IEEE 802.15.4 MULTIHOP FORWARDING THROUGHPUT ANALYSIS IN PRESENCE OF HIDDEN/EXPOSED TERMINALS

Siddarth Sen and Swades De
Electrical Engineering Department, Indian Institute of Technology Delhi, New Delhi, India

ABSTRACT

A wireless network that uses intermediate nodes to transmit data to the destination suffers from the hidden/exposed terminals problem unless specific steps are taken by the protocol implementation to overcome this. The IEEE 802.15.4 standard specifies no such measure. At the same time packet transmission through multiple hops can be more energy efficient than direct packet transmission, and at times it is the only solution. In this paper, a multihop wireless sensor network with hidden/exposed terminals is considered and its throughput performance is analyzed. The analysis is verified by extensive *ns-2* simulations.

I INTRODUCTION AND MOTIVATION

In a distributed networked sensing task, collected data at the field sensors are forwarded to a predetermined sink node – which could be a remote monitoring and control center, or a clusterhead in a hierarchical sensor network. Limited nodal energy and high premium on network lifetime in such a network warrants that the remotely located field nodes communicate to the data sink via multiple hops. Multihop nature of forwarding implies that, in addition to forwarding their own data, the intermediate nodes will be responsible for relaying data of the peripheral nodes. Therefore, field data from multiple nodes are accumulated (in uncompressed or compressed form) as the sink node is approached, and as a result the traffic flow intensity increases in the same direction. As multiple nodes try to forward data to one node at an intermediate stage, contention to access the wireless channel occurs among them. In addition, the hidden/exposed nodes problem in a multihop forwarding leads to queueing/dropping of packets at the intermediate nodes.

Many-to-one forwarding in IEEE 802.15.4 sensor networks has been studied from congestion control fairness perspectives [4], where transport layer scheduling is suitably controlled to avoid packet dropping as they propagate toward the sink. To enable successful many-to-one forwarding, access scheduling mechanisms and buffer requirements were investigated in [13]. Another set of work proposed medium access control (MAC) level solutions to resource constrained multihop sensor networks (e.g., [5, 10, 14]). While the prior works addressed the important issue of data forwarding constraints, to the best of our knowledge, an analytic measure of network throughput in a many-to-one multihop sensor network is still missing.

Systems implementation level many-to-one multihop forwarding constraints, such as message length and buffer size, were studied in [7], where the number of message transmissions was reduced by in-network aggregation. It also showed how the data forwarding performance drastically decreases with increase in hop length, but did not address the effect of multiaccess constraints. A few recent MAC level analytic performance models of CSMA/CA (carrier sense multiple access with collision avoidance) sensor networks include [6, 8, 9, 11]. [8] considered star network topology with beacon-enabled nodes and two-way communication. [11] investigated multiaccess contention in a many-to-one data aggregation scenario with beacon-enabled nodes, where the nodes were modeled such that the field nodes are always in the transmit state and the sink is in the receive state. All of these analytic works addressed the single-hop aggregation problem.

In the current work, we present a stochastic model to characterize the throughput of a multihop many-to-one ad hoc sensor network by accounting the multiaccess collisions and hidden/exposed nodes. The analysis is verified by extensive network simulations using *ns-2*. The developed model can be used to study the effect of network traffic generation rate on the allowable number of forwarding hops, or conversely, for a given maximum number of hops to the sink, maximum allowable traffic generation rate at the nodes.

II CSMA/CA ALGORITHM DESCRIPTION

A detailed explanation of the IEEE 802.15.4 specification can be found in [2]. For the analysis of a multihop network we consider the unslotted CSMA/CA algorithm. Until now, to our knowledge, only the slotted 802.15.4 CSMA/CA analysis has been carried out [8, 11]. While a slotted CSMA/CA is expected to show better performance in comparison to unslotted one, 802.15.4 achieves synchronization amongst the nodes by the transmission of beacon packets by the coordinators. The beacon packets help in setting the internal clocks of all reduced function devices (RFDs). As explained in [1, 2], the nodes wait for periodic reception of beacons. The loss of beacon reception renders a RFD useless (or orphaned) until the next beacon is received and resynchronization can take place. Due to the importance of beacon packets, nodes take special care not to transmit any other packet during the expected arrival of a beacon packet.

