

Energy Saving Routing Approach In Wireless Sensor Networks

Anjali¹, Sunaina²

¹M.Tech Scholar, Electronics and Communication Engineering, IIET Kinana, Jind, Haryana, India.

²Assistant Professor, Electronics and Communication Engineering, IIET Kinana, Jind, Haryana, India.

Correspondions Autour : Anjali

Abstract: Different schemes or algorithms that are implemented at the network layer or at the physical layer of TCP/IP to endorse energy saving so that the network of any system remains sustainable for long time. The techniques discussed in the paper uses the history based contention window control over packet routing in the network layer. The main idea behind this scheme is to control the time of every node which delivers the packet but if in case the proximity node or network does not accept the incoming packets because it is busy, then the transmitter node has to either wait or it tries randomly to deliver the same. This causes the whole system to use more of its energy and this is the main reason that conventionally many other protocols are not good for the system. But our system and our history based contention window control scheme has proved to be worthy as it is good in terms of the time allocation providing the system either to wait or to access other node for the transmission of the system. The energy being consumed has reduced considerably and the efficiency and throughput has increased because of reduced energy consumption.

Keywords: WSN, DARPA, SOSUS, LEACH, HEED, AMRP, CLUDDA

Date of Submission: 15-06-2018

Date of acceptance: 30-06-2018

I. INTRODUCTION

Wireless Sensor Networks consists of individual nodes that are able to interact with their environment by sensing or controlling physical parameter; these nodes have to collaborate in order to fulfill their tasks as usually, a single node is incapable of doing so; and they use wireless communication to enable this collaboration [1]. The definition of WSN, according to, Smart Dust program of DARPA is: "A sensor network is a deployment of massive numbers of small, inexpensive, self powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" [2].

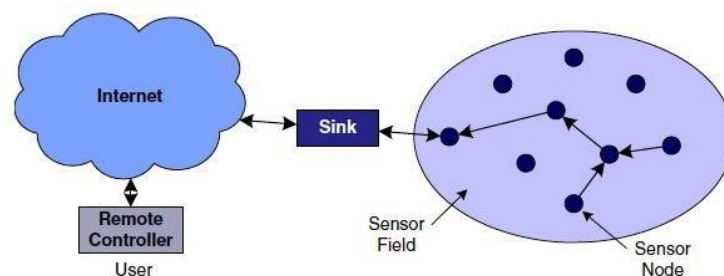


Fig. 1: A typical WSN

1.1 Evolution of Sensor Network

Sensor network development was initiated by the United States during the Cold War [3]. A network of acoustic sensors was placed at strategic locations on the bottom of the ocean to detect and track Soviet submarines. This system of acoustic sensors was called the Sound Surveillance System (SOSUS). Wireless networks based upon IEEE 802.11 standards [4] can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer. The organization has defined the IEEE 802.15 standard [7] for personal area networks (PANs), with "personal networks" defined to have a radius of 5 to 10 m.

1.2 Wireless Sensor Network Model

Unlike their ancestor ad-hoc networks, WSNs are resource limited, they are deployed densely, they are prone to failures, the number of nodes in WSNs is several orders higher than that of ad hoc networks, WSN network topology is constantly changing, WSNs use broadcast communication mediums and finally sensor nodes don't have a global identification tags [15]. The major components of a typical sensor network are:

- **Sensor Field:** A sensor field can be considered as the area in which the nodes are placed.
- **Sensor Nodes:** Sensors nodes are the heart of the network. They are in charge of collecting data and routing this information back to a sink [8].
- **Sink:** A sink is a sensor node with the specific task of receiving, processing and storing data from the other sensor nodes. They serve to reduce the total number of messages that need to be sent, hence reducing the overall energy requirements of the network. Sinks are also known as data aggregation points [5, 6].

II. ROUTING IN WIRELESS SENSOR NETWORKS

Routing is a process of determining a path between source and destination upon request of data transmission. In WSNs the network layer is mostly used to implement the routing of the incoming data. It is known that generally in multi-hop networks the source node cannot reach the sink directly. So, intermediate sensor nodes have to relay their packets. The implementation of routing tables gives the solution. These contain the lists of node option for any given packet destination. Routing table is the task of the routing algorithm along with the help of the routing protocol for their construction and maintenance [9].

