WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Alternative Navigation with Localizability-Aided Localization in Wireless Sensor Networks

Dr. Sheryl Radley[1], Mrs.B Vennilapriya[2], Mrs. N Mohana Priya[3]

Associate Professor[1], Assistant Professor[2,3]
Meenakshi College of Engineering[1,2,3]
Chennai, Tamil Nadu[1,2,3]
sherylannie@gmail.com[1],vennila.pets@gmail.com[2], mohanaamaran22@gmail.com[3]

ABSTRACT:

The navigation service for emergency evacuation is one of the key uses of wireless sensor networks (WSNs), with the purpose of assisting people in safely and rapidly departing from a dangerous place when an emergency occurs. Most existing methods concentrate on determining the safest approach for each individual, while neglecting the possibility of significant detours and traffic congestion created by a big number of individuals hurrying to the exit. Users have PDAs or smart phones that can readily communicate with the sensors. When an emergency arises, the WSN provides users with the essential information so that they can be led out of a dangerous location by interacting with sensors. Combining a wireless network sensor with a navigation algorithm could enable people safely get to a building escape while avoiding hazardous areas. A network is not necessarily completely localizable, leaving a number of nodes that are theoretically unlocalizable. Focus on how to fine-tune network settings so that a network can be localized. However, existing methods are regarded as coarse-grained because they deal equally with localizable and non-localizable nodes, and ignoring localizability results in unnecessary adjustments and costs. To propose a fine-grained approach, localizability-aided localization consists of three phases: node localizability testing, structure analysis, and network adjustment.

Keywords:Wireless Sensor Network,Localizability-Aided Localization, communication networks,emergency evacuation.

INTRODUCTION

Wireless sensor networks (WSNs), also known as wireless sensor and actuator networks (WSANs), are a type of sensor network that uses spatially distributed autonomous sensors to monitor physical or environmental conditions like temperature, sound, and pressure, and to cooperatively pass their data through the network to a central location. Modern networks are bi-directional, allowing sensor activity to be controlled. Wireless Sensor Networks (WSNs) are networks made up of sensors that are deployed ad hoc. These sensors work together to detect some physical phenomenon, and the data is subsequently processed to produce useful findings. Wireless sensor networks are made up of self-organizing protocols and algorithms. Military uses such as battlefield surveillance sparked the creation of wireless sensor networks, which are now utilized in a variety of industrial and consumer applications, including industrial process monitoring and control, machine health monitoring, and so on. The WSN is made up of "nodes," which range in number from a few to hundreds or even thousands, each of which is connected to one (or sometimes several) sensors. A radio transceiver with an internal antenna or a connection to an external antenna, a microcontroller, an electrical circuit for interfacing with the sensors, and an energy source, usually a battery or an embedded form of energy harvesting, are all typical components of a sensor network node. Although functional "motes" of true microscopic proportions have yet to be constructed, a sensor node might be the size of a shoebox down to the size of a particle of dust. Sensor node prices vary widely, from a few dollars to hundreds of dollars, depending on the sophistication of the individual sensor nodes. Sensor node size and cost constraints impose restrictions on resources such as energy, memory, computing speed, and communications bandwidth. WSNs can have a variety of topologies, ranging from a basic star network to a complex multi-hop wireless mesh network. Routing or flooding are two methods for propagating data between network hops.

Wireless sensor networks are an important study area in computer science and telecommunications, with multiple workshops and conferences held each year, such as IPSN, SenSys, and EWSN.

The following are the major characteristics of a WSN: Power consumption restrictions for nodes utilizing batteries, Resilience to node failures, Some mobility of nodes (see MWSNs for extremely mobile nodes), Heterogeneity of nodes, Scalability to large scale deployment Ease of usage, ability to tolerate extreme environmental conditions Design with multiple layers. As a result, the cross-layer can be utilized to make the best modulation in order to increase transmission performance, such as data rate, energy efficiency, and QoS (Quality of Service), among other things. Sensor nodes can be thought of as miniature computers with very minimal interfaces and components. A processor unit with limited computing capability and memory,

sensors or MEMS (with appropriate conditioning circuitry), a communication device (typically radio transceivers or alternatively optical), and a power source (generally in the form of a battery) are the most common components. Energy harvesting modules, secondary ASICs, and even secondary communication interfaces are also possibilities (e.g. RS-232 or USB).

