Fast and Secure Convergecast in Tree Cluster Based Wireless Sensor Network

Mr. S. Kathirvel#, Ms. K. Pradeepa*
#Department of Computer Science and Engineering,
#Kalasalingam University(#Accredited by NAAC),
Krishnankovil, Virudhunagar District, Tamil Nadu.

ABSTRACT

A wireless sensor network is a collection of nodes organized into a cooperative network. It comprising of spatially appropriated self-ruling mechanisms utilizing sensors to screen physical or ecological conditions. Now the days wireless sensor network is applied many applications like military, nuclear power plant such that. In that applications data transmission rate should be in higher manner and the data transmission time by should be very lower and all the nodes are in the cluster should be very secure also. For that single source shortest path algorithm – Dijkstra's algorithm that is going to be used in this project, from this algorithm the intermediate node between the sender and the sink node will be reduced and the data path will be reduced and the data transmission time will be reduced .If the node and the cluster in not secure the sensed data will be read by some one of the intruder. For secure our cluster three tier security scheme will be used in this project. In this security scheme the node, cluster head, sink node are having their own key that is known by only in the own cluster nodes. If any node wants to be sending any data to any one of the node, the sender key is verified by the receiver. From this way the unauthorized node will be eliminated from the cluster. That three tier security scheme is achieved by the MD5 hashing algorithm in this project.

Keywords— MD5 hashing, Single source shortest path, Three tier security.

1. INTRODUCTION

In the sensor hubs are made by the clients and the hubs are sent in the fields. The conveyed hub immediately begins their sensing work and transmitting the sensed data to the controller accordingly the sink hub. This is the essential idea of the sensor hubs, This property is connected in the numerous provision and that requisitions are obliged the information transmission time ought to be in exceptionally lower so are obliged the exchanging information is a speedier way . Fast information gathering with the objective to minimize the timetable length for amassed convergecast has been contemplated and additionally by others , we tentatively researched the effect of transmission power control and different recurrence channels on the calendar length, while the hypothetical angles where we proposed steady consider and logarithmic rough guess calculations on geometric systems (plate charts). Crude information convergecast , where a disseminated time opening work plan is proposed to minimize the schedule length and the time slots , for minimizing those properties we are going to use the single source shortest path algorithm . from this the nodes data path is calculated by their weights or the distance of the node . when the node starts their data transmission to the another node it should choose the shortest path to reach the destination for that the node choose the Dijkstra's algorithm.

2. MOTIVATION

Now a days the sensor devices are used in many variety of applications , such as military applications and nuclear power plant application . In military application the nodes are monitors the human movements on the borders, when the movement is maid the deployed sensor nodes transfer the movement notification to the base station, consider this application the sensor nodes are should transfer the data as much possible to the base station , when the nodes send the data as in delay manner means the reaction of the delay causes the big damage . For avoiding these kinds of problems the sensor nodes are select the shortest path between the sender and the destination node.

3. SHORTEST PATH FINDING AND CLUSTER SECURING ALGORITHM

In this paper we propose the concept of fast data collection towards the network nodes. Single Source Shortest Path algorithm is provide the efficient and faster data collection by avoiding the intermediate node and unnecessary time scheduling in the cluster. And MD5 hashing algorithm is also used in this project for securing the deployed node cluster. The MD5 algorithm is used here as three tier security scheme, from the three tier security we can secure our field node and cluster heads and the sink node . In this security algorithm create the individual public key and the private key for all the nodes . When a node want to send any data to another node means that should know the public key of the receiver node that like a id . and the node add the private key in the sending data too . when the receiver node receives that message the node check the private key of the sender node , like these the other nodes like the cluster heads and sink nodes also follow the method of data transmission, from these way the three tier communication security will manage the security over the cluster .

3.1. Dijkstra's Algorithm

Dijkstra's Algorithm is another well known shortest path routing algorithm. It works on the notion of a candidate neighbouring node set as well as the source's own computation to identify the shortest path to a destination. Another interesting property about Dijkstra's Algorithm is that it computes shortest paths to all destinations from a source, instead of just for a specific pair of source and destination nodes at a time which is very useful, especially in a communication network, since a node wants to compute a shortest path to all destinations.

Algorithm

```
shortest paths ( Graph g, Node s )
 initialise_single_source( g, s )
 S := { 0 }        /* Make S empty */
 Q := Vertices( g ) /* Put the vertices in a PQ */
 while not Empty(Q)
  u := Extract Cheapest( Q );
  Add Node ( S, u );       /* Add u to S */
  for each vertex v in Adjacent( u )
  relax ( u, v, w )
```

Illustration

Sample graph is mentioned above , the 1 -6 nodes are in the edges . The node 1 want to send or reach the node 6 that calculation is explained here that using the Dijkstra's shortest path algorithm .

