Performance Evaluation 66 (2009) 685–700

Contents lists available at ScienceDirect

Performance Evaluation

journal homepage: www.elsevier.com/locate/peva

RETRACTION

Worst case dimensioning and modeling of reliable real-time multihop wireless sensor network

Kambiz Mizanian [*], Hamed Yousefi, Amir Hossein Jahangir

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

ARTICLE INFO

Article history:
Received 1 December 2008
Received in revised form 5 July 2009
Accepted 6 August 2009
Available online 12 August 2009

Keywords:
Reliable real-time
Wireless sensor networks
Queuing theory
Analytical model
Bounded delay and queue

ABSTRACT

Wireless Sensor Network (WSN) should be capable of fulfilling its mission, in a timely manner and without loss of important information. In this paper, we propose a new analytical model for calculating RRT (Reliable Real-Time) degree in multihop WSNs, where RRT degree describes the percentage of real-time data that the network can reliably deliver on time from any source to its destination. Also, packet loss probability is modeled as a function of the probability of link failure when the buffer is full and the probability of node failure when node's energy is depleted. Most of the network properties are considered as random variables and a queuing theory based model is derived. In this model, the effect of network load on the delay, RRT degree, and node's energy depletion rate are considered. Also network calculus is tailored and extended so that a worst case analysis of the delay and queue quantities in sensor networks is possible. Simulation results are used to validate the proposed model. The simulation results agree very well with the model.

© 2009 Elsevier B.V. All rights reserved.

1. Introduction

Wireless Sensor Networks (WSNs) are self-organized ad hoc networks, which are equipped with limited computing and radio communication capabilities [1]. Nodes are capable of sensing, gathering, processing and communicating data, especially the data pertaining to the physical medium in which they are embedded. It is envisioned that a typical WSN consists of a large number of nodes [1]. A typical network configuration consists of sensors working unattended and transmitting their observed or sensed data to some processing or control center, the so-called sink or base station node, which serves as a user interface. Due to the limited transmission range, sensors that are far away from the sink deliver their data through *multihop* communications, i.e. using intermediate nodes as relays. In this case, a sensor may be both a data source and a data router.

Although energy efficiency is usually the primary concern in WSNs, the requirement of low latency communication is getting more and more important in emerging applications. Out-of-date information will be irrelevant and even leads to negative effects on system monitoring and control. Real-time (RT) sensor systems have many applications especially in intruder tracking, medical care monitoring and structural health diagnosis.

WSN differs dramatically from the traditional RT systems due to its wireless nature, limited resources (power, processing and memory), low node reliability, dynamic network topology. Thus, developing real-time applications over WSN should consider not only resource constraints, but also the node and communication reliability and the globally time varying network performance.

This paper establishes a probabilistic fundamental quantitative notion for performance-critical applications on real-time information transfer in multihop wireless networks. However, bounded delay latency is extremely dependent on path

[*] Corresponding author. Tel.: +98 21 66164619; fax: +98 21 66019246.
E-mail addresses: mizanian@ce.sharif.edu, mizanian@mehr.sharif.edu (K. Mizanian).

0166-5316/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.peva.2009.08.003

reliability when any lost packet must be retransmitted and it can cause additional delivery delay. Here, the packet loss probability is the probability of one path's link failure when node's buffer in the end point of the link is full and there is no space for new packets or the probability of one path's node failure when node's energy is depleted and the node does not have any energy for taking more transmissions.

Application areas for sensor networks might be production surveillance, traffic management, medical care or military applications. In these areas it is crucial to ensure that the sensor network is functioning even in a worst case scenario. It must be clear that the sensor network can support all possible communication patterns that might occur in the network without being overloaded. If a sensor network is used for example for production surveillance it must be ensured that messages indicating a dangerous condition are not dropped. If functionality in worst case scenario cannot be proven, people might be in danger and the production system might not be certified by authorities.

As it may be difficult or even impossible to produce the worst case in a real world [illegible] or in a simulation in a controlled fashion an analytical framework is desirable that allows a worst case analysis in sensor networks. Network calculus [4] is a relatively new tool that allows worst case analysis of packet-switched communication networks. Network calculus has successfully been applied to model wired IP-based networks built on QoS technologies like Integrated Services or Differentiated Services [5,6].

In this paper it is shown how network calculus can be tailored and extended so that a worst case analysis of the delay and queue quantities in sensor networks is possible. Also, we propose a new probabilistic analytical model for calculating RRT (Reliable Real-Time) degree in multihop WSNs, where RRT degree describes the percentage of real-time data that the network can reliably deliver on time from any source to its destination. Analytical expressions for reliable real-time degree facilitate the process of designing a WSN that is guaranteed to meet specified throughput and delay requirements. These expressions describe values of a set of variables that will enable the network to meet anticipated soft real-time requirements. In other words, they define the feasibility region in the space of such variables. In the event of dynamically changing network, which is expected in WSN, besides planning and designing, the feasibility region allows optimization of the operation of the network.

Thus, the purpose of this paper is to perform a probabilistic analysis of Reliable Real-time Degree in wireless sensor network, which considers the packet loss and packet delay as real-time measures, and node failure and link failure as reliability metrics. The effect of network load is also examined. Also network calculus is tailored and extended so that a worst case analysis of the delay and queue quantities in sensor networks is possible.

The rest of this paper is organized as follows: in Section 2 a literature survey is presented. In Section 3 the preliminaries and assumption of the problem are clarified. In Section 4 a model for evaluating the reliable real-time degree is derived. In Section 5 network calculus is tailored and extended so that a worst case and bound analysis of the delay and queue quantities in sensor networks is possible. Section 6 presents the simulation results and Section 7 provides some conclusions and future work.

2. Related work

A large amount of research on sensor networks has been recently reported, ranging from studies on network capacity and signal processing techniques, to algorithms for traffic routing, topology management and channel access control.

With regard to analytical studies, results on the capacity of large stationary ad hoc networks are presented in [7] (note that sensor networks can be viewed as large ad hoc networks, but WSNs almost are stationary and all nodes send messages to few sinks). In [7] two network scenarios are studied: one including arbitrarily located nodes and traffic patterns, the other one with randomly located nodes and traffic patterns. The case of tree-like sensor networks is studied in [8], where the authors present optimal strategies for data distribution and data collection, and analytically evaluate the time performance of their solution. An analytical approach to coverage and connectivity of sensor grids is introduced in [9]. The sensors are unreliable and fail with a certain probability leading to random grid networks. Results on coverage and connectivity are derived as functions of key parameters such as the number of nodes and their transmission radius. Some researchers have looked at latency issues from different perspectives. For instance, the approach of Intanagonwiwat et al. [10] exploits latency and credibility trade-off in order to provide a solution to the problem of "How long a node should wait before aggregating and sending its data to its parent", where a parent denotes the next hop. Another in-network data aggregation scheme that aims at minimizing the end-to-end delay is proposed in [11]. This scheme does not consider any latency bound but tries to minimize the average end-to-end delay by concatenating multiple packets into one at MAC layer. The idea is to limit the medium access contention so that the packet queuing delay be reduced. Moreover, they use a feedback mechanism at each sensor node to adjust the number of concatenated packets based on the current traffic conditions. In [12] Abdelzaher et al. a sufficient condition for schedulability under fixed-priority scheduling which allows capacity planning to be employed prior to deployment such that real-time requirements are met at run-time. The bound is derived for load balanced networks, as well as networks where all traffic congregates at a number of sinks. The approach of Chiasserini et al. [13] exploits several performance metrics, among which the distributions of the data delivery delay. They consider that the information sensed by a network node is organized into data units of fixed size, and can be stored at the sensor in a buffer of infinite capacity. They assume that wireless channel is error-free. In [14] Chiasserini et al. presented a methodology to analyze the behavior of large-scale sensor networks. Their approach was based on a fluid representation of all quantities that depend on the specific location within the network topology, and on probabilistic functions to characterize the behavior of individual nodes. They

RETRACTION

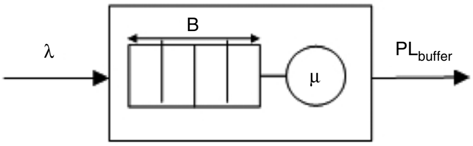


Fig. 1. Structure of sensor network nodes.

