Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A probabilistic approach for predictive congestion control in wireless sensor networks

R. ANNIE UTHRA[1], S. V. KASMIR RAJA[1], A. JEYASEKAR[1], Anthony J. LATTANZE[2]

([1]Department of Computer Science and Engineering, SRM University, Tamil Nadu 6003203, India)

([2]Department of Software Engineering, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA)

E-mail: {annieuthra, svkr, ajeyasekar}@yahoo.com; lattanze@cs.cmu.edu

Received June 28, 2013; Revision accepted Dec. 6, 2013; Crosschecked Feb. 19, 2014

Abstract: Any node in a wireless sensor network is a resource constrained device in terms of memory, bandwidth, and energy, which leads to a large number of packet drops, low throughput, and significant waste of energy due to retransmission. This paper presents a new approach for predicting congestion using a probabilistic method and controlling congestion using new rate control methods. The probabilistic approach used for prediction of the occurrence of congestion in a node is developed using data traffic and buffer occupancy. The rate control method uses a back-off selection scheme and also rate allocation schemes, namely rate regulation (RRG) and split protocol (SP), to improve throughput and reduce packet drop. A back-off interval selection scheme is introduced in combination with rate reduction (RR) and RRG. The back-off interval selection scheme considers channel state and collision-free transmission to prevent congestion. Simulations were conducted and the results were compared with those of decentralized predictive congestion control (DPCC) and adaptive duty-cycle based congestion control (ADCC). The results showed that the proposed method reduces congestion and improves performance.

Key words: Congestion, Rate allocation, Congestion control, Packet loss, Back-off interval, Rate control
doi:10.1631/jzus.C1300175 **Document code:** A **CLC number:** TP393

1 Introduction

In a wireless sensor network (WSN), the sensor nodes scattered in the sensing field sense physical phenomena such as pressure, temperature, and humidity, and transfer these sensed data to the final destination called the gateway node. Congestion occurs in such a network when the offered load of a node exceeds the available capacity of that node or the channel bandwidth drops due to channel fading. Consequently, packets may be dropped at the buffers and require retransmission of those dropped packets, which leads to waste of energy. Therefore, both buffer and link bandwidth must be efficiently used to avoid congestion and packet drop among the nodes.

Congestion needs to be controlled in mission critical applications such as military, disaster management, and mining, as well as in other applications such as habitat monitoring and an environment monitoring system (EMS) to avoid retransmission of packets thereby increasing the lifetime of the nodes in the network. Consider an EMS (Fig. 1) consisting of a number of nodes deployed in the monitoring area (MA) inside a mine to monitor events like fire, oxygen reduction in air, increase in pressure, and leakage of poisonous gases. In this system each sensor node consists of a processor, memory, transceiver, power source, and one or more sensors. These sensor nodes communicate with each other and sensor data are transferred to the gateway node in the system. The gateway node, connected with the Internet, collects data from the sensor nodes and processes the data. Finally, it sends the data to the data collection center for further processing and storage of data. The above said scenario is equally applicable to other applications like the healthcare monitoring system.

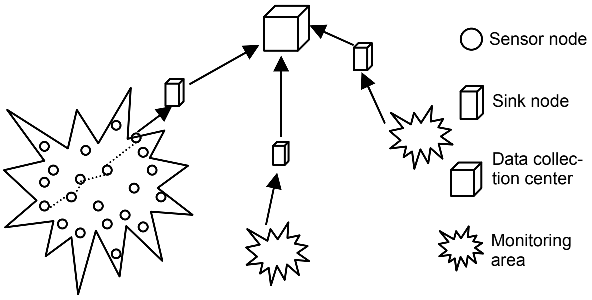

Fig. 1 Architecture of an environment monitoring system

Such wireless sensor network systems are data centric; the sensed data are crucial and should reach the destination, the gateway, through the intermediate nodes. Therefore, data transmission protocols need to mitigate congestion resulting from excess load and a fading channel to avoid packet drop and waste of energy due to the retransmission of dropped packets.

Other reasons for congestion in the network are listed below. The many-to-one nature of the event information flow causes congestion because a number of event sensing nodes send their information to any one of their next hop nodes. This node gets congested if the incoming rate exceeds the outgoing rate, which results in buffer overflow. Moreover, the transmission occurring at the same time causes packet collision. Therefore, node density is a key factor that increases the degree of congestion.

Each node shares a common radio channel with all its neighbors. An inadequate bandwidth reservation may degrade the network performance. Hence, to avoid congestion in the network, the data rate must be controlled and bandwidth must be used efficiently. In this paper, we propose a probabilistic method to detect congestion and propose congestion control methodologies to avoid congestion by efficiently using the buffer and channel bandwidth considering collision-free transmission.

Suitable back-off selection in media access control (MAC) layer congestion control is considered to save the energy of nodes.

2 Related works

Much research has been done to control congestion (Uthra and Raja, 2012) in WSNs. The end-to-end congestion control schemes need to propagate the onset of congestion between the end-systems. This makes the approach slow. In general, the hop-by-hop congestion control scheme reacts faster to congestion and is preferred to for minimizing packet losses in a wireless network. Therefore, the proposed scheme uses congestion algorithms to predict the onset of congestion of a node and gradually reduces the incoming rates by means of feedback messages.

One of the earliest congestion control protocols, congestion detection and avoidance (CODA) (Wan *et al.*, 2003), uses a combination of present and past channel loading and buffer occupancy for detection of congestion. Hop-by-hop and end-to-end congestion control schemes simply drop the packets at the node and use the additive increase multiplicative decrease (AIMD) scheme to control the source rate. This results in retransmission of packets. Fusion (Hull *et al.*, 2004) uses a static threshold value to detect the onset congestion in the network. Normally, it is difficult to find a static threshold value for a dynamic channel environment. Moreover, CODA and Fusion protocols use the broadcast message to inform their neighboring nodes about the congestion though this message is not guaranteed to reach the source.

The congestion control and fairness (CCF) routing scheme (Cheng and Bajcsy, 2004) uses packet service time at the node as an indicator of congestion. However, using the service time alone to determine the onset of congestion may be misleading. Interference-aware fair rate control (IFRC) (Rangwala *et al.*, 2006) is a rate allocation technique which detects congestion based on queue length. When congestion is detected, the rates of the flows are throttled on the interfering tree. When the average queue length exceeds the upper threshold, rates of the flows are adjusted using the AIMD scheme. Consequently, IFRC reduces the number of packets by reducing the throughput.