2.1 Routing Challenges and Design Issues

Depending on the application, different architectures and design goals/constraints have been considered for sensor networks. Since the performance of a routing protocol is closely related to the architectural model [11].

- Network dynamics
- Node deployment
- Energy considerations
- Data delivery models
- Node capabilities
- Data aggregation/fusion

2.2 Routing Objectives

Some sensor network applications only require the successful delivery of messages between a source and a destination. However, there are applications that need even more assurance. These are the real-time requirements of the message delivery, and in parallel, the maximization of network lifetime.

2.3 Characteristics of Routing Protocols

Generally routing protocols are: Application specific; Data centric; capable of aggregating data; Capable of optimizing energy consumption [10].

III. APPROACH USED IN THE RESEARCH WORK

As described in the previous section, it is inefficient for sensor nodes to transmit the data directly to the BS in energy-constrained WSNs of large size. In the past few years wireless network has developed much and many works has been done to increase its performance. Most of them has been done on the basis of 2-D Markov chain model. An intuitive mathematical analysis and simple equations were presented for throughput and packet delay performance of IEEE 802.11 DCF by utilizing a Markov chain model by [11] which is presented below. Markov Chain Model Assumptions are as follows.

- Packets can encounter collisions only due to simultaneous transmissions (no transmission errors)
- There are no hidden stations (all stations can hear others transmissions).
- The network consists of a finite number of contending stations.
- Saturated conditions, i.e. a station have always data ready for transmission.
- The collision probability of a transmitted packet is constant and independent of the number of retransmissions.

The authors in [12], have evaluated the dependency of the RTS/CTS scheme on network size, however, without providing any general expression for the RTS/CTS threshold. But works in [11] and [7] has pointed out that the RTS/CTS handshake does not work as well as expected in theory. Approaches to fix the value of RT can be clustered main lying two types; Dynamic and Static. Authors in has performed analysis to determine RT

values for maximum performance and proposed static value $[RT = 0]$ for all nodes, considering only single hop environment. In others, such as in [13] and [14] packet delivery ratio or transmission probability is emphasized.

IV. PROBLEM IDENTIFICATION & ISSUES

The current cellular networks are classified as the infrastructure dependent networks. The path setup between two nodes is completed through the base station. Ad hoc wireless networks are capable of operating without the support of any fixed infrastructure. The absence of any central control system makes the routing complex compared to cellular networks. The path setup between two nodes in ad hoc network is done through intermediate nodes. For the distributive system to work the mobile nodes of ad hoc network are needed to be more complex than that of cellular networks.

4.1 HIDDEN TERMINAL PROBLEM

Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes. Take a physical star topology with an access point with many nodes surrounding it in a circular fashion: Each node is within communication range of the AP, but the nodes cannot communicate with each other, as they do not have a physical connection to each other. In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as A, can see the access point; but it is unlikely that the same node can see a node on the opposite end of the access points range, B. These nodes are known as hidden. The problem is when nodes A and B start to send packets simultaneously to the access point. Since node A and B cannot sense the carrier, carrier sense multiple access with collision avoidance (CSMA/CA) does network, and collisions occur, scrambling data.

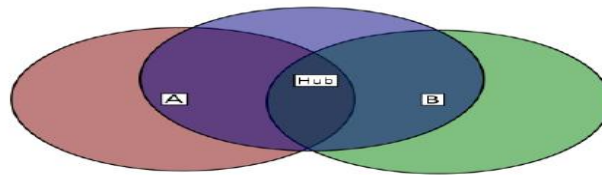


Fig. 2: Hidden Terminal Problem

To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme.

4.2 EXPOSED TERMINAL PROBLEM

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter. Consider an example of 4 nodes labeled R1, S1, S2, and R2, where the two receivers are out of range of each other, yet the two transmitters in the middle are in range of each other.

