Survey on Congestion Control Mechanisms for Wireless Sensor Networks

Ekaterina Dashkova and Andrei Gurtov

University of Oulu, Centre for Wireless Communication
Oulu, Finland
{edashkov, gurtov}@ee.oulu.fi

Abstract. Congestion is very common in 6LoWPAN networks, but classical congestion control techniques do not suit well to the resource constrained environments. The main goal of this paper is to make an overview of the existing congestion control techniques for constrained environment and propose a need for the development of new flexible technique. It shall address all restrictions set by the environment and at the same time be generic enough. If the congestion control mechanism will be implemented at the application layer, i.e. as an improved extension of Constrained Application Protocol, then such solution will not be generic, as only this protocol will have modification. It would be more beneficial if the research will result in a new general solution suitable for the Constrained Application Protocol congestion control mechanism and other protocols.

In this paper an overview of congestion control techniques for constrained environment is made, scenarios of network performance, when congestion can appear and become a catastrophic are underlined. An idea of improving congestion control mechanism of Constrained Application Protocol is proposed.

Keywords: Congestion control, M2M, COAP extension, Scalability, Sensors, Ubiquitous, 6LOWPAN

1 Introduction

Rapid development of wireless sensor networks (WSNs) pushes an idea of connecting WSNs to the Internet. It requires the new REST architecture that would satisfy restrictions of the resource constrained nodes (e.g., 8-bit microcontrollers with only a small RAM and ROM) with weak network connection (e.g., 6LoWPAN with the speed of 250 Kbit/s). To address this need the Constrained Application Protocol (CoAP) [1] has been proposed. It is a generic web protocol that satisfies special requirements of constrained environment, especially considering energy, building automation and other M2M applications. The CoAP protocol can be seen as an implementation of REST architecture for the specific environmental conditions, which is delivered in a number of ways, e.g. by compressing HTTP. The CoAP protocol is based on unreliable UDP transport layer, which does not provide internal

congestion control (CC) mechanisms so the congestion control has to be provided by the upper layers.

Wireless sensor networks often experience significant congestion [2]. To study congestion control in large-scale networks that consist of small devices with tiny processors and small amount of RAM and ROM we have to make some assumptions concerning the observing system, and construct an effective mechanism to predict and avoid congestion.

We believe that a combination of Active Queue Management mechanism (AQM) - Beacon Order-Based Random Early Detection (BOB-RED) [3] and Explicit Congestion Notification (ECN) bits usage can be very effective combination for congestion control mechanism. The most of this solutions can be deployed by the routers or some other intermediate devices that behave as sub-network coordinators. We assume that these devices are not energy constrained and can handle most part of the congestion control mechanism calculations.

The rest of the paper is organized as follows: first we study limitations of the system in Section II, define the scenarios in Section III then make survey on the existing methods in Section IV, and finally make our proposal in Section V. Conclusion finalizes our work.

2 Background of the Study

On the first step we will describe the stack of protocols which is implemented to perform in the network (Fig. 1 is taken from the source [4]).

Layer	*Protocol*
Application	CoAP
Transport	UDP
Network	IPv6
Adaptation	6LoWPAN
MAC	IEEE 802.15.4
Physical	IEEE 802.15.4

Fig. 1. Stack of protocols.

Physical and MAC layers are IEEE 802.15.4 [5] (it means that bandwidth is roughly 250Kbit/sec and maximum packet size is 127 bytes on the physical layer). Due to specification of IEEE 802.15.4 MAC layer uses CSMA/CA with optional TDMA mechanism [6]. On the network layer is IPv6 and transport layer is provided by unreliable UDP, both of them are compressed by Adaptation layer of 6LowPAN and at the top of the stack is CoAP application protocol. Below more detailed description of each layer is presented.

