

Survey on the Challenging Issues in Energy Efficient Methods for Routing in Heterogeneous Wireless Networks

Shruti Halkude¹ S K Padaganur²

¹Student of M.Tech ²Assistant Professor

^{1,2}Department of Electronics & Communication Engineering

^{1,2}BLDEACET, Bijapur, Karnataka, India

Abstract— Our work in this report stems from the fact that most of the open vehicle routing problems are similar to the ones in sensor networks from the assumptions and constraints point of view. Hence, it makes sense to use those techniques in the wireless sensor networks domain such that we can find certain most required solutions for some problems being faced in WSNs. To provide a baseline that this approach is achievable we have proposed one data collection protocol called EDAL which stands for Energy-efficient Delay-Aware Lifetime- balancing data collection protocol. This algorithm design of EDAL provides proof for one result from OVR that the problem formulation is inherently NP-hard. Hence, our research work lays emphasis on both centralized heuristic so as to reduce the computational overhead and a distributed heuristic so as to make the algorithm scalable for large-scale network operations. This data collection protocol, EDAL, that we are introducing is aimed to be closely integrated with compressive sensing, which is a technique that ensures considerable reduction in total traffic cost for collecting sensor readings under loose delay bounds.

Key words: Wireless sensor networks (WSN), Energy efficiency and cost effective data collection method

I. INTRODUCTION

Wireless sensor networks are the networks with a large number of sensor nodes. Each of them collect and route data to the external sink(s) using a transmission regulation. Due to scarcity in the availability of energy, bandwidth, memory and computing abilities of the sensor nodes, the transmission strategy used should ensure minimisation of energy consumption so as to maximize the network lifetime. Usually, the data transmission is many-to-one mode, this may lead to highly non-uniform energy consumptions in the network. Hence, this causes energy holes around the sink and reduction in the network lifetime. Therefore, designing a transmission strategy not only requires for Maximum Possible Energy efficiency (MPEE) but also the Maximum Possible Energy Balancing (MPEB) play an important role in wireless sensor networks.

The cluster based routing protocol (CBRP) was first introduced in 1999 by Jiang et al. In this nodes of wireless sensor networks are divided into smaller groups called clusters. Each cluster has a cluster head that is responsible for carrying out the routing process. Cluster heads communicate with each other through gateway nodes. Routing process is performed by source routing by flooding the network with a route request message. As there is clustered structure there will be less traffic.

Clustering process is described by the following states based on the current node state. They are:

A. Undecided:

This state corresponds to a node that is not a member of any cluster. Therefore, if this node receives a HELLO message from a CH and there is a bi-directional link between them then it joins the cluster and changes its state to be the member of the cluster. Otherwise it looks for any bi-directional links its neighbouring table. If so, it becomes the member of it. If not, it keeps trying again and again.

B. Cluster Head:

If in case, a cluster head finds that there is bi-directional link to another CH then it instead loses its state as CH and further becomes the member of that cluster if the CH has a lower ID. Otherwise it remains in CH state and some other CH becomes the member of this cluster. This is called cluster RE-organization.

C. Member:

If a member loses its state of being a CH, it searches for a bi-directional link to other nodes. If one such link is found, its state changes to a CH if it has the lowest ID, otherwise changes to an undecided state. In order to keep cluster re-organization to a minimum level, the structure of the clusters should change as rarely as possible.

II. ROUTING IN CBRP

CBRP uses two data structures so as to support the routing process: the cluster adjacency table (CAT) and the two-hop topology database [14]. The CAT has information about neighbouring clusters that is whether they are bi-directionally or uni-directionally linked.

A. Route Discovery:

Route discovery is carried out based on source routing. In CBRP only the CHs are flooded with the route request(RREQ) messages and even the gateway nodes receive these messages but they do not broadcast these messages instead forwards it to the next CH.

A node 'A' broadcasts the RREQ message with its own unique ID together with the destination address. The CH that has the route for the particular destination in its routing table, it responds with a route reply message (RREP) back to the source 'A'. The source node then calculates the best of the routes that is the shortest path to the destination node and chooses the same to route the data to the destination node.

