# A Novel Approach based on Reliable Messaging Protocol for Sensor Network Navigation without Locations

Sandeep Singh<sup>1</sup>, Prof. Chahat Jain<sup>2</sup>, Prof. Daljit Singh<sup>3</sup>

<sup>1, 2, 3</sup>(ECE, Guru Nanak Dev Engineering College Ludhiana/ India)

**ABSTRACT**: A network with sensors using wireless connectivity like Telosb mote that helps the people to navigate without the use of internet or data on their smart phones. This application is based on the use of map of an area without paying to any network provider. This application is entirely different from the others by the means of network usage and the cost to prior to their locations with specifying the dangerous areas around the roads. This paper has put forward the idea of a modified reliable messaging protocol which provides the proper way out from dangerous field with navigation routes. This paper accordingly design a system faces nontrivial challenges which gives us effective and efficient protocol. The system supports multiple users simultaneously in a network. Therefore, the system is highly scalable which rebuilt itself in event of dangerous areas on the field. This paper compares and conducts simulation of this protocol with others to examine the scalability and

*Keywords* - *Mapping of roads, Network with sensors using wireless connectivity, Routes for piloting, Telosb mote* 

## I. INTRODUCTION

The emanate field of sensor networks which use wireless connectivity gives us new classes of applications that provide a fast response in large number of fields. Wireless sensor network is used as a data acquisition to transfer data in between two minims or more. It is the fastest and the one the reliable mode of transmission with high security and safe reception at low cost in the field.

Wireless sensor network (WSN) provides advancement in safety of military to agriculture and has various applications in daily routine works as well as monitoring, control and home based networks [1], [2]. WSNs consist of small, inexpensive devices that communicate with each other using a wireless communication based on multi hop keying. A wireless sensor network has some protocols and algorithms to adapt the emerged situation. There are a lot of nodes in the networks. Each node has itself a different identity which makes itself a different executer. Each node consist of processor, sensor, memory, antenna and battery mainly AAA batteries. More than 2 nodes make a cluster. Cluster is nothing just the group of nodes it's just named to identify the group of nodes in the network. Each cluster has one node which control and gives instruction to the whole cluster nodes which itself called a cluster head (CH).

In this work, Reliable Messaging Protocol has been modified based on potential field and skeleton graph approaches. The performance of the network has been analyzed and the proposed work is compared with previous method.

## II. PROBLEM SPECIFICATION

Sensors are the one of the biggest and most powerful deployment of the scientist towards the wireless network. Before these wireless networks were used for data acquisition only. But these sensors give us new application which has to be implemented in the network. So prior to this they have implemented sensors of different types according to avail in the network. In this statement of undertaking individually present a work towards the sensor network navigation scheme but without use of server. It's generally implemented on mountains, hills or GPS denied environments. In this individually made an algorithm which detects the emergency and gives us the best way to go out from emergency occurred in the field. In this section individually deals with objective, methodology and software used for the reliable messaging protocol. Tinyos 2.1.2 is the latest version of tinyos software which operates on open source operating system mainly designed for embedded sensor networks.

## III. DESIGN PRINCIPLES

In this design of advanced reliable messaging protocol is done at Bluetooth technology using ZIGBEX. Then the comparative analysis in terms of output characteristics and linear characteristics are done.

## **Design Procedure**

For designing Sensor network navigation following steps are followed:-

1. Write the Nesc script of the route that is to be design. The Nesc script is used to define the device parameters and process.

2. Device Parameters are the basically the specification of the devices in the details. It includes information such as design rule length unit (technology), devices architecture details such as length, width, height etc.

3. Device process uses the device parameters to form the actual devices. For example it uses different sensor to define the different region of the network such as simple and emergency and uses device parameters to define its length, width and height.

4. In order to make structure from Nesc script we need layout diagram of the device. The layout diagram is used to represent the different types of the devices such telosb-mote, zigbex and mica2.

5. Then the AVR Modeler is used to create the hex file. It is a file that contains device information in the form of binary digits.

The hex file is then load in the device simulator to perform the simulation analysis.

#### Design Process

To build the basic structure of the system individually deploys all the latent nodes on the field. They are used for communication and sensing purposes in the network. They are Telosb mote sensors with low power wireless module [9] for the sensor networks.

Fig. 1 shows black minims on the field which are latent sensor nodes, M shows mobile node and S is the super node which gives instruction to all the nodes. Mobile nodes are worn to convoke the data in distinction to the latent node and send it to the super node.

## A. Deployment of latent sensor nodes

Latent nodes which goes into threatening field individually referred them as the sleeping nodes in the network as shown in the Fig. 1. They can't Transmit or receive any data and so that's why the detection of threatening field [10] is easily possible. Mainly according to sleeping nodes individually detect the threatening field in the network.