The technique of collision avoidance during beacon packet transmission works only if all nodes can hear each other, i.e, when there are no hidden terminals, or there is only one PAN coordinator. In a cluster tree topology which has one PAN coordinator and several coordinators each transmitting beacons, if the coordinator is hidden from a node, then collision avoidance will not work. This situation is depicted in figure 1. In

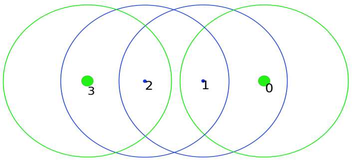

Figure 1: Collision of beacon packets.

the figure, nodes 0 and 3 are coordinators, while nodes 1 and 2 are RFDs. Node 1 is associated with coordinator 0 while node 2 with coordinator 3. Also note 0 is hidden from 2 and 3 is hidden from 1. When 1 and 2 perform collision avoidance of beacons it is only with respect to the beacons they are receiving from their respective coordinators. All coordinators need not necessarily transmit beacons at the same time instant. So while 1 is transmitting a data packet, 2 may be waiting for beacon from 0 which will undergo collision. Loss of beacon packets is especially prominent at high data rates. This fact has been verified through simulation. When a RFD misses a beacon it gets orphaned and cannot transmit data until its re-association with a coordinator. The process of re-association is time consuming and chances of successful re-association is further reduced in the above mentioned situation. It is seen from *ns-2* simulations that at high traffic rates the throughput of the network comes down to zero. Therefore following an unslotted algorithm makes more sense which leads motivation to the analysis of the unslotted CSMA/CA algorithm.

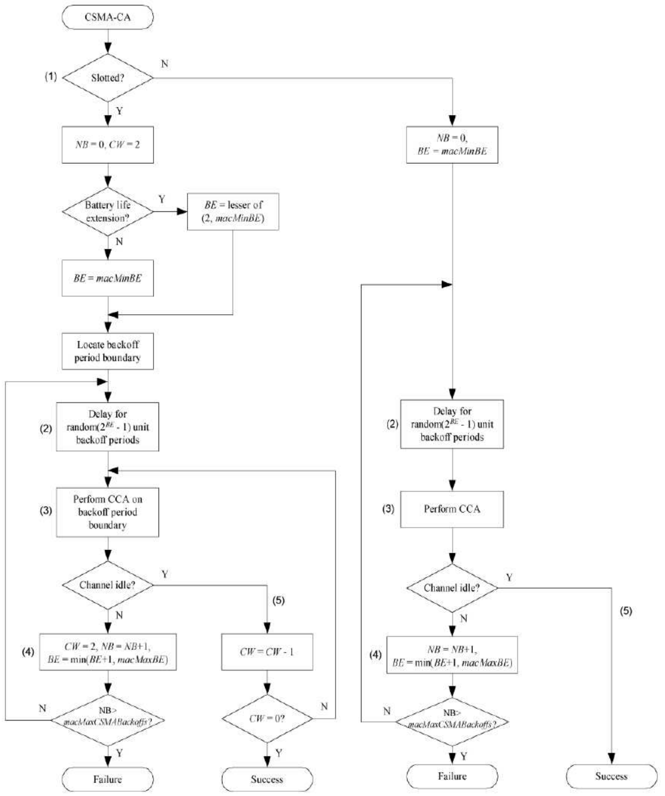

Figure 2: Unslotted CSMA/CA algorithm.

Figure 2, which has been adapted from [1], gives the 802.15.4 CSMA/CA algorithm. NB defines the number of backoff attempts, *macMaxCSMABackoffs*, which is set as 5 in the 802.15.4 standard, after which a channel access failure is declared. BE is the backoff exponent which initially starts with *macMinBE*$= 3$, increments by one for every failure, and freezes at *macMaxBE*$= 5$.

