IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

A Swarm Based Approach to Detect Hole In Wireless Sensor Network

Nidhi[1], Mrs. Pooja Mittal[2]

[1]M. Tech. Student, DCSA, MDU, Rohtak, Haryana, India
nidhi.dalal0@gmail.com

[2]Professor, DCSA, MDU, Rohtak, Haryana, India
mpoojamdu@gmail.com

Abstract

A Sensor network is a network with large number of sensors in it. The broadcasting and the multicasting are the major communication approaches used in such network to distribute some information over the network or the network part. Because of this the congestion over the network increases. A congested network is the reason of different securities flaws over the network. One of such flaw is the hole over the network; the hole can be because of low energy node or because of some selfish node or black hole attack. In this present work we have defined a Swarm Based Intelligent approach to perform the reliable packet delivery over the network. Here we have defined an intelligent decision approach to select the next node based on load and response time. The work is about to improve the network throughput as some bad node or the hole occur over the network. The swarm based approach will do the analysis based on the neighboring nodes and will select the effective path for the communication.

Keyword: *Swarm Based hole, Bad Node, Throughput, and WSN.*

1. Introduction

Wireless Sensor networks (WSN) can be defined as the network of geographically distributed tiny sensor nodes having sensing, computation, and wireless communications capabilities. These tiny sensor nodes communicate with each other using low power wireless data routing protocols [1].In other words, wireless sensor network generally consists of a data distribution network and data acquisition network monitored and controlled by a management center.

Total working of wireless sensor networking is based on its construction. Sensor network initially consists of small or large nodes called as sensor nodes. These nodes are varying in size and totally depend on the size because different sizes of sensor nodes work efficiently in different fields. Wireless sensor networking have such sensor nodes which are specially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery. The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors, a communication device (usually radio transceivers), and a power source usually in the form of a battery.

Current system solutions, protocol frameworks and paradigms typically provide the following services:

1. Periodic Sensing(the sensor devices constantly monitor the physical environment and continuously report their sensors' measurements to a control center),
2. Event Driven(to reduce energy consumption, sensor devices monitor silently the environment and communicate to report when certain events are realized) and
3. Query based (sensor devices respond to queries made by a supervising control center).

1.1 Routing Techniques In Sensor Networks

1.1.1 Flooding

Flooding is an old technique that can also be used for routing in sensor networks. In flooding, each node receiving a data or management repeats it by broadcasting, unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. Flooding is a reactive technique, and it does not require costly topology maintenance and complex route discovery algorithms. However, it has several deficiencies such as

• Implosion: Implosion is a situation where duplicated messages are sent to the same node. For example, if sensor node A has N neighbor sensor nodes that are also the neighbors of sensor node B, sensor node B receives N copies of the message sent by sensor node A.

• Overlap: If two nodes share the same observing region, both of them may sense the same stimuli at the same time. As a result, neighbor nodes receive duplicated messages.

• Resource blindness: The flooding protocol does not take into account the available energy resources. An energy resource aware protocol must take into account the amount
of energy available to them at all times[2].

1.1.2 Gossiping

A derivation of flooding is gossiping [19] in which nodes do not broadcast but send the incoming packets to a randomly selected neighbor. A sensor node randomly selects one of its neighbors to send the data. Once the neighbor node receives the data, it randomly selects another sensor node. Although this approach avoids the implosion problem by just having one copy of a message at any node, it takes a long time to propagate the message to all sensor nodes[2].

1.1.3 Directed Diffusion

Directed Diffusion is a data-centric routing algorithm in which all communication is for named data. It consists of four elements: interests, data messages, gradients and reinforcements. An interest is a task description which is named by, for instance, a list of attribute-value pairs that describe a task. Data are named using attribute-value pairs. A gradient specifies both data rate and the direction along which events should be sent. Reinforcement is used to select a single path from multiple paths[2].