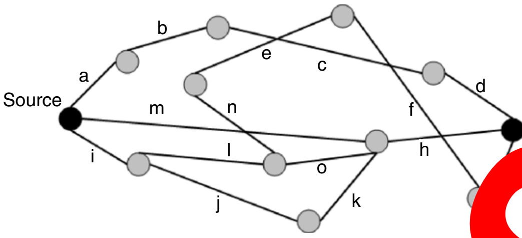


Fig. 2. A sample network consisting of $m/m/1/k$ nodes.

RETRACTION

did not consider the battery discharge of the sensors and the behavior of the nodes dependent on their residual energy. In [15] we proposed a quantitative real-time model for WSNs, and described real-time degree by considering the packet loss and packet delay as real-time measures. However, this model does not consider the probability of node failure due to node energy depletion and its effect on path reliability and real-time degree of WSNs.

3. Preliminaries

For evaluating the reliable real-time degree of wireless sensor networks, we suppose that each node of sensor network has the structure depicted in Fig. 1, i.e. each sensor can receive and transmit, also generates data units according to a Poisson process [13]; so we can model it as an $M/M/1/k$ queue.

Moreover, suppose that the network is a set of such nodes, and its topology is unknown. A sample network is shown in Fig. 2.

For example, there are several potential paths between the source and the destination nodes. Suppose that the path $\{a, b, c, d\}$ is established. If for some reason, this path is disconnected, another path can be used as a replacement. For instance, if link c fails, the paths $\{m, h\}$ or $\{i, l, o, h\}$ can be used.

Consider a transmission over one hop and let i and j ($1 \le i \le N$, and $0 \le j \le N$ with 0 indicating the sink) be the transmitter and the receiver, respectively. The transmission is successful if [7]:

(1) The distance between i and j is not greater than tr (Transmission Range),

$$d_{i,j} \le tr. \tag{1}$$

(2) For every other node, k, simultaneously receiving,

$$d_{i,k} > tr. \tag{2}$$

(3) For every other node, l, simultaneously transmitting,

$$d_{l,j} > tr. \tag{3}$$

In this work we consider a sensor network whose nodes have already performed the initialization procedures necessary to self-configure the system. Therefore, sensors have the knowledge of their neighboring nodes, as well as of the possible routes to the sink. (For instance, through a routing algorithm such as the one proposed in [16]). Since we consider a network of stationary nodes performing, for instance, environmental monitoring and surveillance, the routes and their conditions can be assumed to be either static or slowly changing.

To avoid unsuccessful transmissions, we assume that sensors employ a CSMA/CA mechanism with handshaking, as in the MACA and MACAW schemes [[illegible],18,13] (although, other MAC protocols could be considered as well), and that the radio range of handshaking messages transmission is equal to tr. If i wants to transmit to j and senses the channel as idle, i sends a transmission request to j and waits till either it receives a message indicating that j is ready to receive (i.e., it is active and there are not other simultaneous transmissions that could interfere), or a timeout expires. In the former case, i sends the data to j; in the latter case, i will poll the following next hop. While i is looking for a next hop that is ready to receive, data are buffered at the node waiting for transmission.

An important consideration is that generally in wireless sensor networks, the network topology is unknown. That is, we have to consider anything as statistical. For performing mathematical operations, most of network parameters must be treated as random variables. The following assumptions about nodes and the network itself are made:

1. Network nodes have the same statistical properties.
2. The routing algorithm selects each of alternative paths with equal probability.
3. Initially, there are R paths.
4. The network links and nodes fail independently from each other.
5. If at least one of the path's nodes fails, we consider that path as failed (disconnected).
6. The network paths have the same statistical properties.
7. The number of nodes of a path is a random variable called N with average of $E[N]$.
8. Packet lengths, L, are according to an exponential distribution.
9. The buffer size of each node is b byte or B packets.
10. Packet arrival to each node has the Poisson distribution with parameter λ (it includes the packets generated by the node plus packets arrived at the node from other nodes in the network).
11. The service rate of packet is μ.
12. The network load is r.
13. Transmit rate is t_r.

RETRACTION

4. Evaluating the reliable real-time degree

With the above assumptions, we begin the modeling process.

In this paper we define reliable real-time degree by considering node failure and link failure as reliability measures, and we model energy depletion of a node as the node failure too.

Step 1: We calculate the packet loss of a typical path. The packet loss probability of a path, PL_{path}, is modeled as a function of the probability of link failure when the buffer is full and the probability of node failure when node's energy is depleted.

$$PL_{path} = 1 - \left(\left(1 - PL_{buffer}\right)^{E[N]} \times R_{path}\right) \tag{4}$$

where R_{path} is the probability that none of the path's nodes fail during the deadline and it is calculated by Eq. (24).

Now, we have to calculate the mean value of packet loss in each node. The packet loss probability (link failure probability) is the probability that the node's buffer is full and there is no space for new packets. From queuing theory it is equal to PL_{buffer} [19]:

$$PL_{buffer} = P_{B+1} = \frac{(r)^{B+1}(1-r)}{1-(r)^{B+2}} \tag{5}$$

where r is the average network load at a sensor node and we can find it by Eq. (8). Also B is calculated by:

$$B = \frac{b\mu}{t_r}. \tag{6}$$

Now, assuming that S, the sensing rate, is the new traffic rate emerged in the source node of each source–destination pair, and assuming a retransmission in the event of packet loss. Thus, under the premise that G is the total traffic rate (i.e. the sum of new emerged traffic and the retransmitted traffic), we have the following relation between G and S:

$$S = G\left(1 - PL_{path}\right). \tag{7}$$

Now we have to calculate the value of r. To compute the network load at a sensor node, we note that, because of packet loss probability at the sensor node, the load will be reduced at each successive node from source to a destination. For example, in the ith node, $i = 0, 1, 2, \ldots, E[N] - 1$, this traffic exists in the case of traversing all previous $i - 1$ nodes without packet loss. Therefore the probability of traffic existence is equal to $\left(1 - PL_{buffer}\right)^i$ and because of similarities between nodes and paths statistical properties, we have:

$$r = \left(\frac{G}{E[N]}\right)\sum_{i=0}^{E[N]-1}\left(1 - PL_{buffer}\right)^i = \frac{G[1-\left(1-PL_{buffer}\right)^{E[N]}]}{PL_{buffer} * E[N]}. \tag{8}$$

Comparing these two relationships, (5) and (8), we find out that for calculating the value of PL_{buffer}, we need to know the value of r, and vice versa. Similar problems often occur in the computation of blocking probabilities in circuit-switched networks with fixed routing, in which the well known Erlang fixed-point method can be applied [20,21]. For this type of problem, an iterative method is known to have efficient computation time. The iteration is carried out until convergence is achieved.

Step 2: We calculate the mean value of a typical path's delay, or actually the time duration that it takes for a packet to successfully be delivered to the base station.