B. Routing And Route Improvement:

Since WSN is a mobile network, nodes keep moving in the network. Hence, the topology keeps changing. And even there might be circumstances where the nodes may disappear or may be occurrence of node failure. CBRP uses two mechanisms to improve a route i) Local repair ii) Route shortening.

1) Local Repair:

When a connection between two nodes fails, the CBRP can repair the route there by acting as an intermediate node between the nodes those have lost the link.

2) Route Shortening:

Suppose a node finds a connection between itself and a succeeding node of the route, that may not be its direct successor or a connection between two following nodes respectively. However, this can be done by examining the information stored in the database of the two hop topology. Then it selects the one with the shortest path and excludes the route containing redundant nodes.

C. Problems and Limitations of CBRP:

However there are some limitations of this CBRP. When the networks and the clusters grow to be large, then the overhead per packet increases accordingly. This is because every node of the route to destination has to be included in the routed packet. This leads to an increase in the packet size according to the increase in the path length. And hence leads to the increase in the transmission time. As the cluster size increases, the size of HELLO messages grows and hence there is an increase in the stored data structures.

CBRP supports uni-directional links. This poses to be a problem when using with 802.11 link layer technology as these uni-directional links cannot be supported as the 802.11 protocol knows only the bi-directional links. However, this could be solved by using a new protocol that supports uni-directional links.

Address resolution by using Address Resolution Protocol (ARP) is also a problem. ARP is used to map network IP address with the corresponding MAC addresses. To get the mapping done, the ARP messages are broadcast in the network. When the destination node receives such a request message, it replies with MAC address. If the two nodes are connected in a uni-directional way then one of the nodes will not be able to resolve the other's MAC address by making use of the original ARP. This requires a modification. This modification involves the CH informing the upstream node with the MAC address of the downstream node if both the nodes lie in the same cluster. If the nodes do not lie in the same cluster, then the address resolution is done during the process of adjacent cluster discovery.

III. WIRELESS SENSOR NETWORK: AN OVERVIEW

A WSN consists of a number of sensor nodes each having sensing, computing capability and communication devices such as short-range communication devices over wireless channels. The nodes may be spread over a large geographical area for ex: WSNs can do monitoring for some required phenomenon. In such applications the aim of WSN is to collect environmental data and send it to a sink. The size limitation puts forward challenges for design and management of WSNs; mainly, restrictions in memory, power and communication capacity need to be considered so as to improve the longevity of the nodes. Power restriction is the main thing of concern. The range that a data can be transmitted depends on the power used by the node. Reduction in the power consumption is an important goal in the design of WSN protocols. As data transmission is

expensive, the communication between nodes plays an important role in the power efficiency of these networks.

In the AODV protocol, numbers of routing paths discovered were high as the neighbours were picked in random way and hence the path length of wireless links will increase. These in turn add up to cumulative power consumption and hence we see an increase in energy efficiency.

IV. AODV PROTOCOL OVERVIEW

AODV is energy efficient and reactive routing protocol where routes are determined only when required. Hello messages may be used to check the connectivity with neighbours [3]. In this case, active nodes periodically keep broadcasting a Hello message which will be received by all of its neighbours. Hence, if a node fails to receive several Hello messages from a neighbour then a link is detected to be broken. A source with data to send to an unknown destination, broadcasts Route Request (RREQ) to destination. Each intermediate node upon receiving a RREQ a route to the source is created. If receiving node is the destination node, it generates a Route Reply (RREP) [4]. This RREP is sent only to the source in a hop-by-hop manner. As RREP propagates, each intermediate node creates a route to destination. On reception of RREP at source it keeps a track of the route to destination and begins sending data. On reception of multiple RREPs, the one with the shortest hop is chosen. While data keeps flowing from source to destination, each node along the route updates timers associated with the routes to the source and destination, and even maintains the routes in the routing table. In case a route is not used for some time, the node discards the route from its routing table. If data is in flow and a link break is detected, a Route Error (RERR) is sent to source in a hop-by-hop fashion. As RERR flows towards, each intermediate node invalidates routes to any destination that is unreachable. On receiving RERR, the source invalidates the route and reinitiates route discovery.