A. Physical and Data Link Layers

Implementation of the IEEE 802.15.4 standard of MAC layer [5] specifies two types of modes: non-beacon mode and beacon enable mode. In non-beacon mode, 802.15.4 uses CSMA/CA with optional TDMA mechanism; CCA (Clear Channel Assessment) is carried out before sending on the radio channel; if the channel is occupied, a node forced to wait for a random period of time, before trying to retransmit data one more time. In a beacon-enabled mode, a super-frame structure is introduced; time is divided into different transmission periods (Beacon, CAP (Contention Access Period), CFP (Contention-free Period) and inactive).

B. Network Layer

On the network layer is IPv6 protocol. IPv6 header is 40 bytes long and this is too much for the IEEE 802.15.4 standard as after all deductions there is just 41 bytes left for the transport and application layers. Due to this problem an adaptation layer is used to compress IPv6 header to just 2 bytes.

Usage of ECN bits of the IPv6 header (Fig. 2) for congestion detection is described in details in [7] where one can find detailed description of ECN bits usage only in cooperation with TCP transport entity. One solution for the considering model is to provide capability of ECN approach to work in cooperation with UDP protocol. The first limitation is to make mandatory capability of ECN bits processing to all devices, in the network. One more direction research can follow is dropping old non-relevant information even during multicast to save network resources.

indentation in octets		0							1							2							3						
	indentation in bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
C	96																																
10	128																																
14	160																																
18	192	Destination Address																															
1C	224																																
20	256																																
24	288																																

Fig. 2. IPv6 header format.

C. Transport Layer

Why is there UDP on the transport layer? UDP has several benefits that from the viewpoint of the constrained devices are quite important [6]:

- has a low overhead, its header is just 8 bytes;
- is well suitable for applications for which memory footprint is prioritizing;
- provides multicast delivery;

- UDP has several drawbacks as well:
- doesn't have any recovery mechanism from the packet loss, that occurs in the network quite regularly;
- doesn't have any congestion control mechanism leaving this function to the upper layers;
- doesn't have any mechanism to regulate the size of packets (it should be very small for 6LoWPAN network) – there is no segmentation and re-assembly mechanism.

WSNs are usually deployed by applications for which freshness of information is more crucial then its completeness. It is expected that application will periodically receive fresh data and it is more important to process just coming packets, then to wait for previous ones. And UDP protocol is more suitable in this case.

IPv6 and UDP headers are compressed by 6LoWPAN adaptation layer to be suitable for the limitations of the environment. More detail specification of 6LoWPAN compression can be found in [8].

D. Application Layer

On the application layer of the stack is CoAP protocol, which is easily translated to HTTP and satisfies all limitations of the constrained environment [1]. CoAP protocol already has some CC mechanism, proposed in [9]. One of the goals of the current research is to find a new way to improve its performance and do research in the field of congestion control mechanisms.

CoAP has some primitive congestion control technique described in [9]. It deploys primitive stop and wait mechanism as a retransmission technique, constant values of the retransmission counter and retransmission timer. This mechanism can be improved through using non-constant values of the retransmission timer and the retransmission counter maximum thresholds as well as minimum and maximum thresholds of the intermediate devices buffers. So, new mechanisms of calculating threshold can be implemented. This mechanism may focus on different parameters and techniques, such as Round Trip Time (RTT), analyzing Congestion Experienced bits from the IPv6 header, error rate, and active queue management algorithms.

E. Network Topology and General Assumptions

Assumption that network topology is star will help to study limits of intermediate devices and servers and amount of nodes they can support. The bottlenecks of our system are the channel that connects a group of sensors with the intermediate device and intermediate devices themselves (Fig.3).