On the other hand, the priority-based congestion control protocol (PCCP) (Wang *et al.*, 2006) uses a ratio between packet inter-arrival time and packet service time to determine the congestion level of a node. Congestion information is piggybacked in the header of data packets and broadcasted, and received by child nodes. However, both CCF and PCCP ignore queue utilization, which leads to frequent buffer overflows. This results in increased retransmission.

Moreover, when the source is at multiple hops from the congestion region, the congestion information is not guaranteed to reach the source in case of CODA and PCCP.

Congestion aware routing (Kumar *et al.*, 2008) is an application specific, differentiated routing protocol which uses the data rate to identify congestion and considers data priority to overcome congestion. This protocol is not suitable for applications that have equal priority data. The multi-event congestion control protocol (Hussain *et al.*, 2008), on the other hand, is a network specific protocol which uses packet delivery time and buffer size as indicators of congestion. Based on the buffer size, slot length can be either increased or decreased. The reporting rate can also be adjusted through the slot length. However, packet scheduling and maintaining routing table are overhead in this protocol.

Interference minimized multipath routing (I2MR) (Teo *et al.*, 2008) evaluates multipath for load-balancing. Long-term congestions are determined by monitoring the size of their data transmit buffers, by using exponential weighted moving averages (EWMAs). When a source node is congested, the loading rate is reduced. However, the number of control packets transmitted during path discovery increases. Traffic intensity is taken as a parameter to measure congestion in cluster based congestion control (Karenos *et al.*, 2008). Traffic intensity is measured in terms of arrival rate and the service time of the packets. Rate self-regulation is done in the source node. Rate control is done similar to the AIMD technique.

Congestion is detected in decentralized predictive congestion control (DPCC) (Zawodniok and Jagannathan, 2007) based on buffer occupancies at the nodes, along with the predicted transmitter power. The current queue level tracks the desired queue level. If the queue level exceeds the desired queue level, the designed feedback controller forces the queue level to the target value. The rate of node is calculated based on the outgoing rate and buffer occupancy error (excess data that cannot be accumulated in the buffer). The back-off interval is selected for both rate adaptation and prevention of congestion. However, DPCC fixes a static desired queue level to predict the congestion level. By contrast, the proposed scheme uses an adaptive threshold value and varies the rate based on the predicted congestion level.

Congestion control (Lee and Chung, 2010) is implemented using duty-cycle adjustment in adaptive duty-cycle based congestion control (ADCC). This scheme uses both resource control approaches in terms of the active time of a node and traffic control approaches according to the amount of network traffic for congestion avoidance.

The traffic-aware dynamic routing (Ren *et al.*, 2011) algorithm routes packets around the congestion areas and scatters the excessive packets along multiple paths consisting of idle and under-loaded nodes. A hybrid virtual potential field using depth and queue length forces the packets to eliminate the obstacles created by congestion and move toward the sink. The buffer capacity and data rate are considered as indicators of congestion in the probabilistic approach for congestion control (PACC) (Uthra and Raja, 2011). PACC predicts the onset of congestion in the network. However, outgoing traffic and channel state are not considered for predicting congestion. The proposed method considers incoming and outgoing traffic of nodes and the channel state to determine the onset of congestion.

A predictive control theory was used by Wu *et al.* (2013) to control a network with factors like time delays and packet dropouts. Backward and forward channels are considered to analyze transmission conditions. Accepting and applying newer data, compensating delayed or lost data, and discarding older data are the central law of the strategy. Network utility maximization (NUM) described by Morell *et al.* (2011) uses a convex decomposition technique to achieve an optimal solution. RADAR (Boutsis and Kalogeraki, 2012) uses elapsed times, latencies, and resource loads to dynamically determine the rate allocation. The problem is solved by maximizing the rate to meet the deadline of every application. Mao *et al.* (2012) considered data and battery buffers for maximizing the long-term average sensing rate. The rate control is performed based on the power management framework. Rate allocation in queue-based channel-measurement and rate-allocation (Q-CMRA) (Bhargava *et al.*, 2012) chooses the maximum allowed physical-layer rate based on queue length, and the highest rate is chosen using channel measurement.

Some of the routing protocols that grant reliability, including the multi-path and multi-speed routing protocol (MMSPEED) (Felemban *et al.*, 2006), SPEED (He *et al.*, 2003), and RAP (Lu *et al.*, 2002), use velocity monotonic scheduling. Certain speed is assigned to the packets. The speed of the packet is not clear when the network is congested. Reliability in MMSPEED is achieved through duplicating packets, which further increases congestion.

The protocols introduced earlier (Wan *et al.*, 2003; Cheng and Bajcsy, 2004; Wang *et al.*, 2006; Teo *et al.*, 2008) do not consider congestion due to fading channels in a dynamic environment. The congestion due to the effect of the fading channel is taken into account in the proposed system, which is explained in the following section. Rate reduction was considered in Wan *et al.* (2003), Hull *et al.* (2004), Rangwala *et al.* (2006), and Teo *et al.* (2008), and DPCC performs the rate control. However, the proposed system performs rate reduction and rate regulation based on the adaptive threshold value, which is introduced to trigger the execution of the congestion prediction algorithm, thereby invoking the congestion control algorithm immediately. Thus, the proposed system not only avoids packet drop but utilizes the buffer efficiently.

The overall objective of this paper is to develop (1) a congestion prediction method for detecting the level of congestion of a node, and (2) a congestion control method for mitigating congestion in each node. Congestion is mitigated by (1) controlling the flow rates of all nodes including the source nodes to prevent buffer overflowing using the predicted value, and (2) designing suitable back-off intervals for each node based on channel state and its current traffic. We have designed a mathematical model for congestion control in a network by considering both buffer capacity and link capacity of a node.

3 Probabilistic method for congestion detection

The contribution comes from the fact that the possibility of congestion is predicted ahead of its occurrence and hence the remedial actions can be carried out to eliminate congestion. The estimate of the congestion level is used to reduce the source rate. The level of congestion in each node is detected using the buffer occupancy and an adaptive threshold value on the buffer capacity of that node. The buffer occupancy of node i at time t+1 is given by

$$q_i(t+1)=q_i(t)+u_i(t)-v_i(t), \tag{1}$$

where $u_i(t)$ and $v_i(t)$ are the incoming and outgoing traffic rates of node i at time t, respectively.

