# An Energy Efficient Ring Routing Protocol in Wireless Sensor Network with Cocowa techniques

[1]K.VIJAYA AP, [2]T.MANOJ, [3]E.MANJULA, [4]S.MAYILSAMY
[1,2,3,4] ERODE
[1,2,3,4] INFORMATION TECHNOLOGY DEPARTMENT
VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY, ERODE, INDIA

***Abstract*--In a typical wireless sensor network (WSN), the batteries of the nodes near the sink deplete quicker than other nodes due to the data traffic concentrating towards the sink, leaving it stranded and disrupting the sensor data reporting. To mitigate this problem, mobile sinks are proposed. They implicitly provide load-balanced data delivery and achieve uniform-energy consumption across the network. Along with this routing protocol an approach is proposed to detect selfish nodes in the network. The proposed collaborative contact-based watchdog (CoCoWa) approach is based on the spreading of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. In this collaborative approach reduces the time and increases the precision when detecting selfish nodes.**

***Keywords*-- Wireless Sensor Network, Mobile sink, selfish nodes, data dissemination, energy efficiency, mobility.**

---

## I. INTRODUCTION

In wireless sensor networks (WSNs), energy efficiency is considered to be a crucial issue due to the limited battery capacity of the sensor nodes. Iintrinsic property of WSNs is that the network should be able to operate without human intervention for an adequately long time, since replacing the batteries of the sensor nodes requires significant effort. Due to the converge cast nature of traditional WSN packet forwarding approaches resulting in the concentration of data traffic towards the sinks, the nodes in the vicinity of the static (immobile) sinks are more likely to deplete their batteries before other nodes, leading to the energy hole problem , disruptions in the topology and reduction in the sensing coverage. Moreover, this problem could lead to the isolation of the sinks, hindering the delivery of the sensor data traffic. Mobile sinks are proposed and explored as a possible solution to this problem. Load-balancing is implicitly provided by the sink mobility, shifting the hotspots around the sinks and spreading the increased energy drainage around the sink, achieving uniform energy consumption that extends the network lifetime. . Mobile nodes can directly communicate with each other if a contact occurs. Thus, in the real world, nodes could have selfish behavior, being unwilling to forward packets for others. Selfishness means that some nodes refuse to forward other nodes' packets to save their own resources.

Sink mobility also has security benefits where the mobility makes the sinks more difficult to compromise than static sinks. The sink mobility brings about the problem of sink localization, requiring frequent advertisement of the changing sink position across the network. This operation may result in a significant overhead, which should be minimized to benefit from the energy savings introduced by the mobile sinks. An effective mobile sink routing protocol should also avoid an extreme increase in the sensor data delivery latencies.

In Cooperative networking is currently receiving significant attention as an emerging network design strategy for future mobile wireless networks. Successful cooperative networking can prompt the development of advanced wireless networks to cost-effectively provide services and applications in contexts such as vehicular ad hoc networks (VANETs) or mobile social networks [6]. Two of the basic technologies that are considered as the core for these types of networks are mobile ad-hoc networks (MANETs) [7] and opportunistic and delay tolerant networks (DTNs). The cooperation on these networks is usually contact based. The literature provides two main strategies to deal with selfish behavior: a) motivation or incentive based approaches, and b) detection and exclusion. The first approach, tries to motivate nodes to actively participate in the forwarding activities. The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented. Essentially, watchdog systems overhear wireless traffic and analyses it to decide whether neighbor nodes are behaving in a selfish manner. When the watchdog detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non selfish node). Nevertheless, watchdogs can fail on this detection, generating false positives and false negatives that seriously degrade the behavior of the system.

The sink position information obtained by a sensor node [5] loses its freshness, the sensor data is relayed through the old anchor nodes to the current anchor node, preventing packet losses. Ring Routing does not have any MAC layer requirements except the support for broadcasts. Ring Routing is suitable for both event-driven and periodic data reporting applications. It is not query based so that data are disseminated reliably as they are generated. Ring Routing provides fast data delivery due to the quick accessibility of the proposed ring structure, which allows the protocol to be used for time sensitive applications.