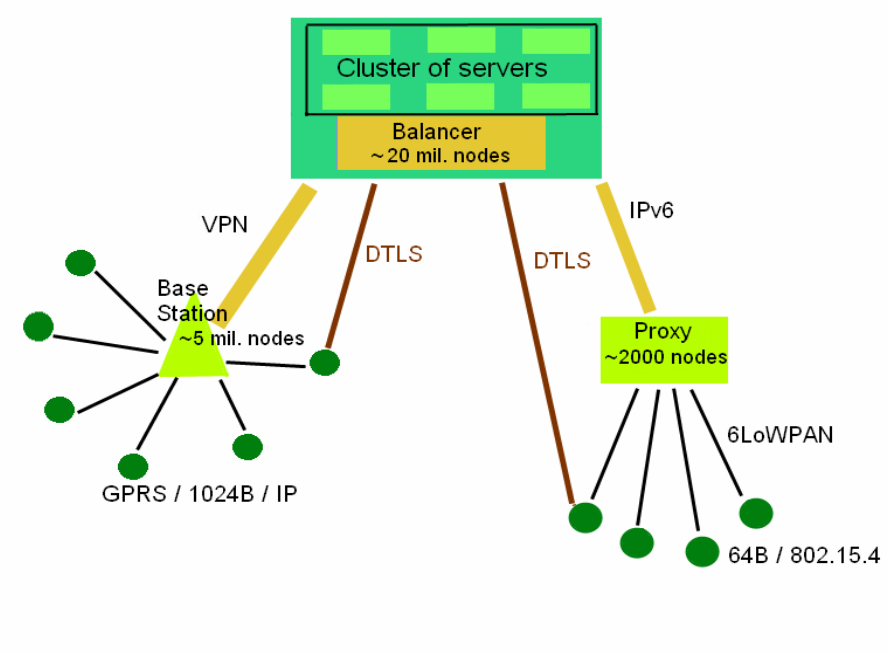

Fig. 3. The network architecture.

It is important to experiment with different values of timeouts, amount of retransmissions and intermediate devices' buffer sizes. The main point is discovering an opportunity to connect as many sensors as possible with the intermediate device by reliable, congestion-free channel and use this channel effectively. Each device in the network has a unique 64-bit extended address or allocated 16-bit short address [5]. We assume that some nodes are battery equipped and some of them are not energy limited (sub-network coordinators). One additional consideration is mobility, and we assume that sensor nodes are static.

The congestion control mechanism in wireless sensor networks should be light and efficient at the same time. Congestion can appear in two main cases: the routers or intermediate device buffers are overflowed or channel collisions took place. Transport layer of the proposed model is unreliable UDP, so congestion control mechanism is going to the application layer and may be supported by information which is gathered and processed on the lower layers (a so called cross-layer solution).

To create a general solution for detecting and avoiding congestion in WSNs it is not enough to propose a new algorithm only on the application layer because in this circumstance innovation can be used only for one particular application case. We propose an idea of developing new mechanisms in congestion control that could later be interpreted as a general solution for the wireless sensor network stack (6LoWPAN networks). Extension of research in the area of congestion control for CoAP by cross-layer congestion control development gives better perspectives and matches the main goals of the research.

3 SCENARIOS OF CONGESTION IN SENSOR NETWORKS

First of all it is important to divide traffic on downstream (from the sink/server to the sensors) and upstream (from the sensors to the sink/server). Obviously, that the downstream traffic has one-to-many nature while upstream many-to-one. The upstream traffic can be classified into four categories: event-based, continues, query-based and hybrid [10].

It is easy to imagine a sensor network for example spread through a national park (the purpose can be just controlling temperature to avoid fire dissemination). Sensors are spread randomly through the territory and below we describe key drawbacks of this network. Devices are energy constrained, but it is hard to maintain them. Because of randomness it is hard to predict how many sensors will be connected with one router or some intermediate device which plays a role of the sub-network coordinator. There can be several scenarios of network performance, effluent from the hybrid data delivery including continuous, event-based, and query-based.

1) Sensors regularly exchange service information or data and sleep for most periods of time. If our network is idle most of the time, we can consider that one intermediate device (proxy) can support 10000 of nodes and process all information from them correctly.
2) Some event took place and a lot of nodes (if not all) in one particular area have to send information to the server. In this situation a congestion collapse can take place. All information will be important and should be delivered in time. “Emergency” data can give additional information as where the fire started and how it is spread. This information will be helpful not only for the decreasing extent of damage but also for investigation of the incidence. This scenario influences greatly on amount of intermediate devices in the network as if all sensors at once will become active. Then limits of the intermediate devices buffer size and processing capability will become critical parameters of the whole system.
3) Server can query information at specific time, nodes can start to send information, interrupt each other, and collision in the channel will occur. Even if it will be enough intermediate devices and there won’t be any buffer queues, this will definitely lead to congestion.

