CIP Based BOND for Wireless Sensor Networks

Mr. P. Dineshkumar[1]
[1]Assistant Professor
[1]Department of IT
[1]Excel Engineering College, Komarapalayam

Abstract—The lifetime of Wireless Sensor Networks restricted by the energy level of the nodes .In traditional WSN, if a sensor node dies the base station could not able to find the dead of the node. Even if predicts it can't able to get the sensing information before it going to die. The node can dies because of animal distraction, natural disaster, battery power consumption. The base station will be in critical situation because of losing node information like identity of the node, reason for dead, and sensed information. In our proposed method the WSN nodes are arranged in cellular structure, to optimize the coverage area, reliability in getting information from the nodes and minimizing loss of information's are improved.

Key words: Wireless Sensor Networks (WSN).

I. INTRODUCTION

A WSN is defined as being composed of large number of nodes which are deployed densely in close proximity to the phenomenon to be monitored. Each node can sense events only within the distance close to it, so called RS sensing range. Two sensor nodes can directly communicate via bidirectional wireless links if their Euclidean distance is not greater than r_c, the communication range.

Sensor Nodes should relay the information via multi hop path to the data collection centre called base station. After being deployed, sensor nodes are usually left unattended for a very long period of time so that they may fail over time due to various reasons such as battery exhaustion, animal distractions and environmental disturbances. As a consequence of node failures, node movements, and other unpredictable factors, the network topology may change with time.

Most of the research [1] [2] methods have been proposed to acquire the sensing information from the node before it becomes victim. For example Chi Zhang and Yanchao Zhang [1] proposed a method to infer the boundary node information. In [2] Bai and Kumar implemented a method to deploy nodes to achieve connectivity and coverage. In [4] LVP-based algorithm requires both the directional information (the orientation of each neighbour) and distance information (the distance to each neighbour), and theoretically can detect all the boundary nodes no matter how the nodes are distributed. By contrast, the NEP-based algorithm merely needs directional information, but can only find the local (or global) convex points of the coverage boundary. Both algorithms can be applied to WSNs of arbitrary topologies. They are also truly distributed and localized by merely needing the minimal position information on one hop neighbours and a few simple local computations, and thus are of high scalability and energy Efficiency.

A. Boundary Node Detection Scheme

For example say that nodes si and sj (i ≠ j and si; sj Є V) are neighbours or there exists a direct wireless link between them if the Euclidean distance between them is no larger than rc, i.e., ǁ sj – sj ǁ ≤ rc. We also denote by Neig (sj) the neighbours of node si (not including sj). In addition, two nodes si and sj are said to be connected if there is at least one path consisting of direct wireless links between them, similarly a set of nodes is called connected if at least one path exists between each pair of nodes in the set. The fundamental connected unit of WSNs is called a cluster:

Definition 1 (cluster). A connected set of nodes is said to be a cluster if the inclusion of any other node not in this set will break the connectedness property.

We write Clust (sj) for the cluster containing node sj. Based on the sensing model, the sensing disk (or coverage) of node si can be given by

$$Diskj = Disk(sj, sj) = \{ u \in IR2 : ||u - si|| \leq rs \}$$

Specifically, let 0 indicate the origin, we have Disk0 = Disk (0, rs). Then the coverage corresponding to a cluster can be defined as follows:

Definition 2 (boundary and interior node). We define boundary nodes of Clust (sj) as those whose minimum distances to δ Cover (sj) are equal to rs, i.e.

$$BN(sj) = \{ u\ Clust(sj) : min\ || u - v || = rs$$

for v Є δCover (sj)}

Accordingly, we call all the other nodes in Clust (sj) as interior nodes, i.e,

$$IN(sj) = \{u \in Clust(sj) : u \neq BN(sj)\}$$

B. Coverage Inference protocol

How to use BOND to build a practical CIP?

Our design philosophy is that, since the minimum information required to describe the coverage is the positions of boundary nodes, we just need to detect boundary nodes. In other words, our scheme can ensure that, for the BS to reconstruct the "coverage image" without any distortion, the information transmitted from sensors to the BS is minimized.

1) Neighbourhood Monitoring and Self-Detection

After the deployment of the WSN, we assume that localization techniques are available for sensor nodes to decide their positions. Each node then collects the position information of its neighbours by broadcasting its own position, and executes BOND to detect whether it is a boundary node.