The threshold value of node i is calculated using

$$\begin{gathered}\alpha_i(t+1)=\frac{v_i(t)}{u_i(t)}(\mathrm{BUFMAX}_i-q_i(t)),\\ u_i(t)>0,\ v_i(t)>0,\ u_i(t)>v_i(t),\end{gathered} \tag{2}$$

where BUFMAX_i is the maximum buffer size of node i and $\alpha_i(t+1)$ is the threshold value of buffer for the given flow rate considering the remaining capacity of node i. $\alpha_i(t+1)$ is inversely proportional to the incoming traffic, and directly proportional to the outgoing traffic and the remaining buffer capacity. Therefore, the threshold value decreases as the incoming traffic increases. $\alpha_i(t+1)$ specifies the desired queue level at t+1 based on the current traffic. Eq. (2) can be applied under the condition that there is data flow in the node or that the incoming traffic is larger than the outgoing traffic. Threshold $\alpha_i(t+1)$ is set to $\alpha_{\max}$, when outgoing traffic exceeds incoming traffic or $u_i(t)$ is zero. The adaptive threshold allows nodes in the system to tolerate bursting data flows. Table 1 illustrates the threshold values $\alpha_i(t+1)$ for certain conditions.

Table 1 Illustration of threshold values

Initial condition	Incoming traffic, $u_i(t)$ (packet/s)	Outgoing traffic, $v_i(t)$ (packet/s)	Threshold $\alpha_i(t+1)$
Buffer empty	2	1	$0.5\mathrm{BUFMAX}_i$
	4	1	$0.25\mathrm{BUFMAX}_i$
Buffer not empty	2	1	$0.5(\mathrm{BUFMAX}_i-q_i(t))$

Based on the conditions listed in Table 1, the following can be stated. When the buffer is empty and the incoming traffic is greater than double the outgoing traffic, the threshold is set to 50% of the buffer size. If the buffer is not empty, for example, the buffer contains 10 packets and BUFMAX_i is 32 packets, then we calculate the available space as 22 packets. In this example, the threshold is set to 50% of the available space, which is 11. This threshold value helps the node trigger the congestion control algorithm when the total number of packets exceeds the threshold value.

The buffer occupancy of a node is compared with its threshold value to detect congestion.

1. There is no congestion in the node if $q_i(t)<\alpha_i(t)$.

2. If $q_i(t)$ reaches BUFMAX_i, the maximum capacity of the buffer, and $u_i(t)>v_i(t)$, then the packets received by node i will be dropped. This results in buffer overflows, which in turn causes congestion.

3. Therefore, the proposed method detects congestion when $\alpha_i(t)<q_i(t)<\text{BUFMAX}_i$. When the buffer occupancy exceeds the threshold value, the level of congestion increases; i.e., as the number of packets increases to more than the threshold value, the occurrence of congestion also increases.

Hence, the probability of occurrence of congestion at node i is

$$\begin{aligned} & P_i(\alpha(t)+k) \\ & = p(\alpha(t)+k)+\sum_{n=1}^{k-1} p(\alpha(t)+n \mid \alpha(t)+(k-n)) \quad (3) \\ & = \beta_i^k(t). \end{aligned}$$

The time varying parameter $\beta_i^k(t)$ describes the probability for the onset of congestion of node i when there are k packets more than the threshold value. The proof of Eq. (3) is given in the Appendix. All the nodes that are in the communication range of node i belong to N_i, which is the neighborhood of node i. The probability of node i receiving a packet from node j, where $j\in N_i$ $\forall j$, is given by

$$p_{ij} = p_i / \eta, \quad (4)$$

where $\eta=|N_i|$, p_i is the probability of node i absorbing the packet from the neighboring nodes, and $1-p_i$ denotes the probability of node i dropping the packet. Nodes are uniformly and independently distributed. The probability that a node is in the neighborhood of node i is equal to A_i, which is the communication area of node i and has a value of unity.

The probability of node i having neighborhood size η is given by

$$P_i^\eta = p(|N_i|=\eta) = \binom{n-1}{\eta-1}(1-A_i)^{n-\eta} A_i^{\eta-1}. \quad (5)$$

The expected receiving probability of node i is

$$E[P(i)] = \sum_{\eta=1}^{n} p_{ij} P_i^\eta = \frac{p_i}{nA_i}[1-(1-A_i)^n]. \quad (6)$$

The level of congestion of a node is estimated using Eqs. (3) and (6) and propagated to the previous hop nodes for indicating the onset of congestion. A zero value of $\beta_i^k(t)$ indicates no congestion of a node, and $0<\beta_i^k(t)<1$ provides the level of congestion. Algorithm 1 gives the algorithm for congestion prediction, executed by every node in the network.

Algorithm 1 Congestion occurrence prediction

Calculate threshold value α and determine the possibility of congestion of a node.

Initialize:

BUFMAX is set to the maximum size of the buffer of the node; n is set to the number of neighboring nodes from which the node receives packets; A is set to the power level of the node.

```
Prediction()
// calculate the threshold value
 α=(v/u)*(BUFMAX−q);
 if (α>q)
    status=0;            // no congestion
 else if (q>α && q<BUFMAX)
    k=q−α;
    S=0;
    for (i=1; i<k; i++)
       S=S+pow(p/(n*A)*(1−pow((1−A), n)), i);
       status=S;          // possibility of congestion
    end for
 else
    status=1;            // congestion
 end if
// send feedback message to the source
 if (status!=0)
    set ECB=1;
    piggyback status into ACK;
 else
    set ECB=0;
    error=(α–q)*(1−g);
    piggyback error into ACK;
 end if
 send ACK to previous hop nodes
```

4 Congestion control methodology

Network congestion occurs when either the incoming traffic (received and generated) exceeds the capacity of the node or the link bandwidth drops due to channel fading caused by path loss, shadowing, and Rayleigh fading. Therefore, we have proposed two methodologies for congestion control, after predicting the occurrence of congestion. The first methodology is based on algorithms rate regulation (RRG) and split protocol (SP), which regulate data traffic of the receiver node by utilizing the buffer capacity. The second congestion control method determines the back-off interval of each node to adjust the outgoing rate of a node based on channel capacity.