All sensors are divided between routers, proxies or some other intermediate devices which play the role of sub networks coordinators [5]. At each moment sensor can connect some sub network or disconnect from it (for example, one device can broke up, while a new one can be sent to the territory).

4 CONGESTION CONTROL MECHANISMS

New research directions and resent solutions solving the congestion problem in wireless sensor networks were studied [11] - [16]. The first fact that is underlined in most part of discovered sources is that classical TCP-based congestion detection and avoidance technique is not suitable for the wireless sensor networks, as it consumes a

lot of resources and is very aggressive from the view point of constrained devices and unstable environment.

There are two types of congestion in wireless sensor networks: buffer congestion and channel collision. Channel collision can be overcome using mechanisms employed by the data link layer: Carrier Sense Multiple Access (CSMA), Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA). These mechanisms help to share medium through frequency division FDMA, time division TDMA and sampling medium on the existence of the transmission of some other node CSMA. Below these techniques will be described in more details.

A large number of techniques exist which were invented especially for the wireless sensor networks. These methods are deployed by different layers of the OSI stack.

A. Data Link Layer Techniques

TDMA-based techniques as **Self-organizing Medium Access Control (SMACS)** [17]; TDMA techniques should be included to the data link layer congestion control mechanism as nodes have to switch-off for some time, to avoid idle listening and through this avoid energy starvation of the device. This is an important case because listening and transmitting are both very energy-expensive operations in a low-power radio;

On-demand TDMA extension of IEEE802.15.4 MAC layer with priority-based communication scheduling mechanism in nearby routing devices is described in [18]. This approach proposes an idea of extending existing active period of work, by using additional communication period (ACP), in the inactive period of the standard IEEE802.15.4 MAC superframe;

Hybrid TDMA/FDMA-based medium access [19] - this scheme balances between optimal number of channels and gives the minimal power consumption;

CSMA. There are two most popular modifications of CSMA protocols: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Ethernet networks use CSMA/CD mechanism as their links are full duplex, but wireless networks use CSMA/CA, for half-duplex channels. One more difference between them is that CSMA/CA sampling channel by the jam signal and by this way preventing any data loss. When CSMA/CD use strategy of sending real data packets and only after collision occurs (two devices start transmission in one time) this algorithm conducts device to wait for random period of time and send a jam signal.

B. Network Layer Techniques

Beacon Order Based RED (BOB-RED) - Active queue management techniques such as BOB-RED are effective in networks with dozens of sensors connected to few intermediate devices (routers). BOB-RED in comparison with classical RED has strong advantage as it divides traffic on real-time and non-real time. With the help of such virtual queues it becomes easier to calculate priority of each particular piece of

data and mark or drop packet when buffer overflows. Through marking packets because of the buffer overflow it becomes easier to inform sensors about congestion that router or some other intermediate device experiences. That can influence on the retransmission counter and retransmission timer values and slow down amount of upcoming packets to the congested intermediate node and filter emergency information. This approach consists of a virtual threshold function, a dynamic adjusted per-flow drop probability, a dynamic modification of beacon order (BO) and super-frame order (SO) strategy that decrease end-to-end delay, energy consumption, and increase throughput when there are different traffic type flows through the intermediate node [3]. Technique allows adapting BO and SO of each intermediate device individually to satisfy the requirements of each intermediate device in the WSN. BOB-RED assigns BOi, SOi for each neighbor node *i*, of the particular intermediate device. It is highly efficient in large-scale wireless sensor networks as deployed by the intermediate devices (which have more resources and calculating capabilities). Authors of [3] propose a relationship between qualities of service with the parameters (minimum and maximum thresholds, queue types and etc.) They divide all the factors influencing end-to-end delay into five levels depending on their values.