RESEARCH CHALLENGES IN WIRELESS SENSOR NETWORKS

A brief history of SN research is offered, however the overview of technical obstacles and issues presented may be more fascinating, from which we might highlight some pertinent items: WSN in a tough environment; network ability (leastways neighbors); network control and routing; querying and tasking (should be as simple and clear as possible); plus security considerations (low latency, survivability, low probability of detecting communications, high dependability) Security: The terms "authentication," "integrity," "privacy," "non-repudiation," and "anti-playback" are often used interchangeably. The more the reliance on information provided by networks, the greater the risk of secure information transfer in networks. Several well-known cryptography, steganography, and other techniques are used to ensure the secure transmission of various types of data through networks. In this section, we'll go through the principles of network security, with a focus on wireless sensor networks.

Cryptography: Encryption and decryption techniques developed for traditional wired networks cannot be readily applied to wireless networks, particularly wireless sensor networks. WSNs contain small sensors that are severely hampered by a lack of processing, memory, and power. When applying encryption systems to WSNs, such as what kind of keys are generated or distributed, security mechanisms such as encryption may cause increased delay, jitter, and packet loss in wireless sensor networks. How are keys maintained, revoked, assigned to new sensors added to the network, or renewed to ensure network security? Pre-loaded or integrated keys are unlikely to be a cost-effective solution. Steganography: Unlike cryptography, which seeks to hide only the essential parts of a communication, steganography aims to hide the entire message. Steganography is the art of hiding information in multimedia material by embedding a note (image, sound, video, etc.). The main goal of steganography is to change the carrier in such a way that it is undetectable, and so appears to be normal.

Secure Physical Layer Access: Frequency hopping could be used to provide physical layer secure access in wireless sensor networks. With a minimal cost in memory, processing, and resources, a dynamic mixture of parameters such as hopping set (available frequencies for hopping), dwell time (interval each hop), and hopping pattern (the sequence in which the frequencies in the available hopping set are employed) might be blended. Important aspects of physical layer safe access will be the efficient design, which allows the hopping sequence to be adjusted in less time than it takes to discover it, and the use of a synchronized clock by both the transmitter and receiver. It is possible to use a system like the one presented in to create secure physical layer access using singular vectors and channel generated modulation. Attacks on wireless sensor networks can be viewed from two different perspectives. The first is an attack from security mechanisms, and this band is outstanding from the ground up (like routing mechanisms). The most significant threats in wireless sensor networks are signaled by ideas.

Localization is one of the most important approaches in a wireless sensor network. Target / source localization and node self-localization are the two most common types of place estimation methods. The energy-based technique is primarily introduced in target localisation. After that, we look into node self-localization methods. Because of the extensive use of wireless sensor networks, the localisation algorithms used in various applications are diverse. There are various challenges that require the use of unique circumstances. We offer a broad overview of these difficulties in this paper: Non-line-of-sight localization, node selection criteria for localization in energy-constrained networks, sensor node scheduling to optimize the tradeoff between localization performance and energy consumption, cooperative node localization, and localization algorithm in heterogeneous networks are all topics covered in this paper. Finally, we discuss the criteria for evaluating localization in a wireless sensor network. Node self-localization refers to the complete process of estimating an unknown node's position inside a network. And a WSN is made up of a large number of low-cost nodes that are densely distributed in a certain area to assess specific phenomena. The most important goal would be to figure out where the target is. Localization is important since some travelers are unsure of the exact position of various fixed or mobile gadgets. One example is the monitoring of humidity and temperature in forests and/or fields, where thousands of sensors are placed by plane, leaving the operator with few options for influencing the node's location. To infer the positioning of individual devices, an efficient localization algorithm could use all of the free information from the wireless sensor nodes. Another use will be the positioning of a mobile robot based on the strength of the received signal from the number of radio beacons set at recognized places around the factory floor. The fundamental purpose of a location estimation method is to calculate the geographic coordinates of network nodes in the deployment region that are unknown. The process of finding the geographical positions of sensors in wireless sensor networks is known as localization. Only a few sensors (anchors) within the networks have prior knowledge of their geographic locations. To find the placements of the remaining sensors, localization algorithms use anchor location information and distance estimates between surrounding nodes.