II Literature Survey

C. Intanagonwiwat, proposed directed diffusion routing strategy in[6] is based on attribute-value querying and when queried, nodes establish gradients to the query initiator and send the attribute-value pair to the query initiating node.In [7], David et al. propose a refinement to the directed diffusion algorithm proposed in [7], named Rumor routing. Rumor routing is applicable in areas where nodes do not have a coordinate system. In this, the query generated is sent on randomly until it finds nodes which are on the path to the event destination. Servetto et al. recently proposed in [8], a routing algorithm (Servettos' algorithm) which reduces the load on the central node in a single source–single destination communication. This algorithm divides the network into expansion and compression phases. Nodes belong to different diagonals of the grid. During expansion phase, the load per node decreases with the increase of number of nodes on diagonal. During the compression phase, the reverse process proceeds, and with the decrease in number of nodes on each diagonal, the load per node increases. . In another paper [9],Stefan et al. analyze the reliability of the system in the case of node failures. They split the data packet into multiple segments in such a way that the original data can be constructed from subset of all the segments. They route these mutliple segments on multiple paths and at the destination construct the original message from the messages received. Fan Ye[10],proposed in this paper describe TTDD, a Two-Tier Data Dissemination approach that provides scalable and efficent data delivery to multiple mobile sinks. Each data source in TTDD proactively builds a grid structure which enables mobile sinks tocontinuously receive data on the move by fooding queries within a local cell only. TTDD's design exploits the fact that sensor nodes are stationary and location-aware to construct and maintain the grid structures with low overhead. Badr and Podar[11] proposed a zig-zag routing policy and showed its optimality for shortest-path routing on square or infinite grid networks with independent link failures . Sanjay Shakkottai[12] proposed an unreliable wireless sensor grid-network with n nodes placed in a square of unit area. derive a sufficient condition for connectivity of the active nodes (without necessarily having coverage).If the node success probability p(n) is small enough,

we show that connectivity does not imply coverage. All the routing algorithms mentioned in [4], [5],[6], [7], [8],[9] [10], [11], [12] do not address the protocol performance in Al l to Al l communication mode.
Energy conservation is the most important concern in Wireless Sensor Networks applications which should be considered in all aspects of these networks. Greedy Approach as intelligent tools show great compatibility with WSN's characteristics and can be applied in different energy conservation schemes of them.

The most important application of Greedy Approachs in WSNs can be summarized to sensor data prediction, sensor fusion, path discovery, sensor data classification and nodes clustering which all lead to less communication cost and energy conservation in WSNs. Another classification for Greedy Approach based methods can be according to Greedy Approach topologies that applied such as Self Organizing Maps, Greedy Approachs, recurrent Greedy Approachs, Radial Basis Functions etc..As future work, more studies are required on different types of Greedy Approach topologies and training algorithms which would be more compatible with WSNs platforms in the terms of lower computation time. A primary constraint in wireless sensor networks (WSNs) is obtaining reliable and prolonged network operation with power-limited sensor nodes. There is an exciting new wave in sensor applications-wireless sensor networking- which enables sensors and actuators to be deployed independent of costs and physical constraints of wiring[13]. For a wireless sensor network to deliver real world benefits, it must support the following requirements in deployment: scalability, reliability, responsiveness, power efficiency and mobility.

In this new approach an intelligent analysis is used to process the structure of a wireless sensor network (WSN) and produce some information which can be used to improve the performance of WSNs' management application[16]. Wireless sensor networks need to be managed in different ways; e.g. power consumption of each sensor, efficient data routing without redundancy, sensing and data sending interval control, etc. The random distribution of wireless sensors, numerous variables which affect WSN's operation and the uncertainty of different algorithms (such as sensors' self-localization) give a fuzzy nature to WSNs [3, 4]. Considering this fuzzy nature and numerous details, a Greedy Approach is an ideal tool to be used to cover these details which are so hard to be explicitly discovered and modeled

Even if their resources in terms of energy, memory, computational power and bandwidth are strictly limited, sensor networks have proved their huge viability in the real world, being just a matter of time until this kind of networks will be standardized and used broadly in the field. One of the important problems that are related to the use of wireless sensor networks in harsh environments is the gap in their security.

The paper by Curiac, Daniel, Volosencu, Constantin, Doboli, Alex, Dranga, Octavian, and Bednarz, Tomasz (2007) provides a solution to discover malicious nodes in wireless sensor networks using an on-line Greedy Approach predictor based on past and present values obtained from neighboring nodes. This solution can also be a way to discover the malfunctioning nodes that were not a subject of an attack. Being localized on the base station level, our algorithm is suitable even for large-scale sensor networks.
Preserving energy or battery power of wireless sensor network is of major concern. As such type of network, the sensors are deployed in an ad hoc manner, without any deterministic way. The standard routing protocols can be applied into wireless sensor network by using topology modified by Greedy Approach which proves to be energy efficient as compared with unmodified topology.

Greedy Approach has been proved to be a powerful tool in the distributed environment. Here, to capture the true distributed nature of the Wireless Sensor Network (WSN), Greedy Approach's Self-Organizing Feature Map (SOFM) is used[15].