V. TARP FOR SECURE WIRELESS SENSOR NETWORKS

Sensor networks are inherently collaborative environments. Though a node will be able to carry out some tasks like sampling an attribute or broadcasting a message, the overall purpose of the network will not be achieved without the collaborative work of several or all of the nodes [6]. Tasks requiring collaboration include application tasks like calculation of average temperature in an area, system tasks like synchronization and networking tasks like routing.

Wireless sensor network protocols and applications usually implement these tasks with the assumption of a co-operative environment in which case the nodes interact with each other. But this is not applicable practical [8]. For some or the other reasons, nodes and the entire network may not behave as expected by the designer. Therefore it is needed to design nodes to establish trust level for other nodes. Communicating with untrustworthy nodes results in resource wastage, e.g. time, energy, bandwidth, power, etc. Hence, it is very much necessary to check whether the node will be behaving as expected. Factors influencing the necessity of trust mechanisms in sensor networks are: i) Application requirements ii) System requirements iii)

limitation of traditional security mechanisms and iv) Across-network interoperability.

Consequently, insider threat accounts to an important security issue in WSN as traditional security mechanisms like authentication and authorization, cannot detect insider attackers who are unfortunately legal members of the network [5]. Insider attackers may disrupt the network by dropping, manipulating or misrouting the data packets. This would pose to be a serious threat in applications like military surveillance system which is designed to monitor the battlefield and other critical infrastructures. As WSNs are made up of many tiny sensor nodes, trust mechanism is usually implemented as distributed system where every node can evaluate, update and store the trustworthiness of other nodes on the basis of trust model.

Generally, trust mechanism works in three stages i) node behaviour monitoring ii) trust measurement and iii) insider attack detection. Watchdog is a popular monitoring mechanism. Other two stages are carried out by a trust model such as beta trust model and entropy based trust model by making use of the data collected by the watchdogs. In such trust mechanisms, if an insider attacker A drops packets from its neighbour, in the long run, the watchdog in N monitors and records this misbehavior by node A (stage 1). Node N then lowers the A's trust value (stage 2) and in case the trust value goes below a trust threshold, N will consider node A as untrustworthy and remove it from its neighbour list (stage 3). Still there are many problems associated with this mechanism i) watchdog has security vulnerabilities due to some of the weaknesses of WSNs like distributed sensors, limited transmission and reception range and multi-hop routing. ii) No trust model can prevent inside attackers from dropping packets completely. This is mainly because, a particular packet drop out, and we cannot actually distinguish whether it was dropped by an attacker or was an outcome of contention or noise. Hence, an inside attacker can hide its identity behind network traffic or say noise. iii) Inside attacker along with other insiders will be having the internal knowledge about the network and the security mechanisms against attacks. By using this knowledge, inside attackers can make their attacks intelligently such that their identity will not be revealed.

VI. IMPROVED ENERGY EFFICIENCY AND REDUCED DELAY WITH SCHP IN WSNs

As sensor nodes operate on battery, they are usually deployed in harsh environments. Hence, energy efficiency is a main design issue for WSNs. In the long run many efforts have been made for the design of energy efficient routing techniques. However there existed an efficiency- delay trade off though it increased the network lifetime. In some applications like environment monitoring, instruction detection etc, delay cannot be tolerated. A self knowledge technique which works together with sub cluster head protocol (SCHP) had been proposed to reduce the delay due to link stability problem in SCHP. Each node will be having knowledge about its neighbours. The sender sends in accordance with the receiving capacity of the receiver which in turn gives better link stability. This results in a reduced delay and even is proved as energy efficient [13].