Several performance metrics were measured in [3]:

- average end-to-end can be decreased by decreasing the packet retransmissions;
- packet delivery ratio (PDR) which equals the ratio of received packets to the send packets is used for denoting the network performance;
- energy consumption which is measured only on the intermediate device.

With the help of numerous of simulation results and performance metrics analysis in [3] it was proven that BOB-RED can lessen the congestion by early detecting the queue status to drop packet to decrease the retransmission of arriving packets.

C. Transport Layer Techniques

Datagram Congestion Control Protocol (DCCP) developed by the IETF, the standard was accepted in year 2006 [20]. Recently it supports TCP-like congestion control mechanism and TCP-Friendly Rate Control (TFRC).

Pump Slowly Fetch Quickly (PSFQ) [21] - 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 designed with the assumption that sensors application generates light traffic. This proposal opposite to the main use case we consider (preventing congestion collapse when network is under heavy load).

Sensor Transmission Control Protocol (STCP) – protocol focuses on the sensor transmission requirements – [22] it is a general protocol of the transport layer which satisfies requirements of the constrained devices. The most part of the functionality is realized on base stations or intermediate devices. Functionality includes mechanisms

for early congestion detection and avoidance, variable reliability and support of several applications in one network.

Light UDP - [23] transport layer protocol, the main feature of which is that damaged packets are not dropped but delivered for the application layer for further analysis. This approach can be effectively deployed by applications for which delivery of all data has more priority than its integrity (multimedia protocols, stream video, voice IP). The main issue of this approach is that CheckSum field doesn't cover the whole packet but the current part of the header which is important for the future transmissions.

Reliable UDP - [24] transport layer protocol, the main feature of which is that it is working on the UDP/IP stack and provides reliable in order delivery. This protocol doesn't support classical congestion control technique or "slow start" mechanisms.

D. Techniques with Cross-Layer Nature

Fusion technique [25] combines tree mechanisms which cover different layers of the classical stack: hop-by-hop flow control (transport layer), rate limiting source traffic and prioritized data link layer that gives backlogged node priority over non-backlogged nodes for access to the shared medium.

Congestion Detection and Avoidance (CODA) [16] technique combines three mechanisms: receiver-based congestion detection; open-loop hop-by-hop backpressure; and closed-loop multi-source regulation. As it is proved by ns-2 simulation results this mechanism can be very effectively deployed by event driven networks, which perform under the light load most of the time, but after some critical event become heavy loaded.

5 OUTLINE OF OUR APPROACH

A lot of techniques exist, but because of the protocol stack that we have and specific scenario that we consider there can be incompatibility with some of these techniques. We propose an idea of using ECN bits in the IPv6 header together with CoAP acknowledgement and active queue management technique BOB-RED on the side of the intermediate devices such as routers.

There are several types of data [26]:

- regular data that is sent by the sensors. In this case, it will be more crucial to keep data up-to-date than to gather it all but with delays because of the retransmissions;
- sometimes data that is sent by the sensor contains information about event that occurs in the network. Delivery of this particular piece of information should have priority in the channel as due to the situation, even delay of such data can be dangerous;
- requests for some service information from sensors to the proxies/routers and servers have to be fully delivered as it is crucial for the further correct work of the whole network. This data can be delayed, as it is non-urgent. This data is

important because sensors are going into sleep mode to avoid idle listening and spending energy resources;

- at the same time the flow of service information from the proxies, routers, other intermediate devices and servers has to be fully delivered to all sensors for the same reason listed above;

Due to the cases described above it is crucial to deliver as much data as possible, but at the same time remember about the relevance of the transmitted data and follow its priority.