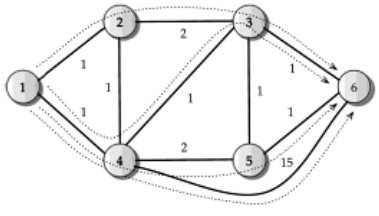

Fig 1 sample path identifying graph

Path	Cost
1-2-3-6	$d_{12}+d_{23}+d_{36}=4$
1-4-3-6	$d_{14}+d_{43}+d_{36}=3$
1-4-5-6	$d_{14}+d_{45}+d_{56}=4$
1-4-6	$d_{14}+d_{46}=16$

Table1. Path identified from node 1 to node 6, along with associated path cost.

By the table the shortest path flow is identified , based on the cost factor the node will be visit by the node .

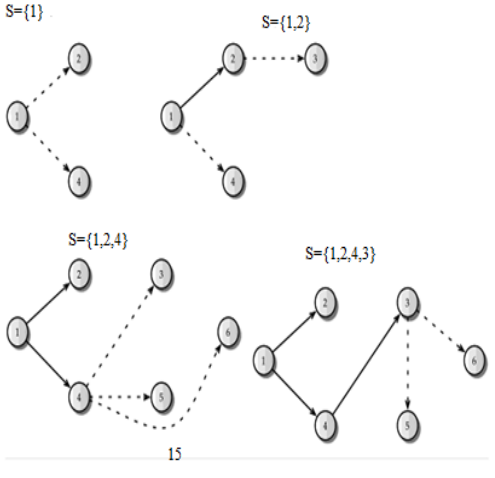

Fig 2 Interactive view of Dijkstra's Algorithm

Thus the way of flow the path will be identified by the dijkstra's algorithm. The remaining node will be eliminated in the resultant graph.

3.2. MD5 Algorithm

The clustering nodes are should be in very secure manner for that we use the Md5 Message-Digest Algorithm is a generally utilized cryptographic hash capacity that transforms a 128-bit (16-byte) hash quality. Md5 has been used in a wide mixed bag of security requisitions. Utilizing Md5, produce a key quality and doled out for every hub in the system, while sending the information to objective, the key worth has been checked by the hand-off hubs and end hub for security. This module guarantees the safe transmission of information parcels over the remote sensor system. Therefore unapproved hub can't send information to the system. Utilizing this security module the greater part of the ambushes in the remote sensor systems, for example reproduction strike, DDos assault, parodying assaults could be evaded based on these algorithm the private key and public key was developed from these algorithm , the public key was announced in the developed cluster but the private key was kept in secure by all the nodes . when the node start the data transmission time only the key was send to the requested node .

Algorithm

Step 1 – Append padded bits

The message is padded so that its length is congruent to 448, modulo 512

A single "1" bit is appended to the message, and then "0"bits are appended so that the length in bits equals 448 modulo 512

Step 2 – Appended length

A 64 bit representation of b is appended to the result of the previous step .

The resulting massage has a length that is an exact multiple of 512 bits

Step 3 – Initialize MD buffer

A four – word buffer (A, B, C, D) is used to compute the message digest.

Step 4 – Process message in 16-word blocks

Four auxiliary functions that take as input three 32-bit words and produce as output one 32-bit word.

Step 5 –Output

The message digest produced as output is A, B, C, D

That is output begins with the low-order bite of A, and end with the high-order bite of D.

4. RESULTS AND ANALYSIS

Fig 3 one hob neighbour table screen

Thus our proposed system was simulate by the Network Simulator 2 and that's terminal screens are display here

From the above picture Fig 3 we can get the detail of one hob neighbour node detail for the all deployed nodes, Based on the one hob neighbour table only the data will be send to the receiver from the sender node.