Some of the advantages of WSN are adaptability, battery operand nodes, self-configurable, comprehensive sensing range, application specific and error tolerance. As the sensors are battery operand it is not feasible to recharge or replace the batteries so energy efficiency and hence network lifetime is one of the main issues of WSNs.

In SCHP with self-knowledge, the sender node keeps knowledge of all parameters like delay, threshold, packet size, energy of its one hop neighbours and makes transmissions according to receiver's capacity. Thus, helps maintain the link stability thereby avoiding congestion in the link. And hence most of the energy is utilised for productive packet transfer. Therefore, this technique poses to be both energy efficient and delay constrained. A minimum threshold is set for all parameters, for all the neighbouring nodes and the nodes satisfying these threshold levels will be considered as candidates of relay node. Among those, the node with lowest delay and maximum energy is chosen as relay node. If in case the node dies after sometime, the next eligible candidate will be chosen and attempt is made to reconfigure the dead node. Hence, the time and energy that would otherwise be wasted in re-establishing the link that can be lost due to congestion is saved and hence accounts to increase the lifetime and reducing the delay.

VII. LOAD BALANCING AND DATA COLLECTION METHODS FOR ENERGY SAVING IN WSNs

Data collection is a major function of applications in WSNs. Most important issue in designing a data collection algorithm is how to save energy of sensor nodes while maintaining the requirements of applications [10]. As WSNs are characterized by centralized data collection, multi-hop communication and many to one traffic, leads to severe packet collision, network congestion and packet loss and hence even results in hot-spots of energy consumption therefore leading to premature death of sensor nodes and hence the entire network. A load balancing data collection method that classifies sensor nodes into different layers and calculates their distance to sink node and further divides the sense zone into many clusters. Routing trees are then put up between sender and sink based on energy metrics and communication cost. In order to save energy the target of data collection scheme will be adopted. This method provides more uniform energy consumption among the nodes and hence can increase the lifetime of the WSNs.

VIII. DELAY-EFFICIENT DATA COLLECTION WITH DYNAMIC TRAFFIC PATTERNS IN WSN

In order to reduce the energy, the sensor nodes do not inform every sensed data to the base station [2]. And hence, the network traffic of continuous data collection application varies in an unpredictable manner.

Data collection is the gathering of all the information from all the sensor nodes at the base station. Usually, TDM is the best method to collect the information from all the sensors to the base station as the probability of collision is very less and high probability of successful transmission involving one packet per slot. To reduce the energy consumption, nodes may not send the information on every packet slot. And hence, there will be dynamic traffic patterns in the network.

Wenbo Zhao et al. were the first researchers to consider dynamic traffic patterns in WSN. In this the authors specified using TDM approach which can effectively deal with the change in the traffic patterns [15]. However, this result in data collection delay as the parent node waits for the data from the entire children node before sending data to its children node.

Data collection can be done in two ways:

A. Aggregation of Data:

Aggregation of data from all the children nodes. This involves an internal node together with its own data compressing the data from all children node and sending all of the data in a single packet in a single packet slot.

B. Non-Aggregated Data Transmission:

Non-aggregated data transmission in this each of the node sends its own data in multiple data slots. This involves an internal node requiring more data slots than any of the children node as it has to transmit all the data from all the children nodes.

A data collection protocol called delay-efficient traffic adaptive scheme was introduced to reduce the amount of energy involved in data collection involving the dynamic traffic patterns.

The contributions of this scheme are:

- (1) Propose an algorithm for scheduling sensor nodes to report data within minimum delay
- (2) Provide an adaptive mechanism to allow sensor nodes to reduce their idle listening according to the change of network traffic.

This algorithm can achieve up to 20% improvement in data collection delay simultaneously keeping the energy consumption at reasonable level.