## II. RELEATED WORK

Kemal Akkaya and Mohamed Younis [1] describes the Routing in sensor networks has attracted a lot of attention in the recent years and introduced unique challenges compared to traditional data routing in wired networks. In this paper, we have summarized recent research results on data routing in sensor networks and classified the approaches into three main categories, namely data-centric, hierarchical and location-based. Data-centric protocols are query-based and depend on the naming of desired data, which helps in eliminating many redundant transmissions. Hierarchical protocols aim at clustering the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy. Location-based protocols utilize the position information to relay the data to the desired regions rather than the whole network. The last category includes routing approaches that are based on general network-flow modelling and protocols that strive for meeting some QoS requirements along with the routing function.

Pietro Michiardi and Refik Molva[2] described in this section is used as a basis for the security mechanism that solves the problems due to misbehaving nodes by incorporating a reputation mechanism that provides an automatic method for the social mechanisms of reputation. Furthermore the formulae presented in the following sections are conceived in order to minimize problems due to false detection of a nodes' misbehaviour. As an example, disadvantaged nodes that are inherently selfish due to their precarious energy conditions shouldn't be excluded from the network using the same basis as for malicious nodes: this is done with an accurate evaluation of the reputation value that takes into account a sporadic misbehaviour.

Can Tunca[3] describes the energy efficiency is the most important issue for wireless sensor networks (WSN) since sensor nodes have limited batteries. Replacing the batteries of sensor nodes is likely to require significant effort therefore; WSNs have to be able to operate without human intervention for an adequately long time. In WSNs with static (immobile) sinks, the nodes close to the sinks are more likely to deplete their battery supplies before other nodes due to the intersection of multi- hop routes and concentration of data traffic towards the sinks. This problem is referred to as the hotspot problem. Node deaths would lead to disruptions in the topology and reduction of sensing coverage. Moreover, sinks could become isolated and sensor data generated across the network would no longer be obtained. Therefore, routing protocols designed for immobile sinks have to incorporate load-balancing in order to achieve uniformity of energy consumption throughout the network.

Enrique Hernández-Orallo[4]describes the Watch dog, watchdog has two functions: the detection of selfish nodes and the detection of new contacts. The detection of selfish nodes can generate the following events about neighbour nodes: PosEvt (positive event) when the watchdog detects a selfish node, NegEvt (negative event) when the watchdog believes that a node is not selfish, and NoInfEvt (no info event) when the watchdog does not have enough information about a node. The detection of new contacts is based on neighbourhood packet overhearing; thus, when the watchdog starts receiving packets from a new node it is assumed to be a new contact, and so it generates an event to the network information module shown in figure 1.

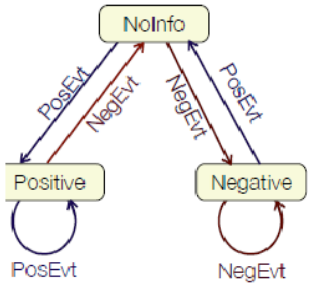


**Figure 1**

## III. SYSTEM ADVANTAGE

The proposed system includes Mobile sink for load balanced data delivery across the network and solving the problem to detect selfish nodes in the Ring routing. The proposed collaborative contact-based watchdog (CoCoWa) approach is based on the spreading of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. The proposed system has following advantages.

- Delay of forwarding packets is reduced.
- Energy consumption is reduced using mobile sink routing.
- Less Latency, Network lifetime is increased.

## IV. ARCHITECTURE

*Ring routing*

Ring Routing, a novel hierarchical routing protocol for wireless sensor networks with a mobile sink. The protocol imposes three roles on sensor nodes: ring node, regular node, and anchor node. The basis of Ring Routing is (i) advertisement of sink position to the ring, (ii) regular nodes obtaining the sink position information from the ring whenever necessary, and (iii) nodes

disseminating their data via the anchor nodes, which serve as intermediary agents connecting the sink to the network. Three simple assumptions are made before going into the details of the protocol:

- Sensor nodes are aware of their own positions. The position information may be based on a global or a local geographic coordinate system defined according to the deployment area. Determining the position of the nodes might be achieved using a satellite based positioning system such as global positioning system (GPS) or one of the energy-efficient localization methods proposed specifically for WSNs.
- Every sensor node should be aware of the position of its neighbours. This information enables greedy geographic routing and can be obtained by a simple neighbour discovery protocol.
- The coordinates of a network centre point has to be commonly known by all sensor nodes. The network centre does not have to be exact and can be loaded into the sensors' memories before deployment. The ring structure encapsulates the network centre at all times, which allows access to the ring by regular nodes and the sink. The network centre is marked with an "X" in various example ring structures like a) small, b) medium, c) large, d) Imperfect in figure 2.