A packet traversing from source to destination waits a time equal to W in each node where W includes queuing time plus transmission delay, then enters a link and has a propagation delay equal to t_p. Therefore, as there are N nodes and $N - 1$

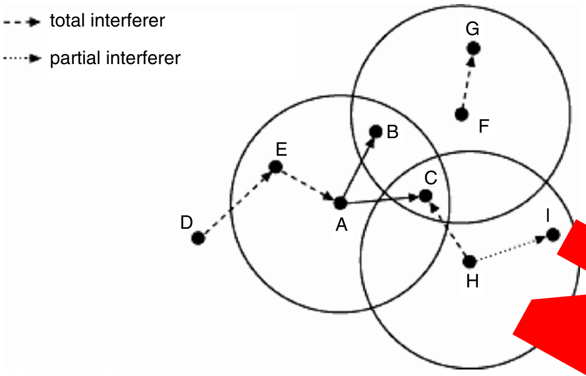


Fig. 3. Example of channel contention and hindered transmissions.

links, the path's delay is:

$$Delay_{path} = \sum_{i=1}^{E[N]} W + (E[N]-1)\,E\left[t_p\right]$$
$$= \sum_{i=1}^{E[N]} W + \frac{E\left[Len_{path}\right]}{C}. \tag{9}$$

And, as we proved in our paper [15] W is:

$$W = \frac{r'\left[1+(B+1)\,r'^{B+2}-(B+2)\,r'^{B+1}\right]}{\lambda\,(1-r')\left(1-r'^{B+1}\right)} \tag{10}$$

where r' as an effective traffic rate, is:

$$r' = \frac{r}{\beta} \tag{11}$$

$$W = \frac{L}{\tilde{\lambda}} \tag{12}$$

$$\tilde{\lambda} = \lambda\,(1-\pi_{B+1}) = \lambda\left(1-\frac{(r')^{B+1}\,(1-r')}{1-(r')^{B+2}}\right). \tag{13}$$

And the above formulas result in:

$$W = \frac{r'\left[1+(B+1)\,r'^{B+2}-(B+2)\,r'^{B+1}\right]}{\lambda\,(1-r')\left(1-r'^{B+1}\right)} \tag{14}$$

Len_{path} is a random variable and represents the cumulative distribution of links' length. C is the radio speed or more precisely, the propagation speed of radio waves in the space. β is the probability to transmit a data unit in a time slot given that the buffer is not empty.

Step 3: We calculate the probability that a data unit is transmitted in a time slot. It accounts for the channel contention, i.e., it would be equal to 1 if there were no contention on the wireless medium.

As described in Section [illegible], a [illegible] transmission attempt is successful if the conditions expressed in (1)–(3) are satisfied. Thus the computation of β requires a careful investigation of the interference produced by other sensors trying to transmit in proximity of the node for which we want to estimate β. In order to explain our approach, consider the set of nodes shown in Fig. 3.

The transmission range of three nodes, $\{A, F, H\}$, is represented by a circle. Assume that we want to estimate the parameter β of node A, which has two next hops, B and C. We need to find all transmissions that could potentially interfere with the transmission of A to its next hops. Let (X, Y) denote the transmission from the generic node X to the generic node Y. We notice that transmissions like (D, E) and (H, C) violate condition (2) since the receivers are within the radio range of A; a special case is given by the transmissions whose receiver is A itself (e.g., (E, A)). Instead, transmissions like (F, G) and (H, I) meet condition (2) and violate condition (3) since the transmitters interfere with A's next hops. In addition, we observe that transmissions as (D, E), (E, A), (H, C) and (F, G) totally inhibit A's transmission, thus we call them *total interferers* [13]. Instead, transmissions like (H, I) do not necessarily prevent A from sending data (e.g., (A, B) could take place), thus we call them *partial interferers* [13]. To estimate β for the generic sensor i we proceed as follows. First we compute for each node n ($1 \leq n \leq N$) the probability $I^i(n)$ that a transmission in which n is involved as either transmitter or receiver, totally inhibits i's transmission (*total interferer*). Our approach is based on the knowledge of the average transmission rates $r_{n,m}$ between n and its generic receiver m. So based on [13]:

$$I^i(n) = \sum_{m=1}^{N} r_{m,n} 1_{\{d_{(n,i)} \leq tr\}} + \sum_{m=0}^{N} r_{n,m} 1_{\{d_{(m,i)} > tr\}} V^i(n) \tag{15}$$

where $m = 0$ denotes the sink and $1_{\{\cdot\}}$ is the indicator function. The first summation on [illegible]ight hand side accounts for the transmissions violating (2) or destined to i, while the second summation accounts for th[illegible]missions that meet (2) but violate (3). The term $V^i(n)$ is equal to 1 if there exists at least one next hop of i within the [illegible]sion range of n, with n being different from i:

$$V^i(n) = \begin{cases} 1 & \exists k \in H^i : d_{(n,k)} \leq tr, \quad n \neq i \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

where H^i is the set of next hops of i. Then, β^i is estimated as follows [13]:

$$\beta^i = \prod_{n=1}^{N} \left[1 - I^i(n)\right]. \tag{17}$$

$$\beta = \frac{\sum_{i=1}^{E[N]} \beta^i}{E\left[N\right]}. \tag{18}$$

Now, for evaluating the reliable real-time degree of a path, we employ the following reasoning:

If the path does not fail, as long as the values of packet l[illegible]nd packets' delay do not exceed a specific threshold, the reliable real-time degree is equal to one. When these value[illegible]xceed t[illegible] thresholds, the value of reliable real-time degree has inverse relation with the packet loss and delay to their [illegible]shold. [illegible]w, if this path fails, with some probability, a spare path is chosen, and then the reliable real-time degree of t[illegible]h determines the reliable real-time degree of the previous one.

However, packet loss and delay have different uni[illegible]surement and we cannot apply mathematical operation on both of them simultaneously. Therefore we embed [illegible]acket loss into the notion of delay: when a packet loss occurs and the source receives a NACK, or does not rec[illegible]CK and a timeout occurs, a random time interval between 1 and K elapses and then the packet is retransmitted. We [illegible]der the time of transmitting of a packet of average length as the unit of this interval. So a value equal to $T\left(2\text{[illegible]} - 1)\text{[illegible]}_p\right] + \frac{K+1}{2}\right)$ is added to path delay, where $T = \frac{(G-S)}{S}$ indicates the ratio of retransmitted packets to the new [illegible]ets. Considering packet loss and retransmission, the total delay of the path is:

$$Delay_{path} = \sum_{i=1}^{E[N]} W + \frac{E\left[Len_{path}\right]}{C} \text{[illegible]} \left(\frac{2E\left[\text{[illegible]}\right]}{C} + \frac{K+1}{2}\right) \tag{19}$$

$$Delay_{path} = \sum_{i=1}^{E[N]} W + \frac{(2T+1\text{[illegible]}\left[Len_{pa\text{[illegible]}}\right.}{C} \text{[illegible]} \frac{(K+1)\,T}{2}. \tag{20}$$

However, finding *RRT degree* [illegible] th[illegible]ltin[illegible]e goal of this section and it describes the percentage of real-time data that the network can reliably deliv[illegible]e f[illegible] any source to its destination. Having the above relations in the mind and the similarity of the statistical propert[illegible] paths help us to obtain *RRT degree* as the following equation:

$$RRT\_degree = (1 - \text{[illegible]})^{E[N]} \times (1 - MissRatio) \times (1 - P_{failure}). \tag{21}$$

As we assume that o[illegible]ac[illegible]l to each node has the Poisson distribution with parameter λ, so we can assume that time interval between pa[illegible]s the exponential distribution, so *MissRatio* is calculated as:

$$MissRatio = e^{-\frac{1}{Delay_{Path}} \times T_{Delay}} \tag{22}$$

where T_{Delay} is the threshold values for packets' delay. So, if $Delay_{path}$ exceeds the thresholds, miss ratio begins to increase and reliable real-time degree begins to decrease with inverse relation.

Considering the fact that initially there are R non-failed paths. If a path fails, it can be substituted by another path and this continues until there are no paths for data transmission. $P_{failure}$ is equal to the probability that R paths fail and there are no spare paths for data transmission that you can find it on Eq. (23):

$$R_{Total} = 1 - P_{failure} = 1 - (1 - R_{path})^R. \tag{23}$$

RETRACTION

RETRACTION

Step 4: We calculate the reliability of a typical path. The path reliability, R_{path}, is equal to the probability that none of the path's nodes fails during the deadline (T_{Delay}). Therefore:

$$R_{path} = e^{-\left(\frac{1}{Path\ Lifetime}\right) \times T_{Delay}} \tag{24}$$

where failure rate, $\frac{1}{Path\ Lifetime}$, is the expected number of failures during the path lifetime.