4.1 Congestion control using the rate allocation scheme

The rate allocation scheme takes into account buffer occupancy, and incoming and outgoing rates of a node. Every node executes Algorithm 1 to determine the possibility of congestion, $\beta_i^k(t)$ (called the status value). The non-zero value of $\beta_i^k(t)$ is communicated as a feedback message between the upstream nodes. The feedback message is signaled to minimize the effect of congestion on the hop-by-hop basis by estimating the incoming and outgoing traffic flows when the adaptive rate allocation scheme (RRG or SP) is implemented at each node. Upon receiving the feedback message, the upstream node reduces its rate proportional to the status value given by the receiver node. The feedback information which consists of the status information is piggybacked to the acknowledgement (ACK) frame. This ensures that the feedback is successfully received by the nodes in the previous hop and avoids the transmission of extra control messages. The outgoing rate of neighboring nodes around the congested node is estimated in two different scenarios, as explained below.

Case 1: rate regulation (RRG)

When the queue level $q_i(t)$ exceeds the threshold value $\alpha_i(t)$, the status value $\beta_i^k(t)$ is propagated to the previous hop nodes toward the source node. Every previous hop node that receives the feedback message reduces its outgoing rate proportional to the status value.

$$u_i(t+1) = (1-\beta_i^k(t))u_i(t). \tag{7}$$

The desired incoming traffic rate of the receiver node i is calculated using Eq. (7). This methodology is named rate reduction (RR).

For the optimum use of a buffer, RR is modified into RRG. If $\beta_i^k(t)>0$, the outgoing rate of the source node is reduced proportional to the status value as in RR; otherwise, the outgoing rate of the source node is increased proportional to $e_i(t)$, where $e_i(t)$ is the buffer occupancy error of node i, defined as $e_i(t)=q_i(t)-\alpha_i(t)$. $e_i(t)$ specifies the number of packets that can be accommodated in the buffer to reach the threshold value. The incoming rate of the receiver node is estimated using

$$u_i(t+1) = (1-\beta_i^k(t))u_i(t) + (1-g_i)e_i(t), \tag{8}$$

where $0 \le g_i \le 1$. g_i is set to 1 for the non-zero value of $\beta_i^k(t)$ and RRG reduces the rate. Otherwise, g_i is varied between 0 and 1, and RRG increases the rate. In Fig. 2, the upstream nodes A and B receive feedback messages, i.e., the status value or error value, from the receiver node C and either reduce or increase their data rate as specified in the feedback message.

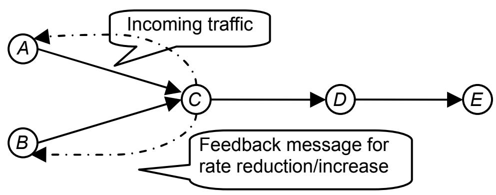

Fig. 2 Feedback message propagation for the previous hop nodes

The status value or the buffer occupancy error is piggybacked into the ACK packet. The explicit congestion bit (ECB) of ACK is set to 1 for the non-zero value of $\beta_i^k(t)$ and 0 when $\beta_i^k(t)$ is 0. The previous hop nodes that receive feedback from the upstream node check the ECB value. If ECB is set to 1, then the node reduces its outgoing rate proportional to its status value. Otherwise, the outgoing rate is incremented proportional to $e_i(t)$. The algorithm for RRG is shown in Algorithm 2.

Algorithm 2 Rate allocation

Calculate the new outgoing rate of a node based on ECB (explicit congestion bit), status, error values of the ACK packet.

```
RateRegulation()
 UnPack(ACK);  // Unpack the ACK packet to obtain ECB,
               // status, or error
 if (ECB==1)
    v=v–status*v;
 else
    v=v+error;
 end if
 RouteDataPacket();  // Route the data packet with new rate v
```

Case 2: split protocol (SP)

The earlier method RRG uses ACK to piggyback the feedback messages. To avoid the overhead of piggybacking the feedback messages into the ACK packet, the outgoing rate of the receiver node is increased. Hence, the feedback message is not propagated to the previous hop nodes in case of SP; instead, the receiver forwards the packets to more than one upstream neighbor node (Fig. 3). The receiver node executes the prediction algorithm and finds the status value. When the status value is greater than zero, additional neighbor nodes are selected for packet forwarding towards the gateway node, in order to meet the incoming traffic. Additionally, the outgoing traffic of the receiver node is increased proportional to the status value using Eq. (9). The optimal use of the buffer is achieved through $e_i(t)$, the buffer occupancy error.

$$v_i(t+1) = (1+\beta_i^k)v_i(t) - (1-g_i)e_i(t). \tag{9}$$

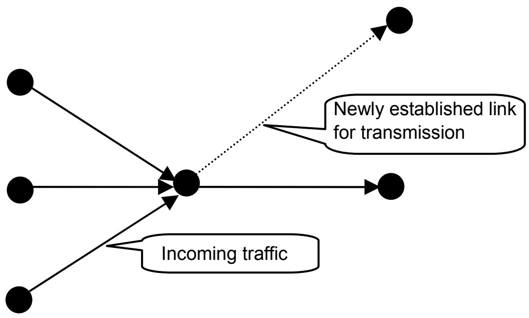

Fig. 3 New data transmit path using the split protocol (SP)

4.2 Congestion control using channel quality

When selecting the outgoing rate using the above algorithms RRG and SP, the fading channels are not considered. However, a fading channel is common in wireless networks. Under a fading channel situation, the transmitted packets from the node are dropped and thus will not reach the receiving node. Therefore, the retransmission of packets is required. To avoid packet drop due to channel fading at a given node, back-off intervals are adjusted suitably at the transmitter node. The back-off interval selection scheme plays a major role in deciding which node gains access to the channel.

We utilize channel quality to assess the onset of congestion. The capacity of the physical communication channel is known a priori for any network. However, the actual capacity available for transmission is influenced by channel fading. Hence, an estimate of the channel capacity is modeled by the Rayleigh distribution. Thus, the rate is selected by modifying the back-off intervals of the nodes around the congested node and the back-off interval of the congested node itself. To achieve successful transmission in a shared channel, a collision-free rate allocation is implemented by satisfying the sufficient condition (Cheng *et al*., 2009) of bandwidth allocation. Therefore, we propose a back-off selection algorithm such that the link capacity is utilized efficiently. A fading channel results in the reduction of channel quality, which in turn reduces the channel capacity. The back-off interval selection scheme specifies the time interval for data transmission. When back-off time increases (or decreases), the transmission rate also increases (or decreases), which avoids the dropping of packets due to fading.