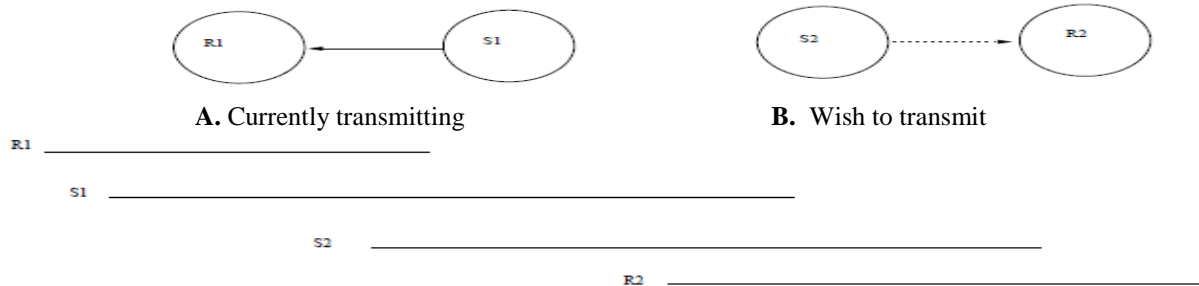


Fig. 3: Exposed Terminal Problem

Here, if a transmission between S1 and R1 is taking place, node S2 is prevented from transmitting to R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor S1. However note that R2 could still receive the transmission of S2 without interference because it is out of range from S1.

4.3 ADVANTAGES OF RTS-CTS MECHANISM

- To reduce frame collisions introduced by the hidden terminal problem.
- Originally the protocol fixed the exposed terminal problem as well, but modern RTS/CTS include ACKs and do not solve the exposed terminal problem. This mechanism helps to solve this problem only if the nodes are synchronized. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes.

4.4 DISADVANTAGES OF RTS-CTS MECHANISM

- Inhibiting Non-interfering Parallel Transmission
- False Blocking
- Virtual Jamming

4.5 RTS THRESHOLD VALUE

We can adaptively set the value of RTS-Threshold based on network traffic then inter mixing these two schemes can be easily achieved. Our main proposal is too use basic scheme for relatively small sized packets and use RTS/CTS mechanism for relatively large size packets. To incorporate this idea, the value of RTS-Threshold needs to be intelligently set to a value such that $\eta \times 100$ percent of packet's size fall below that value. Mathematically it can be described as follows: suppose the sizes of packets owing through a node are $s_1, s_2, s_3 \dots s_n$ (in ascending sorted order) with probability $P_1, P_2 \dots P_3$. Then the value of RTS-Threshold is set to a value such that:

$$P_r\{S \leq \text{RTS-Threshold}\} = \eta \quad (4.1)$$

where S is a random variable denoting packet size. A node at first learns the sizes of the packets it is generating or forwarding as an intermediate node for a certain time interval. Then it sets the value of RTS-Threshold for the next interval using the above equation. It also continues that its learning process in the subsequent intervals and adjusts the RTS-Threshold dynamically from one interval to another.

Let us denote P_i be the probability that a packet's size is less than or equal to s_i . Then, mathematically:

$$P_i = P_r\{S \leq s_i\} = \left(\frac{\sum_{j=1}^i f_j}{\sum_{k=1}^n f_k} \right) \quad (4.2)$$

Note that using the above equation $P_i = 1$. Actually P_i is the cumulative distribution function (CDF) for the different packet sizes. Using this CDF, calculation of new RTS-Threshold is pretty simple. Let, P_r is the greatest probability less than η , P_s is the packet size at P_r , C_r is the least probability greater than η , and C_s is the packet size at C_r .

Using linear interpolation the trafficobserver calculates the current RTS-Threshold using the equation below:

$$RT_{current} = \left\lfloor P_s + \frac{(\eta - P_r) * (C_s - P_s)}{(C_r - P_r)} \right\rfloor \quad (4.3)$$

The average RTS-Threshold is updated as

$$RT_{average} = \left\lfloor \alpha * RT_{preview} + (1 - \alpha) * RT_{current} \right\rfloor \quad (4.4)$$

where, $RT_{preview}$ =previous RTS-Threshold and α controls the relative weight of recent and past history of RTS-Threshold calculation. The value of α lies between 0 to 1.