CIP protocol, both interior and boundary nodes are required to broadcast an Existence Updating Packet (EUP) to their neighbours for a random period of time exponentially distributed with rate TEUP. In addition, each interior node, say Si, maintains a timer C0(j) of expiry value much larger than TEUP for each of its non-consulting neighbours, say, Si. If Si does not overhear any packet (either a EUP or data packet) from Sj before C0 (j) expires, it will treat Sj as a dead neighbour, which can become alive if Si overhears any packet from it later. Node Si also maintains two timers for each of its consulting neighbours, say, sk: the neighbour monitoring timer C1(k) and the neighbour query timer C1 (k). If Si does not overhear any packet from Sk before C1(k) expires, it unicasts a Neighbour Query Packet (NQP) to Sk and starts C2(k). If still alive, Sk is required to send back an EUP immediately and wait for an ACK from Si. If node Si still does not overhear any packet from Sk before C2(k) expires, Si will treat Sk as a dead neighbour and re execute BOND with alive neighbours as input. In general, the expiry values of C0(j) and C0 (k) should be in the same order of TEUP, in order to guarantee that with high probability, each node will receive EUPs from all alive nodes in its neighbourhood. The expiry values of C2 (k) should be much smaller than TEUP because we require that the node which receives the NQP needs to send back an EUP immediately.

The reason for doing so is that data packets and EUP-like broadcast packets are subject to loss due to wireless transmission errors or collisions. As a result, a node may falsely identify an alive neighbour as a dead one. two timers for consulting neighbours to ensure both a shorter response delay and a lower false positive rate: although the expiry value of C1 (k) is small which may significantly increase the accuracy. Therefore Adopting one-timer (C0) scheme for non-consulting neighbours and two-timer (C1 and C2) scheme for consulting neighbours, our design achieves a better balance among accuracy, delay, and communication overhead

2) Self-Reporting of Boundary Nodes

Whenever identifying itself as a boundary node, a sensor node should send its position information to the BS, which can reconstruct the "image of the coverage" based on all the received position information of boundary nodes.

3) Explicit ACKs from the BS

The packet loss ratio due to collisions or noise is high in the WSN, boundary nodes need some mechanisms to ensure that their reports have been received by the BS. Otherwise, they have to repeatedly resend their report, which causes energy waste. The issue of reliable sensor-to-BS communication, thus far, has not been addressed thoroughly in WSN research [3] community. The work on reliable communication in WSNs first appears in [2], and then in. The reliability in a WSN is firmly dependent upon the specific application, and there is no one-for-all solution. BS to send individual ACK to each boundary node from where the report has been received at the BS.. To maintain this routing tree, each node only needs to add one entry into its routing table with the destination as the BS and the next hop as its one-hop parent node. For the BS-to-sensor unicast communication, the situation will be totally different.

II. RELATED WORK

Current methods for optimizing the node coverage area are based on boundary node detection algorithm and CIP protocol.

First we propose a novel architecture for WSN in order to reduce loss of information, and to improve reliability.

Second we show the analytical approach for sensing the information from the victim node before it dies.

III. PROPOSED SYSTEM

Boundary node detection and CIP protocol are used to find the neighbours and communicating with neighbours. Our proposed architecture contains a cellular structure of sensors inside the sensing node.

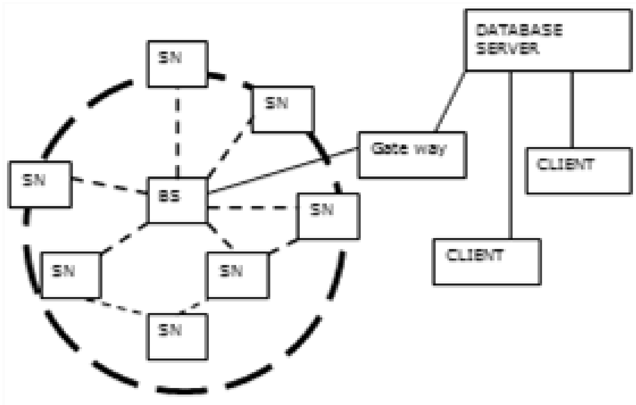


Fig. 1: General Architecture of WSN

The nodes within the boundary send the information to the base station via interior nodes of the connected coverage area. The base station in turn sends the sensed information to database server through gateway and further processed by the clients.