Power-Consumption: When connecting a sensor node to the mains is problematic or impossible, a wireless sensor node is a popular option. However, because the wireless sensor node is usually located in a difficult-to-reach place, changing the battery on a regular basis will be costly and cumbersome. Making sure that there is always enough energy available to power the system is an important consideration when introducing a wireless sensor node. The rate of facility consumption for sensors in a wireless sensor network varies substantially depending on the communication protocols used by the sensors. The Gossip-Based Sleep Protocol (GSP) saves energy by implementing routing and various MAC functionalities. GSP's efficacy has already been shown through simulation. However, no prototype system has ever been constructed before. GSP was deployed on the Mica2 platform, and measurements were taken to see how much the network lifetime improved. The results of energy consumption, sent and received power, the minimum voltage supply required for operation, the effect of transmission power on energy consumption, and several methods for measuring the time of a sensor node are presented. The behavior of sensor nodes towards the end of their lifespan is described and analyzed.

LITERATURE REVIEW

The wired network has existed for decades, far longer than the internet. Wired networks are more secure and have quicker transmission speeds than wireless networks. Wires, on the other hand, are one of the most significant developing issues in wired networks. Complex wiring and power cords are tough to manage and reduce flexibility significantly. The bottleneck in the development of a wired network is wiring and rewiring. As wireless technology advances, an increasing number of people prefer to use a wireless network as their end-user network. WSN offers its own advantages over standard wireless networks, such as low cost and low energy usage [1]. Each sensor board has very minimal onboard resources, such as computer speed, storage, and energy source, in order to save money. Onboard components are designed to consume as little energy as possible to have a long lifetime with a restricted power supply, usually batteries. The transmission power of radio, for example, is 1000 times lower than that of Wi-Fi routers. WSN is always installed in difficult-to-reach regions, and self-configuration is a design aim as well.

Because physical measurements are primarily regulated by the rule of diffusion, most physical phenomena have substantial spatial and temporal correlations. The topic of tracking contours represented by binary sensors is investigated in this work, with a focus on light-weight preservation of contours that evolve over time. A variety of tracking and monitoring applications have motivated this abstracted challenge. Scenarios involving contour tracking Consider the following use case: the sensors are used to detect and track chemical contamination [2]. Each sensor detects the chemical concentration in its immediate environment. The pollution map demonstrates substantial geographical correlation and is generally modeled and depicted by a smooth signal field [3], as chemical contamination often emanates from some pollution source, and pollutants are typically propagated by water current, wind, or diffusion. With sensor readings above a danger threshold, contaminated regions spontaneously form a number of (potentially nested) blobs. The blobs may change, merge, or separate over time, reflecting pollutant movement and/or pollution remediation success. A group of targets moving in a field, for example, may notify nearby monitoring sound sensors [4]. In nature, target movements such as human, vehicle, and animal movements tend to cluster. The contour of acoustic readings above a given threshold can be tracked to monitor a group target. Contour changes offer crucial information, such as the formation of a team or gathering, vehicle dispersion, or specific animal actions. It facilitates improved tracking [5].

We suggest using the sensor network architecture as a cyber-physical system to navigate internal users through potentially dangerous areas. In contrast to earlier work, our proposed application treats the sensor network as a data collecting medium, but in our navigation application, in-situ interactions between users and sensors become pervasive [6]. Furthermore, human safety and time constraints are vital to our goal's accomplishment. The design of an effective and efficient navigation protocol involves nontrivial issues without any prior information of user and sensor locations. We suggest embedding a road map system in the sensor network without providing position information in order to provide users with guaranteed safety when traveling routes [7]. In order to rebuild the road map in the event of modifications in dangerous locations, we design effective road map update processes. Each user in this navigation system just makes local queries to get their navigation route. The system is highly scalable, allowing it to accommodate several users at the same time. To test the effectiveness of this architecture, we build a prototype system with 36 TelosB motes.
Over a continuous scalar field, we investigate the challenge of data-driven routing and navigation in a distributed sensor network. We specifically address the challenge of locating a set of sensors with readings that fall within a given range. The iso-contour query problem is what it's called. We devise a gradient-based routing technique in which the query message follows the signal field gradient or derived values from any query node and successfully discovers all iso-contours of interest [8]. Because of the presence of local maxima and minima, guaranteed delivery necessitates pre-processing of the signal field and the distributed creation of a contour tree. The gradient routing approach has the following properties: I the pre-processing message complexity is linear in the number of nodes, and the storage requirement for each node is a small constant, as shown by simulations; (ii) the gradient routing approach uses only local node information, and its message complexity is close to optimal, as shown by simulations; and (ii) the pre-processing message complexity is linear in the number of nodes, as shown by simulations. The same pre-processing also makes it easier to calculate routes between any two nodes if the route falls within a user-specified range of values.

