iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** XI **Month of publication:** November 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Formation and Detection of Holes in Wireless Sensor Networks

V. Venkatesa Kumar[1], S. Arif Khan[2], P. Renuka Devi[3], J. Dhandapani[4]
Assistant Professor, PG Scholar
Department of Computer Science and Engineering, Anna University Regional Centre

***Abstract**: Monitoring the desired Region of interest (RoI) is one amongst the most services provided by Wireless Sensor Network. In Region of interest (RoI) the emergence of holes is inevitable because of random preparation and environmental factors. Due to these factors the nodes in the network get affected and hence the holes are formed. In this work various types of holes their characteristic and major cause for the hole formation are discussed. Also Distributed Hole Detection (DHD) algorithm is proposed for the detection and identification of holes.*

Index Terms – Wireless Sensor Networks, Network holes, Hole detection, Region of Interest, Sensor Nodes

I. INTRODUCTION

A wireless sensor network is composed of small detector nodes each capable of sensing some development, doing a little restricted processing and communicating with each other. These tiny sensor nodes are deployed in the target field in large numbers and they collaborate to form an ADHOC network capable of reporting the phenomenon to a data collection point called sink or base station. These networked sensors have several potential applications i.e., they can be used for tracking of object, intrusion detection, surroundings and different hazard and structural observation, traffic control, inventory management in manufacturing plant environment and health related applications etc. Some of the challenges that needed to be overcome by WSN are connectivity, coverage, Energy Consumption and limited battery life. In WSN, gathered information can be shared from one mobile node to another. Sensing and Communicating are the two tasks that a node can perform simultaneously. These tasks can be accomplished only if the node is able to communicate with neighbors for onward transmission of the sensed data to sink. But these tasks cannot be implemented in real world scenarios

Several anomalies can occur in wireless sensor network that impact their functionality resulting in different kinds of holes namely: Coverage holes, Routing holes, Jamming holes, Worm holes [1]. Coverage holes arise due to random deployment, presence of obstructions and node failures. So, the target field which is said to be 100% covered may have coverage holes. If nodes may not be able to communicate with other node correctly then routing holes arises. Malicious nodes can jam the communication to arise jamming holes. Worm holes arises by denial of service attacks in overwhelm regions.

Monitoring the specified region of interest is one of the main services provided by wireless sensor network [2]. Also the main duty is to sense the environment and communicate the information. Region of interest must be completely covered at all time. Due to their inner nature of wireless sensor network and external attacks the emergence of holes is unavoidable. Therefore the holes occurred are neither detected nor reported so the task is not completed.

In this work such exceptional circumstance is discussed with special attention to the phenomenon that occurs in region of interest. The holes related problems are grouped together in four categories namely: Coverage holes, Routing holes, Jamming holes, Worm holes. Also, the process such as identification of hole, Discovery of hole and border detection is discussed.

The work is organized as follows. The hole related problems and reasons for hole formations are discussed in Section II and Section III. Section IV V VI elaborate about identification of hole, discovery of hole and border detection .Section VII concludes the paper.

II. PROBLEM DEFINITION

Various types of holes that occur in wireless sensor networks and their characteristic are discussed.

A. Coverage Holes

Coverage holes will not exist if the target point is covered by at least required degree of coverage. Coverage holes are formed due to

the following reasons:

1. Design of the sensor node fails
2. Unsystematically arrangement of sensor nodes in the area
3. Poor installment
4. Power depletion
5. Topology failure
6. Presence of obstacles

If there is a set of sensors and a target area, no coverage holes exist in the target area. The target area is covered by *k* sensors where *k* is the require degree of coverage. Coverage hole problem is defined on application requirement based on the higher degree or lower degree of coverage of a given target area for fault tolerance using triangulation based positioning protocols [3]. In multiple coverage requirements multiple connections is used for single link or node failure. But in Single Coverage requirement the protocols which work on the assumption the communication range is twice the sensing range and also it satisfies the connectivity constraint.