5 Back-off interval selection

Let R_i denote the data generated by node i and R_{ij} the data transmitted from node i to node j. Therefore, the incoming traffic of node i is given by

$$\sum_{j\in N_i} R_{ji} + R_i. \tag{10}$$

Let $c(t)$ denote the link capacity of node i. Node i should satisfy the following conditions for collision-free transmission:

(i) When node i is sending data, it should not receive data from its neighboring nodes.

(ii) When node j is receiving data from node i or sending data to node i, it should not send or receive data from its neighboring node k, $\forall k\in N_j$ and $k\neq i$.

Conditions (i) and (ii) can be represented as follows:

(i) $\sum_{j\in N_i}(R_{ij}+R_{ji})$. Node i should either transmit data to $j\in N_j$ or receive data from one of its neighbor nodes, j.

(ii) $\sum_{j\in N_i}(R_{ij}+R_{ji})+\sum_{j\in N_i}\sum_{k\in N_j}(R_{jk}+R_{kj})$.

Hence, the condition given in Eq. (11) should be satisfied for collision-free transmission as well as congestion-controlled transmission:

$$B_i=\sum_{j\in N_i}(R_{ij}+R_{ji})+\sum_{j\in N_i}\sum_{k\in N_j}(R_{jk}+R_{kj})\leq c(t). \quad (11)$$

The required rate of node i is a fraction of channel bandwidth. The back-off interval of the neighbor nodes of node i, BOFF(t)=1/$u_i(t)$, is adjusted to achieve the required rate. The data rate $u_i(t)$ is calculated as follows:

$$u_i(t)=\left(c(t)\sum_{j\in N_i}R_{ij}+R_i\right)\Big/B_i. \quad (12)$$

When the channel bandwidth drops to zero due to severe fading, the back-off intervals are set to a large value to prevent unnecessary packet transmission.

6 Simulation results

In the simulation the tree based routing protocol is used to transmit the data, which is typical for a sensor network since the nodes at the leaf transmit data to the sink node at the root of the tree through the intermediate nodes. The performances of the proposed schemes RRG and SP are analyzed and compared with DPCC and ADCC. Finally, the back-off selection algorithm is combined with RR and RRG, and the results are analyzed. Every node is initialized with a data rate of 5 kb/s. The buffer maximum and α_{max} of each node are set to 32 and 27 packets, respectively, with the packet size of 512 bits. Parameter A is taken as the power level of the node, set to −5 dBm.

Packets dropped at the intermediate nodes due to congestion will cause low network throughput and decrease energy efficiency due to retransmissions. Consequently, the total number of packets dropped at the intermediate nodes will be considered as a metric for the designed congestion control methods. Fig. 4 shows the network structure used for simulation, which follows a tree topology for packet forwarding.

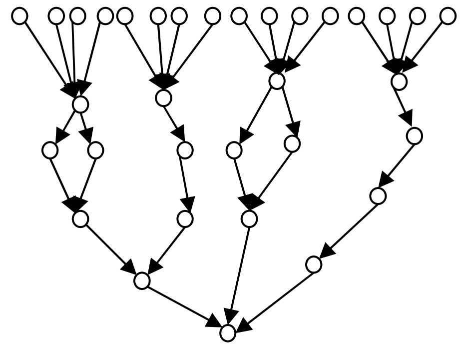

Fig. 4 Node arrangement in the simulation topology

The network topology is scalable, and the proposed schemes can be adapted for large network topology since the intermediate node that receives data packets from three to four neighbor nodes and transmits to a single node is considered for analyzing the per node packet drop. The outgoing rate of the node considered for analysis is set to either one third or one fourth of the incoming rate of that node.

6.1 Rate regulation

Fig. 5a illustrates the queue utilization of the intermediate node that receives packets from three neighbor nodes. The ratio between outgoing and incoming traffic is initially 0.33; i.e., the outgoing traffic of the node is one third of the incoming traffic. Fig. 5a shows that the buffer size is maintained approximately at 16 for DPCC and 2 for ADCC, whereas the buffer size reaches a maximum of 30 packets for RR and is maintained approximately at 24 packets for RRG. The optimal use of the buffer at the receiver node is achieved in RRG among the four methods. The non-zero status value indicates the congestion level in the initial time duration as the incoming traffic is more than three times the outgoing traffic (Fig. 6a). This results in a reduction in the source rate and an increase in the rate ratio (Figs. 5b and 6b). The status value becomes zero when the outgoing to incoming traffic ratio is stabilized at 1, as can be seen by comparing Figs. 5b and 6a. When the buffer reaches the maximum threshold value, which is 27 packets, the status value becomes non-zero, which again causes a reduction in the source rate and an increase in the outgoing to incoming traffic ratio.

The ratio between the outgoing and incoming rates is stabilized at 1.1 for RR and around 1 for RRG (Fig. 5b). The packet drop is completely avoided in RRG, DPCC, and ADCC. Fig. 6b shows the outgoing traffic rates of source nodes 1, 2, and 3 while using RRG, DPCC, and ADCC, respectively. The source node decreases its rate according to the status value and increases it based on the error value. The control parameter g is set to 1 for the non-zero status value and set to 0.7, 0.8, and 0.9 to increase the source rate. ADCC reduces the source rate and stabilizes at 1.6 KB of the source rate, which is the same as RR. The source rate of DPCC ranges between 1.1 and 1.3 KB.

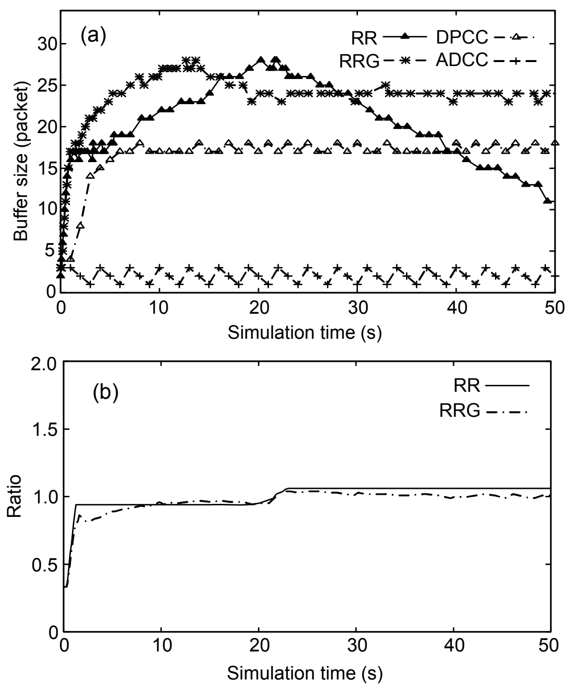

Fig. 5 Performance of rate regulation (RRG) for an intermediate node that receives data from three neighbor nodes and sends out data to a single node
(a) Queue utilization; (b) Ratio between outgoing and incoming traffic rates

6.2 Split protocol

The performance of SP is evaluated using two scenarios. The receiver node transmits the data to an additional upstream node. In addition, the outgoing rate of the receiver node is calculated and adjusted based on the status value. The difference between the previous cases and the SP is that the data rate is increased based on the status value. To use the buffer in an optimum way, the data rate is regulated based on the value of the buffer occupancy error (SP-regulate) as in Eq. (9).