A. Cellular Structured Sensor Node Coverage

In traditional architecture of WSN the node which is alive will send the information to base station via interior nodes. The base station could not able to collect the coverage information, sensed data from the high powered victim node due to environmental failures like human attacks, animal intervention and battery power consumption.

We propose a Cellular Structured Sensors, to improve the efficiency of getting the sensed data. Figure (2) shows a sensor arrangement in a single node.

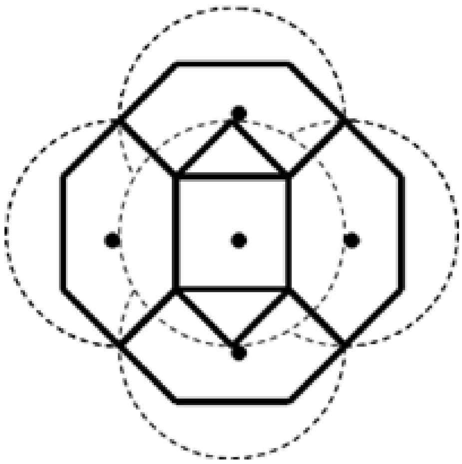


Fig. 2: Coverage area before a node dies

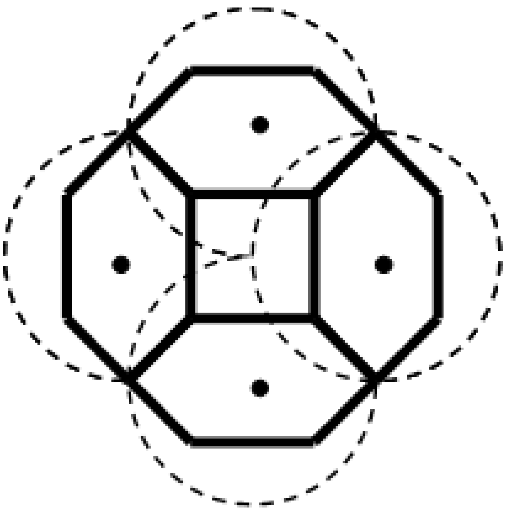


Fig. 3: Coverage area after a node dies

B. Cellular Sensors Deployment

The information from the particular node is sensed by the sensors arranged in a cellular structure. A sensor in a cellular structure will have its own sensing range so that the coverage area of a sensor will be more compared with the traditional methods. A collection of sensors placed in a node is named as cellular sensors. The sensor having the higher threshold in power is chosen as head of the sensor dynamically, to reduce battery power consumption. In fig (3), the sensor which dies in mid in position loses the sensed information about the region of interest. If the information is lost the base station will not aware of the information gathered by the dead node.

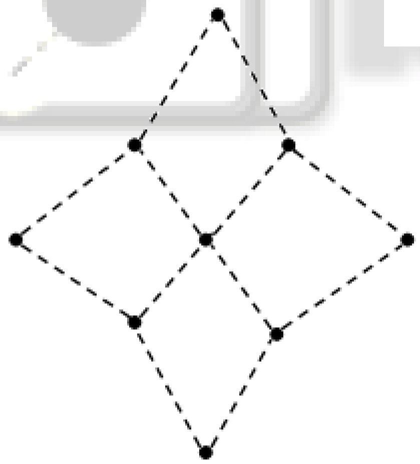
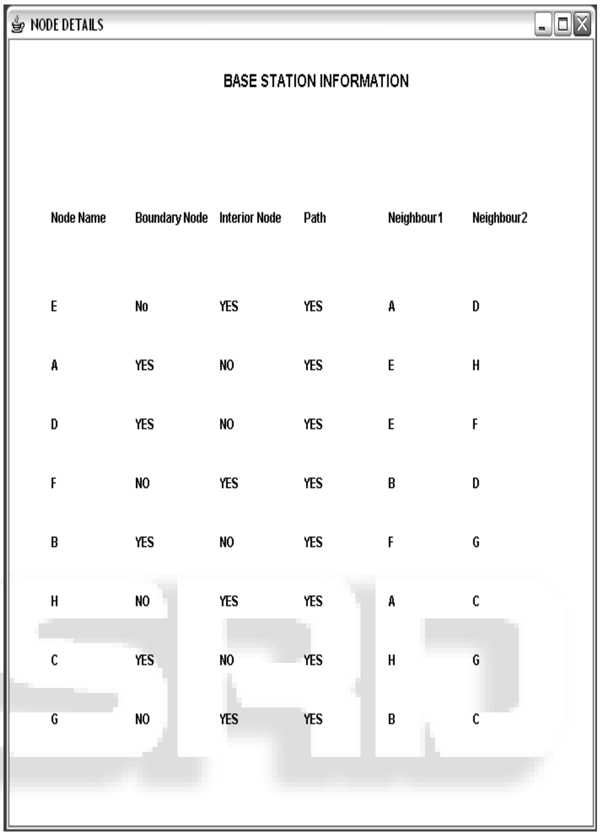