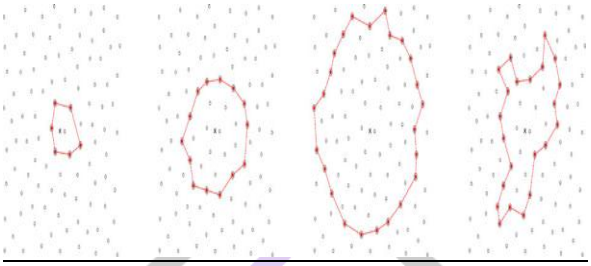

**Figure 2**

*Ring construction*

The ring consists of a one-node-width, closed strip of nodes that are called the ring nodes. As long as the ring encapsulates the pre-determined network center, it can change. The shape of the ring might be imperfect as long as it forms a closed loop. After the deployment of the WSN, the ring is initially constructed by the following mechanism: An initial ring radius is determined. The nodes closer to the ring, which is defined by this radius and the network center, by a certain threshold are determined to be ring node candidates. Starting from a certain node (e.g. the node closest to the leftmost point on the ring) by geographic forwarding in a certain direction (clockwise/counter clockwise), the ring nodes are selected in a greedy manner until the starting node is reached and the closed loop is complete. If the starting node cannot be reached, the procedure is repeated with selection of different neighbour's at each hop. An example ring construction scenario is depicted in figure 3.

Ring construction is dependent on the location information of the nodes, which is known to contain some inaccuracy based on the utilized technology. In order to provide evidence for the localization error tolerance of Ring Routing, we applied a Monte-Carlo analysis to determine the successful ring construction probability under varying degrees of localization error. In our analysis, we assumed that 200 nodes are uniformly deployed over an area of size 600m x 600 m where the communication ranges of the nodes are assumed to be 80 m and the default ring radius is set to 150m. We modelled the localization error as 2D Gaussian distribution where the mean error is varied as presented. For each corresponding error value, we sampled 20K WSN topology instances and booked the number of successful ring constructions.

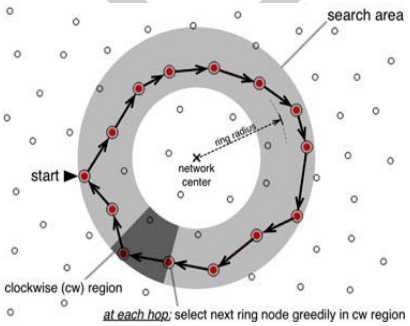


**Figure 3**

*Obtain sink position*

A source node, that has data available, has to obtain the position of the AN(Anchor Node) before disseminating data to the sink. The fresh position of the AN is stored in the ring. In order to retrieve it, a mechanism similar to the delivery of ANPI packets to the ring is used. The source node sends an AN Position Information REQuest (ANPIREQ) packet towards