V. FORMULATION AND PRESENTATION OF THE PROBLEM

We assume that the noise over the wireless channel is white Gaussian with spectral density equal to $N_0=2$. In our model we define N_0 as the power of the thermal noise:

$$N_0 = N_t * N_f \quad (5.1)$$

Where N_f denotes the circuit noise value, k the Boltzmann constant, T the temperature in Kelvin and W is the frequency bandwidth. For the BPSK modulation, the bit error probability is given by [7]:

$$P_b^{BPSK} = Q\left(\sqrt{\frac{2 * E_b}{N_0}}\right) \quad (5.2)$$

and for QPSK (4-QAM) is:

$$P_b^{BPSK} = Q\left(\sqrt{\frac{2 * E_b}{N_0}}\right) - Q^2\left(\sqrt{\frac{2 * E_b}{N_0}}\right) \quad (5.3)$$

Where E_b/N_0 is the average signal to noise ratio per bit. The E_b/N_0 of the received signal is derived from SNR using the following relationship:

$$\frac{E_b}{N_0} = SNR \cdot \frac{W}{R_b} \quad (5.4)$$

where R_b (1 and 2 Mbps) is the maximum bit rate of transmission mode and W (2 MHz) is the spread bandwidth of the signal. Considering the data packet format shown in the probability of error for packet is:

$$p = PER = 1 - (1 - P_e^{PLCP} - P_e^{payload}) \quad (5.5)$$

where P_e is the probability of error for PLCP (or Payload) and is given by:

$$P_e = 1 - (1 - P_b) \quad (5.6)$$

P_b is derived from equation 2 and 3 for 1 Mbps and 2Mbps data rate respectively.

5.1 MODEL APPROACH

In this Bianchi model, the time is divided into slots of variable duration based on what happens during a slot: no transmission, correct transmission, collision. The model computes among others the probability that a station transmits in a slot τ , the probability that a transmitted packet collides with other transmissions p , and the saturation throughput of a station $Z(p; \tau)$, which is a function of τ and p as well as other physical parameters. The packet loss probability is computed as:

$$p = 1 - (1 - \tau)^{n-1} \quad (5.7)$$

Where n is the total number of STAs. The model also gives the expression of τ as a function of the packet loss probability p using the Markov chain that describes the system. Let B be the function relating p and τ in this model, then:

$$\tau = B(p) = \frac{1-p^{m+1}}{1-p} b_{0,0} \quad (5.8)$$

$b_{0,0}$ (Which is the stationary probability to find the Markov chain in state (0; 0)) can be obtained from solving the Markov chain as shown in Equation (5.9). Equations (5.7) and (5.8) are solved for the values of p and τ . Once these probabilities are obtained, this model computes the saturation throughput $Z(p, \tau)$ of a station. None of the above models have considered the channel characteristics (PHY layer).

5.2 DISTANCE AWARE MODEL

Using Equation (5.5), the packet loss probability can be computed as follow:

$$p_k = 1 - (1 - P_b^{PLCP})^{L_{PLCP}} \cdot (1 - P_b^{payload})^{L_{payload}}, \quad (5.9)$$

where $PLCP$ and $L_{payload}$ are PLCP and Payload length respectively, and $P_x b$ is bit error probability for part x of the packet (PLCP or Payload). $P_x b$ can be computed using Equation (5.2) and (5.3) considering transmission mode.