Coverage holes is assumed uniform in all directions and represented by unit disc model

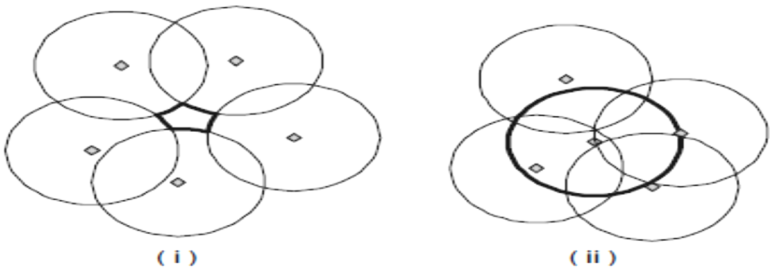


FIG.1: (i) Coverage holes with unit disk sensing model (ii) Sensor with dark grey sensing circle is necessary if degree of coverage required is 2 [1]

B. Routing Holes

If the nodes are not available (or) if the available nodes cannot participate in the routing data then routing hole exists in the sensor network. Routing holes occur due to following reasons

1. Failure of sensor nodes
2. Battery depletion
3. Structural collapse physically destroying the nodes
4. Local minimum phenomenon faced in geographic greedy forwarding

In Fig.2, a node x tries to forward the traffic to one of its 1-hop neighbor that's geographically nearer to the destination than the node itself. This forwarding process stop once it cannot realize that there is no 1-hop neighbor closer to the destination than itself and therefore the solely route to destination needs that packet moves quickly farther from the destination to x or y. This special case is stated as local minimum phenomenon and is additionally possible to occur whenever a routing hole is encountered.

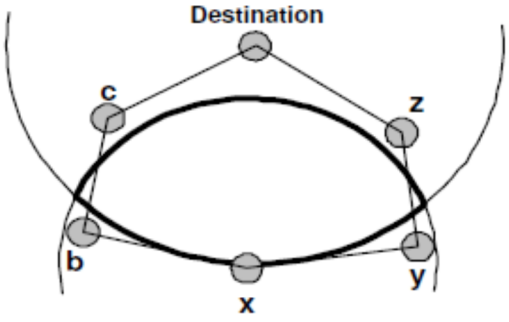


FIG.2: Local Minimum Phenomenon in greedy forwarding [1]

C. Jamming Holes

Jamming holes are caused due to high frequency signal. In wireless network when the high frequency signal comes in, the network breaks the signal and connects with the new signal. The other reasons for the causes of jamming holes are given as

1. Installing jammers in nearby areas
2. Presence of obstacles

Jamming can be divided into two classes such as deliberate and unintentional. Deliberate electronic jamming occurs when a adversary is making an attempt to impair the functionality of the sensor network by meddling with communication ability of sensor node. This adversary can be either laptop–class attacker [4] which is capable of attacking a larger area of sensor network or mole-class attacker [4]. Unintentional jamming occurs when more than one deployed nodes get malfunctioned.

D. Worm/Sink Holes

Worm holes are caused when the data is lost in between the traffic. Therefore both the sender and the receiver couldn't know whether the data is received or sent. Worm Holes can be formed due to the following reasons:

1. Denial of services
2. Low computational power
3. Limited Memory
4. Insecure Wireless Channel

In worm holes malicious nodes plays an important role [5]. Malicious nodes settled in several part of the sensor network produce a tunnel among themselves. Then they begin forwarding packets received at one part of the sensor network to the opposite finish of the tunnel employing a separate radio communication channel. The receiving malicious node then replays the message in alternative part of the network. This causes the node settled in several components of networks to believe that they're neighbors leading to incorrect convergence.

III. CAUSES FOR HOLE FORMATION

There are many causes for hole formation. The main causes for the hole formation are the destruction of nodes by environmental disaster or the node doesn't involve in working of network.

In sensor networks there is a node known as faulty node. A node is said to faulty if it does not produce the same result as the other neighbor node produces. So a faulty node can be said as destroyed node which stops from working and do not involve in network activities.

In this topic we highlight the main reasons for the sensor node destruction that causes holes in network. Some of the major reasons for the destruction of nodes and the creation of holes are given in this section.

A. Power Depletion

Every node in the network is equipped with some amount of battery power which provides energy for the nodes. The energy inside the node would carry out the task and perform communication with other nodes. Energy is consumed when they perform operations in network. So the power gradually decreases and at one stage the energy finishes and the node is dead. It is difficult to recharge when the energy is deployed in hostile region or forest where human interaction is not possible [6].

In some regions a group of nodes are carried in the network. In those regions the energy reduced are quicker than other nodes. So the energy level of all groups comes to an end and the nodes are destroyed that causes a hole in the network.

B. Physical Destruction

Physical destruction is another major cause for holes in the network. Wireless sensor networks are deployed in hostile region. In those regions the nodes could also be destroyed by means of natural disasters like earthquake, volcanic eruption and tsunami. Similarly the outburst of fire would destroy all the nodes that are deployed in the forest region.

C. Presence of Obstacles

Wireless sensor networks are deployed in hostile regions .There are some areas where the nodes will find difficult to operate. For example if we assume that nodes are deployed in dense forest then a pond of water or a mountain or presence of animals in between the nodes would act as an obstacles and it causes an hole in the network.