Now, we have to calculate the mean value of lifetime for a typical path. The energy cost of a node is computed as follows.

$$E_{i,j} = E_{i,j}^{(tx)} + E_j^{(rx)} \tag{25}$$

where $E_{i,j}$ is the energy cost for transferring a data unit from node i to its next hop in path, namely j. It is equal to the sum of the transmission energy spent by $i(E_{i,j}^{(tx)})$ and the reception energy consumed by $j(E_j^{(rx)})$. In the transmitting mode, energy is spent in the front-end amplifier, which supplies the power for the actual RF transmission, in the transceiver electronics and in the node processor implementing signal generation and processing functions. In the receiving mode, energy is consumed entirely by the transceiver electronics and by processing functions, such as demodulation and decoding. Therefore, $E_j^{(rx)}$ is due to the transceiver electronics ($E^{(ele)}$) and to processing functions ($E^{(proc)}$), while $E_{i,j}^{(tx)}$ has to account for $E^{(ele)}$, $E^{(proc)}$ as well as for the energy consumption due to the amplifier, that is assumed to be proportional to the squared distance between transmitter and receiver [22].

$$E_{i,j} = \left[2\left(E^{(ele)} + E^{(proc)}\right) + d_{i,j}^2 E^{(amp)}\right] \tag{26}$$

where $E^{(amp)}$ is a constant value and $d_{i,j}$ is the distance between i and j in the disk of unit radius.

So, the energy consumption ratio for a typical path is computed as follows.

$$e(path) = \sum_{i=0}^{E[N]} (\lambda E_{i,i+1}). \tag{27}$$

So, the mean value of node's energy consumption ratio is

$$e(node) = \frac{e(path)}{E\,[N]}. \tag{28}$$

The network lifetime is defined as the smallest time that it takes for at least one node in the network to drain its energy beyond the point where it can function normally.

$$Path\ Lifetime = \frac{\min\{B_i, i \in (0, E[N]-1)\}}{e(node)} \tag{29}$$

where B_i is the residual energy of node i on the path at the moment of new packet transmission.

5. Evaluation of delay and queue bounds

Different applications running on top of a sensor network might have different requirements regarding the information extracted from the field. One important requirement is a bound on the maximum *information transfer delay* for data delivery. If information is delayed too long on the transport path, the application cannot use the information as it is considered outdated. At each hop of the transport path, a message can be delayed. If a sensor node that generates a message is some hops away from the sink, the message delay accumulates over the hops. If several messages are delayed in one node at the same time, buffer space for the messages must be available. Thus, information transfer delay is correlated with the *buffer requirements* of a sensor node. The delay at each node is caused by two interdependent aspects. First, the delay depends on the traffic that a node has to process *(arrival rate)*. Second, the node needs a specific amount of time to receive process and send a message *(service rate)*. The first aspect depends on the *network topology*, as the traffic that enters a node might be generated by several other nodes. The second aspect is dominated by the *reception delay*.

In the remaining it is shown how network calculus can be tailored and extended so that a worst case analysis of the relevant quantities in sensor networks is possible.

5.1. Background on network calculus

Network calculus is a tool to analyze flow control problems in networks with particular focus on determination of bounds on worst case performance. It has been successfully applied as a framework to derive deterministic guarantees on throughput, delay, and to ensure zero loss in packet-switched networks [4]. Network Calculus is a mathematical tool based on *min-plus* and *max-plus* algebras for designing and analyzing deterministic queuing systems [4].

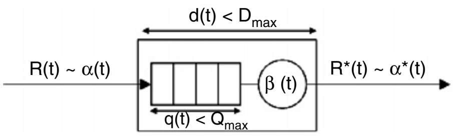


Fig. 4. System representation in Network Calculus theory.

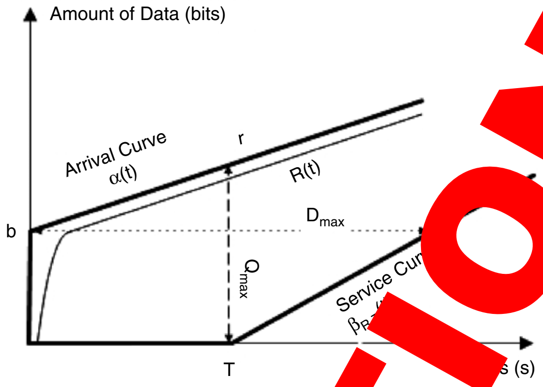


Fig. 5. Delay and back[illegible]

RETRACTION

What makes it different from traditional queuing theory is that it is concerned with worst case rather than average case or equilibrium behavior. It thus deals with bounding proce[illegible] called arrival and service curves rather than arrival and departure processes themselves.

A basic system representation is illustrated in Fig. 4.

For a given data flow, the **input function** is the cumulativ[illegible]al f[illegible]tion denoted by $R(t)$, which represents the number of bits that arrive during the interval [0, t]. We denote by $R^*(t)$ th[illegible]**ut function** of the flow, which represents the number of bits that leave the system during the interval $[0, t]$[illegible]t, some basic definitions and notations are provided before some basic results from network calculus are summarize[illegible]ts can be found in [4].

- It exists an **arrival curve** $\alpha(t)$ that upper bounds R[illegible] that $\forall s, 0 \le s \le t, R(t) - R(s) \le \alpha(t-s)$. This inequality means that the amount of traffic that arrives to receiv[illegible]vice in any interval $[s, t]$ never exceeds $\alpha(t-s)$. It is also said that $R(t)$ is constrained by $\alpha(t)$, or $R(t) \sim \alpha$[illegible]
- It exists a minimum **service curve** $\beta(t)$ gua[illegible]ite[illegible] $R(t)$. This means that the output flow during any given busy period $[t, t+\Delta]$ of the flow is at least equal to [illegible]), [illegible] $+\Delta) - R^*(t) \ge \beta(\Delta)$, where $\Delta > 0$ is the duration of any busy period.

The knowledge of the arrival and ser[illegible] curves [illegible]bles the computation of the delay bound D_{max}, which represents the worst case response time of a message[illegible] the backlog bound Q_{max}, which is the maximum queue length of the flow.

The **delay bound**, D_{max}, for a data[illegible]an arrival curve $\alpha(t)$ that receives the service curve $\beta(t)$ is the maximum horizontal distance between $\alpha(t)$ an[illegible](t) (s[illegible]5), and is expressed as follows:

$$D_{max} = h(\alpha, \beta) = \sup_{s \ge 0} \{\inf \text{[illegible]} \ge 0 | \alpha(s) \le \beta(s+\tau))\} \ge d(t), \quad \forall t \qquad (30)$$

$h(\alpha, \beta)$ is also often called the [illegible]iz[illegible]al d[illegible]ation between α and β.

The **backlog bound**, Q_{max}, fo[illegible]flo[illegible]with an arrival curve $\alpha(t)$ that receives the service $\beta(t)$ is the maximum vertical distance between $\alpha(t)$ and $\beta(t)$, and [illegible]ressed as:

$$Q_{max} = v(\alpha, \beta) = \text{[illegible]}\, s) - \beta(s)) \ge q(t), \quad \forall t \qquad (31)$$

$v(\alpha, \beta)$ is also often ca[illegible]ertical deviation between α and β.

In Network Calculus, it is [illegible]ssible to express an upper bound for the output flow and the equivalent service curve for the concatenation of two serv[illegible]e curves.

The output function $R^*(t)$, of a flow $R(t)$ constrained by an arrival curve $\alpha(t)$ that traverses a system offering a service curve $\beta(t)$, is constrained by **output bound** $\alpha^*(t)$:

$$\alpha^*(t) = (\alpha \odot \beta)(t) \ge \alpha(t) \qquad (32)$$

where $\odot$ is the **min-plus deconvolution.** Let f and g be wide-sense increasing and $f(0) = g(0) = 0$. Then their deconvolution under min-plus algebra is defined as:

$$(f \odot g)(t) = \sup_{s \ge 0} (f(t+s) - g(s)).$$

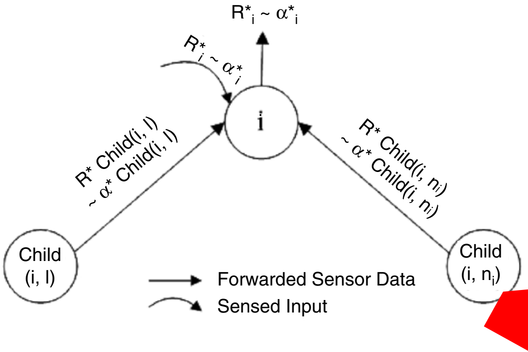


Fig. 6. The sensor network model.