We can consider several steps of congestion detection by examining the packet coming to the queue of the intermediate device:

1) If the queue is almost empty, then packet is accepted and waits for its turn to be processed and sent to the end point. After receiving such packet an end point replies with the CoAP acknowledgement.
2) If the queue is filled with some packets, but its length doesn't exceed the maximum threshold defined in the device, then the packet is marked with the Congestion Experienced bit and sent to the end point. The end point sends an acknowledgement but with the marked field (or just bit). This mark says to the sender the amount of retransmissions should be decreased by 1 and value of the retransmission timeout should be increased till the random value from the interval [1,5*recent_value; 1,9*recent_value]
3) If queue is filled with some packets, and its length exceeds the maximum threshold defined in the device, then the upcoming packet is dropped by the intermediate device. In this case end point doesn't receive anything and no acknowledgement will be sent. If on the sender side after the retransmission timer expires and there will be no acknowledgement received, the retransmission timer and retransmission counter should be halved.

This idea is quite simple and is based on the already existing technology (BOB-RED), but at the same it defines a small modification to the proposed technique. All static parameters became dynamic now, and their values change depending on the type of congestion.

Considering the security aspect of the system one more parameter was taken into account. Adversary can try to flood the network by "urgent traffic" and prevent network further correct work. In this scenario all resources of the network will be governed to process only "urgent traffic". This will lead to the situation when data from the "honest nodes" will be lost or delayed while adversary data will flood the network and can finally lead to the network collapse. To avoid this scenario one more limit should be taken into account, it is amount of the "urgent traffic" (real-time data) that can be transmitted by each sensor node. Due to this aspect there are two options that authors are considering:

- calculating ratio of the "urgent traffic" to the whole generated traffic of the node to prevent sending more "real-time data" than some fixed threshold;
- implementing specific timer after expiration of which a packet with "urgent" data can be sent.

Decision of which of two ways to choose is left for the future work and further discussions.

6 Conclusion

Wireless sensor networks often experience congestion, so an advanced congestion control solution is required. The CC mechanism should differ from its sibling deployed in the Internet. A lot of research and solutions were published targeted to solve the congestion problem in resource restricted communications. For our purpose most of them are not suitable because of the fixed protocol stack and assumptions concerning network topology and mobility.

We made a survey on congestion control mechanisms for wireless sensor networks and formulate an effective algorithm satisfying all underlined assumptions. The key approach is using BOB-RED active queue management mechanism to predict the overflow of the intermediate devices buffers. Modifications to the application layer CC mechanism were proposed. At the moment model for testing proposed technique is being built.

Future work is to develop and prototype the congestion control solution for CoAP, measure and evaluate its performance by simulations and in a large-scale sensor testbed.

Acknowledgments. Authors would like to thank the Massive Scale Machine-to-Machine Service (MAMMOTH) project and Tekes for financial support. We would like to thank Jussi Haapola for conducting the organization process of the research.

References

1) Z. Shelby, K. Hartke and C. Bormann, "Constrained Application Protocol (CoAP)", Internet-Draft draft-ietf-core-coap-07, Expires: January 9, 2012.
2) S.H. Moon, S.M. Lee and H.J.Cha, "A Congestion Control Technique for the Near-Sink Nodes in Wireless Sensor Networks", Lecture Notes in Computer Science, Vol 4159, pp 488-497, 2006.
3) M.-Sh. Lin, J.-Sh. Leu, W.-Ch. Yu, M.-Ch. Yu and J.-L. C Wu, "BOB-RED queue management for IEEE 802.15.4 wireless sensor networks", EURASIP Journal on Wireless Communications and Networking 2011.
4) M. Kovatsch, S. Duquennoy and A. Dunkels, "A Low-Power CoAP for Contiki", *In Proc. of the IEEE Workshop on Internet of Things Technology and Architectures*, October 2011.
5) IEEE Std 802.15.4-2011 IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).
6) J.-Ph. Vasseur and A. Dunkels, "Interconnecting Smart Objects with IP", Morgan Kaufmann publishers, 2010, ISBN: 978-0-12-375165-2.
7) K. Ramakrishnan, S. Floyd and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.
8) G. Montenegro, N. Kushalnagar, J. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.
9) L. Eggert "Congestion Control for the Application Protocol (CoAP)" Internet Draft draft-eggert-core-congestion-control-01 Expires July 31, January 27, 2011.