EXISTING SYSTEM

The users in this Mobile Environment are equipped with PDAs or smart phones that can easily communicate with the Sensors. When an emergency arises, the WSN gives critical information to users, allowing them to be led out of a hazardous area via sensor interaction. Combining a wireless network sensor with a navigation algorithm could enable people safely get to a building escape while avoiding hazardous areas. For emergency situations, we present a simple navigation method. CANS uses the level set approach to follow the evolution of the exit and the hazardous area's boundaries, such that persons close to the danger experience moderate congestion at the cost of a minor detour, while people further away avoid unnecessary detours. To begin with, human navigation seeks a safe-critical path, as opposed to packet loss or energy efficiency, which is the initial objective in packet routing. Second, due to the limited movement speed of people, human navigation takes substantially longer than typical packet routing. And which are crucial for a quick evacuation since they primarily focus on identifying the shortest/safest path for each individual, while other less-than-ideal (but still safe) channels are left unused for the majority of the evacuation procedure.Fig 2. Architectural diagram of ATmega328 IC

PROPOSED SYSTEM

We used localizability-assisted localization in the suggested system (LAL). It's a methodical approach. A distance graph is decomposed into two connected components grouped in a tree topology. The root contains beacons, and modifications are made along the tree's borders from the root to the leaves. Localizability-assisted localization differentiates nodes based on their localizability. Localizability-aided localization converts all no localizable in one round via vertex augmentation. Localizability-assisted localization networks are localizable and can be localized using existing localization methods. Adjustment based on components. When a network is deployed in an application field, it may not be ready for localization due to some systemic or environment issues that were unknown during the design process. Thus, in Localizability-aided localization, which detects localizable and non-localizable nodes in a network for subsequent adjustment, node localizability testing is performed first. LAL treats nodes differently depending on how localizable they are and where they are in the component tree. Localizability-aided localization converts all non-localizable objects in a single round via vertex augmentation.

Admin keeps track of all of the block, user, and exit information. When a user enters the block, he or she creates their own path. If the user exits right away, his or her trail will vanish. The user's path will be tracked as they move through the block. In the event of an emergency, the sensor sends out an alert signal and directs each user to the safest and closest exit.