D. Lower Density Regions

The holes are formed due to non-uniform deployment. In those regions the density of nodes becomes lower than other regions. In such cases the nodes become static. So it forms lack of communication from one node to another and it forms a hole.

E. Topology Failure

In wireless sensor networks topology plays an important role. On designing the network the topology should be chosen properly else it leads to the coverage hole in the network. So the topology failures also lead to hole in the network

IV. PROPOSED SOLUTION

In this section the way to detect a hole within the node of the network is discussed. A mechanism called Distributed hole detection (DHD) is proposed to identify the boundary nodes and discover holes.

V. HOLE DETECTION

To detect a hole Fang et al. [7] proposed a rule named TENT rule. This rule is used to check the node in the network whether it is a stuck node. A stuck node is a node where packets can possibly get stuck in greedy multi hop forwarding. For example we can assume that p and q are nodes .A node p is said to be stuck node if the location of the q is outside p's transmission range so there is no 1-hop neighbors of p is closer to q. The TENT rule states if the angle is not spanned by a pair of its angularity adjacent neighbors greater than $2\pi/3$ then it is not a stuck node. To identify holes in the network we must precede three steps

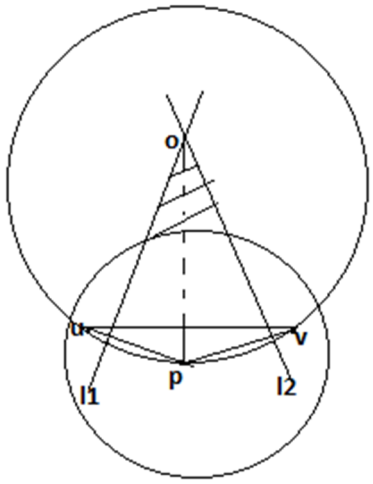


Fig. 3: p is a strongly stuck node [11]

VI. IDENTIFICATION OF HOLE

To identify stuck nodes we must assess the existence of a hole. By executing TENT rule [8] we can check whether the node p is a stuck node by following these steps.

1. Let *u* and *v* be the pair of angularity adjacent nodes.
2. Divide the plan into 4 quadrants and draw a perpendicular bisector of up and *vp, l1, l2*.
3. *l1* and *l2* intersect at a point o (see fig.3)

Finally, if communication range of *o* is outside *p*, then the angle $\widehat{vpu}$ is a stuck angle and *p* is a stuck node.

VII. DISCOVERY OF HOLE

Every node that marked as stuck node would trigger the discovery of holes by TENT rule. By using this process the hole boundary is found.

A stuck node s_i with an ID (same ID for hole and node) creates a new discovery packet. The mission of this node is to collect location information and forward to next boundary node s_{i+1} by Right hand rule. Node s_{i+1} inserts its location information and forwards to another node s_{i+2}. This Process is repeated until the packets travel around the hole. Next node s_i extracts and select 2 nodes s_m ands_n. So the distance between them is the longest between any two nodes and also the hole center is calculated.

There is no coordination between the stuck nodes which sends the HD packet. Without coordination there will be redundancy in the discovery process that causes unnecessary traffic and collision. To avoid these collision the prevent redundancy mechanism is introduced. This mechanism is used to remove HD packets as soon as possible. If a HD packet arrives and finds that the packet has a hole-ID greater than hole-ID that has already passed it will considered redundant and it will be deleted. Finally the node which has the smallest Hole-ID removes the HD packet and it is known as Hole Manager (HM). Hole Manager is responsible for the hole healing announcement.

VIII. BORDER DETECTION

The nodes on the limit of region of interest (ROI) execute the TENT rule. As a result it detects stuck nodes and starts the process even if the nodes are not stuck nodes (they are the borders of the network). To avoid the hole discovery process launched on non-stuck nodes network boundary nodes are identified.

To find the network boundary the following steps are followed:

1. DHD is launched by stuck nodes to identify the nodes that surround the hole.
2. To identify the network boundary four Boolean variablex_{max},y_{max},x_{min},y_{min} defined in the packets.
3. If the packets find that it has a higher or lower value it sets the corresponding Boolean variable to 1.
4. At the end, the largest hole which defines the network boundary will be defined by the coordinatesx_{max},y_{max},x_{min},y_{min} and it cancels the healing process launched by Hole Manager.