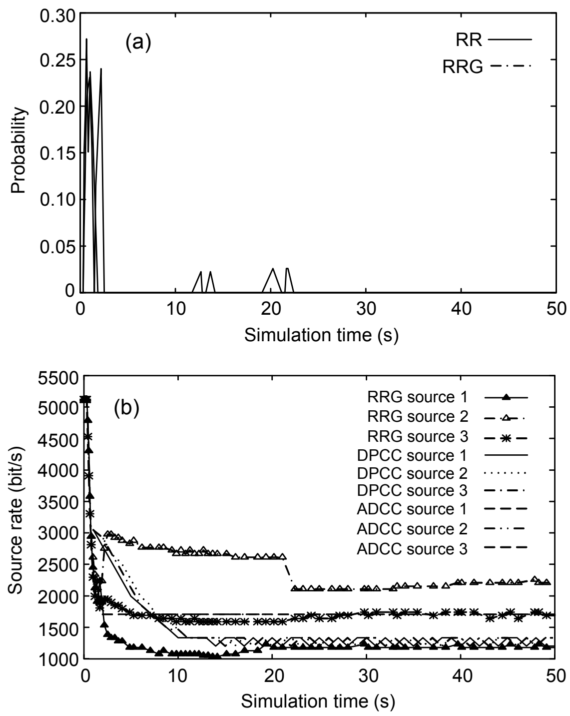

Fig. 6 Performance of rate regulation (RRG) for an intermediate node that receives data from three to four neighbor nodes and sends out data to a single node
(a) Congestion probability; (b) Transmission rate of source nodes

These two scenarios are compared in Fig. 7. The source rate in both SP and SP-regulate remains unchanged. The outgoing rate of the receiver node is adjusted so that the outgoing/incoming ratio is stabilized at 1 and 1.1 (Fig. 7b) while using SP-regulate and SP, respectively. The increase in the outgoing rate corresponds to the increase in the status value as seen in Fig. 7c. The buffer size is maintained at an average of three in case of SP and maintained approximately at around 27 for SP-regulate, which uses the buffer more efficiently than DPCC and SP.

6.3 Back-off interval selection

Simulations are conducted using a 10-kbps channel with Rayleigh fading. The buffer size, packet size, and routing protocol (tree topology) are the same as in the initial setup. The channel capacity is varied based on Rayleigh fading. The source rate and transmitter rate are controlled by RR, RRG, and the back-off interval. Hence, the channel utilization algorithm, Mac back-off selection, is combined with RR (Mac-RR) and RRG (Mac-RRG). Fig. 8 shows the buffer occupancy for Mac-RR and Mac-RRG.

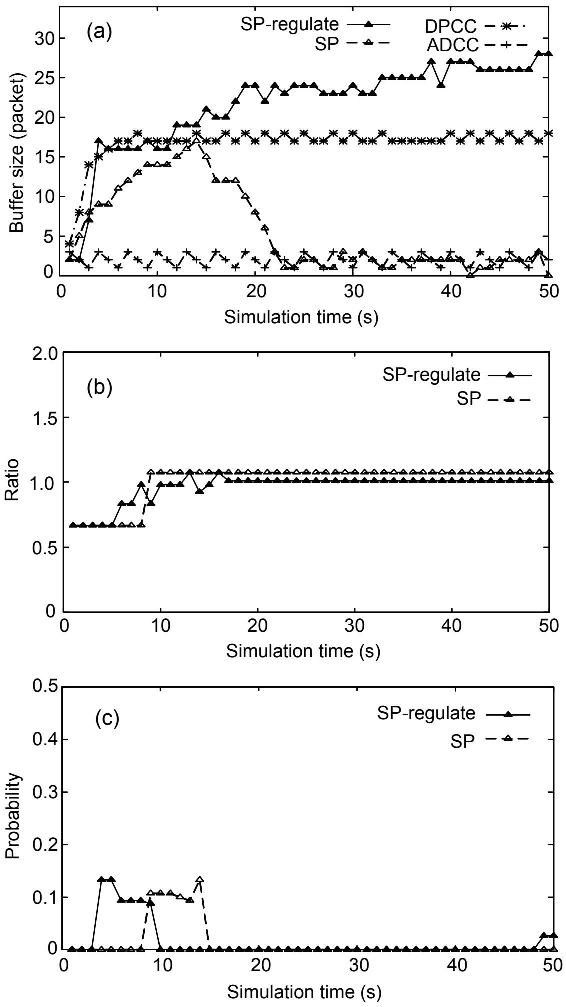

Fig. 7 Performance of the split protocol (SP) for the transmitter node that receives data from three neighbor nodes and sends out data to two upstream nodes
(a) Queue utilization; (b) Ratio between outgoing and incoming rates; (c) Probability of congestion

Buffer utilization is approximately the same for Mac-RR, Mac-RRG, and DPCC. Mac-RRG regulates the outgoing traffic of the source in order to meet the outgoing traffic of the receiver node in the presence of channel fading and the rate ratio varies with respect to time (Fig. 9b). The simulation results are tested in the bad channel condition. This is reflected by the status value as shown in Fig. 9a. This causes the rate ratio to fluctuate, as shown in Fig. 9b.