3. Proposed Work

Holes in network decrease the efficiency of a network. Holes lead to uncovered regions in a sensor network, increased latency as more traffic will be sent via lesser route options which ultimately leads to early power exhaustion of the sensor nodes. In a static wireless sensor network, nodes do not move and remain at same location at which they were deployed. Proposed protocol intends to use this basic property of a

wireless sensor network. For a given static wireless sensor network, if route maintenance is required for any given transmission it means either any or some of the nodes have failed or any or some of the links amongst the nodes which were earlier available are no more available. So when ever such events occur, we propose hole detection algorithm should be performed.
In order to find the hole in network path, the following constraints have to be taken into consideration:

1. Sensors in the network are placed to form a grid and coordinate of each node is known. Each node is static.
2. Each node is at a distance of 1 Unit from its neighbors.
3. Any given node can communicate with its neighbor located to top, bottom, right, left, top-left, top-right, bottom-left, bottom-right.
4. Each node maintains neighbor table and routing table. Each entry in Neighbor table contains Neighbor name (NEIGH) and Neighbor state (NSTATE). NSTATE can have three values:

Sr.	VALUE	REPRESENTS
a	1	Connected
b	0	Not connected
c	-1	Dead

Table 1: Possible Neighbor state values

5 Forward Search are used for route discovery and backward are used to set Pheromone value of discovered path.
6 Unique Sequence number is assigned to each new Forward ants and Diagnostic ants.
7. Diagnostic ants will be fed in network when a non-responding node is found during route discovery or route maintenance.

Proposed method tries to find holes by using information generated about network topology during route discovery and route maintenance. Each node in network maintains neighbor list, in which, name of each neighbor is stored along with status of respective neighbor. Individual nodes are responsible for maintaining status of neighbor. Each node also maintains routing table, in which routing information is stored along with pheromone value of each node. If for same destination, multiple entries are available in routing table of a node then the route with highest pheromone is selected.

The algorithm for the hole detection is given as under

SWARM_ROUTING (SOURCE S, SINK Si)

Step 1: S sends FANT towards Si

Step 2: Next hop is chosen depending on routing table and neighbor table information

2.1: If NSTATE := 0 OR -1; FANT is not sent to that NEIGH

2.2: If NSTATE := 1; FANT can be sent to NEIGH

2.3: Route (if available) with highest pheromone value is chosen from routing table.

2.4: If no route is available FANT will be broadcasted to neighbors after validating each neighbor with 2.1 and 2.2.

Step 3: If a NEIGH or selected NextHOP do not respond then

NPHER := 0;

NSTATE := 0;

and NODE-STATUS[NEIGH] will be initiated. Current node will select an alternative route and send FANT trough that node.

Step 4: If no NextHOP is achievable from current node then previous node will be informed to choose any alternative path.

Step 5: If FANT reaches destination it will be destroyed and BANT using route stack information will traverse back to source, incrementing pheromone level along the path.

Else Go To Step 2

4. Result Validation:

The detailed implementation and testing of proposed approach is presented in this chapter. Simulation is done using the network simulator tool NS version 2.34. Comparison testing was conducted with other state-of-the-art routing algorithms such as DSDV and DSR. The Following Performance Evaluation matrices are used to calculate the performance of the network:

i) Throughput:

Throughput of network is defined as total number of packets received at each destination node divided by total number of packets transmitted by each source node over the network.

ii) Loss-rate:

Loss-rate of the network indicates number of packets dropped during transmission. It is calculated as total number of packets dropped per second in the network.

iii) Link delay:

It is the time taken by the link to transfer a packet from the source node to destination node.

Under simulation scenario, simulation parameters like number of nodes, network area, network type etc are defined which are crucial to a networks performance. We are going to discuss two scenarios. In both scenarios, coordinate location of each node is available. Asensor network composed of various nodes as shown in Fig. 1 has been created using Tcl scripting. Green nodes represent active nodes in the network and yellow node represent those nodes that have lost connection with any of its neighbors.

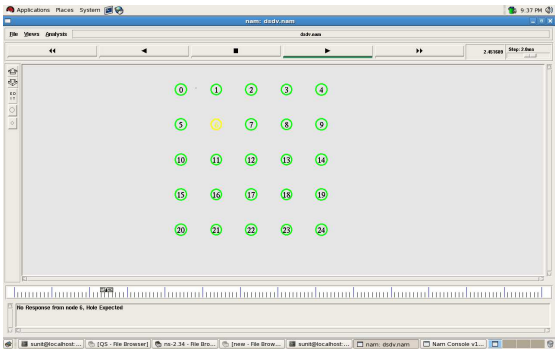

Figure 1 : Sensor Network

The scenario used for this work is shown in figure1 and all the related parameters respective to this scenario is shown in table 2.