RETRACTION

We consider the following corollary as an application of Eq. (32) to the case of a linear arrival curve and a rate-latency service curve. The proof can be found in Appendix.

Corollary 1. *Assume that a flow is constrained by an arrival curve* $\alpha(t) = b + r \cdot t$ *and the node provides a guaranteed service curve* $\beta_{R,T}(t) = R \cdot (t - T)^+$ *to the flow. Then, the output bound of the flow can be expressed as:*

$$\alpha^*(t) = \alpha(t) + r \cdot T \tag{33}$$

Concatenation of nodes. Assume that a flow $R(t)$ traverses systems $S1$ and $S2$ in sequence, where $S1$ offers service curve $\beta_1(t)$ and $S2$ offers $\beta_2(t)$. Then, the resulting system S, defined by the concatenation of the two systems $S1$ and $S2$, offers the following service curve to the flow:

$$\beta(t) = (\beta_1 \otimes \beta_2)(t) \tag{34}$$

where $\otimes$ is the **min-plus convolution** defined for f, g as:

$$(f \otimes g)(t) = \inf_{0 \le s \le t} (f(t-s) + g(s)).$$

5.2. Sensor network system model

In this paper the common class of single base station oriented operation models is assumed. Within the traffic that is modeled only the sensor reports are taken into account. Traffic generated from the base station towards the nodes (e.g. interests [23] to set up the network structure or to configure the nodes) is explicitly not taken into account. This is considered feasible based on the assumption that the traffic flowing towards the sensors is magnitudes lower than traffic caused by the sensing events. Furthermore, it is assumed that the routing protocol being used forms a tree in the sensor network. Hence N sensor nodes arranged in a directed acyclic graph are given.

As we can find in Fig. 6 each sensor node i senses its environment and thus is exposed to an input function R_i corresponding to its sensed input traffic. If node i is not a leaf node of the tree then it also receives sensed data from all of its child nodes $child(i, 1), \ldots, child(i, n_i)$, where n_i is the number of child nodes of sensor node i. Sensor node i forwards/processes its input which results in an output function R_i^* from node i towards its parent node.

Now the basic network calculus components, arrival and service curve, have to be incorporated. First the arrival curve $\bar{\alpha}_i$, of each sensor node in the field has to be derived. The input of each sensor node in the field, taking into account its sensed input and its children input, is given by:

$$\bar{R}_i(t) = R_i(t) + \sum_{j=1}^{n_i} R^*_{child(i,j)}(t) \tag{35}$$

Thus, the arrival curve for the total input function for sensor node i is given by:

$$\bar{\alpha}_i(t) = \alpha(t)_i + \sum_{j=1}^{n_i} \alpha^*_{child(i,j)}(t). \tag{36}$$

Finally, the output of sensor node i, i.e. the traffic which it forwards to its parent in the tree, is constrained by the following arrival curve:

$$\alpha_i^*(t) = (\bar{\alpha}_i \oslash \beta_i)(t) = \left(\left[\alpha_i + \sum_{j=1}^{n_i} \alpha^*_{child(i,j)}\right] \oslash \beta_i\right)(t). \tag{37}$$

In order to calculate a network-wide characteristic like the maximum information transfer delay or local buffer requirements especially at the most challenged sensor node just below the sink (which is called node 1 from now on) an iterative procedure to calculate the network internal flows is required:

1. Let us assume that arrival curves for the sensed input α_i and service curves β_i, for sensor node i, $i = 1, \ldots, N$, are given.
2. For all leaf nodes the output bound α_i^* can be calculated according to (32). Each leaf node is now marked as "calculated".
3. For all nodes having only children which are marked "calculated" the output bound α_i^* can be calculated according to (37) and they can again be marked "calculated".
4. If node 1 is marked "calculated" the algorithm terminates, otherwise go to step 3.

After the network internal flows are computed according to this procedure, the local worst-case buffer requirements B_i and per node delay bounds D_i for each sensor node i can be calculated according to (30) and (31):

$$B_i = v\left(\bar{\alpha}_i, \beta_i\right) = \sup_{s \geq 0} \left\{\bar{\alpha}_i\left(s\right) - \beta_i\left(s\right)\right\} \tag{38}$$

$$D_i = h\left(\bar{\alpha}_i, \beta_i\right) = \sup_{s \geq 0} \left\{\inf\left\{\tau \geq 0 : \bar{\alpha}_i\left(s\right) \leq \beta_i\left(s + \tau\right)\right\}\right\}. \tag{39}$$

To compute the total information transfer delay $\bar{D}_i$ for a given sensor node i, the per node delay bounds on the path $P(i)$ to the sink need to be added:

$$\bar{D}_i = \sum_{i \in p(i)} D_i. \tag{40}$$

The maximum information transfer delay in the sensor network can then obviously be calculated as

$$\bar{D} = \max_{i=1,\ldots,N} \bar{D}_i. \tag{41}$$

Due to the traffic aggregation inside the network the concatenation result cannot be applied directly, there is in fact a way to still derive a network-wide service curve based on modified service curves that take into account the effects of cross-traffic on a data flow [4]. However, the bounds achieved in this way are not necessarily lower than for (41). This depends on the actual parameters of arrival and service curves. Furthermore, we believe that the hop-by-hop calculation will lend itself better towards integrating in-network processing into future more elaborate extensions of the model.

5.3. *Traffic model*

In the following subsection traffic model will be instantiated with concrete arrival and service curves and their influence on the worst case behavior of the system are discussed in a qualitative fashion.

5.3.1. *Arrival curve*

Maximum sensing rate. The simplest option to bound the sensing input at a given sensor node is based on its maximum sensing rate which is either due to the way the sensing unit is designed or limited to a certain value by the sensor network application's task in observing a certain phenomenon. For example, it might be known that in a temperature surveillance sensor system, the temperature does not have to be reported more than once per second at most. The arrival curve for a sensor node i corresponding to simply having a bound on the maximum sensing rate is given by

$$\alpha_i\left(t\right) = p_i t = \gamma_{p_i,0}\left(t\right). \tag{42}$$

Note that the assumption is made that each sensor node has its individual arrival curve respectively maximum sensing rate. This arrival curve can be used in situations where all sensor nodes are set up to periodically report the condition in a sensor field. Thereby each sensor has a maximum possible rate with which the sensing information can be reported.

Average sensing rate. Depending on the sensor network application the maximum sensing rate arrival curve might lead to very conservative bounds if the maximum sensing rate is only rarely the actual sensing rate. In this situation it would be much more useful if the arrival curve could be based on the average sensing rate. Additionally, there should be permission of some short-term fluctuations if the sensing must be intensified for certain periods of high activity in the field. However, in order to avoid the use of the maximum sensing rate arrival curve it is crucial that the time during which the average sensing rate may be exceeded can be upper bounded. In many applications that should be possible since after some time the phenomenon will disappear again or has to be acted on such that it disappears again (e.g. in a sensor network that also comprises actuators). The arrival curve that captures the average sensing rate with short-term fluctuations for sensor node i is given by

$$\alpha_i\left(t\right) = s_i t + b_i = \gamma_{s_i,b_i}\left(t\right). \tag{43}$$

This affine arrival curve can be shown to be equivalent to the famous token/leaky bucket as it is known from traditional traffic control [4]. It allows sensing at a higher rate than s_i for short periods of time but in the long run only allows sensing at the average rate s_i.