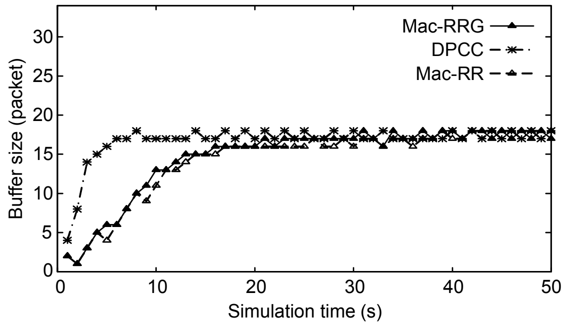

Fig. 8 Queue utilization of back-off interval selection combined with RR and RRG for an intermediate node that receives data from three neighbor nodes and sends out data to a single node

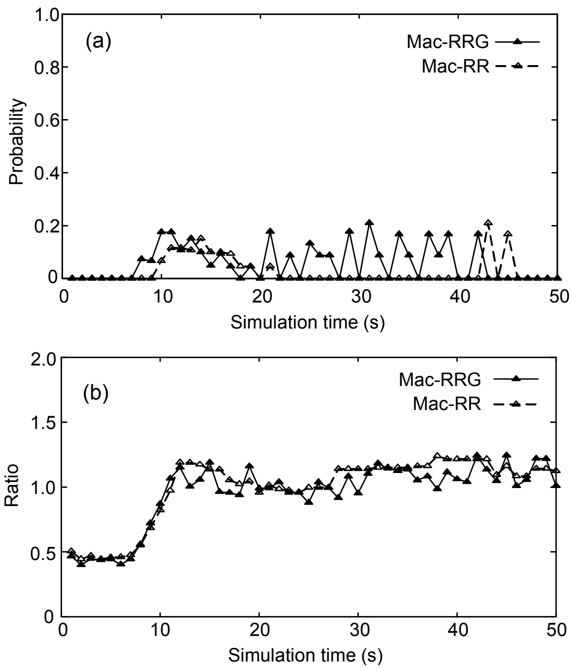

Fig. 9 Performance of back-off interval selection combined with RR and RRG for an intermediate node that receives data from three to four neighbor nodes and sends out data to a single node
(a) Probability of congestion; (b) Ratio between outgoing and incoming traffic

As a whole, the packet drop is completely avoided in all the proposed methods, namely RRG, SP, Mac-RR, and Mac-RRG. There is no packet drop in DPCC. However, use of the buffer is not optimal.

Only 50% of the buffer is used efficiently in DPCC, whereas the buffer capacity is efficiently used by RRG, SP-regulate, Mac-RR, and Mac-RRG. Buffer occupancy is more than 80% in case of RRG and SP-regulate. Mac-RR and Mac-RRG use the maximum channel capacity. Data loss due to the sudden increase in the data rate can be avoided by the varying nature of the threshold value. The fixed threshold in DPCC results in packet drop when there is bursting data traffic.

The source rates of RRG and SP are compared with those of the existing systems DPCC and ADCC in Table 2. Though RRG increases the data rate when there is no congestion, the source rates are reduced (Fig. 6b). As the congestion control method RRG reduces the source rate, it may not be useful for mission critical applications where the data must be generated within the given time interval and are considered vital. This method can be used by non-mission-critical applications. Thirty-three percent of the initial source rate is preserved in RRG, equal to the incoming traffic, whereas DPCC preserves only 25% of the initial source rate. ADCC also preserves 33% of the source rate, but it does not consider channel capacity, which leads to packet drop.

Table 2 Source rate comparison between congestion control methodologies

Congestion control method	Final rate		
	Source 1	Source 2	Source 3
RRG	1179	2206	1689
SP	5120	5120	5120
DPCC	1201	1333	1333
ADDC	1706	1706	1706

The initial rate is 5120 for all the three sources and four methods

On the other hand, SP conserves the source rate by increasing the receiver node transmission rates when there is congestion. Hence, 100% of the data rate is maintained. Thus, this method is suitable for mission critical applications such as mining and battle field monitoring. Back-off interval selection can be combined with both RRG and SP to use the channel capacity efficiently.

To analyze the accuracy of the congestion prediction method, the simulations are performed with 10 source nodes and one receiver node. Simulations are run 1500 times to collect sufficient statistics for calculating the accuracy of the congestion prediction model. The number of active neighbor nodes sending packets to the receiver node is varied randomly between 1 and 10. The prediction model controls the source rate in accordance to the change in incoming packets.

In RRG, the source rates are increased to use the buffer occupancy. When the buffer occupancy of the receiver node is maintained at the maximum threshold value and a sudden increase of incoming packets from more neighbor nodes, congestion occurs in the receiver node and the accuracy of the prediction model becomes 98.6%. SP works with 100% efficiency as it increases the outgoing rate of the receiver node. The outgoing rate of the receiver node can be increased in SP, till it reaches the maximum channel capacity.

7 Conclusions

This paper presents a congestion prediction method and congestion control schemes where congestion is mitigated by controlling the outgoing traffic of the source nodes and selecting the back-off interval of all nodes based on the channel condition. The incoming rate of the receiver node is mitigated by considering buffer occupancy using RRG, whereas SP regulates the node transmission rate. Additionally, the back-off interval selection scheme mitigates the outgoing flow of each node. Simulation results show that the proposed schemes increase the per-node throughput and reduce energy in the network by avoiding packet drops (Energy efficiency is not shown explicitly in this paper. Since there is no re-transmission of packets, energy consumption of every node is reduced). The source data rate is preserved in case of RRG and SP. The performance in terms of node throughput increases when the back-off interval selection algorithm is combined with RR and RRG because the incoming and outgoing traffic is balanced. As the buffer occupancy is minimal in case of RR and SP, burst of data traffic can be handled well.

Acknowledgements

We thank the faculty of Department of Computer Science and Engineering, SRM University, for providing constructive comments which greatly improved the quality of the paper.