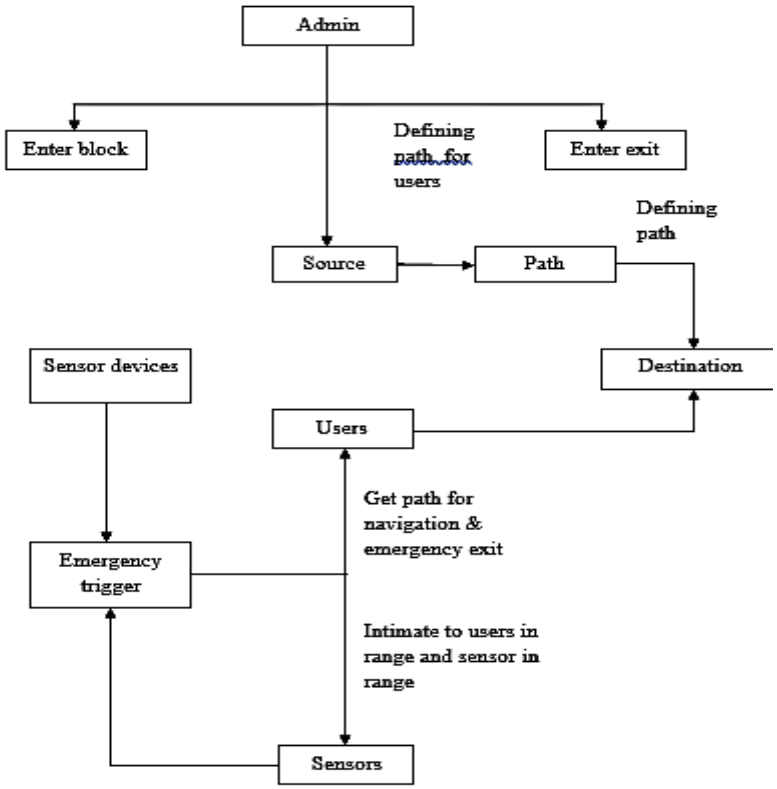

Figure 1. Architecture Diagram

EXPERIMENTAL RESULTS

Integration testing is a method of building a program's structure while also doing tests to find interface issues. Integration testing, in other words, is the entire testing of the product's collection of modules. The goal is to create a program system out of untested components. This is your last chance to catch and fix mistakes. After the program has been constructed and the documentation and relevant data structures have been designed, the software testing process begins. Errors in software must be corrected, which necessitates the use of software testing. Otherwise, the program or project is not considered finished. Software testing is an important part of software quality assurance since it provides the final check on specification design and code. Testing is the process of running a program with the goal of identifying errors. A good test case design is one that has a chance of uncovering an error that has yet to be detected. A successful test is one that uncovers an error that has yet to be identified.

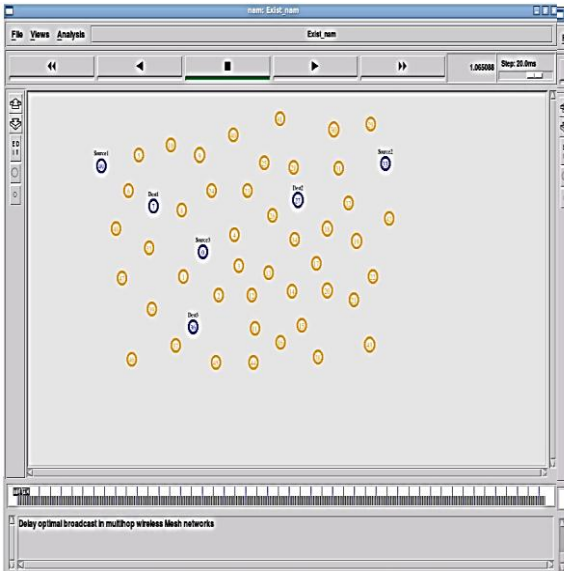

Figure 2. Bluetooth Protocol

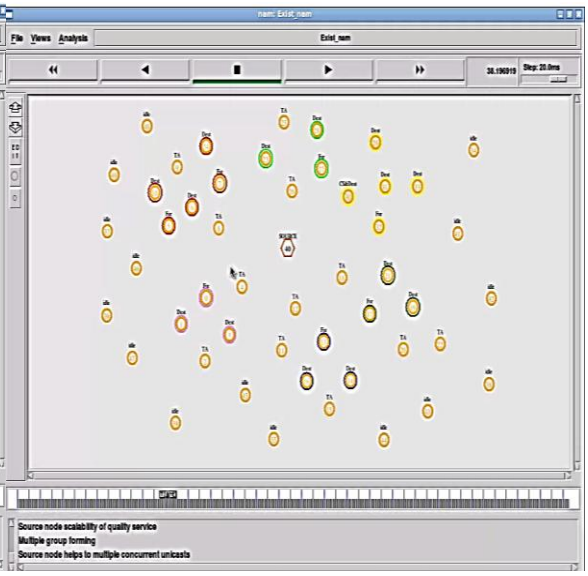

Figure 3. Gives multiple path

Figure 2 shows that bluetooth protocol is used for the transmission of packets.Range is very short of about 0-10m.Sum times dropper can occur which cannot handle multiple delivery of packets.So there occurs a delay in delivery of packets and packets are not sent at the right time.Figure 3 shows thatmain source checks the number of nodes for each floor.Trusted Authority(TA) is assigned for each section.From the TA,signals are sent to the user to nearest destination.It checks the number of nodes within the specific region.By using this people within the area try to move to the nearest exit.