Fig: 4: Connected Coverage Area

1) Base Station Information

Our proposed method, overcomes the loss of information, and achieves maximum coverage by using Cellular Structured Sensors. In Fig (3) shows that, if a node dies, the information about it, can be sensed by the neighbour sensor placed at the neighbour node or by the node boundary sensors. In fig (4) the cellular structured sensors are configured and placed in connected coverage area and information are send to base station via multi hop topology.
fig (5) base station gathers all the information from the connected nodes and analyse whether the path is alive. If alive the information will be stored in the base stations database. The base station forms an image of connected nodes. Fig (6) shows the path information of the connected nodes based upon the information received from the nodes to base station. The path established by the interior can be detected by the connected nodes. If a boundary node or interior node dies, the base station conforms only when it does not receives information from the neighbour node. Thus the victim node is identified by the path information database, collected by the base station.

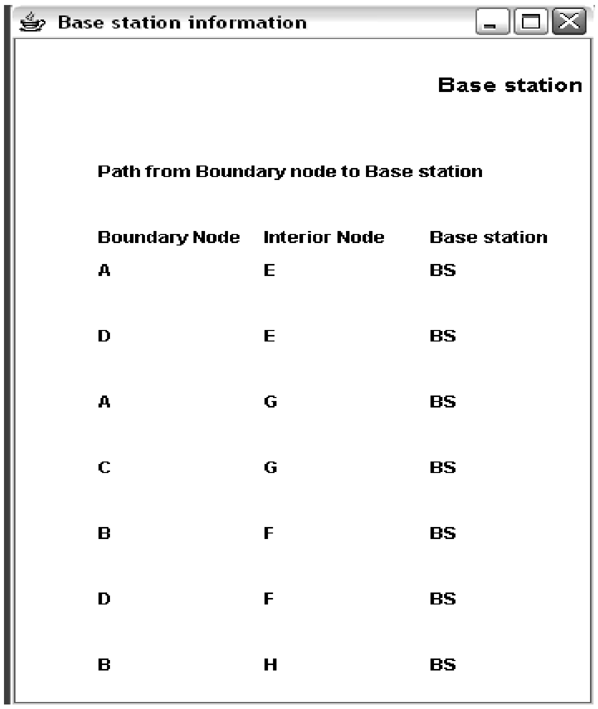


NODE DETAILS

BASE STATION INFORMATION

Node Name	Boundary Node	Interior Node	Path	Neighbour1	Neighbour2
E	No	YES	YES	A	D
A	YES	NO	YES	E	H
D	YES	NO	YES	E	F
F	NO	YES	YES	B	D
B	YES	NO	YES	F	G
H	NO	YES	YES	A	C
C	YES	NO	YES	H	G
G	NO	YES	YES	B	C

Fig. 5: Information received by base Station



Base station information

Base station

Path from Boundary node to Base station

Boundary Node	Interior Node	Base station
A	E	BS
D	E	BS
A	G	BS
C	G	BS
B	F	BS
D	F	BS
B	H	BS

Fig. 6: Path Information of connected nodes

2) Information Collection by Base Station

In fig(7) depicts the information sensed by the connected nodes. The information will be sent to the base station for further processing. The base station stores the information by the order of path it receives from the connected nodes. Figure (8) illustrates the normal work flow between connected nodes and base station.