References

Bhargava, V., Jose, J., Srinivasan, K., *et al*., 2012. Q-CMRA: queue-based channel-measurement and rate-allocation. *IEEE Trans. Wirel. Commun.*, **11**(11):4214-4223. [doi:10.1109/TWC.2012.091812.120813]

Boutsis, I., Kalogeraki, V., 2012. RADAR: adaptive rate allocation in distributed stream processing systems under bursty workloads. Proc. 31st Symp. on Reliable Distributed Systems, p.285-290. [doi:10.1109/SRDS.2012.55]

Cheng, M., Gong, X., Cai, L., 2009. Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks. *IEEE Trans. Wirel. Commun.*, **8**(7):3770-3779. [doi:10.1109/TWC.2009.081134]

Cheng, T.E., Bajcsy, R., 2004. Congestion control and fairness for many-to-one routing in sensor networks. Proc. 2nd Int. Conf. on Embedded Networked Sensor Systems, p.148-161. [doi:10.1145/1031495.1031513]

Felemban, E., Lee, C., Ekici, E., 2006. MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Trans. Mob. Comput.*, **5**(6):738-754. [doi:10.1109/TMC.2006.79]

He, T., Stankovic, J.A., Lu, C., *et al*., 2003. SPEED: a stateless protocol for real-time communication in sensor networks. Proc. 23rd Int. Conf. on Distributed Computing Systems, p.46-55. [doi:10.1109/ICDCS.2003.1203451]

Hull, B., Jamieson, K., Balakrishnan, H., 2004. Mitigating congestion in wireless sensor networks. Proc. 2nd Int. Conf. on Embedded Networked Sensor Systems, p.134-147. [doi:10.1145/1031495.1031512]

Hussain, F.B., Cebi, Y., Shah, G.A., 2008. A multievent congestion control protocol for wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.*, **2008**:803271. [doi:10.1155/2008/803271]

Karenos, K., Kalogeraki, V., Krishnamurthy, S.V., 2008. Cluster-based congestion control for sensor networks. *ACM Trans. Sens. Netw.*, **4**(1):5:1-5:39. [doi:10.1145/1325651.1325656]

Kumar, R., Crepaldi, R., Rowaihy, H., *et al*., 2008. Mitigating performance degradation in congested sensor networks. *IEEE Trans. Mob. Comput.*, **7**(6):682-697. [doi:10.1109/TMC.2008.20]

Lee, D., Chung, K., 2010. Adaptive duty-cycle based congestion control for home automation networks. *IEEE Trans. Consum. Electron.*, **56**(1):42-47. [doi:10.1109/TCE.2010.5439124]

Lu, C., Blum, B.M., Abdelzaher, T.F., *et al*., 2002. RAP: a real-time communication architecture for large-scale wireless sensor networks. Proc. 8th IEEE Real-Time and Embedded Technology and Applications Symp., p.55-66. [doi:10.1109/RTTAS.2002.1137381]

Mao, Z., Koksal, C.E., Shroff, N.B., 2012. Near optimal power and rate control of multi-hop sensor networks with energy replenishment: basic limitations with finite energy and data storage. *IEEE Trans. Automat. Contr.*, **57**(4):815-829. [doi:10.1109/TAC.2011.2166310]

Morell, A., Vicario, J.L., Vilajosana, X., *et al*., 2011. Optimal rate allocation in cluster-tree WSNs. *Sensors*, **11**(4):3611-3639. [doi:10.3390/s110403611]

Rangwala, S., Gummadi, R., Govindan, R., *et al*., 2006. Interference-aware fair rate control in wireless sensor networks. Proc. Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications, p.63-74. [doi:10.1145/1159913.1159922]

Ren, F., He, T., Das, S., *et al*., 2011. Traffic-aware dynamic routing to alleviate congestion in wireless sensor networks. *IEEE Trans. Parall. Distr. Syst.*, **22**(9):1585-1599. [doi:10.1109/TPDS.2011.24]

Teo, J.Y., Ha, Y., Tham, C.K., 2008. Interference-minimized multipath routing with congestion control in wireless sensor network for high-rate streaming. *IEEE Trans. Mob. Comput.*, **7**(9):1124-1137. [doi:10.1109/TMC.2008.24]

Uthra, R.A., Raja, S.V.K., 2011. PACC: probabilistic approach for congestion control in wireless sensor network. *CiiT Int. J. Wirel. Commun.*, **3**:985-990.

Uthra, R.A., Raja, S.V.K., 2012. QoS routing in wireless sensor networks—a survey. *ACM Comput. Surv.*, **45**(1):9.1-9.12. [doi:10.1145/2379776.2379785]

Wan, C.Y., Eisenman, S.B., Campbell, A.T., 2003. CODA: congestion detection and avoidance in sensor networks. Proc. 1st Int. Conf. on Embedded Networked Sensor Systems, p.266-279. [doi:10.1145/958522.958523]

Wang, C., Sohraby, K., Lawrence, V., *et al*., 2006. Priority-based congestion control in wireless sensor networks. Proc. IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing, p.22-31. [doi:10.1109/SUTC.2006.1636155]

Wu, Y., Yuan, Z., Wu, Y., 2013. A predictive control strategy for networked control system with destabilizing transmission factors. *Adv. Sci. Eng. Med.*, **5**(1):83-90. [doi:10.1166/asem.2013.1226]

Zawodniok, M., Jagannathan, S., 2007. Predictive congestion control protocol for wireless sensor networks. *IEEE Trans. Wirel. Commun.*, **6**(11):3955-3963. [doi:10.1109/TWC.2007.051035]

Appendix: Proof of Eq. (3)

Let $P(\alpha(t)+1)$ be the probability of a node having one packet greater than the threshold value at time t. $P(\alpha(t)+1)=p(\alpha(t)+1)$, where $p(\alpha(t)+1)$ is the probability of one packet arrival, calculated using Eq. (3). Similarly,

$$P(\alpha(t)+2)=p(\alpha(t)+2)+p(\alpha(t)+1|\alpha(t)+1).$$

The probability that the node contains more than two packets above the threshold value depends on two new arrivals of packets or one new arrival provided that there exists one packet more than the threshold value. When generating such functions, we have (for simplicity, $\alpha(t)$ is replaced as α)

$$
\begin{aligned}
&P(\alpha+1)=p(\alpha+1),\\
&P(\alpha+2)=p(\alpha+2)+p(\alpha+1|\alpha+1),\\
&P(\alpha+3)=p(\alpha+3)+p(\alpha+1|\alpha+2)+p(\alpha+2|\alpha+1),\\
&\quad\cdots\\
&P(\alpha+k)=p(\alpha+k)+p(\alpha+1|\alpha+(k-1))+p(\alpha+2|\alpha+(k-2))\\
&\qquad+\ldots+p(\alpha+(k-1)|\alpha+1).
\end{aligned}
$$

In general,

$$P(\alpha+k)=p(\alpha+k)+\sum_{n=1}^{k-1}p\left(\alpha+n\,|\,\alpha+(k-n)\right),$$

where k=2, 3, …, BUFMAX−α with k=1 as the initial condition.