IX. HYBRID ENERGY EFFICIENT DISTRIBUTED (HEED) PROTOCOL FOR INCREASING NETWORK LIFETIME

One of the important protocols that increases the network lifetime is HEED protocol heterogeneous WSNs [1]. This protocol considers two parameters to decide who will be the cluster head. It considers the residual energy of the node and the node density to decide upon the cluster head. Depending upon the node types, it defines one level, two level and three level heterogeneity and HEED protocols are accordingly specified as hetHEED-1, hetHEED-2 and hetHEED-3, respectively. Here we also consider one more parameter distance and apply fuzzy algorithm to decide a cluster head. Accordingly, HEED protocols are specified as HEED-FL, hetHEED-FL-2, hetHEED-FL-3 [11].

When there is only single class for all the nodes, then we consider that all the nodes have the same energy and that each of the nodes is treated in the same way. However we considered the classification into three levels as mentioned and it has been proved that as the heterogeneity increases in the network the network lifetime increases accordingly

It was seen that increasing the energy in the network so as to increase the heterogeneity, the network lifetime was increased at higher rates especially in case of hetHEED-FL-3. It was seen that an increase in the energy by 74.2% leads to an increase in network lifetime by 213.38%.

Using fuzzy logic in the protocol without any increase in the energy levels, it was seen that the network lifetime increased by 114.85% of the original HEED.

Increasing the heterogeneity along with fuzzy algorithm increased the network lifetime manifold. For example: approximate increase of energy by 19% increased the network lifetime by 387.94%

X. EXISTING SYSTEMS AND THEIR OUTCOMES

Routing protocols for WSNs has been classified into many types based on the application for ex: location based, data centric based, multi-path based, mobility based, Qos based and hierarchical based.

Location based routing protocols make use of the information about the location of the nodes to relay the data of the required regions rather than of the whole network. For ex: minimum energy consumption network, greedy anti-void routing, geographical and energy aware routing.

In data centric routing protocol, the nodes employ flood based transmission schemes. For ex: directed diffusion and rumour routing.

In multiple path routing protocols, the nodes used multiple path to improve the network performance. For ex: sensor-disjoint multipath protocol.

In Quality of Service (QoS) based routing protocol, the network makes a balance between energy consumption by nodes and data quality besides QoS parameters that are delay, energy and bandwidth during transmission of the data. For ex: sequential assignment routing, energy aware routing.

Hierarchical routing protocols also called cluster routing, involves clustering. Low energy adaptive clustering hierarchy (LEACH) was the first clustering protocol. In this routing is done by the cluster heads and as time passes, the role of cluster head is changed from node to node so that single node does not drain up all of its energy in routing data of various nodes.

TEEN protocol was introduced that uses the hierarchical structure. This protocol senses the sudden changes in the network and responds to it by changing the parameters of interest accordingly. Therefore, such protocols are essential in critical applications.

Later Manjeshwar and Agarwal modified the TEEN protocol to APTEEN protocols that was meant for both the time critical protocols and periodic data collections.

Later an improved version of LEACH was introduced by Raghvendra and Lindsey that included efficient transmission of data from sensor nodes. It uses the chain of sensor nodes. Each of the nodes sends its data through its chains to the cluster head. Cluster head on the other hand aggregates the information from all the sensors and removes all the redundant data packets and then transmits all the data to the base station or say sink. But it was not usually used in large networks due to excess delay introduced by this method.

Smaragdakis et al. introduced SEP. It was an extension of LEACH that used hierarchical clustering and heterogeneity. Here the cluster head is selected based on the weighted election probabilities of each node in accordance to their respective energies.

Electricity domain protocol (EECS) elects the cluster head based on the maximum residual energy decided

through local radio communications. It is used in the applications requiring periodic gathering of the sensed data using WSNs. It uses load balancing and energy efficiently. But one disadvantage is that it requires global information about the distance of all the cluster heads to the base station.

DEEC was introduced by Li et al. for two or multiple level heterogeneous networks. This protocol selects the cluster head by computing the ratio of residual energy of each of the node and the average network energy. The node having the higher ratio is likely to be elected as the cluster head. The nodes that are nearer to the sink require more energy than the farther nodes as there is extra burden of transmitting data from nearby neighbours. Therefore, they form smaller clusters to balance the load among the cluster heads.