III ANALYSIS OF THE CSMA/CA ALGORITHM

The analysis of unslotted CSMA/CA is an extension from [11] with modifications to accommodate the unslotted algorithm. According to the non-persistent CSMA model, if a node senses that the channel is idle, it transmits its packet. As computation of the channel idling probability in a given backoff slot is not easy, it is approximated with the steady state probability that the channel is idle. Thus, every node sees a probability p_i^c that the channel is idle at any given back-off slot. Similarly, computing the probability that a node begins transmission in any generic backoff slot is difficult. This probability is approximated with the steady-state probability that a node transmits, p_t^n. The 802.15.4 standard specifies that the number of backoff slots a node has to wait at each random backoff stage should be drawn from a uniform distribution. For the purpose of simplified analysis, we replace the uniform distribution with a geometric distribution of the same mean so that the backoff algorithm is memoryless.

We consider a network with random distribution of nodes where all nodes may not hear each other. As the channel access is unslotted CSMA/CA based, there is no synchronization among the nodes and no inactive periods in the superframe. The nodes perform either uplink or downlink transmission and there is no acknowledgement of packet reception. The packet size is fixed to N backoff slots, arriving at a Poisson rate of λ packets per packet duration. Thus the probability that a packet will arrive in a backoff slot is $p = \lambda/N$. There is no buffering of packets. We consider a sufficiently arbitrary network to present the analysis. This would ensure the validity of the analysis and proof that it can be extended to any other topology as well. Here, we consider the scenario shown in figure 3.

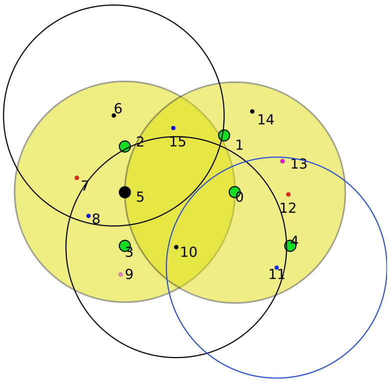

Figure 3: Topology of nodes with hidden terminals.

For the topology of figure 3, Table 1 gives a list of nodes that can hear each other. Based on the CSMA/CA algorithm presented in section II, the Markov chain model of a node is shown in figure 4. Since each node has different set of neighbors, each node will have its own set of steady state probabilities. As the number of nodes increases, the number of states also increases. Also note that, as the nodes share the common wireless channel, steady state probability of a particular node is dependent on the state of every other node of the network. As a result, the states of all nodes have to be *simultaneously* solved for a convergent solution. While the analysis is straightforward, as the number of nodes increase, convergence issues may arise. From the nodal Markov chain model, the following equations can be

Table 1: List of nodes that sense each other

Node No	Nodes it senses
0	5,10,11,12,13,14,15
5	6,7,8,9,10,15
6	15,5,8,7
7	15,6,8,9,5
8	7,6,5,9,10
9	5,7,8,10
10	5,11,8,9
11	13,12,10
12	14,11,13
13	14,11,12
14	15,12,13
15	14,6,5,7

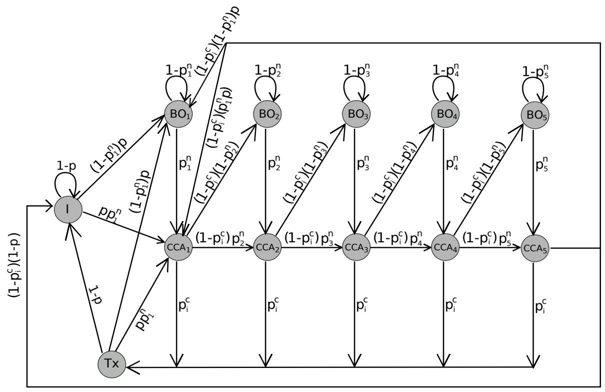

Figure 4: Markov chain model of a transmitting node.

inferred.