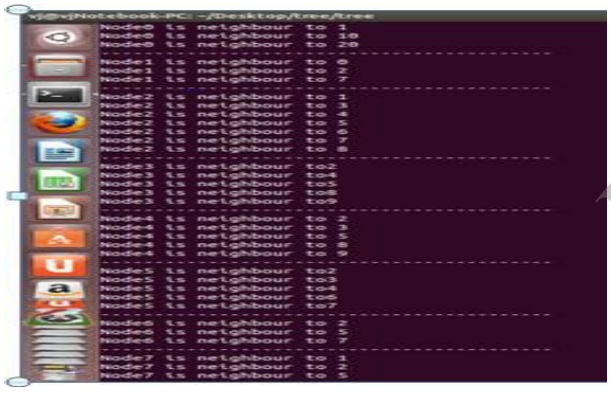

Fig 4 Neighbour node allotment

Based on the Fig 4 one hob neighbour table the neighbour node is allotted that screen is showed in Fig 4

If the data transmission is depend on the neighbour node allotment the sender data need to reach the multiple nodes , By this the Data Transmission time will be increase . But we need to achieve the fast data collection over the nodes , for these we need to avoid unnecessary time slots and reduce the Data Transmission time . These problems is overcome by the Single Source Shortest Path algorithm

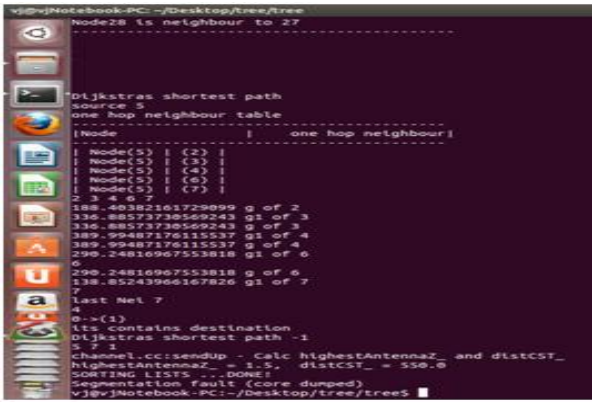

Fig 5 Dijkstra's shortest path calculation

Based on the Fig 5 the dijkstra's calculation is done . After the Dijkstra's calculation the shortest path will be generated . Based on the shortest path only the data will reach the destination from the source node. When the terminal process is over , the Simulator tool will be generate the data flow from the source node based on the Dijkstra's algorithm .

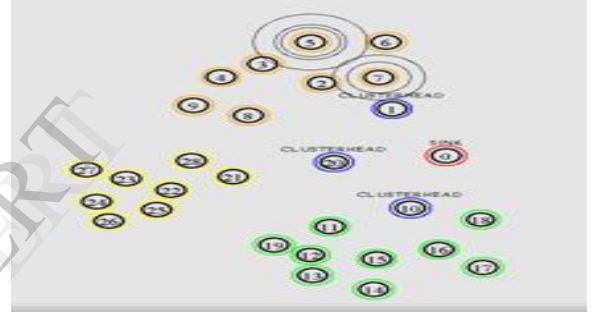

Fig 6 Data Transmission from node 5-7

The Fig 6 shows the data transmission between the node 5-7, because the shortest path 5-7-1 is identified by the Dijkstra's algorithm . Based on the shortest path the node 5 send the data to the node 7 .

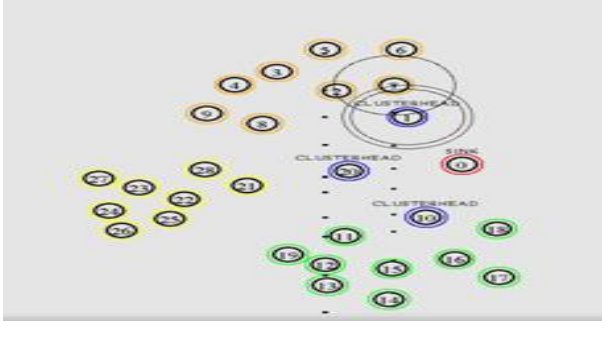

Fig 7 Data Transmission from node 7-1

The Fig 7 shows the data transmission between the node 7-1 , because the shortest path 5-7-1 is identified by the Dijkstra's algorithm . Based on the shortest path the node 5 send the data to the node 7 already , then the received data is transmitted to the cluster head (node 1) by the node 7 .

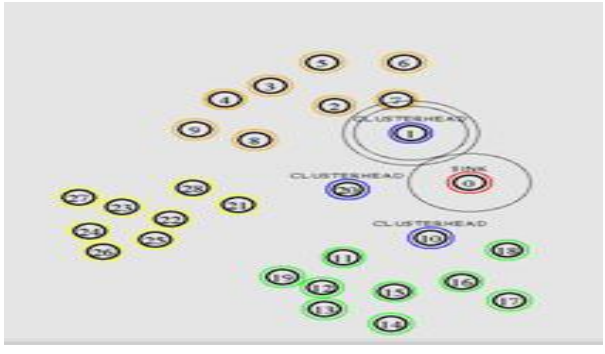

Fig 8. Data Transmission from Cluster head to Sink node

At the final the cluster head will send the received data to the sink node . by this single source shortest path algorithm , the need to transfer over the 2 intermediate node only , so the data will be reach the destination as much as possible.