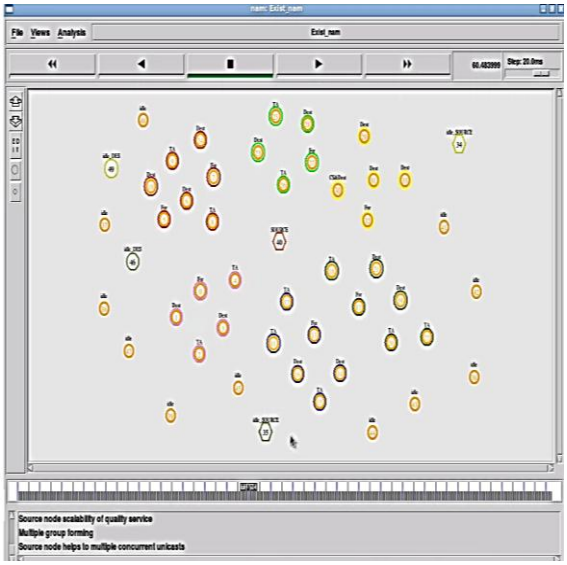

Figure 4. Idle source and destination

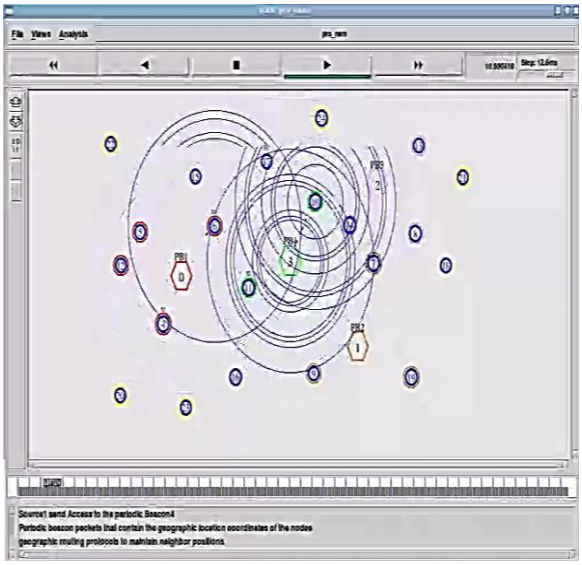

Figure 5. Lift movement

Figure 4 shows that here idle source is used for helping in navigation of people who just entered the mall. But congestion is not taken into account. Figure 5 shows that in the proposed system, lift alignment can be done to rescue people struck within the lift. Main source indicates the lift for the nearest destination.