TABLE 1: Comparison of proposed solution to hole and border detection problem

PROPOSED SOLUTION	ALGORITHM USED	DRAWBACKS
[9]	DISTRIBUTED SCHEME ALGORITHM	For a large WSN with a few holes this method is not efficient.
[10][11]	CENTRAL CONTROL ALGORITHM	High complexity (e.g., for [4] the time complexity is O (N^5), where N is the number of nodes.
[12]	LINEAR TIME ALGORITHM	Requires a high node density
[13]	COORDINATE –FREE METHOD	Assumes a uniform node distribution and also requires high node density
[14]	DISTRIBUTED ALGORITHM	Based on a repetitive network flooding

[7]	BOUND HOLE ALGORITHM	High message complexity
[15]	HOLE BOUNDARY DETECTION ALGORITHM	Requires synchronization among nodes

IX. CONCLUSION

Wireless Sensor Networks application can be found in every part of life. One of the existing problems occurring in such environment is the formation of network holes. This paper has proposed about the formation of network holes and their causes. These causes leads problem in data reliability and data routing. For this purpose the advantages of hole detection are discussed and it also ensures the reliability of data.

REFERENCES

[1] N. Ahmed, S.S. Kanhere, and S. Jha, "The Holes Problem in Wireless Sensor Networks: A Survey," SIGMOBILE Mobile Computing Comm. Rev., vol. 9, n. 2, pp. 4-18, 2005.
[2] B. Wang, Coverage Control in Sensor Networks. Springer, 2010.
[3] D. Nicules and B. Nath, "Ad-hoc positioning system (APS) using AoA," In *Proceedings of the IEEE INFOCOM*, 2003.
[4] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In *1st IEEE International Workshop SNPA'03*, May 2003
[5] Anthony D. Wood and John A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, Oct 2002.
[6] J. Staddon, D. Balfanz, G. Durfe. "Efficient tracing of failed nodes in sensor networks", in proc. of 1st ACM international workshop on Wireless Sensor Networks and Applications (WSNA), Atlanta, Georgia, September 2002.
[7] Q. Fang, J. Gao, and L.J. Guibas, "Locating and Bypassing Holes in Sensor Networks," Mobile Networks and Applications, vol. 11, no. 2, pp. 187-200, 2006
[8] Abdelhamid Mellouk Khalid Assnoune, Mustapha Reda Senouci," Localized Movement-Assisted Sensor Deployment Algorithm for Hole Detection and Healing", VOL. 25, NO. 5, MAY 2014
[9] B. Kun, T. Kun, G. Naijie, L.D. Wan, and L. Xiaohu, "Topological Hole Detection in Sensor Networks with Cooperative Neighbors,"Proc. Int'l Conf. Systems and Networks Comm. (ICSN '06), p. 31, 2006.
[10] R. Ghrist and A. Muhammad, "Coverage and Hole-Detection in Sensor Networks via Homology," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), pp. 254-260, Apr. 2005
[11] V. De Silva, R. Ghrist, and A. Muhammad, "Blind Swarms for Coverage in 2-D," Proc. Robotics: Science and Systems, pp. 335-342, June 2005.
[12] F. Stefan and K. Christian, "Hole Detection or: How Much Geometry Hides In Connectivity" Proc. 22nd Ann. Symp. Computational Geometry (SCG '06), pp. 377-385, 2006.
[13] S.P. Fekete, A. Kr€oller, D. P fisterer, S. Fischer, and C. Buschmann, "Neighborhood-Based Topology Recognition in Sensor Networks," Proc. Int'l Workshop on Algorithmic Aspects of Wireless Sensor Networks, pp. 123-136, 2004.
[14] Y. Wang, J. Gao, and S.B. Mitchell, "Boundary Recognition in Sensor Networks by Topological Methods," MobiCom '06, pp. 122-133, 2006.
[15] A. Shirsat and B. Bhargava, "Local Geometric Algorithm for Hole Boundary Detection in Sensor Networks," Security and Comm. Networks, vol. 4, no. 9, pp. 1003-1012, 2011