$$
\begin{aligned}
\pi(i) &= (1-p)\pi(i) + (1-p)\pi(tx) + (1-p_i^c)(1-p)\pi(cca_5) \\
\pi(bo_1) &= (1-p_1^n)\pi(bo_1) + p(1-p_1^n)\pi(i) + p(1-p_1^n)\pi(tx) \\
&\quad + p(1-p_i^c)(1-p_1^n)\pi(cca_5) \\
\pi(cca_1) &= p_1^n\pi(bo_1) + p(p_1^n)\pi(i) + p(p_1^n)\pi(tx) \\
&\quad + p(1-p_i^c)(p_1^n)\pi(cca_5) \\
\pi(bo_2) &= (1-p_2^n)\pi(bo_2) + (1-p_i^c)(1-p_2^n)\pi(cca_1) \\
\pi(cca_2) &= p_2^n\pi(bo_2) + (1-p_i^c)p_2^n\pi(cca_1) \\
\pi(bo_3) &= (1-p_3^n)\pi(bo_3) + (1-p_i^c)(1-p_3^n)\pi(cca_2) \\
\pi(cca_3) &= p_3^n\pi(bo_3) + (1-p_i^c)p_3^n\pi(cca_2) \\
\pi(bo_4) &= (1-p_4^n)\pi(bo_4) + (1-p_i^c)(1-p_4^n)\pi(cca_3) \\
\pi(cca_4) &= p_4^n\pi(bo_4) + (1-p_i^c)p_4^n\pi(cca_3) \\
\pi(bo_5) &= (1-p_5^n)\pi(bo_5) + (1-p_i^c)(1-p_5^n)\pi(cca_4) \\
\pi(cca_5) &= p_5^n\pi(bo_5) + (1-p_i^c)p_5^n\pi(cca_4) \\
\pi(tx) &= p_i^c\sum_{j=1}^{j=5}\pi(cca_j)
\end{aligned}
$$

The normalizing condition for the above Markov chain is:

$$\pi(i) + \pi(tx) + \sum_{j=1}^{j=5}[\pi(cca_j) + \pi(bo_j)] = 1$$

From renewal theory [12], the steady state transmission probability of a node, p_t^n can be derived from the Markov equations as:

$$p_t^n = \frac{\pi(tx)}{\pi(i) + N\pi(tx) + 0.4\sum_{j=1}^{j=5}\pi(cca_j) + \sum_{j=1}^{j=5}\pi(bo_j)}$$

The Markov model of the channel for successful transmission from any node to any other neighbor is given in figure 5. From the Markov model of the channel, the following equations are obtained:

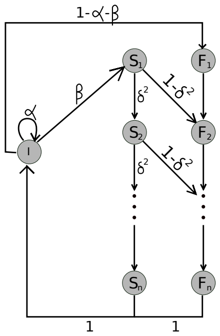

Figure 5: Markov model of the channel of a particular node

$$
\begin{aligned}
\pi(S_j) &= \delta^{j-1}\beta\pi(i), j\epsilon(1,N) \\
\pi(F_1) &= (1-\alpha-\beta)\pi(i) \\
\pi(F_j) &= \pi(F_{j-1}) + (1-\delta)\pi(S_{j-1}), j\epsilon(2,N) \\
1 &= \pi(i) + \sum_{j=1}^{j=N}[\pi(S_j) + \pi(F_j)]
\end{aligned}
$$