XI. CONCLUSION

We observed that CBRP is energy efficient but puts forward the size limitation. Also that AODV routing protocol is an active routing protocol in which routes are determined only when needed therefore we see power conservation in it. We see that the dependency between a central trust authority and other nodes in a network makes complication in trust establishment of pure ad-hoc networks. Also the network security and node's trust evaluation is another important challenge in WSN. In order to decrease the total cost in the network and to improve the energy-efficiency of the network, the Energy efficient Delay Aware Lifetime balancing data collection has been proposed. This algorithm will discover multiple paths in such a way that the number of hops per route will be decreased by a large amount hence reducing the cost of network and improving the energy-efficiency of the network.

REFERENCES

- [1] Pavan K. Pothuri, Venkatesh Sarangan, and Johnson P. Thomas, "Delay-constrained, energy-efficient routing in wireless sensor networks through topology control. Published in: Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference. Pp 35-41.
- [2] Agam Gupta, Mansi Gupta and Anand Nayyar, "Approaches for Combating Delay and Achieving Optimal Path Efficiency in Wireless Sensor Networks", IJCSMC, Vol. 3, Issue. 5, May 2014, pg.105 – 111.
- [3] "AODV Routing Protocol Implementation Design" Ian D. Chakeres Dept. of Electrical & Computer Engineering University of California, Santa Barbara, Elizabeth M. Belding-Royer Dept. of Computer Science University of California, Santa Barbara
- [4] I. D. Chakeres and E. M. Belding-Royer. The Utility of Hello Messages for Determining Link Connectivity. In Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC), pages 504. 508, Honolulu, Hawaii, October 2002
- [5] Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks Youngho Cho and Gang Qu Department of Electrical and Computer Engineering and Institute for Systems Research University of Maryland, College Park, USA Yuanming Wu School of Optoelectronic Information University of Electronic Science and Technology Chengdu, Sichuan, China
- [6] Javier Lopez, Rodrigo Roman, Isaac Agudo, and Carmen Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," Computer Communications, Vol 33, 2010.
- [7] Suk-Bok Lee and Yoon-Hwa Choi, "A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks," In Proc. of the fourth ACM workshop on Security of ad hoc and sensor networks (SANS), 2006.
- [8] TARP: A Trust-Aware Routing Protocol for Sensor-Actuator Networks Abdelmounaam Rezgui Dept. of Computer Science Virginia Tech Blacksburg, VA 24061, USA. Mohamed Eltoweissy, The Bradley Dept. of Electrical and Computer Engineering Virginia Tech Arlington, VA 22203, USA
- [9] L. Xiong and L. Liu. Peer Trust: Supporting Reputationbased Trust for Peer-to-Peer Electronic Communities. IEEE Trans. on Knowledge and Data Engineering (TKDE), 16(7):843–857, July 2004.
- [10] V. Shnayder, M. Hempstead, B. rong Chen, G.W. Allen, and M. Welsh. Simulating the power consumption of large-scale sensor network applications. In J. A. Stankovic, A. Arora, and R. Govindan, editors, SenSys, pages 188–200. ACM, 2004
- [11] Heterogeneous HEED Protocol for Wireless Sensor Networks by Satish Chand, Samayveer Singh, Bijendra Kumar. Wireless Peers Communication (2014) 77:2117–2139 DOI 10.1007/s11277-014-1629-y
- [12] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422.
- [13] Lindsey, S., & Raghavendra, C. (2002). PEGASIS: Power-efficient gathering in sensor information systems. In IEEE aerospace conference proceedings (Vol. 3, pp. 1125–1130)
- [14] Smaragdakis, G., Matta, I., & Bestavros, A. (2004). SEP: A stable election protocol for clustered heterogeneous wireless sensor networks. In Second international workshop on sensor and actor network protocols and applications (SANPA 2004).
- [15] Lindsey, S., Raghavendra, C. S., & Sivalingam, K.M.(2002).Data gathering algorithms in sensor networks using energy metrics. IEEE Transactions on Parallel and Distributed Systems, 13(9), 924–935