Next step we look for the power of signal transmitted by STA i at the AP. We denote such power with X_i and we define it as:

$$X_i = Y_i \cdot L(D_i), \quad (5.10)$$

where $L(D_i)$ expresses the power with which the signal of STA i arrives at the AP after being attenuated over distance D_i and calculated using simple path loss model:

$$L(D_i) = \frac{P_0}{D_i^\alpha}. \quad (5.11)$$

Having the power of each STA at the AP, we can compute the interfering power a packet transmitted by STA k faces. We denote this power by I_k and write it as:

$$I_k = \sum_{i \neq k}^n Y_i \cdot L(D_i). \quad (5.12)$$

This allows writing the following expression for the SNR at the AP of a packet/signal coming from STA k at the given distance dk :

$$SNR_k = \frac{L(d_k)}{N_o + I_k} = \frac{L(d_k)}{N_o + \sum_{i \neq k}^n Y_i \cdot L(D_i)} . \quad (5.13)$$

Assuming independence of Y_i , as in the Bianchi model, $f_{I_k}(x)$ can be expressed as an $n - 1$ convolution:

$$f_{I_k}(x) = f_{X_1} \otimes \dots \otimes f_{X_{k-1}} \otimes f_{X_{k-2}} \otimes \dots \otimes f_{X_n}(x) . \quad (5.14)$$

In the analysis above, we kept the distance from STA i to the AP random denoted by D_i , except for STA k for which we are computing p_k . Then we compute p_k for two cases. First, we compute it when the stations' positions are known (the D_i are deterministic): the only randomness in this case lies in the dynamics of the MAC layer. Second, we compute p_k for a more general case where nodes are uniformly distributed in the plane.

5.3 FIXED TOPOLOGIES

Suppose we are given the distance vector $D = \{d_1; \dots; d_n\}$, where d_i describes the distance of STA i to the access point. Since all distances are fixed, we omit in this section the index of distance from loss and transmission probabilities. For an STA k , we aim at finding the *pdf* of I_k . I_k gives the interfering power produced by all the other STAs at the AP. To compute I_k , we need $f_X(x)$, the *pdf* of the power at the AP of an individual STA. For an STA i , $f_{X_i}(x)$ can be written as:

$$f_{X_i}(x) = \delta_x(0)(1 - \tau_i) + \delta_x(L(d_i))\tau_i , \quad (5.15)$$

5.4 RANDOM TOPOLOGIES

We consider now the case where the STAs are uniformly distributed in a disk of radius r around the AP. Thus, the *pdf* of D (the distance to the AP of an STA) has the following form:

$$f_D(d) = \{1_{0 \leq d \leq r}\} \frac{2d}{r^2} \quad (5.16)$$

5.5 THROUGHPUT CALCULATION

We now derive the throughput of a single STA k at given distance dk . In the case of a fixed topology this throughput depends on the position of all other STAs and their transmission probabilities $\tau_{i,i}$,

$$P_k = 1 - \int_{x=0}^{\infty} (1 - Q\left(\sqrt{\frac{2L(d_k)W}{(N_o + x)R}}\right))^{L_{PLCP} + L_{Payload}} f_{I_k}(x) dx . \quad (5.17)$$

$$F_{X_i}(x) = (1 - E[\tau_i(D_i)]) + 1_{\{P_0/r^\alpha \leq x \leq P_0\}} E[\tau_i(D_i)] \left(1 - \frac{(L^{-1}(x))^2}{r^2}\right) . \quad (5.18)$$

$$f_{X_i}(x) = \delta_x(1 - E[\tau_i(D_i)]) + 1_{\{P_0/r^\alpha \leq x \leq P_0\}} \frac{2}{\alpha r^{2\alpha}} \left(\frac{P_0}{x}\right)^{\frac{2}{\alpha}} E[\tau_i(D_i)] . \quad (5.19)$$

In case of random topologies, the throughput depends on the other STAs average location and their average transmission probability $E[\tau_{i,i}(D_i)]$. Consider first the case of fixed topology. The throughput of an STA k is given by the function $Z(p_k; \tau_{i,i})$, which has the following form:

$$Z(p_k, \tau_k) = \frac{\tau_k(1 - p_k)L}{(1 - P_{tr})\sigma + P_{tr}P_sT_s + P_{tr}(1 - P_s)T_c} \quad (5.20)$$

ACKNOWLEDGEMENT

I would like to express my special appreciation and thanks to my Research Guide Mrs. Sunaina, Assistant Professor (IET Kinana, Jind, Haryana) who has been tremendous guide for me. I would like to thank her for encouraging me for research and allowing me to grow as a researcher as this advice has been priceless for my career. I would also like to thank all of my teachers & family those supported me in writing and incited me to strive towards my goal.