To determine the probability of success (or throughput) from node 5 to node 0, we observe that, it is possible only if in a given backoff slot node 5 transmits while node 15 and 10 are quite as they will sense the channel to be idle. Also the nodes which cannot not sense the transmissions from node 5 to node 0 will have to be quiet for *two* backoff slots for a successful transmission. Thus $\beta_0 = p_{t|i0}^{n5} * (1-p_{t|i0}^{n15}) * (1-p_{t|i0}^{n10}) * (1-p_{t|i0}^{n14})^2 * (1-p_{t|i0}^{n13})^2 * (1-p_{t|i0}^{n12})^2 * (1-p_{t|i0}^{n11})^2$, where $p_{t|i0}^{n12}$ stands for the probability that node 12 will transmit given that node 0 senses the channel to be idle in the previous backoff slot. α_0 is the probability that given node 0 senses the channel to be idle in the previous backoff slot, it continues to sense an idle channel in the next back off slot. Thus $\alpha_0 = (1-p_{t|i0}^{n11}) * (1-p_{t|i0}^{n12}) * (1-p_{t|i0}^{n13}) * (1-p_{t|i0}^{n14}) * (1-p_{t|i0}^{n10}) * (1-p_{t|i0}^{n15}) * (1-p_{t|i0}^{n5})$. δ_0 is the probability that none of the hidden nodes transmit and is given by $\delta_0 = (1-p_t^{n14}) * (1-p_t^{n13}) * (1-p_t^{n11}) * (1-p_t^{n12})$. The throughput S can be determined by solving the Markov model of figure 5 and is basically the steady state probability $\pi(S_n)$ multiplied by the number of backoff slot durations a packet is of (i.e N) and is given by $S = N * \delta^{(2*(N-1))} * \beta * p_{i0}^c$ where p_{i0}^c is the probability that node 0 senses the channel to be idle which in this case is the same as $\pi(i)$. The non-linear simultaneous equations can be solved numerically to get the throughput. The above analysis is verified using *ns-2*. The results are shown in figure 6.

To analyze the multihop forwarding throughput, we consider a simple multihop topology as shown in figure 1. In this case

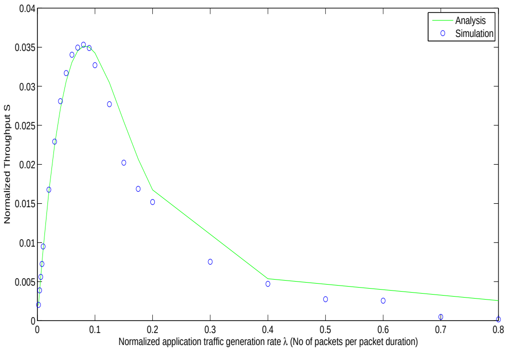

Figure 6: Simulation and analysis plots

nodes 0, 1, and 2 are the coordinators while the node 3 is a RFD. Packets flow from left to right, i.e., from node 3 to 0. Each node generates packets at the rate λ (except node 0). The nodes 1 and 2 are also involved in packet forwarding. While the application traffic arrival process is Poisson, the departure of packets from the queue need not be Poisson [3]. However, for tractability of the analysis, Poisson departure process is assumed here, and the results are compared with the simulation.

The analysis of the multihop network with hidden/exposed terminals is extended from the single hop case. The only difference being the MAC layer of the node now not only receives packets from the application layer but also from the network layer. The MAC layer continues to get packets from the application layer in a Poisson fashion as before. From the network layer it may no longer be Poisson. For comparing the results, we *assume* network layer of node 2 forwards packets from node 3 at the Poisson rate λ. Application layer also generates packets at the Poisson rate λ. Thus the MAC layer has independent streams of Poisson packets arriving at the rate 2λ. Thus, $p = (2\lambda/N)$. Again *we assume* that the network layer of node 1, forwards packets arriving from node 2 at the rate 2λ. Thus the MAC layer has a Poisson steam of rate 3λ (application + network), or $p = 3\lambda/N$.

From the topology (figure 1) there are basically 3 *different* types of nodes receiving data. This is one of the reasons (apart from the simplicity) this topology was chosen. Node 2 has a hidden node (node 1) which interferes with its reception. Node 1 has no hidden nodes, however, its own packet transmission interferes with the packets it receives from node 2 which cause degradation of throughput. Node 0 on the other hand has absolutely no interference and its throughput is limited only by the rate of transmission of node 1. In figures 7, 8, 9 we show the various simulation and analysis plots of the different nodes. As expected node 2 suffers the most in terms of throughput performance. This is verified by both the analysis and simulation. The difference in analysis and simulation can be attributed to the Poisson assumption of departure process in the analysis. Node 1 shows better performance again as expected but at high traffic rates degradation in throughput due to collisions between its own transmissions and node 2's transmissions. The analysis and simulation plots show close agreement even with the Poisson assumption that we have made. Node 0 suffers from no collisions at all. Since there are *no packet collisions* at node 0 as the traffic rate increases the throughput characteristics monotonically *increases*. While this may be contrary to most throughput characteristics, the fact is verified by *both* simulation and analysis. Again the Poisson assumption in this case holds good.