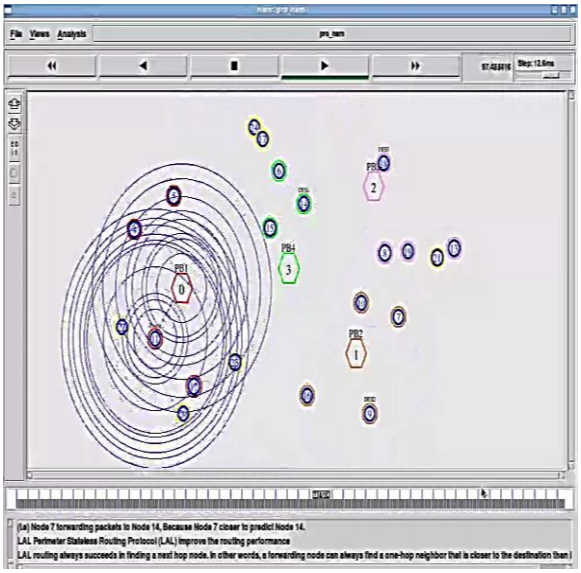

Figure 6 Neighbour Selection

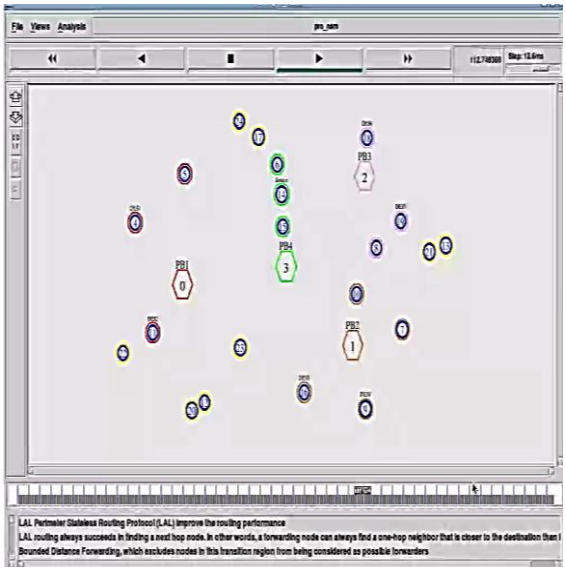

Figure 7 Single source and multiple destinationpaths

Figure 6 shows that neighbours who are uneducated are intimated to the nearest neighbour for easy navigation to the nearest exit. Figure 7 shows that single source is given multiple paths available. Shortest path is given for the user. As the user keeps moving their positions are updated are different available paths are given. Figure 8 shows that many source and destination are guided to the nearest path simultaneously. Delay is greatly reduced without much packet loss.

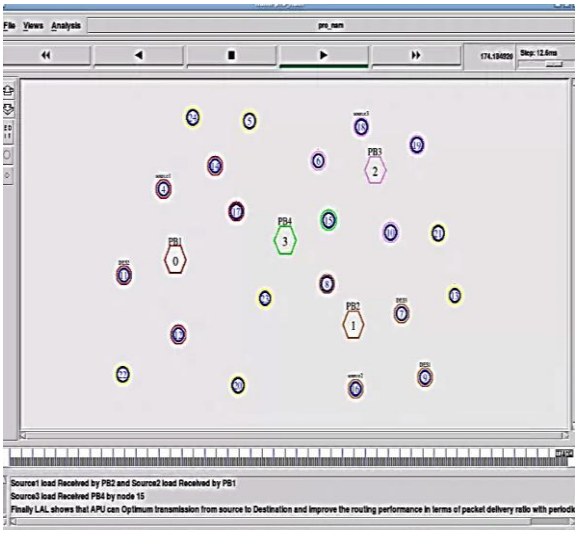

Figure 8 Multiple source and multiple destination paths

Delay refers to the time taken for a packet to be transmitted across a network from source to destination. Hence delay has to be reduced in LAL protocol in order to improve the reliability. When used in the context of communication networks, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node. Throughput is usually measured in bits per second, and sometimes in data packets per second (p/s or pps) or data packets per slot. In the proposed system it is calculated using LAL protocol (Localisation Aided-Localisability) the graphs are simulated and are shown below.