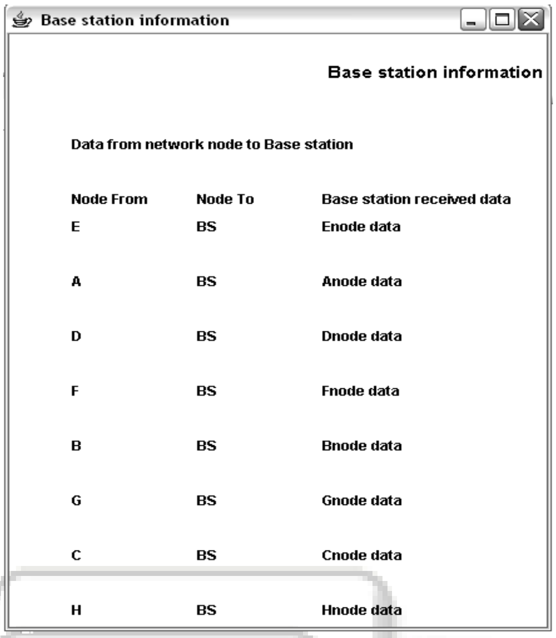


Fig. 7: Data Collection by nodes to base station

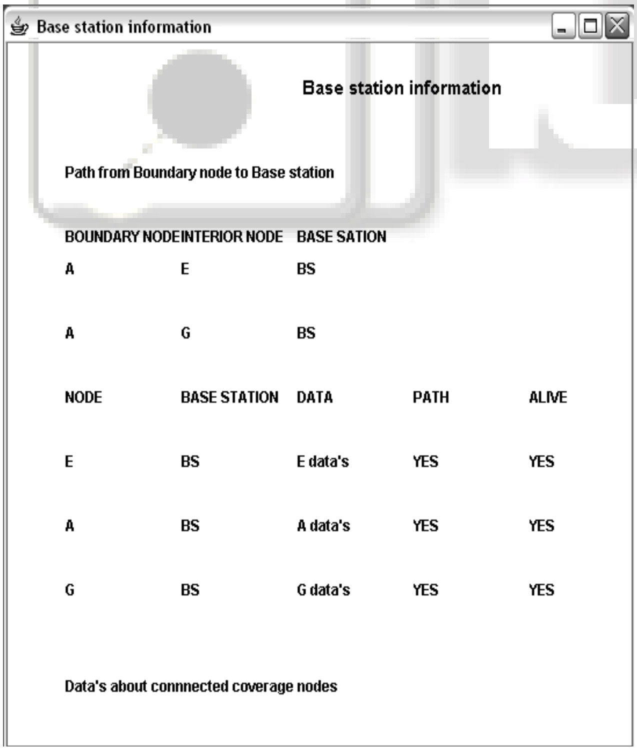


Fig. 8: Sample Path connection

For example, Consider a path connection between node a to base station via node e and g. Node A uses the boundary node detection algorithm[1] to self-detect whether it is boundary node. If so, it will send information to immediate neighbour nodes to base station, that it is boundary node and the information sensed by it. The base station receives information of node A with the information of its neighbour node. In our example Node A is the boundary node and Node E, G is interior nodes. Interior nodes E and G send the information of boundary node A to base station, as

$$BS_{Info} = BN_{Info} + IN_{Info} \quad (3.1)$$

Where,

BS_{Info} = Base Station,

BN_{Info} = Boundary Node Information

IN_{Info} = Interior node or neighbour node

Thus the base station collects information of the connected nodes, and verifies its correctness by packet matching [1].

3) Detecting Victim Node

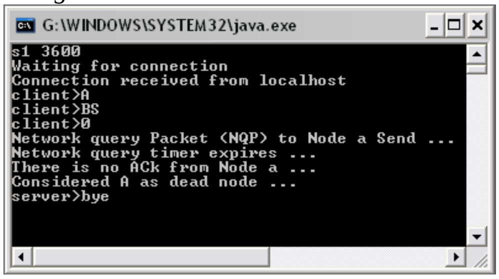


Fig. 9: Network Query Packet and Timer

The base station detects the victim node, by the information received by the neighbor node of the victim node. The neighbor node will send Network Query Packet (NQP) to the victim node and waits for acknowledgment until the Network Query Timer (NQT) expires. In fig (9) shows a NQP that, if the acknowledgment for the victim node is not received by the all the neighbor nodes, then the base station conforms the victim node as dead node. Fig (10) illustrates the base station verification of new path and verification of existing path. The base station declares the dead of the victim node and sends acknowledgment to alive nodes of the connected region.