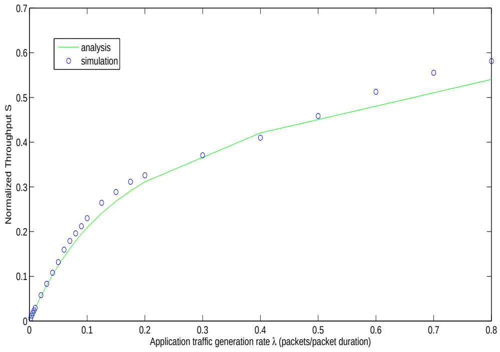

Figure 7: Simulation vs analysis of the throughput characteristics of node 0

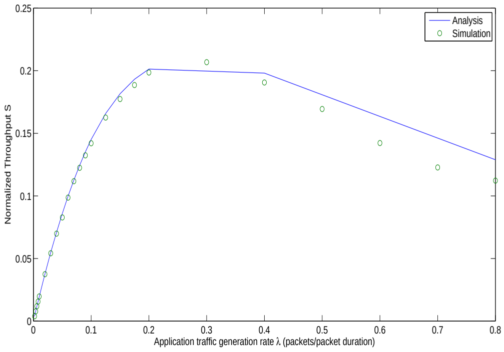

Figure 8: Simulation vs analysis of the throughput characteristics of node 1

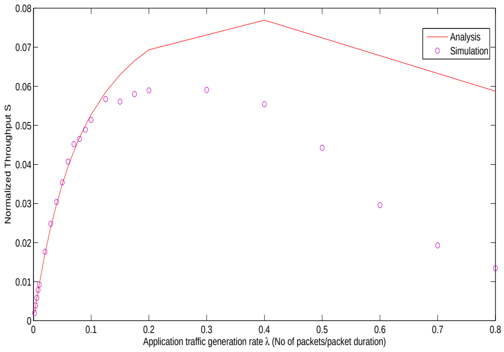

Figure 9: Simulation vs analysis of the throughput characteristics of node 2

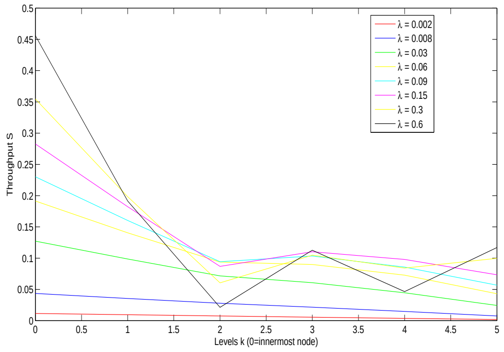

Figure 10: Throughput characteristics of a multihop network

IV STUDY OF THROUGHPUT CHARACTERISTICS OF A MULTI-HOP NETWORK

Here we study the throughput characteristics of the nodes as their distance from the central sink (node 0) varies. As the number of nodes increase, the mathematical analysis of such a system becomes exceedingly cumbersome. We therefore carry out the study via network simulations. It may be noted that, the *multihop* forwarding study in 802.15.4 network using ns-2 has never been carried out before. In our implementation, several issues in ns-2 had to be first rectified* before the multihop forwarding study could be carried out.

As a first step, we consider a simple chain topology similar to the one shown in figure 1, where the number of traffic generating nodes are now increased to 6 (instead of 3). The resulting throughput characteristics are plotted in figure 10. At lower levels of traffic as we proceed to the right, i.e., toward node 0, we see a monotonic increase of throughput as expected due to traffic aggregation. However, as the traffic begins to saturate an interesting *wave like* characteristics begin to develop. The alternating increase and decrease of throughput can be attributed to the hidden/exposed terminals effect. A lower throughput implies more collisions or channel busy state. Since the node with a lower throughput finds the channel busy most of the time, it transmits less often (e.g., node 2 in figure 10). This has an positive impact on the neighboring node (node 3) which now suffers less from the hidden terminal effect. As a result, it has a higher throughput.