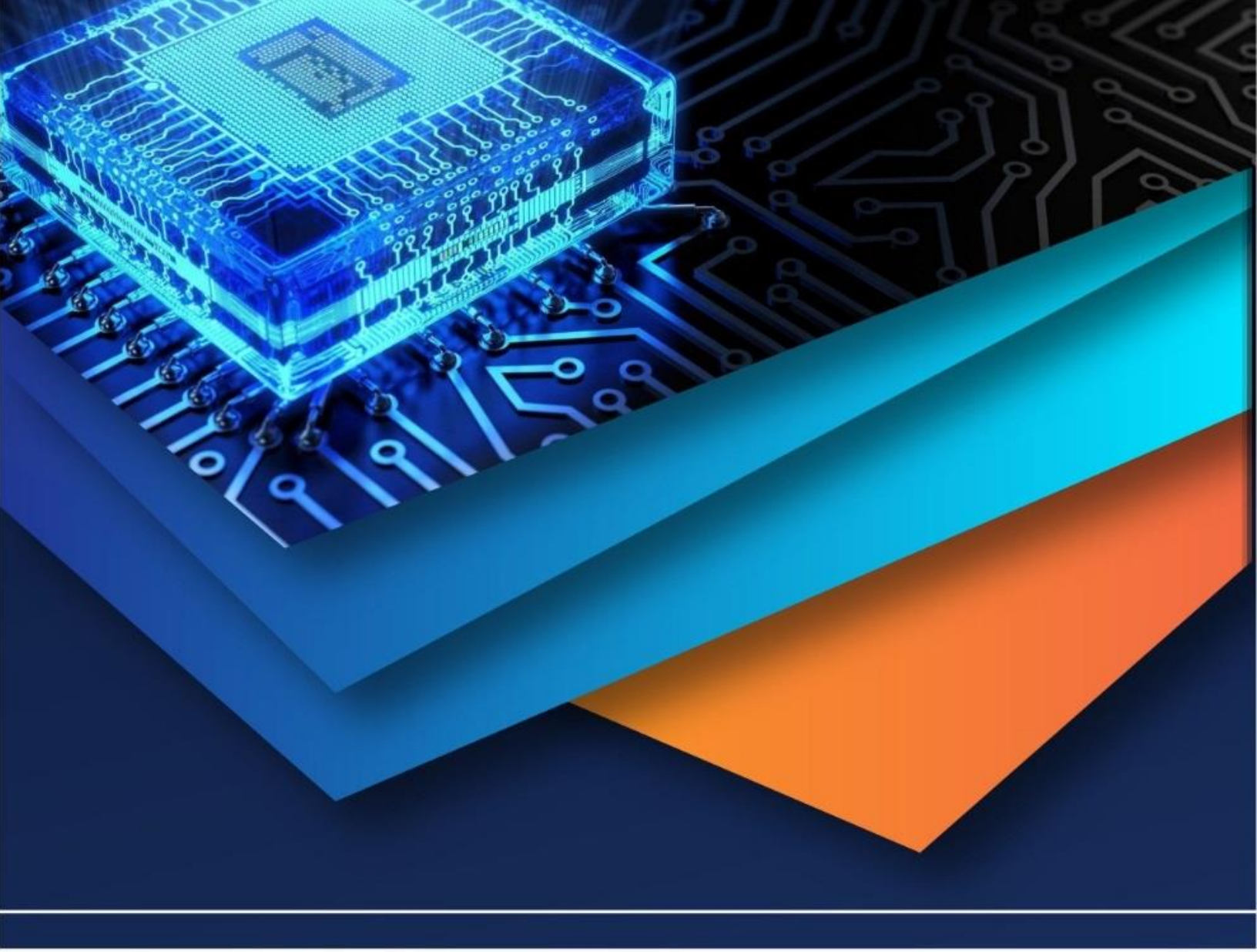
BIBLIOGRAPHY

Dr.V.Venkatesakumar is presently working as Assistant Professor in The Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Engineering Degree from Bharathiyar University, Master of Engineering Degree and Ph.D from Anna University Chennai. He has more than ten years of Teaching Experience. He has published many papers in reputed International Journals and has chaired many Conferences. He is a Life Member of International Association of Computer Science and Information Technology, International Association of Engineers and in many International Associations. His research interest includes Cloud Computing, Internet of Things, Big Data Analytics, Operating System, Software Engineering and Web Technologies.

Arifkhan.S completed his B.E in Computer Science and Engineering in 2013 from College Of Bannari Amman Institute Of Technology in Sathyamangalam. Currently, He is pursuing his M.E Computer Science and Engineering from Anna University Regional Centre, Coimbatore. His research areas include Cloud Computing, MANET, VANET and Wireless Networks

Renuka Devi.P completed her B.E in Computer Science and Engineering in 2013 from college of Nehru Institute of Engineering and technology in Coimbatore. Currently she is pursuing her M.E Computer Science and Engineering from Anna University Regional Centre, Coimbatore. His research areas include Software Engineering, Protocols and Wireless Networks.

Dhandapani.J is pursing M.E Computer Science and Engineering (Specialization with Networks) in the Department of Computer Science and Engineering, Anna University Regional Centre, Coimbatore. He received his Bachelor of Technology from The Rajaas Engineering College, Anna University, Tirunelveli. He has published paper in reputed International Journal. His research interests are Wireless networks, Network Security, Security Protocols and Network Management, Web mining, and VANET.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY