensor nodes. The protocol operates by determining the reliability achieved and congestion condition in the current network state. [17] Firstly, it periodically computes the reliability r based on how many packets are received successfully in a time interval. In the second step, the protocol deduces the required frequency f of the sensor nodes from r. Finally, ESRT informs all the sensor nodes about f through an assumed channel with high power. ESRT identifies five distinct regions in which it operates: i) No Congestion, Low reliability, ii) No Congestion, High reliability, iii) Congestion, High Reliability, iv) Congestion, Low Reliability and v) Optimal Operating Region—which actually is the region with No Congestion, Medium-High Reliability. The aim is to identify the current operating state of the network and to bring it into Optimal Operating Region. The event-to-sink reliability is checked, if found lower than required, the reporting frequency of source nodes is adjusted aggressively in order to still maintain the target reliability level; if the reliability is higher than required, then the reporting frequency is conservatively reduced so that energy can be conserved while still maintaining the reliability of network. Thus, this self-configuring nature of ESRT protocol makes it robust even with dynamic changing topologies in the network. The best benefit resulting from ESRT [18] is its capability of energy-conservation by dynamically controlling the sensor reporting frequency. A disadvantage associated with ESRT is the fact that all nodes are treated equally due to which in case of congestion in one region of the network, all the nodes are forced to reduce their data rate, negatively affecting the network's throughput. Thus, it is able to provide fairness among the nodes since data rate reduction is applied on all the nodes in the network, even if there is congestion in a particular area in the network.

4.3.2 GARUDA Protocol

S. Brahma et al. [19] have discussed this protocol which is a reliable data transport protocol. This protocol provides reliable point-to-multipoint data delivery from the sink node to the sensor nodes. It comprises of the following elements

- an efficient pulse based solution for reliable short messages delivery;
- a virtual infrastructure called the core, that is instantaneously constructed during the course of a single packet flood; which is used to approximate a near optimal assignment of all the local designated servers,
- a two-stage NACK (negative acknowledgment) based recovery process that minimizes the overheads resulting from the retransmission processes in the network, and performs out-of-sequence forwarding to leverage the significant spatial re-use possible in a WSN;

The traffic direction flow implemented in GARUDA is downstream and it provides both: packet and destination related packet reliability.

4.3.3 STCP Protocol

It is a scalable and reliable transport layer protocol where the majority of functionalities are dealt at the sink [20]. It supports networks with multiple applications and provides additional functionalities such as controlled variable reliability as well as congestion detection and avoidance. In this protocol, before transmitting any packet, the sensor nodes inform the sink through a "Session Initiation Packet". [21] Through this initiation packet, the sink gets to know about the number of flows initiated from a source node, the type of data that is to be transmitted, the transmission rate, and the required reliability. When the moment the sink node receives this packet, it sends an ACK packet to the source node, and only then the source node starts transmitting the packets. Since the sink is aware of the rate of transmission from the source, the expected arrival time of the next packet can be determined. The sink node maintains a timer and sends a negative acknowledgement packet, if it does not receive a packet within the expected arrival time. Reliability is measured as the fraction of total packets successfully received by the network. For controlling the congestion, nodes inform the sink [22] whether they are experiencing any buffer overflow situation, and by setting their congestion notification bit value equal to 1, while the sink informs the source node about a congested path by setting the congestion bit on the ACK packet. In this case, a source node may change its routing path or decrease the data sending rate to mitigate congestion.

4.3.4 RCRT Protocol

Paek *et al.* proposed this protocol [23], which focuses on reliable delivery of data from the source to sink, while avoiding any intermediate congestion collapse. It works on the transport layer and its traffic management functionality is implemented on the sink. RCRT attempts to achieve 100% reliable data delivery in the network based on a NACK scheme. So, in case, there are packet losses, the sink requests the source for retransmission of the missing packets by sending a NACK with the missing packet numbers. RCRT implements following basic components at the sink:

- A congestion detection component which detects congestion in the network by checking upon the round trip time values, rate adaptation, and rate allocation, which if found more than the expected values means congestion has occurred and there is a need to decrease the flow rates to control congestion;

- The 'time to recover loss' [24] is used as an indicator of congestion detection in the wireless sensor network. Therefore, as long as the network is able to repair the packet losses (within around the Round Trip Time) the network in not congested.
- However, if the packet losses cannot be redeemed by the network then it figures out that there are congested spots in network.
- In case congestion occurs, RCRT applies a rate adaptation mechanism [25] to control it. With the help of the rate allocation mechanism, specific transmission rates are allocated to each data flow whenever the application on which the network is running changes.

5. Comparative analysis of the congestion control protocols discussed in the paper

The following table (Table 1) compares the congestion control protocols- ARC, CODA, CCF, Fusion, BGR and HTAP over the parameters of congestion detection mechanism, congestion notification methodology used [26] (whether it is implicit or explicit), the direction of traffic flow (whether from source to sink, or from sink to source [27]), whether the protocol is able to achieve fairness or not and the performance of protocol on the energy conservation [28].

Table 1 Congestion 'Control' Protocols

Protocol/ Mechanism	Congestion Detection	Congestion Notification	Congestion Mitigation	Traffic Direction	Fairness Achieved	Energy Conservation
ARC	Detected by whether the packets are successfully forwarded or not	Implicit	Traffic Control	Source to Sink	Yes	Medium
CODA	Buffer occupancy level and load level of the wireless channel	Explicit	Traffic Control	Source to Sink	No	High
CCF	Packet Service Time	Implicit	Traffic Control	Source to Sink	Yes	Low
Fusion	Buffer occupancy level and load level of the wireless channel	Implicit	Traffic Control	Source to Sink	No	High
BGR	Buffer occupancy level and load level of the wireless channel	Implicit	Resource and Traffic Control	Source to Sink	Yes	N/A
HTAP	Buffer Occupancy level	Implicit	Recourse Control	Source to Sink	No	High

The following table (Table 2) compares the congestion avoidance protocols – Siphon, LACAS, Priority based Medium Access Protocol and the Buffer and Rate Control based Congestion Avoidance Algorithm on two parameters – the congestion detection mechanism adopted by the protocols and the congestion avoidance mechanism implemented [29].

Table 2 Congestion Avoidance Protocols

Protocol/ Mechanism	Congestion Detection	Congestion Avoidance Mechanism
Siphon	Buffer Occupancy, Sink load and wireless channel load conditions	Traffic redirection through virtual sinks
Buffer and Rate Control based Congestion Avoidance Algorithm	Buffer Occupancy and wireless channel load	Traffic Control
Priority based Medium Access Protocol	Buffer Occupancy	The most congested nodes are given the highest priority and given the channel access also on priority
LACAS	N/A	Learning automata states to adjust flow rates

The following table(Table 3) compares ESRT, GARUDA, STCP, and RCRT, the reliable data transport protocols on three parameters – the reliability mechanism adopted by the protocol(whether it is hop-by-hop or end-to-end), the traffic direction (whether it is downstream or upstream) and the level at which the reliability is achieved by the protocol [30].

Table 3 Reliable Data Transport Schemes

Protocol/ Mechanism	Reliability Mechanism	Traffic Direction	Reliability level achieved
ESRT	Hop-by-Hop	Downstream	Packet
GARUDA	Hop-by-Hop	Downstream	Packet and Destination Related
STCP	End-to-End	Upstream	Event and packet
RCRT	Hop-by-Hop	Upstream	Packet

6. Conclusion

In this paper, we presented a brief review of reliable and congestion control protocols in wireless sensor networks. Congestion control protocols are reactive protocols whereas the congestion avoidance protocols work in pro-active manner. The reliable transport protocols basically ensure that the data to be transmitted through the wireless sensor networks reaches correctly at its intended destination and, in this process, the data is not getting corrupted, that is the integrity of the data is maintained. The data reliable transmission protocols are needed in areas having real time and crucial data applications. The study of different protocols is done and a comparative analysis of the protocols is concluded. Congestion has a deep impact on the energy consumption, efficiency, packet delivery ratio, delay in data delivery and the lifetime of a wireless sensor network, hence it is very important to monitor and control the congestion. The review conducted on congestion control protocols has shown that the type of application and data flow type influence the traffic control deeply. Since reliability is the crux functional area of the transport layer, it is crucial to ensure the dependability of the applications operating on wireless sensor networks.

References

[1] B. Sharma and T. C. Aseri, “A comparative analysis of reliable and congestion-aware transport layer protocols for wireless sensor networks,” International journal of Sensor Networks, vol. 2012, 14 pages, Dec. 6, 2012.
[2] B. Sharma and T. C. Aseri, “A hybrid and dynamic reliable transport protocol for wireless sensor networks,” Computer and Electrical Engineering, vol. 48, pp. 298-311, November 2015.
[3] Rahman, Md Obaidur, M. M. Monowar, and C. S. Hong, "A capacity aware data transport protocol for wireless sensor network," Computational Science and Its Applications(ICCSA ’09), Springer Berlin Heidelberg, pp. 491-502.
[4] Flora, D. F. Jenolin, V. Kavitha, and M. Muthuselvi, "A survey on congestion control techniques in wireless sensor networks," International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT ‘11), IEEE press, 2011.
[5] R. Prabha, P. K. Gouda, Manjula S H1, K R Venugopal, and L M Patnaik, “ MTADF : multi hop traffic aware data for warding for congestion control in wireless sensor networks,” International Journal of Wireless & Mobile Networks (IJWMN ‘15), Feb. 2015, vol. 7, no. 1.
[6] J. Zhao, L. Wang, S. Li, X. Liu, Z. Yuan, and Z. Gao, (2010, October). “A survey of congestion control mechanisms in wireless sensor networks,” The Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP ‘10), IEEE press, 2010, pp. 719-722.
[7] J. Wan, H. Yan, Q. Liu, K. Zhou, R. Lu, and D. Li, “Enabling cyber–physical systems with machine–to–machine technologies,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 13, no. 3-4, pp.187-196.
[8] S. Zafar, “A survey of transport layer protocols for wireless sensor networks,” International journal of Computer applications, vol.33, no.1, pp.44-50, November 2011.
[9] M. A. Kafi, et al., “Congestion control protocols in wireless sensor networks: A survey,” IEEE Communications surveys and tutorials, vol.16, no. 3, pp.1369-1390, March 2014.
[10] E. Dashkova and A. Gurtov, “Survey on congestion control mechanisms for wireless sensor networks,” Internet of Things, Smart Spaces, and Next Generation Networking, vol.7469, pp.75-85, 2012.

[11] C. Sergiou, V. Vassiliou, and A. Paphitis, "Hierarchical tree alternative path (HTAP) algorithm for congestion control in wireless sensor networks," Journal of Ad-hoc Networks, vol.11, no. 1, pp. 257-272, January 2013.
[12] G. Srinivasan and S. Murugappan, "A survey of congestion control techniques in wireless sensor networks," International Journal of Information Technology and Knowledge Management, pp. 413-415, 2011.
[13] Alam, M. Mahbub, and C. S. Hong, "Buffer and rate control based congestion avoidance in wireless sensor networks," Proceedings of Korea Information Processing Society, pp. 1291-1293, May 2007.
[14] Patil, Dipti, and S. N. Dhage, "Priority-based congestion control protocol (pccp) for controlling upstream congestion in wireless sensor network," International Conference on Communication, Information & Computing Technology (ICCICT '12), IEEE press, 2012.
[15] V. Tickoo and S. Gambhir, "A comparison study of congestion control protocols in WBAN," International Journal of Innovations and Advancement in Computer Science, vol. 4, no. 6, June 2015.
[16] Sankarasubramaniam, Yogesh, Ö . B. Akan, and I. F. Akyildiz, "ESRT: event-to-sink reliable transport in wireless sensor networks," Proc. of the 4th ACM International Symposium on Mobile Ad hoc Networking & Computing, pp. 177-188, 2003.
[17] V. Michopoulos, L. Guan, G. Oikonomou, and I. Phillips, "A comparative study of congestion control algorithms in IPv6 wireless sensor networks," Proc. IEEE Int. Conf. Distributed Computing in Sensor Systems and Workshops (DCOSS '11), June 2011, pp. 1–6.
[18] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (Important) things," IEEE Communication Surveys Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.
[19] Brahma, Swastik, M. Chatterjee, and K. Kwiat, "Congestion control and fairness in wireless sensor networks," The 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE press, 2010, pp. 413-418.
[20] W. W. Fang, J. M. Chen, L. Shu, T. S. Chu, and D. P. Qian, "Congestion avoidance, detection and alleviation in wireless sensor networks," J. Zhejiang Univ.—Sci. C, vol. 11, no. 1, pp. 63–73, 2010. Available: http://dx.doi.org/10.1631/jzus.C0910204
[21] K. Zheng, F. Hu, W. Wang, W. Xiang, and M. Dohler, "Radio resource allocation in LTE-advanced cellular networks with M2M communications," IEEE Communications Magazine, vol. 50, no. 7, pp. 184–192, 2012.
[22] J. Jin, M. Palaniswami, and B. Krishnamachari, "Rate control for heterogeneous wireless sensor networks: Characterization, algorithms and performance," Computer Networks, vol. 56, no. 17, pp. 3783–3794, November 2012. Available: http://www.sciencedirect.com/science/article/pii/S1389128612003131
[23] Paek, Jeongyeup, and R. Govindan, "RCRT: rate-controlled reliable transport for wireless sensor networks," Proc. of the 5th international conference on Embedded networked sensor systems, pp. 305-319, 2007.
[24] Spachos, Petros, P. Chatzimisios, and D. Hatzinakos, "Cognitive networking with opportunistic routing in wireless sensor networks," IEEE International Conference on Communications (ICC '13), IEEE press, 2013, pp. 2433-2437.
[25] P. Spachos, Petros, P. Chatzimisios, and D. Hatzinakos, "Energy aware opportunistic routing in wireless sensor networks," Globecom Workshops (GC Wkshps), IEEE press, 2012, pp. 405-409.
[26] C. sergiou et al, "A comprehensive survey of congestion control protocols in wireless sensor networks," IEEE Communications surveys and tutorials, vol.16, no. 4, pp.1839-1859, December 2014.
[27] Ali Ghaffari, "Congestion control mechanisms in wireless sensor networks: A survey," Journal of Network and Computer Applications, vol. 52, pp. 101–115, June 2015.
[28] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, P. Polakos, "Wireless sensor network virtualization: A survey," Communications Surveys & Tutorials, vol.18, no.1, pp. 553-576, 2016.
[29] Mocanu, D. Constantin, Vega, M. Torres, Liotta, and Antonio, "Redundancy reduction in wireless sensor networks via Centrality Metrics," IEEE International Conference on Data Mining Workshop (ICDMW '15), pp. 14-17, November 2015.
[30] M. Collotta, G. Pau, "A solution based on bluetooth low energy for smart home energy management," Energies, vol. 8, no. 10, pp. 11916-11938, October 2015.