Algorithm 1. Utilization of latent nodes

- 1. While PURE do
- 2. Disclose the site
- 3. If site! = Threatening fields! = main minim then



Fig. 1: Structure of the whole system.

- 4. Send piloting specifications
- 5. Else
- 6. Node preserve rest & shut off monitor
- 7. End if
- 8. If piloting retort! = TRUE then
- 9. node retain rest
- 10. else

- 11. simulcast piloting message
- 12. end if
- 13. end while



Fig. 2. Motile nodes (a) Raster scanning (b) Mobile node site.

Firstly in the whole area raster scanning has to be done as shown in figure above. It is from one sensor to another but it only done in between mobile nodes, no latent node is included in this scanning. After this all the mobile nodes near the area of threatening field make a shape as shown in Fig. 2(b) which detect and make the whole threatening area a dead zone.

Algorithm 2: Mobile nodes describes threatening fields

- 1: while signal gathered the latent nodes' signal act
- 2: Do raster overlooking
- 3: Haul the element
- 4: Outset algorithm
- 5: if element = 0 then
- 6: if other mobile nodes! = 1 halt then
- 7: halt like a latent node
- 8: send memo of alarm
- 9: else reprieve the element
- 10: end if
- 11: else
- 12: raster overlooking
- 13: end if
- 14: end while

#### B. Escorting Piloting on the Road Map

In general way piloting can be described in 3 sections.

1) Where I am now (Decide the site of user) – In this mobile node is in which latent node decide the site of the user on the field.

2) Where should I go – Mobile node detects latent node and then latent node find the cluster in the mobile nodes which controls all the mobile nodes [11] in the network also called as super node. Then super node gives instructions to nodes to make a safe path from mobile node user to the end or destination.

3) How to arrive – just follow the mobile to mobile nodes in latent nodes and go to the super node you reached on the destination as shown in figure above.

Algorithm 3: Piloting of mobile sensor user 1: While action message gathered = TRUE Do 2: if appeared! = TRUE then 3: if mobile cautioning message! = TRUE then 4: avail Bluetooth 5: else 6: use same and repeat it 7: end if 8: else

Special Issue - AETM'16

- 9: send message is attained 10: inform node is shut off 11: end if
- 12: end while

## C. Reacting to Emergency Dynamics and Route Efficiency

This depends upon the edge weights of the road map. It is used to find sub path and short path from the emergency event to the destination. The weight of the edge is based on the length of the edge. Edge weights are just for some time and after that interval it expires. The weight of edge e is:

Algorithm 4: Roadmap Edge Query

- 1. If message gathered
- 2. Obtain it if in ruling area
- 3. Set transmitting node a dawning node
- 4. Set hii to step toll in message plus 1
- 5. Execute forwarding rule to check if message should be re-transmitted
- 6. If yes, re-transmit message

7. Execute reply rule to check if concern result should be transmitted. If yes, Weigh time to transmit result and set timer transmit Timer to time-out at the final time

8. Else if species ism reply gathered

IV.

V.

- 9. Else if transmit Timer timed out
- 10. Transmit conclusions to user

## IMPLEMENTATION EXPERIENCE

To contrivance such a protocol in system, individually need to meticulously dwell some technical matter when exploiting in this propositions in a sensor network. In this individually approximate the space of two nodes by closing the counting of hops from transmitter to receiver means from start to end. Individually describe some volatiles which verdict the prestige of each node. Threat marks ongoing node dwell in or out to the threatening area. If threat is 1 then it occupies in the threatening area if 0 then does not possess threatening area. *Dist* records the space from the ongoing node to the tolerable area on the threatening field, and *s.mSet* analyze and save the combination of nodes on the horizon areas of threatening field. *Next Hop.r.s* and *s.rDist* are two fickles that chronicles the rated information for the node on the map road site. *Next Hop* fetch and save the number close to next hop sensor forth the direction on the road close to path. *Dist* detects the nearest distance to the areas of the threatening events crop up from the ongoing node to the shut off node.

#### PERFORMANCE EVALUATION

The performance ratio is defined to be  $h/h_{opt}$ . A higher ratio demonstrates an improved security of the prepared track, as the closest surface from the track to the threatening areas is larger.

## A. Minimum Distance to Threat

In minimum distance to threat H denote the closest area from the prepared track to the threatening areas, and  $h_{opt}$  specify the minimum distance to the threatening areas from the originating path that maximizes d. For a path touching any two minima's presented on the streets,  $h/h_{opt} = \text{constant}$ .

Where  $h_{opt=} \{ 1/(d+x)^{\beta-1} \}$ 

## **B.** Abbreviated Path

Abbreviated path is also depends upon the performance ratio which is  $1/l_{opt}$ . Individually appraise the path capability by correlating the area of the route deal in each access with the area of the abbreviated path that does not go over from the threatening areas  $l_{opt}$ .