The wave pattern of throughput variation in a multihop IEEE 802.15.4 network basically shows the unfairness of such a protocol at high traffic rates. These characteristics also lead to non-uniform consumption of energy amongst the alternating nodes. Thus, we can infer that the protocol is not suited for multihop transmission at high traffic rates.

V CONCLUSION

In this paper we provided an analytic model of throughput performance of an IEEE 802.15.4 network in presence of hidden/exposed terminals. First, our analysis captured the performance of a one-hop cluster. Then we extended the model to a multihop cluster, where the central sink is reached via multiple hops. In the analysis, certain simplifying, however weak, assumptions were made, which served as a way to analytically extend the single-hop results to the multihop case. The accuracy of the throughput model was verified via *ns-2* simulations. Our *ns-2* simulation based studies of a multihop 802.15.4 network also brought out certain weaknesses of the protocol under specific traffic conditions.

The analysis can be further extended to capture the nodal energy consumption and network lifetime, thereby aiding network planning and deployment. As a future work, we also plan to conduct more simulations to study the throughput performance in a generalized many-to-one multihop forwarding in a randomly deployed network.

ACKNOWLEDGMENT

This research was supported by the Department of Science and Technology (DST) under the grant nos. SR/S3/EECE/054/2007 and SR/S3/EECE/073/2008, and the Council of Scientific and Industrial Research (CSIR) under the grant no. 22/448/07/EMR-II.

REFERENCES

[1] Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs), IEEE Std 802.15.4, 2003.

[2] E. Callaway, P. Gorday, and L. Hester. Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks. *IEEE Commun. Mag.*, 2002.

[3] R. L. Disney, R. L. Farrell, and P. Renato de Morais. A characterization of M/G/1 queues with renewal departure processes. *Management Science*, 1973.

[4] C. T. Ee and R. Bajcsy. Congestion control and fairness for many-to-one routing in sensor networks. In *Proc. ACM Sensys*, Baltimore, MD, USA, Nov. 2004.

[5] A. El-Hoiydi. Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks. In *Proc. IEEE ICC*, Apr. 2002.

[6] K. Leibnitz, N. Wakamiya, and M. Murata. Modeling of IEEE 802.15.4 in a cluster of synchronized sensor nodes. In *Proc. Intl. Teletraffic Congress*, pages 1345–1354, Beijing, China, Aug. 2005.

[7] S. Madden, M. Franklin, J. Hellerstein, and W. Hong. TAG: A tiny aggregation service for ad hoc sensor networks. In *Proc. OSDI*, Boston, MA, USA, Dec. 2002.

[8] J. Misic, S. Shafi, and V. B. Misic. Performance of a beacon-enabled IEEE 802.15.4 cluster with downlink and uplink traffic. *IEEE Trans. Parallel and Distrib. Syst.*, 17(4):361–376, Apr. 2006.

[9] T. R. Park, T. H. Kim, J. Y. Choi, and W. H. Kwon. Throughput and energy consumption analysis of IEEE 802.15.4 slotted CSMA/CA. *Electron. Lett.*, 41(18):1017–1019, Sept. 2005.

[10] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In *Proc. ACM SenSys*, Baltimore, MD, USA, Nov. 2004.

[11] I. Ramachandran, A. Das, and S. Roy. Analysis of the contention access period of IEEE 802.15.4 MAC. *ACM Trans. Sensor Networks*, 3(1):1–29, Mar. 2007.

[12] S. M. Ross. *Introduction to Probability Models*. Academic Press, 2007.

[13] V. Tarau and C. Weyer. Long-term reliable data gathering using wireless sensor networks. In *Proc. 4th Intl. Conf. on Networked Sensing Systems*, pages 252–259, Braunschweig, Germany, June 2007.

[14] W. Ye, J. Heidemann, and D. Estrin. An energy-efficient MAC protocol for wireless sensor networks. In *Proc. IEEE INFOCOM*, pages 1567–1576, New York, NY, USA, June 2002.

---

*The authors can be contacted for the modified *ns-2* code