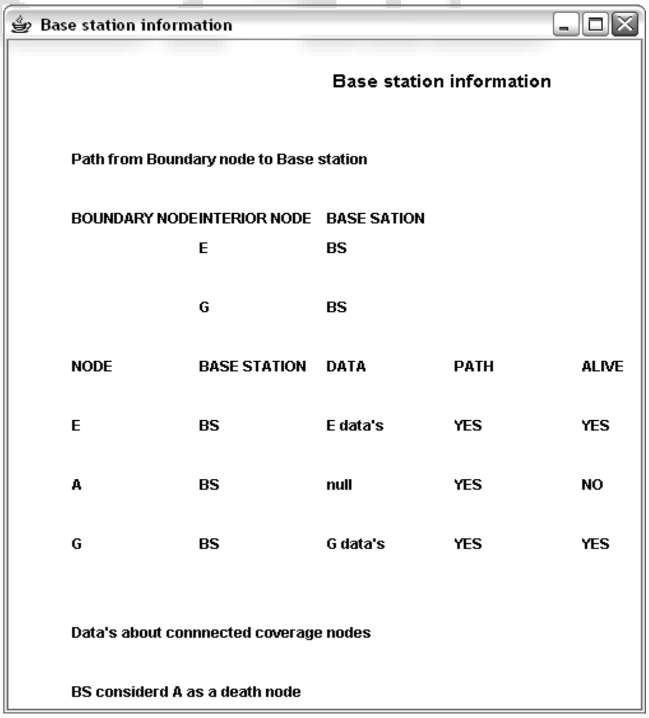


Fig. 10: Victim Node Detection

C. Efficient Node management Technique

In our proposed method a node consist of five low power sensors were used. The sensor having the highest threshold value can act as a header of the node. The head sensor packet value can be calculated as follows,

1) Let Sij be the sensors in the node Ni7. .
2) Node Ni consists of collection of sensors. Here Sensors Sij's placed in the central part of the Hexagon in the node Ni.
3) Hs ij be the head of the sensor in a node Ni, which dynamically change based on their weight.
4) Head Assignment,
   Let W ij[S ij] = W [k] (3.2)
   Initially t=0, where t is a time measure,
   At t=0, HS ij = S ij when j=1
5) If t>0 and W ij [t] < W ij [t+1] then
   Hs ij = max [W ij (t)] (3.3)

The header sensor sends the collected packet Information to the base station. Likewise all the header sensors of the entire connected network sends the collated information to base station. If a particular sensor in a node dies the subordinate sensors or the sensors of the connected area, will gather the information. So, there is no loss of information and maximum coverage is achieved in our work.

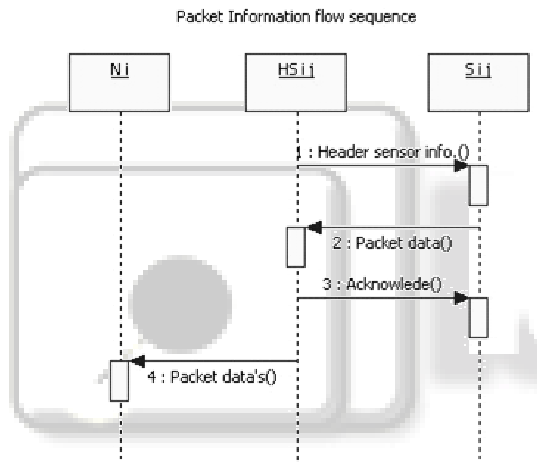
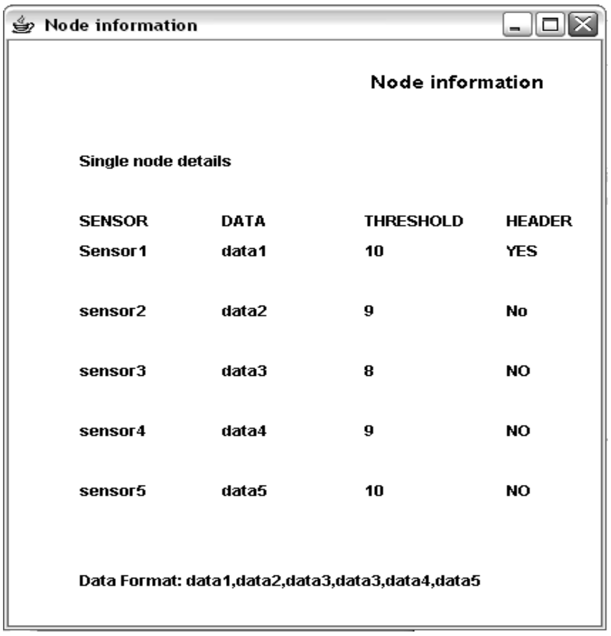