This arrival curve can be used to describe situations in which sensors usually report with a low rate. If a phenomenon is detected in the vicinity of the sensor, the sensing rate is increased for a fixed amount of time.

RETRACTION

5.3.2. Service curve

The service curve captures the characteristics with which sensor data is forwarded by the sensor nodes towards the sink. It abstracts from the specifics and idiosyncrasies of the link layer and makes a statement on the minimum service that can be assumed even in the worst case.

Rate-latency service curve. A typical and well known example of a service curve from traditional traffic control in a packet-switched network is given by

$$\beta_{R,T}\,(t) = R\,(t - T)^{+} \tag{44}$$

where $R \geq r$ is the guaranteed bandwidth, T is the maximum latency of the service and the notation $(x)^{+}$ denotes x if $x \geq 0$ and 0 otherwise. This service curve is typically used for servers that provide a bandwidth guarantee with certain latency. The latency T refers to the deviation of the service (e.g. blocking factor of non-preemptive transmissions). This is often also called a rate-latency service curve and results from the use of many popular packet schedulers (for example Weighted Fair Queuing (WFQ) [24]) many of which can be generalized as guaranteed rate or latency-rate schedulers [25,26]. While for sensor networks there may often be neither a necessity nor the resources (energy, computational power, memory capacity) for a sophisticated scheduling algorithm like WFQ, the class of rate-latency service curves is still very interesting. This is due to the fact that the latency term nicely captures the characteristics induced by the application of a duty cycle concept. Whenever the duty cycle approach is applied there is the chance that sensed data or data to be forwarded just arrives after the last duty cycle (of the next hop) is just over and thus a fixed latency occurs until the forwarding capacity is available again. So, with some new parameters the following service curve for a sensor node i is obtained:

$$\beta_i = \beta_{f_i,l_i}\,(t) = f_i\,(t - l_i)^{+}\,. \tag{45}$$

Here f_i, and 1_i denote the forwarding rate respectively forwarding latency for sensor node i.

5.3.3. Delay and backlog bound

The delay bound *Dmax* (presented in Fig. 5) guaranteed for the data flow with the arrival curve $\alpha\,(t) = b + r \cdot t$ (also called (b, r)-curve) by the service curve $\beta_{R,T}\,(t) = R \cdot (t - T)^{+}$ is computed as follows [4]:

$$D_{max} = \frac{b}{r} + T \tag{46}$$

and the backlog bound is expressed as [4]:

$$Q_{max} = b + r \cdot T\,. \tag{47}$$

In our analysis, we will use the previous linear arrival curve and the rate-latency service curve since they accurately represent the system.

5.4. Analytical model of a realistic scenario

The intention of this example is to analytically explore the possible range of the characteristics discussed above in a realistic scenario. Thereafter it is analyzed in which operation range a state of the art sensor node could be used to form the sensor field.

Topology and routing of the sensor field is assumed to be a grid, the distance between the sensors is d. Fig. 7 shows the lower half of a grid shaped sensor field with the base station (sink) located in its center. The size of the field is $8d \times 8d$, containing $N = 80$ sensors each with an idealized transmission range of $\sqrt{2}d$.

For the routing protocol, the Greedy Perimeter Stateless Routing (GPSR) protocol is used [27]. All nodes in GPSR must be aware of their position within a sensor field. Each node communicates its current position periodically to its neighbors through beacon packets. In a given static scenario, these beacons have to be transmitted only once. Upon receiving a data packet, a node analyzes its geographic destination. If possible, the node always forwards the packet to the neighbor geographically closest to the packet destination. If there is no neighbor geographically closer to the destination, the protocol tries to route around the hole in the sensor field. This routing around a hole is not used in the described topology. In Fig. 7 the resulting structure of the communication paths is shown.

Sensing activity. It is assumed that the sensor field is used to collect data periodically from each of the sensors. Each sensor can report with a maximum report frequency of p. Thus, the maximum sensing rate arrival curve described by (42) is used to model the upper bound of the sensing activity of each node in the sensor field. A homogeneous field is assumed, hence

$$\alpha_i\,(t) = pt = \gamma_{p,0}\,(t)\,. \tag{48}$$

Each node additionally receives traffic from its child nodes according to the traffic pattern implied by the topology and the routing protocol (see Fig. 7). Therefore, the arrival curve $\bar{\alpha}_i$ for the total input of a sensor node i is given by Eq. (36). Later it will be shown in detail how the relevant $\bar{\alpha}_i$ can be calculated.

RETRACTION

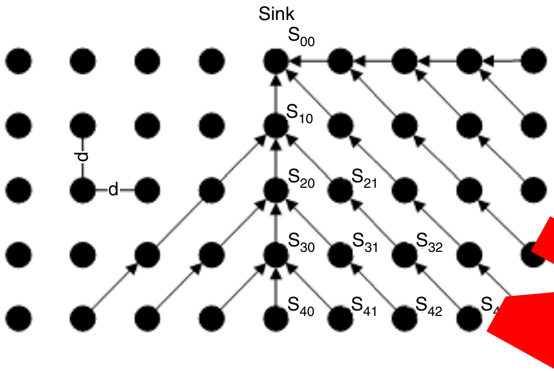


Fig. 7. Sensor field with grid layout.

RETRACTION

Packet Forwarding scheme can be described by the rate-latency service curve as described by Eq. (45):

$$\beta_i(t) = \beta_{f,l}(t) = f\,(t-l)^+ . \tag{49}$$

Calculation. After defining the scenario, the previous equations can no [illegible] used to evaluate the characteristics of interest and their interdependencies. The goal of the calculation is to determine the characteristics at the sensor node with the worst possible traffic conditions. In this example this is node s_{10}. If the characteristics in this node are determined and the node is dimensioned to cope with them, all other nodes in the field (assuming homogeneity) are dimensioned properly as well.

First the output bound α^*_{40} of the leaf node s_{40} has to be calculated using [illegible]), (47) and (32):

$$\alpha_{40} = \gamma_{p,0}, \qquad \beta_{40} = \beta_{f,l} = \beta, \qquad \alpha^*_{40} = \alpha_{40} \odot \beta_{40} = \text{[illegible]}_{l}. \tag{50}$$

The output bound for node s_{40} is also the output bound of the other leaf nodes (e.g. $\alpha^*_{40} = \alpha^*_{41} = \alpha^*_{42} = \alpha^*_{43}$). Now the output bounds for the nodes one level higher in the tree can be calculated using Eqs. (49), (47), (48) and (38):

$$\bar{\alpha}_{30} = \gamma_{p,0} + 3\alpha^*_{40} = \gamma_{p,0} + 3\gamma_{p,pl} = \gamma_{4p,3pl}, \alpha^*_{30} = \bar{\alpha}_{30} \odot \text{[illegible]}_{4p,7pl}. \tag{51}$$

The calculation can now be repeated until node s_{1} [illegible]:

$$\bar{\alpha}_{10} = \gamma_{p,0} + 2\alpha^*_{21} + \alpha^*_{20} = \gamma_{16p,34pl}, \alpha^*_{10} = \bar{\alpha}_{10} \odot \text{[illegible]}_{16p,50pl}. \tag{52}$$

After the arrival curve for node s_{10} is calculated, the worst case buffer requirements B_{10} and the information transfer delay D can be calculated according to Eqs. (39) [illegible] (40):

$$B_{10} = v\,(\bar{\alpha}_{10}, \beta) = 50pl$$

$$D_{10} = h\,(\bar{\alpha}_{10}, \beta) = l + \frac{34pl}{f}, \qquad D_{\text{[illegible]}} = \text{[illegible]}) = l + \frac{13pl}{f}$$

$$D_{30} = h\,(\bar{\alpha}_{30}, \beta) = l + \frac{3pl}{f}, \qquad \text{[illegible]}\,h\,(\bar{\alpha}_{40}, \beta) = l$$

$$D = D_{40} + D_{30} + D_{20} + D_{10}\ \text{[illegible]}\ 4l + \frac{50pl}{f}.$$

6. Simulation results

In this section we use GloMoSim [28] to study the reliable real-time degree of wireless sensor networks.

GloMoSim is a scalable discrete event simulator developed by UCLA. This software provides a high fidelity simulation for wireless communication [illegible] detailed propagation, radio and MAC layers. Table 1 describes the detailed setup for our simulator. The communication parameters are mostly chosen in reference to the Berkeley Mote [29] specification.

There are two typical traffic patterns in sensor networks: a base station pattern and a peer-to-peer pattern.

In our evaluation, we use a base station scenario, where 6 nodes, randomly chosen from the left side of the terrain, send data to the base station at the middle of the right side of the terrain. The average hop count between the node and base station is about 8–9 hops. Each node generates flow with a rate of 1 packet/second. In order to evaluate the end-to-end delay we increase the rate of this flow step by step from 1 to 100 packets/second over several simulations.

Fig. 8 plot shows the end-to-end delay. At each point, we average the end-to-end delays of all the packets from the 96 flows (16 runs with 6 flows each). As you can see in Fig. 8, by increasing the packet transmission rate, end-to-end delay increases as well. As the rate increases, the buffer full probability increases as well and the lost packets must be retransmitted until they are successfully delivered to the sink.

Table 1
Simulation settings.

MAC layer	MACA [17]
Routing layer	DSR [16]
Radio layer	RADIO-ACCNOISE
Propagation model	TWO-RAY
Bandwidth	200 Kb/s
Payload size	32 Byte
Terrain	(200 m, 200 m)
Node number	100
Node placement	Uniform
Radio Range	40 m
R	2
Transmit power consumption	26.7 mw
Receive power consumption	22.6 mw

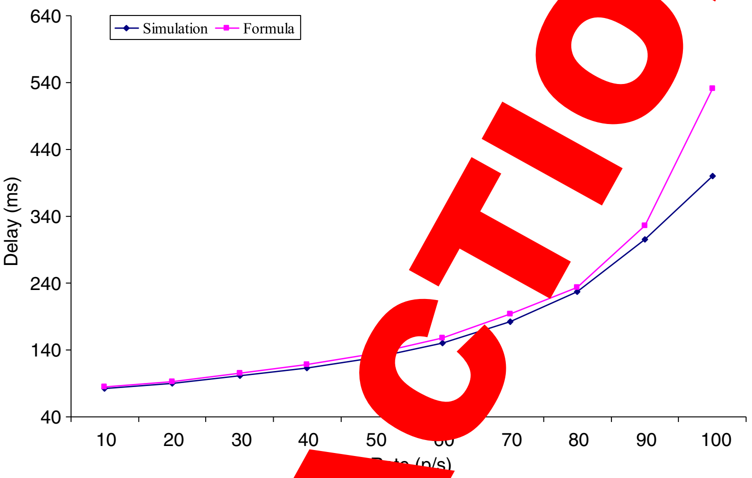


Fig. 8. End-to-end delay under different network loads.

RETRACTION

Fig. 9 shows the miss ratio. We assume that T_D is 150 ms and as can be seen in Fig. 9, by increasing the packet transmission rate, miss ratio increases as well. The reason is that when the rate increases, then the average end-to-end delays will increase too.

The reliable real-time degree is a metric in soft real-time systems. We set the buffer size to 50 packets. In the simulation, some packets are lost due to full buffer. We also consider this situation as a deadline miss. The result shown in Fig. 10 is the summary of 16 randomized runs. When the packet rate increases, the buffer full probability and node failure probability increase as well. Hence the packet loss increases too. Another consequence of the rate increase is the end-to-end delay augmentation. So the packet rate increment, yields decrease of reliable real-time degree (percentage of on time successfully delivered data).

Fig. 11 plot shows the node energy consumption rate versus data rate. When the packet transmission rate increases, the node energy consumption rate increases as well.

7. Conclusions and future work

We introduced in this paper a [illegible] reliable real-time degree, based on a queuing theory model for general-case wireless sensor network in which all nodes are $M/M/1/k$ queues. Parameters such as packet loss, packets' delay and path lifetime were considered as important factor in determining the reliable real-time degree of such network. We have analyzed a semi-qualitative phenomenon, so that we can predict the real-time behavior of network in the case of stochastic events. Simulation results are in accordance with the model. It was shown that increasing the network load has a negative impact on the reliable real-time degree.

Also we use network calculus and extended it, so that a worst case analysis of the delay and queue quantities in sensor network is possible, and we can predict the bounded value of delay and buffer.

The model could be modified to take into account some aspects that have not been addressed in this work and that can be interesting subject of future research. For instance, a model of other queuing policy or firm real-time can be included and some of the assumptions that we made while developing the analytical model, such as those on all the nodes are active and none of them in sleep mode, can be modified. Furthermore, we point out that the model can be extended to describe various

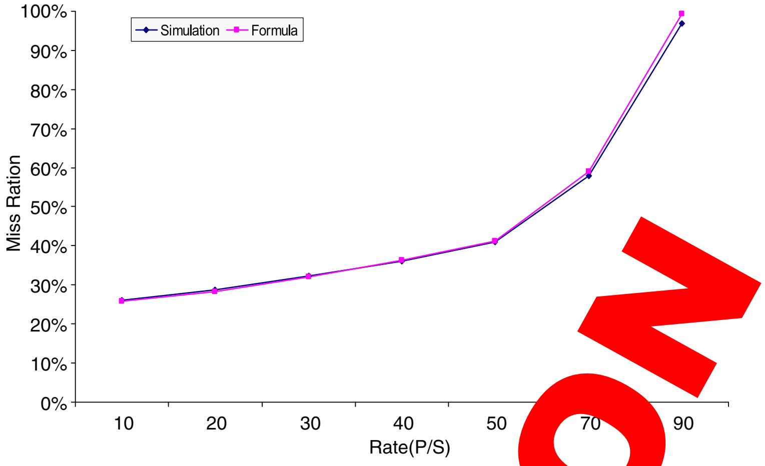


Fig. 9. MissRatio under different network loa

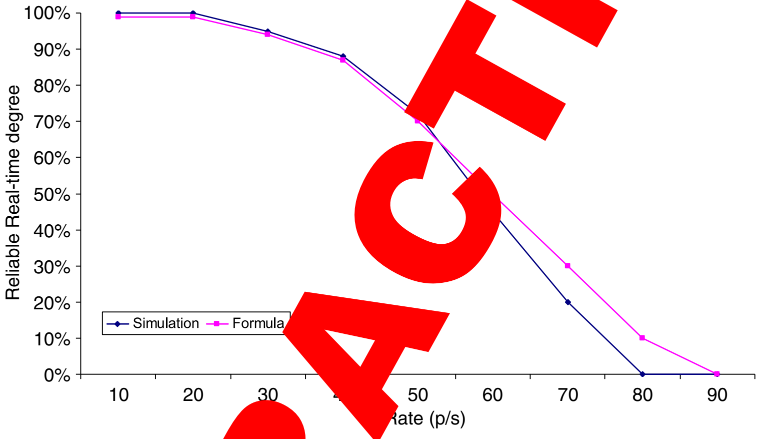


Fig. 10. Re e re ree under different network loads.

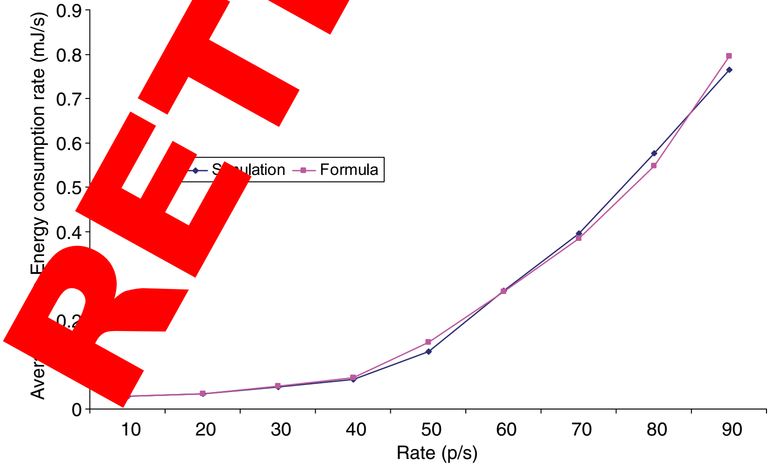


Fig. 11. Node energy cost under different network loads.

RETRACTION

aspects in the design of sensor networks, such as data aggregation or backpressure traffic mechanisms. Finally, cluster-based network architectures as well as the case where the network topology varies could be studied.

Acknowledgements

The authors wish to thank the anonymous referees for their comments, which significantly improved the presentation of this paper. This work was partly supported by Iran Telecommunication Research Center (ITRC) grant 7724/500.

Appendix. Proof of Corollary 1

By definition, we have:

$$\alpha^*(t) = (\alpha \oslash \beta)(t)$$
$$\alpha^*(t) = (\alpha \oslash \beta)(t) = \sup_{s \geq 0} (\alpha(t+s) - \beta(s)).$$

Using the definition of α and β, we get:

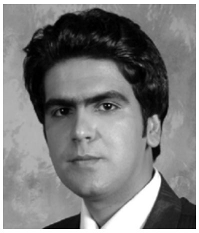
$$\alpha^*(t) = \sup_{s \geq 0} \left(b + r \cdot (t+s) - R \cdot (s-T)^+\right)$$
$$\alpha^*(t) = \max\left(\sup_{0 \leq s \leq T} \left(b + r \cdot (t+s) - R \cdot (s-T)^+\right), \sup_{T \leq s} \left(b + r \cdot (t+s) - R \cdot (s-T)^+\right)\right)$$
$$\alpha^*(t) = \max\left(b + r \cdot (t+T) - R \cdot (T-T)^+, b + r \cdot (t+T) - R \cdot (T-T)^+\right)$$
$$\alpha^*(t) = b + r \cdot (t+T) = \alpha(t) + r \cdot T.$$

References

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine (2002) 102–114.
[2] G.J. Pottie, W.J. Kaiser, Wireless integrated network sensors, Communications of the ACM 43 (5) (2000) 51–58.
[3] J.A. Stankovic, T.F. Abdelzaher, C. Lu, L. Sha, J. Hou, Real-time communication and coordination in embedded sensor networks, Proceedings of the IEEE 91 (7) (2003) 1002–1022.
[4] J.Y. Le Boudec, P. Thiran, Network Calculus: A Theory of Deterministic Queuing Systems for the Internet, in: Lecture Notes in Computer Science LNCS, vol. 2050, Springer, 2001.
[5] R. Braden, D. Clark, S. Shenker, Integrated services in the internet architecture: an overview, in: RFC, vol. 1633, 1994.
[6] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the differentiated services field (DS Field) in the IPv4 and IPv6 headers, in: Proposed Standard RFC, vol. 2474, 1998.
[7] P. Gupta, P.R. Kumar, The capacity of wireless networks, IEEE Transactions on Information Theory 46 (2) (2000) 388–404.
[8] C. Florens, R. McEliece, Packet distribution algorithms for sensor networks, IEEE INFOCOM (2003) 1063–1072.
[9] S. Shakkottai, R. Srikant, N.B. Shroff, Unreliable sensor grids: coverage, connectivity and diameter, IEEE INFOCOM 2 (2003) 1073–1083.
[10] C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, Impact of network density on data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, 2002, pp. 457–458.
[11] T. He, B.M. Blum, J.A. Stankovic, T.F. Abdelzaher, AIDA: adaptive application independent aggregation in sensor networks, ACM Transactions on Embedded Computing System 3 (2) (2003) 426–457.
[12] T.F. Abdelzaher, K.S. Prabh, R. Kiran, On real-time capacity limits of multihop wireless sensor networks, in: Proceedings of the 25th IEEE Real-Time Systems Symposium, RTSS, 2004, pp. 359–370.
[13] C.F. Chiasserini, M. Garetto, Modeling the performance of wireless sensor networks, IEEE INFOCOM 1 (2004) 7–14.
[14] C.F. Chaiasserini, R. Gaeta, M. Gribaudo, D. Manini, M. Meo, Fluid models for large-scale wireless sensor networks, Performance Evaluation 64 (7–8) (2007) 715–736.
[15] K. Mizanian, A.H. Jahangir, A quantitative real-time model for multihop wireless sensor networks, in: Third International Conference on Intelligent Sensors, Sensor Networks and Information Processing, ISSNIP'07, 2007, pp. 79–84.
[16] D.B. Johnson, D.A. Maltz, Dynamic source routing in ad Hoc wireless networks, Mobile Computing 353 (1996).
[17] P. Karn, MACA: A new channel access method for packet radio, in: 9th Computer Networking Conference, 1990, pp. 134–140.
[18] V. Bharghavan, A. Demers, S. Shenkar, L. Zhang, MACAW: A media access protocol for wireless LANs, in: ACM SIGCOMM'94, 1994, pp. 212–225.
[19] L. Kleinrock, Queuing systems, Volume I: Theory, first edition, John Wiley & Sons, 1975.
[20] F.P. Kelly, Loss networks, The Annals of Applied Probability 1 (3) (1991) 319–378.
[21] W. Whitt, Blocking when service is required from several facilities simultaneously, AT&T Technical Journal 64 (8) (1975) 1807–1856.
[22] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless micro sensor networks, in: 33rd International Conference on System Sciences, HICSS '00, 2000, 10pp.
[23] U. Roedig, A. Barroso, C.J. Sreenan, Determination of aggregation points in wireless sensor networks, in: Proceedings of the 30th Euromicro Conference, EUROMICRO'04, 2004, pp. 5003-5010.
[24] A. Demers, S. Keshav, S. Shenker, Analysis and simulation of a fair queuing algorithm, in: Proceedings of ACM SIGCOMM, 1989, pp. 3–12.
[25] P. Goyal, S.S. Lam, H. Vin, Determining end-to-end delay bounds in heterogeneous networks, in: Proceedings of 5th International Workshop on Network and Operating System Support for Digital Audio and Video, NOSSDAV95, in: LNCS, vol. 1018, Springer, 1995.
[26] D. Stiliadis, A. Varma, Latency-Rate Servers: A general model for analysis of traffic scheduling algorithms, IEEE/ACM Transactions on Networking 6 (5) (1998) 611–624.
[27] B. Karp, H.T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, Mobile Computing and Networking (2000) 243–254.
[28] X. Zeng, R. Bagrodia, M. Gerla, GloMoSim: A library for parallel simulation of large-scale wireless networks, in: Proceedings of the 12th Workshop on Parallel and Distributed Simulations, PADS '98, 1998.
[29] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, System architecture directions for network sensors, ASPLOS (2000) 93–104.

RETRACTION

Kambiz Mizanian received his M.Sc. degree in Computer Engineering in 1996 and his second M.Sc. degree in Utilization and System Management in 2001 both from Sharif University of Technology (SUT), IRAN, where he is currently a Ph.D. candidate in Sharif University of Technology (SUT), IRAN. His research interests include Computer network's Modeling & Performance evaluation, Ad hoc and Wireless Sensor Network, Network Processor's Performance evaluation, real-time systems and Industrial Automation.



Hamed Yousefi received his M.Sc. degree in Computer Engineering in 2009 from Sharif University of Technology (SUT), IRAN, where he is currently pursuing his Ph.D. degree. His research interests include Wireless Ad hoc & Sensor Networks, Performance and Dependability Modeling, Energy Efficient & Real-time & Reliable Communications.

Amir Hossein Jahangir, Associate Professor, received his Ph.D. in Informatics Engineering, Institut National Sciences Appliquees, Toulouse, France, in 1989. His research interests include [illegible] networks, Performance and dependability evaluation of networks and architectures, High performance and parallel Computer Architectures, Computer arithmetic, and Real-time Systems. He has also served during his career as the dean of Computer Engineering Department, Head of Computing Center, and Department's Graduate Studies chair.

RETRACTION