Algorithm 5. The abbreviated path Algorithm.

- 1: Let H be a target sensor
- 2: H telecastmessage=  $(H_{id}, my_{id}(H), hidden= 0)$
- 3: **for** sensor s<sub>a</sub>**do**
- 4: **if** receive (h, q, pod) **then**
- 5: if I am not a sensor and warm-risk<sub>i</sub>=warm-risk<sub>Hid</sub> then do nothing
- 6: if I am a sensor or warm-risk<sub>i</sub>= warm-risk<sub>Hid</sub> then
- 7: Guage the hidden integration from the output to here##
- 8: **if**  $H_g$ > hidden+ pod(r,q) **then**

9: pot (r, q) is the hidden integration from satosq##

- 10:  $h_g = pod + pod(r, q)$
- 12: brior<sub>h</sub>= q
- 13: telecast  $(H_{id} = r, my_{id}(s_a), H_g)$



Fig. 3. Comparative Results Of The Performance Ratios (A) Minimum Distance To The Threat, (B) Abbreviated Path.

#### VI. CONCLUSION

The future of technology aim for sensors that can send its research data and images from any part of the world and also sensors that can gives high speed connectivity and provides piloting services to people at any place and anytime. With the proper analysis, this work has put forward the idea for wireless sensor network communication but with a better and advanced approach. A system which is highly flexible yet compact with reliability and improved connectivity summed up as an efficient but low cost as its priority has been discussed. In comparison with the previous approaches, this work has come up with advancement of 10 % - 30 % in the factors described in reliable messaging protocol. Minimum distance to threat has been improved from the previous versions with approximately 60%. Another tremendous change, recorded as 20-25 %, which can be noticed is in case of the abbreviated path

#### REFERENCES

- P. Dahiya, "Comparison of two algorithms used to improve the energy of low energy nodes in WSN," International Conference on of advance research in computer science and management studies, India, vol.1, no.6, pp. 40-44,11 November 2013.
- [2] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," IEEE Communication Survey, vol. 15, no. 2, pp. 551-591, May 2013.
- [3] S. Giannoulis, C. Koulamas1, C. Emmanouilidis, P. Pistofidis, D. Karampatzakis, "In Proceeding of Wireless Sensor Network Technologies for Condition Monitoring of Industrial Assets." Springer, Berlin Heidelberg, pp.33-40, May 2013.
- [4] S. Mamalis, S. Basilis, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "Clustering in wireless sensor networks." RFID and Sensor Networks: Architectures, Protocols, Security and Integrations, 1st edition,pp. 324-353, Norway, Canada, CRC press, 12 November 2009.
- [5] Dargie, Waltenegus, and Christian Poellabauer, "Fundamentals of wireless sensor networks: theory and practice." 1st edition, pp. 5-8, University of California, Canada, John Wiley & Sons, 5 July 2010.
- [6] Y. C. Tseng, M. S. Pan, and Y. Y. Tsai. "A distributed emergency navigation algorithm for wireless sensor networks." Proceedings of the IEEE, Hsin-chu, Taiwan, Vol.39, no.7, pp. 55-62, September 2006.
- [7] M. S. Pan, C. H. Tsai, and Y. C. Tseng. "Emergency guiding and monitoring applications in indoor 3D environments by wireless sensor networks." International Journal of Sensor Networks, Hsin-chu, Taiwan, Vol.1, no.1, pp. 2-10, January 2006.

- [8] V. Katiyar, N. Chand, and N. Chauhan, "Recent advances and future trends in Wireless Sensor Networks," International Journal of Applied Engineering Research, Dindigul, Tamil Nadu, India, vol.1, no.3, pp. 330-342, 29 September 2010.
- P. Levis, S. Madden and D. Culler, "Tinyos: An Operating System for sensor networks." In Ambient intelligence. Springer Berlin Heidelberg, vol.1, no. 2, pp. 115-148, 11 January 2005.
- [10] B. Cross, (2004, May 10). Telosb Datasheet (1st Ed.) [Online]. Available: www.willow.co.uk
- [11] Zhenjiang Li, Yunhao Liu, Jiliang Wang, and Zheng Yang. "Sensor network navigation without locations." IEEE Transaction on parallel and distributed systems, Rio-de jenerio, Brazil, vol. 24, no. 7, pp. 1436-1446, July 2013.
- [12] S.Singh, N.S.Grewal, "Improved deployment of sensor in reliable masseging protocol for sensor network navigation without locations." International Journal Of Recent Advances In Engineering & Technology, india, vol.3, pp. 2347-2812, October 2015.