Fig. 11: Path Information Sequence


Node information

Node information

Single node details

SENSOR	DATA	THRESHOLD	HEADER
Sensor1	data1	10	YES
sensor2	data2	9	No
sensor3	data3	8	NO
sensor4	data4	9	NO
sensor5	data5	10	NO

Data Format: data1,data2,data3,data3,data4,data5

Fig. 12: Node configuration

Fig 11illustrates the sequence of the path information gathered by the head sensor node of the connected region and it transmits the data to the neighbour node. Fig (12) shows the efficient node management technique, to identify the header of highest threshold value of the sensors in a particular node. The header sensors having the same threshold value can be chosen based on the distance of neighbour nodes.

IV. CONCLUSION

In this paper, we propose a cellular architecture sensor for wireless sensor networks. The architecture arrangement provides modern solution to security critical and military application. Future potential work as load balancing, Network health monitoring

REFERENCES

[1] Chi Zhang, Student Member, IEEE, Yanchao Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE "A Coverage Inference Protocol for Wireless Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 6, JUNE 2010.

[2] X. Bai, S. Kumar, D. Xuan, Z. Yun, and T. Lai, "Deploying Wireless Sensors to Achieve Both Coverage and Connectivity," Proc. ACM MobiHoc, May 2006.

[3] C. Zhang, Y. Zhang, and Y. Fang, "Detecting Boundary Nodes in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Networking, Sensing and Control, Apr. 2006.

[4] C. Hsin and M. Liu, "Self-Monitoring of Wireless Sensor Networks," J. Computer Comm., special issue on sensor networks, vol. 29, no. 4, pp. 462-476, Feb. 2006.

[5] C. Zhang, Y. Zhang, and Y. Fang, "Localized Algorithms for Coverage Boundary Detection in Wireless Sensor Networks, Wireless Networks, vol. 15, no. 1, pp. 3-20, Jan. 2009.

[6] H. Zhang and J. Hou, "Maintaining Sensing Coverage and on connectivity in Large Sensor Networks," Wireless Ad Hoc and Sensor Network, vol. 1, nos. 1/2, pp. 89-123, Jan. 2005.

[7] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks. John Wiley Sons, Inc., 2005.

[8] M. Cagalj, S. Capkun, and J. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2006.

[9] Q. Fang, J. Gao, and L. Guibas, "Locating and Bypassing Routing Holes in Sensor Networks," Proc. IEEE INFOCOM, Mar. 2004.

[10] M. Franceschetti, L. Booth, M. Cook, R. Meester, and J. Bruck, "Percolation of Multi-Hop Wireless Networks," Technical Report UCB/ERL M03/18, Electrical Engineering and Computer Science Dept., Univ. of California, Berkeley, 2003.

[11] A. Ghosh, "Estimating Coverage Holes and Enhancing Coverage in Mixed Sensor Networks," Proc. Ann.

IEEE Int'l Conf. Local Computer Networks (LCN '04), Nov. 2004.
[12] P. Gupta and P.R. Kumar, "Critical Power for Asymptotic Connectivity in Wireless Networks," Stochastic Analysis, Control, Optimization and Applications: A Volume in Honour of W.H. Fleming, Birkhauser, 1998.
[13] P. Hall, Introduction to the Theory of Coverage Processes. John Wiley Sons, Inc., 1988.
[14] J.M. Hellerstein, W. Hong, S. Madden, and K. Stanek, "Beyond Average: Towards Sophisticated Sensing with Queries," Proc. Second Int'l Workshop Information Processing in Sensor Networks (IPSN '03), Mar. 2003.
[15] C. Hsin and M. Liu, "Self-Monitoring of Wireless Sensor Networks," J. Computer Comm., special issue on sensor networks,vol. 29, no. 4, pp. 462-476, Feb. 2006.
[16] C.F. Huang and Y.C. Tseng, "The Coverage Problem in a Wireless Sensor Network," Proc. Second ACM Int'l Workshop Wireless Sensor Networks and Applications (WSNA '03), Sept. 2003.ZHANG ET AL.: A COVERAGE INFERENCE PROTOCOL FOR WIRELESS SENSOR NETWORKS 863
[17] S. Kapoor and X. Li, "Proximity Structures for Geometric Graphs,"Algorithms and Data Structures, Springer, July 2003.
[18] H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks. John Wiley Sons, Inc., 2005.