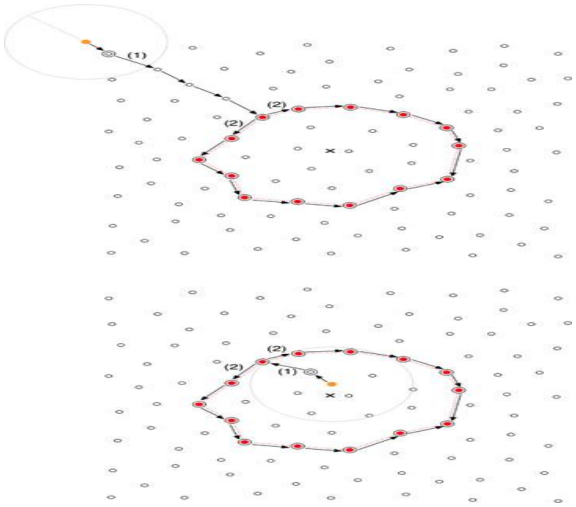

**Figure 4**

AN position advertisement. Figure 4 (a) Sink is outside the ring and (b) Sink is inside the ring (towards the network centre if the node is outside the ring, away from the network centre if it is inside the ring). The source node's position is also included in the ANPIREQ packet. The ring node receiving the ANPIREQ packet generates an AN Position Information RESPonse (ANPIRESP) packet which contains the current AN's position and sends it to the source node making the request via geographic routing, by using the position of the source node retrieved from the ANPIREQ packet. Upon reception of the ANPIREQ packet, the source node learns the position of the AN and can now send its data towards it. The pseudocodes of the procedures for handling ANPIREQ and ANPIRESP packets.

```
1: procedure PROCESSANPIPACKET(ANPIpacket)
2:     if role = regularnode then
3:         record anchor node position and MAC address information
4:         if ringnode ∈ neighbors then
5:             send ANPIpacket to ringnode
6:         else
7:             destinationPosition ← ANPIpacket.destinationPosition
8:             GEOGRAPHICROUTING(ANPIpacket, destinationPosition)
9:         end if
10:    else if role = ringnode then
11:        record anchor node position and MAC address information
12:        create ANPISpacket
13:        set anchor node position and MAC address information in ANPISpacket
14:        send a copy of ANPISpacket to cwringneighbor
15:        send another copy of ANPISpacket to ccwringneighbor
16:    end if
17: end procedure
18: procedure GEOGRAPHICROUTING(packet, destinationPosition)
19:    for all n ∈ neighbors do
20:        if distance(n.position, destinationPosition) < minDistance then
21:            minDistance = distance(n.position, destinationPosition)
22:            targetnode ← n
23:        end if
24:    end for
25:    send packet to targetnode
26: end procedure
```

Pseudo code for processing ANPI packets.

*Cocowa architecture*

A selfish node usually denies packet forwarding in order to save its own resources. This behaviour implies that a selfish node neither participates in routing nor relays data packets. A common technique to detect this selfish behaviour is network monitoring using local watchdogs. A node's watchdog consists on overhearing the packets transmitted and received by its neighbours in order to detect anomalies, such as the ratio between packets received to packets being retransmitted. By using this technique, the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not). It is based on the combination of a local watchdog and the diffusion of information when a contact between pairs of nodes occurs.

A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure5 shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non- selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this

information to it; so, from that moment on, both nodes store information about this positive (or negative) detection. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes shown in figure 5.

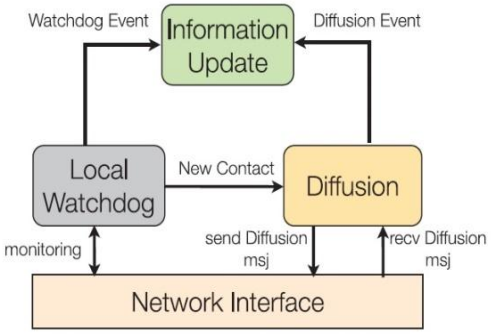


**Figure 5**

## V. PROPOSED SYSTEM DESCRIPTION

*Network Configuration*

We consider networks with 35 nodes. The mobile nodes are randomly and uniformly deployed in a square area of size 1000×800 m. The node transmission range is set to 250 m. Nodes move at the speed of 5m/ms across in the network field among Access Points. Data traffic is generated for 100 packets per millisecond over the whole network. Each packet is randomly and uniformly assigned to a source, excluding nodes that are one hop from the sink. The chosen source queues the assigned packets and transmits them as soon as possible. The maximum queue length per node is set to 50 packets. A newly generated packet is accepted by the source only if its buffer is not full.

*Neighbor selection*

In this module, an intermediate node assigns the highest priority to the packet with the closest deadline and forwards the packet with the highest priority first. Queue length threshold is set to avoid queuing congestion, we set up a space utility threshold TUs for each node as a safety line to make the queue scheduling feasible. In CoCoWa, after receiving a forward request from a source node, an intermediate node Ni with space utility less than threshold e TUs replies the source node. The replied node Ni informs the source node about its available workload rate, and the necessary information to calculate the queuing delay of the packets from the source node. The source node selects the replied neighbor nodes that can meet its deadline for packet forwarding based on the calculated queuing delay.