10) C. Wang, B. Li, K. Sohraby, and M. Daneshmand, “Upstream Congestion Control in Wireless Sensor Networks Through Cross-Layer Optimization”, IEEE Journal on Selected Areas in Communications, Vol 25, No 4, pp 786-795, May 2007.
11) V. Michopolous, L. Guan, G. Oikonomous and I. Phillips, “A comparative study of congestion control algorithm in IPv6 wireless sensor networks”, *In Proc. of the 3rd International Workshop on Performance Control in Wireless Sensor Networks,* June, 2011.
12) R. Chakravarthi, C. Gomathy, S. K. Sebastian, Pushparaj. K and V. B. Mon, “A survey on congestion control in wireless sensor networks”, *International Journal of Computer Science and Communication*, Vol 1, No 1, pp 161-164, January-June 2010.
13) M. Lunden and A. Dunkels, “The Politecast Communicative Primitive for Low-Power Wireless”, *ACM SIGCOMM*, Vol 41, No 2, April 2011.
14) S. R. Heikalabad, A. Ghaffari, M. A. Hadian and H. Rasouli, “DPCC: Dynamic Predictive Congestion Control in wireless sensor networks”, *IJCSI International Journal of Computer Science Issues*, Vol.8, Issue 1, pp 472-477, January 2011.
15) J.-P. Sheu, L.-J. Chang and W.-K. Hu, “Hybrid Congestion Control Protocol in Wireless Sensor Networks”, *Journal of Information Science and Engineering*, Vol 25, pp 1103-1119, May 2008.
16) Ch.-Y. Wan, Sh. B. Eisenman and A. T. Campbell, “CODA: Congestion Detection and Avoidance in Sensor Networks”, *In Proc. of SenSys’03,* November, 2003.
17) K. Sohrabi, J. Gao, V. Ailawadhi and G. J Pottie, “Protocols for Self-Organization of a Wireless Sensor Network”, *In Proc. of the 37th Allerton Conference on Communication, Computing and Control*, September 1999.
18) T. Zhong, M. Zhan and W. Hong, “Congestion Control for Industrial Wireless Communication Gateway”, *In Proc. of International Conference of Intelligent Computation Technology and Automation 2010*, pp 1019-1022, 2010.
19) E. Shih, S. H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang and A. Chandrakasan, “Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks”, *In Proc. of ACM Mobicom’01*, pp 272-286, July 2001.
20) E. Kohler, M. Handley, S. Floyd, “Datagram Congestion Control Protocol (DCCP)”, RFC 4340, March 2006.
21) C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, “PSFQ: a Reliable Transport Protocol for Wireless Sensor Networks”. *In Proc. of First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA 2002)*, pp. 1-11, USA, Atlanta, September 2002.
22) Y.G. Iyer, Sh. Gandham and S. Venkatesan, “STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks”, 2005.
23) L-A. Larzon, M. Degermark, S. Pink, G. Fairhurst, “The Lightweight User Datagram Protocol (UDP-Lite)”, July 2004, RFC 3828.
24) T. Bova, T. Krivoruchka, “Reliable User Datagram Protocol”, Internet Draft draft-ietf-sigtran-reliable-udp-00 Expires August 1999, February 1999.
25) B. Hull, K. Jamieson and H. Balakrishnan, “Mitigating Congestion in Wireless Sensor Networks”, *In Proc. of SenSys’04*, November. 2004.
26) “Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems”, Edited by M. Ilyas and I. Mahgoub, CRC Press, 2005 (Weilian Su, Erdal Cayirci, Özgur B. Akan “Overview of Communication Protocols for Sensor Networks”).
27) A. Gurtov and R. Ludwig, “Lifetime packet discard for efficient real-time transport over cellular links”, ACM Mobile Computing & Communications Review, Vol 7(4), pp 32-45, October 2003.