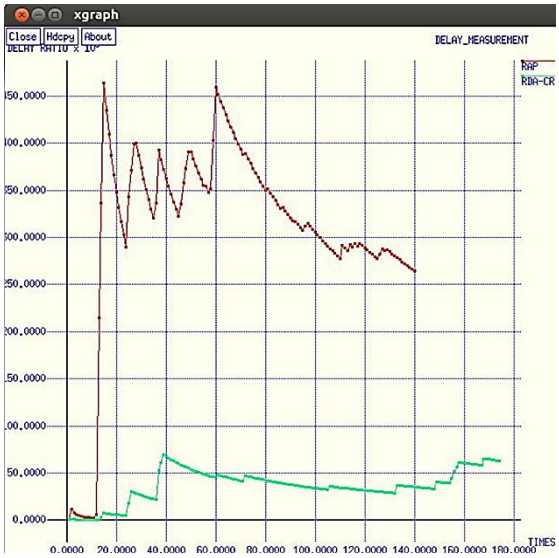

Figure 9. Delay analysis

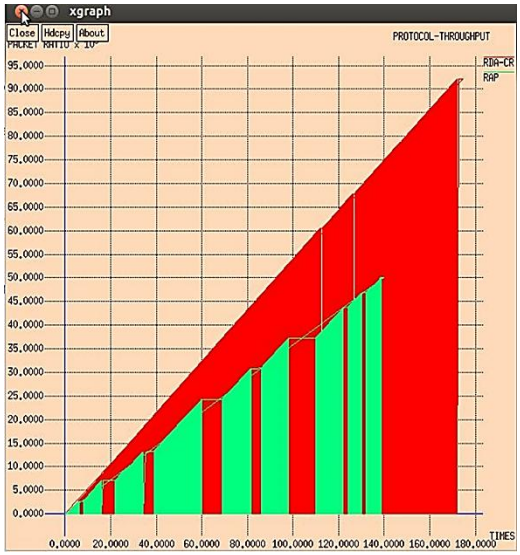

Figure 10. Throughput graph

Figure 9 shows the Delay analysis and Figure 10 shows the Throughput graph. Channel measurements are indispensable for wireless system design. It is the wireless channel that determines the ultimate performance limits of any communication system. In the beginning of cellular communications, fading and path loss of narrow band channel were the key figures of merit. This has changed with wide band multi antenna, multiuser system. New important of the radio channel became obvious: the channels frequency selectivity, directivity, Polari metric properties and their relation to channel of the users. Figure 11 shows the Channel Measurement and Figure 8.12 shows the Loss analysis

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Greater value of Loss ratio denotes the poor performance of the protocol.Loss ratio is the number of packets dropped during transmission compared to the number of packets that have been sent out by the sender.

Figure 11. Channel Measurement

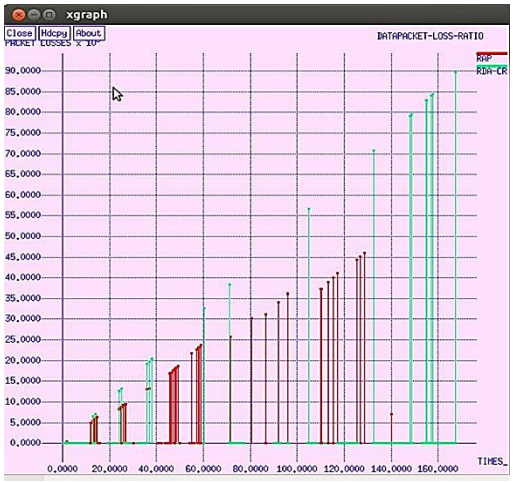

Figure 8.12. Loss analysis

CONCLUSION AND FUTURE SCOPE

Addressing to the this problem, we havemade sure that maximum people gets rescued that the time of danger by guiding them with proper instructions. We have used Greedy perimeter state routing which helps in movement of lift. Previously people where guided with multiple paths and only one possible exit through which they can move out which leads to much congestion. Butusing LAL, people are provided with multiple paths and also various other paths available thereby reducing congestion. LAL helps to assist people in escaping from a hazardous (dangerous area) region quickly when an emergency occurs with guaranteed safety, while avoiding excessive congestion's and unnecessary detours where adaptive positions are dynamically updated and helps in neighbour navigation. So, we hope this may fall in our future studies.

REFERENCE

[1]. Y. Song, B. Wang, Z. Shi, K. Pattipati, and S. Gupta(2014), "Distributed algorithms for energy-efficient even self-deployment in mobile sensor networks," IEEE Trans. Mobile Comput., vol. 13, no. 5, pp. 1035–1047

[2]. C. Fischer and H. Gellersen(2010), "Location and navigation support for emergency responders: A survey," IEEE Pervasive Comput., vol. 9, no. 1, pp. 38–47

[3]. J. Wang, Z. Li, M. Li, Y. Liu, and Z. Yang(2013), "Sensor network navigationwithout locations," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 7, pp. 1436–1446

[4]. M. Bocca, O. Kaltiokallio, N. Patwari, and S. Venkatasubramanian(2014),"Multiple target tracking with RF sensor networks," IEEETrans. Mobile Comput., vol. 13, no. 8, pp. 1787–1800

[5]. Q. Li, M. De Rosa, and D. Rus(2003), "Distributed algorithms for guidingnavigation across a sensor network," in Proc. 9th Annu. Int.Conf. Mobile Comput. Netw., pp. 313–325.

[6]. E. Xu, Z. Ding, and S. Dasgupta(2013), "Target tracking and mobile sensornavigation in wireless sensor networks," IEEE Trans. MobileComput., vol. 12, no. 1, pp. 177–186

[7]. C. Buragohain, D. Agrawal, and S. Suri(2006), "Distributed navigationalgorithms for sensor networks," in Proc. 25th IEEE Int. Conf. Comput.Commun., pp. 1–10.

[8]. Y.-C. Tseng, M.-S. Pan, and Y.-Y. Tsai(2008), "Wireless sensor networksfor emergency navigation," Computer, vol. 39, no. 7, pp. 55–62.