The NS2 simulation is done and we analysed Throughput, delay and packet drop for the flow taken.

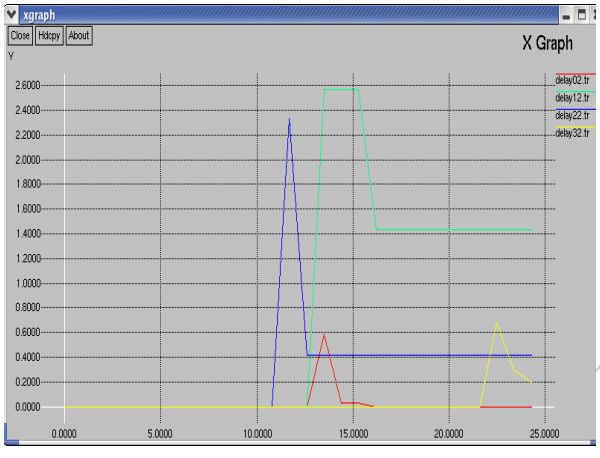

Fig 9. Delay in the simulation phase

The above graph defines the delay in the simulation phase. The experiment was running 25 seconds of time. End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination during the simulation time.

We saw how the sensed information are meet thrown is a speedier way. We executed the Single Source Shortest Path calculation over the different deployments and that simulation is run for the requirement. The TDMA scheduling scheme have the limitation of one node only can transfer the data at that time period but in Multi Channel Scheduling scheme overcome the limitations. The military and atomic power plant sensor requisitions are utilized as a part of extremely speediest data accessing entrance to provisions, so we consolidate the Multi Channel Assignment Scheme and Single Source Shortest Path Algorithm for accomplish the quick data accessing in the conveyed field.

5. CONCLUSION

In this paper, we accomplish the quick convergecast in WSN where the nodes convey utilizing single source shortest path algorithm to minimize schedule length and intermediate node. We deliver the confinements because of interference and half-duplex transceivers on the node and the exploded techniques are overcome by the multichannel assignment scheme. We discovered that while transmission power control helps in diminishing the length, multiple channels are more adequate that is realized in this paper. We have developed the data convergecast and data transmission over the sensor network is an faster manner . But the nodes authentication is not verified by any other , by the chance the intruder node will be in our cluster , there may be the chance of attack our nodes and service , so we can improve the security over the sensor nodes in future .

REFERENCES

1. S. Gandham, Y. Zhang, and Q. Huang, “Distributed time-optimal scheduling for convergecast in wireless sensor networks,” Computer Networks, vol. 52, no. 3, pp. 610–629, 2010.
2. K. K. Chintalapudi and L. Venkatraman, “On the design of mac protocols for low-latency hard real-time discrete control applications over 802.15.4 hardware,” in IPSN ’08, pp. 356–367.
3. I. Talzi, A. Hasler, S. Gruber, and C. Tschudin, “Permasense: investigating permafrost with a wsn in the swiss alps,” in EmNets ’07, Cork, Ireland, pp. 8–12.
4. S. Upadhyayula and S. Gupta, “Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced convergecast (dac) in wireless sensor networks,” Ad Hoc Networks, vol. 5, no. 5, pp. 626–648, 2011.
5. T. Moscibroda, “The worst-case capacity of wireless sensor networks,” in IPSN ’07, Cambridge, MA, USA, pp. 1–10.
6. T. ElBatt and A. Ephremides, “Joint scheduling and power control for wireless ad-hoc networks,” in INFOCOM ’02, Jun, pp. 976–984.
7. O. D. Incel and B. Krishnamachari, “Enhancing the data collection rate of tree-based aggregation in wireless sensor networks,” in SECON ’08, San Francisco, CA, USA, pp. 569–577.
8. Y. Wu, J. Stankovic, T. He, and S. Lin, “Realistic and efficient multi-channel communications in wireless sensor networks,” in INFOCOM ’08, pp. 1193–1201.
9. A. Ghosh, O. D. Incel, V. A. Kumar, and B. Krishnamachari, “Multi-channel scheduling algorithms for fast aggregated convergecast in sensor networks,” in MASS ’09, Macau, China.
10. V. Annamalai, S. Gupta, and L. Schwiebert, “On tree-based convergecasting in wireless sensor networks,” in WCNC ’03, vol. 3, pp. 2011–2012.