Parameter	Value
Number of Nodes	25
Topography Dimension	400 m x 400 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Network Topology	Grid

Table 2 : Scenario Parameters

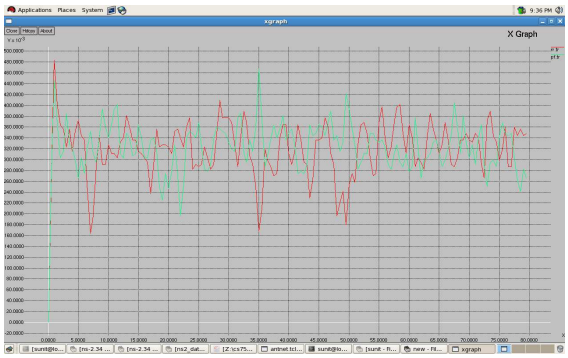

Figure 2 : Throughput Comparison

Throughput of network is defined as total number of packets received at each destination node divided by total number of packets transmitted by each source node over the network. Figure 2 represents comparison of throughput for proposed protocol and simple wireless sensor network. Green curve represents proposed protocol and red curve simple wireless sensor network. In this graph, it can be observed that throughput of proposed protocol have more

peaks then ridges as compared to throughput of simple wireless cluster sensor network, so proposed protocol is more efficient.

4. Conclusions

We proposed a swarm intelligence based routing algorithm that initiates or call hole detection mechanism. The proposed routing algorithm is similar to most swarm based algorithm the only difference is how it handles when a neighbor do not respond to a route discovery request or when a existing route breaks.

Acknowledgments

I would like to express my deepest gratitude toward my guide Mrs. Pooja Mittal, M.D University, Dept. of Computer Science & Applications Rohtak, Haryana, India for showing great interest in my thesis work, this work could not finished without his valuable comments and inspiring guidance.

References

[1]. Lewis, F.L., "Wireless Sensor Networks Smart Environments: Technologies, Protocols, and Applications", New York: ed. D.J. Cook and S.K. Das, John Wiley, 2004, pp.1-18.

[2].Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey On Sensor Networks", in Proc. of the IEEE Communications Magazine, vol.40, Issue: 8, pp. 102-114, August 2002

[3].Qiangfeng Jiang and D. Manivannan, "Routing Protocols for Sensor Networks", in Proc. of the IEEE Conference, 2004, pp. 93-98.

[4].C. L. Barett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith, "Parametric Probabilistic Sensor Network Routing," Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 122–131, San Diego, California, September 2003.

[5].B. Krishnamachari, D. Estrin, and S. Wicker, "Modelling Data-Centric Routing in Wireless Sensor Networks," Proceedings of the 2002 IEEE INFOCOM,New York, NY, June 2002.

[6].C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proceedings of the 6th57 annual international conference on Mobile computing and networking, pp. 56–67, Boston, Massachusetts, August 2000.

[7].D. Braginsky, and D. Estrin, "Rumor Routing Algorithm for Sensor Networks,"Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pp.22–31, Atlanta, Georgia, 2002.

[8].S. D. Servetto, and G. Barrenechea, "Constrained Random Walks on Random Graphs: Routing Algorithms for Large Scale Wireless Sensor Networks," Proceedings of the 1st ACM international workshop on Wireless sensor networks andapplications, pp. 12–21, Atlanta, Georgia, September 2002

[9].S. Dulman, T. Nieberg, J. Wu, and P. Havinga, "Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks," WCNC Workshop, vol. 3, pp. 1918-1922, New Orleans, March 2003.

[10]. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proc. of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.

[11]. C.Han, R.K. Rengaswamy, R. Shea, E. Kohler, and M. Srivastava. SOS: A dynamic operating system for sensor networks. In MobiSys '05,2005.

[12]. D. E. Goldberg, Genetic algorithms in search, optimization, and machine l earning, Addison Wesley.

[13]. Demirkol I, Ersoy C, Alagoz F, (2006) "MAC Protocols for Wireless Sensor Networks: aSurvey", IEEE Communications Magazine.

[14]. Estrin D., Govindan R., J. Hsseidemann S. & Kumar S." Next Centuary challenges, scalable coordination in sensor network. In: Mobile Computing and Networking 199: 263-270.

[15]. Frank Oldewurtel and Petri M¨ah¨onen," Neural Wireless Sensor Networks"