*Packet Scheduling*

In this module, we further reduce the stream transmission time, a distributed packet scheduling algorithm is proposed for packet routing. This algorithm assigns earlier generated packets to forwarders with higher queuing delays and scheduling feasibility, while assigns more recently generated packets to forwarders with lower queuing delays and scheduling feasibility, so that the transmission delay of an entire packet stream can be reduced.

We use to denote the time when a packet is generated, and use CoCoWa technique to denote the delay requirement. Let WS and WI denote the bandwidth of a source node and an intermediate node respectively, we use TS→I - Sp /WS to denote the transmission delay between a source node and an intermediate node, and TI→D - Sp/WI to denote the transmission delay between an intermediate node and an AP. Let Tw denote the packet queuing time and Tw(i) denote the packet queuing time of ni. The source node needs to calculate Tw of each intermediate node to select intermediate nodes that can send its packets by the deadline.

*Selfish node elimination*

In COCOWA, the selfish nodes overhear and cache packets. From the overhearing, the nodes know who have received the packets. When a source node begins to send out packets, it scans the content for duplicated chunks in its cache. If the sender finds a duplicated chunk and it knows that the selfish has sent this chunk before, it replaces this chunk with its signature.

## VI. PERFORMANCE EVALUATION

All mobile nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. We evaluate our proposed method with respect to the following metrics: Throughput, E2E latency, Packet loss ratio.

*CoCoWa Throughput:* is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.

*Packet loss ratio***:** measures the ratio of packets have been dropped during transmission time

*End to end latency***:** It refers to the time taken for a packet to be transmitted across a network from source to destination.

These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file.

## VII. CONCLUSION

Through this paper a novel of mobile sink routing protocol Ring Routing, by both considering the benefits and the drawbacks of the existing protocols in the literature. Ring Routing is a hierarchical routing protocol based on a virtual ring structure which is designed to be easily accessible and easily reconfigurable. The design requirement of our protocol is to mitigate the anticipated

hotspot problem observed in the hierarchical routing approaches and minimize the data reporting delays and also include the CoCoWa as a collaborative contact-based watchdog to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful false positives, false negatives and malicious nodes.

CoCoWa is based on the diffusion of the known positive and negative detections. When a contact occurs between two collaborative nodes, the diffusion module transmits and processes the positive (and negative) detections. Finally, using CoCoWa we can reduce the effect of malicious or collusive nodes. If malicious nodes spread false negatives or false positives in the network CoCoWa is able to reduce the effect of these malicious nodes quickly and effectively.

## VIII. ACKNOWLEDGMENT

"Dr. M. Jayaraman, Principal of our college thanks for put applicable sponsor acknowledgments for our research."

## REFERENCES

[1] Kemal Akkaya and Mohamed Younis"A Survey on Routing Protocols for Wireless Sensor Networks" Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County Baltimore, MD 21250 kemal1.

[2] Pietro Michiardi and Refik Molva "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks"

[3] Can Tunca, Sinan Isik, M. Yunus Donmez, and Cem Ersoy, "Distributed Mobile Sink Routing for Wireless Sensor Networks: A Survey" *Senior Member, IEEE.*

[4] Enrique Hernández-Orallo, Manuel D. Serrat Olmos, Juan-Carlos Cano,Carlos T. Calafate, "Evaluation of Collaborative Selfish Node Detection in MANETs and DTNs" Pietro Manzoni Department de Informatics de Sistemasy Computadores. Universidad Politécnica de Valencia. Valencia, Spain.

[5] Chatzigiannakis, A. Kinalis, and S. Nikoletseas, "Efficient data propagation strategies in wireless sensor networks using a single mobile sink," Comput. Commun., vol. 31, no. 5, pp. 896–914, 2008.

[6] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in Proc. Int. Conf. Commun. Workshop, 2010, pp. 1–5.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. ACM Mobicom Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 255–265.

[8] C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks," in Proc. Adv. Commun. Technol., Feb. 2010, vol. 2, pp. 1087–1092.

[9] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in DSR based ad-hoc networks," in Proc. IEEE Global Telecommun. Conf., 2002, pp. 178–182.