REFERENCES

- [1] Akyildiz, I., Su, W. and Sankarasubramaniam, Y., 2002. "A survey on sensor networks", *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114.
- [2] Kumar, R., Khanna, D.R., Verma, P., and Jangra, S. (2012). A study of diverse wireless networks. *IOSR Journal of Engineering (IOSRJEN)*. e-ISSN: 2250-3021. p-ISSN: 2278-8719. 2(11). pp. 01-05.
- [3] Yick, J., Mukherjee, B. and Ghosa, D., 2008. "Wireless sensor network survey", *Computer Networks*, vol. 52, no. 12, pp. 2292–2230.

- [4] Wattenhofer, R., Li, L., Bahl P., and Wang Y., 2001. "Distributed topology control for power efficient operation in multihop wireless ad hoc networks", in Proc.IEEE InternationalConference on Computer Communications INFOCOM2001,Anchorage, USA, pp. 1388–1397.
- [5] Kumar, R., Khanna, D.R., and Verma, P. (2014). Middleware Architecture of VASNET and its Review for Urban Monitoring & Vehicle Tracking. International Journal of Emerging Research in Management & Technology. ISSN: 2278-9359. 3(1). pp. 41-45.
- [6] Kumar, R., Khanna, D.R., Verma, P., and Surender. (2013). A Proposed work on Node Clustering & Object Tracking Processes of BFOA in WSN. International Journal of Computer Science & Communication. ISSN: 0973-7391. 4(2). pp. 207-212.
- [7] Younis, O., Krunz, M., and Ramasubramanian, S., 2006 "Node clustering in wireless sensor networks: recent developments and deployment challenges", IEEE Netw., vol. 20, no. 3, pp. 20–25.
- [8] Sharma, R., Garg, M. and Sharma, P. (2013). Secure aggregation in Wireless Sensor Networks: A review. International journal of Advanced research in computer science (IJARCS). ISSN 0976-5697. 4(11). pp. 86-92.
- [9] Kumar, R., Vats, J., and Kumar, A. (2011). A Comparative Study of Routing Protocols. International Journal of Computer Science and Information Technologies (IJCSIT) ISSN 0975 – 9646. 2(5). pp. 1962-1964.
- [10] Kumar, R., Khanna, D.R., Verma, P., and Jangra, S. (2013). Comparative Analysis and Study of Topology Based Routing Protocols for Vehicular Ad-hoc Networks. 2nd National Conference on Advancements in the Era of Multi Disciplinary Systems (AEMDS-2013) Proceedings Published in ELSEVIER. ISBN: 978-93-5107-057-3. pp. 775-778.
- [11] Chee-Yee, C. and Kumar, S. P., 2003. "Sensor networks: evolution, opportunities, and challenges", Proceedings of IEEE, vol. 91, no. 8, pp. 1247–1256.
- [12] Alemdar, H. and Ersoy, C., 2010. "Wireless sensor networks for healthcare: a survey", Computer Networks, vol. 54, no. 15, pp. 2688–2710.
- [13] Pantazis, N. A. and Vergados, D., 2007. "A survey on power control issues in wireless sensor networks", IEEE Commun. Surveys Tuts., vol. 9, no. 4, pp. 86–107.
- [14] Chang, J. H. and Tassiulas, L., 2000. "Energy conserving routing in wireless adhoc networks", Proc. IEEE International Conference on ComputerCommunications INFOCOM2000, Tel-Aviv, Israel, pp. 22–31.
- [15] Kuorilehto, M., Hannikainen, M. and Hamalainen T. D., 2005. "A survey of application distribution in wireless sensor networks", EURASIP Journal onWireless Communications and Networking, vol. 2005, no. 5, pp. 774–778.

Anjali "Energy Saving Routing Approach in Wireless Sensor Networks "IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 6, 2018, pp. 42-48