iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

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

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

By-Passing Infected Areas in Wireless Sensor Networks Using Voting Based Routing Protocol

Srinidhi Priyanka T G[1], Kushalatha M R [2]
[1,2] *Asst Professor ,Department of ECE, NMIT, Bangalore, Karnataka, India*

Abstract--Wireless Sensor Network have been the front line innovation in different remote occasion observing applications, particularly in unsafe zones , threatening situations, battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. Security is One of the major challenges wireless sensor networks facing today.The sensed data in Wireless Sensor Network is abnormalised due to to several attacks, hardware failure and software corruption would cause infected node . these infected nodes will reduce the whole functionality of the network operation and also produce the faulty data consequently this leads to misleading of the packets ,incorrect decision making and false analysis in real time applications. Although several existing methods BOUNDHOLE ,GAR, TWIN ROLLING BALL algorithms are used to avoid these problems but their performance are bounded by their limitations. While transmitting the packet the void problem can also occur that makes the packet unreachable towards the destination. This becomes challenge to avoid routing problem in Greedy routing protocol. Especially the active attacks would decrease the Qos parameters of the System , this paper mainly focuses on the identification of the malicious node using WTE method and avoiding them. Hence this paper will give give solution by adapting Voting based Routing protocol that identifies the malicious node and bypasses the incoming traffic to uninfected region which is also a reliable path . Thus the Performance of the System enhances than the exisiting method , We are also concerned about the packets on the fly that may affect when problem occurs. Besides solving these problems , the proposed method has greatly improved the studied Qos parameters and decrease the energy consumption of the whole system.

Keywords: Wireless Sensor Network, Active attack, Void problem,GAR approach, Voting based Routing protocol

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a gathering of substantial number of independent sensor hubs which are spatially conveyed over a geological territory fundamentally connected to control and screen the physical changes in nature through parameters like pressure, temperature and sound and so on. A WSN system can likewise effectively forward the information between the hubs in bi course with capacity of detecting. Because of a few focal points of these systems it has been utilized as a part of different applications particularly in Military for outskirt observation, mechanical applications and shopper applications etc. Size of the system begins from couple of hubs to hundred and thousand of hubs relying on the application arranged. Every sensor hub has a capacity of detecting the natural changes and convey these data to its neighbour hub inside of its range .To empower these exercises every hub has bolstered structure, for example, radio handset with an inner receiving wire ,a self fueled battery as a vitality source, and a microcontroller to process the information. A WSN can be a homogeneous or heterogeneous system and the size and expense of every hub changes from little to enormous as application differs yet they are restricted by few asset requirements, for example, memory, vitality, rate and correspondence data transmission which makes a system frail while executing progressively.

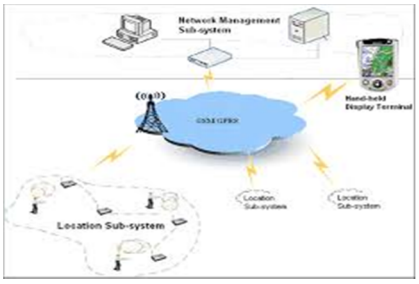


Fig 1: WSNs Architecture and its Operation

WSN's more popularly applied in remote monitoring applications, hazardous environment and hostile environment. Any unexpected event may occur in between while transmitting that involves communication of outstanding data to sink node and also they are restricted by energy constraints and other resource limitations. Communication in the WSNs are is crucial because of its state of various intermediate nodes which also forward the data to another node until the destination reaches,this also requires lots of energy consumption by all the node which decrease the life of the node while maintaining connectivity.

A. Problem Statement

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks. Here we are mainly concerned with active attacks , The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack.

The following attacks are active in nature.

Routing Attacks in Sensor Networks
Denial of Service Attacks
Node Subversion
Node Malfunction
Node Outage
Physical Attacks
Message Corruption
False Node
Node Replication Attacks
Passive Information Gathering

1) *Routing Attacks In Sensor Networks:* The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages. An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information.

Create routing loops
Extend or shorten service routes
Generate false error messages
Increase end-to-end latency

2) *Denial of Service (Dos)*: is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed.

A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader. Wsn's are vulnerable to all these attacks and limited by their capabilities. These threats will lead to critical drawbacks such as complete node failure that also cause destructive effects on underlying monitoring applications.Nodes which experience these attacks are called as infected node and they completely fail to perform the communication task and normal sensing. Hence performance of the system comes down.

Aforementioned problem has the high tendency to produce the faulty data (values that deviated from actual reading) . Data generated by these nodes may also contain anamolies that causes serious intermittent connection over the entire network.because of this packets will not reach the destination . in between packet loss happens or packets will get stuck in the malicious node. Some of these packets may contain significant information about the emergence situation, cause severe consequences that effect the whole utilizing network.Hence there is an imperative need to timely detect the infected nodes and avoid them by passing them. This requires fast alternative routes to be reconstructed in order to divert the packets to their destination.

B. Objectives

This paper is concern to address the following issues:

To design a method that can identify the infected node and bypass them by fast alternative route
To divert the packets from infected region to the uninfected region.
To establish a reliable alternative path and minimize the aforesaid problems and enhancing performance of the System.

II. RELATED WORK

The routing issues has the most significant interests in WSN among all the inherent issues such as Fault- resilence, network lifetime, sensor localisation, sink mobility.They are many routing protocols are proposed for sensor network namely Greedy forwarding algoritm that transfer the packet to sink node by finding its shortest distance comparison. This technique is very efficient that requires minimum energy consumption but it suffers from the local minima problem(infected node) also called as void problem, holes problem. Local minima is a situation where it cannot forward the packet to its neighbour because it cannot find its neighbour.Some of the methods employed to avoid this problem but has additional energy expenditure and poor scalability. Our Basic idea is to avoid this local minima situation considering it as a infected node. this approach introduces BOUNDHOLE algorithm that separates the boundary of the holes and routes the packet based on GF. However this require the nodes to remember the shape of the previous holes, that requires extra memory and also holes become dynamic in nature. Greedy Antivoid Routing approach has been designed where a Rolling ball is attached or hinged at the node having local minima and rotating in clockwise direction. The first node that hits the ball will be selected as a next hop. This process is repeated until packet safely reaches the destination. Whereas this introduces long routing path by visiting all the unnecessary nodes . To avoid this unnecessary visit a Twin Rolling Ball approach is used in which two rolling ball are attached to local minima node and rotating both of them clockwise and anticlockwise direction . the first node that hit ball from either of the direction and uninfected than it is taken as the next hop.this process is repeated until it reaches destination but this faces exit gate node problem ie it cannot overcome from the loop until last node in the transmission range occurs and also causes high energy consumption and end to end delay. Our proposed Voting based Routing protocol will minimise these effects by consuming less energy, and reduce the number of computation overheads.

III. PROPOSED SYSTEM

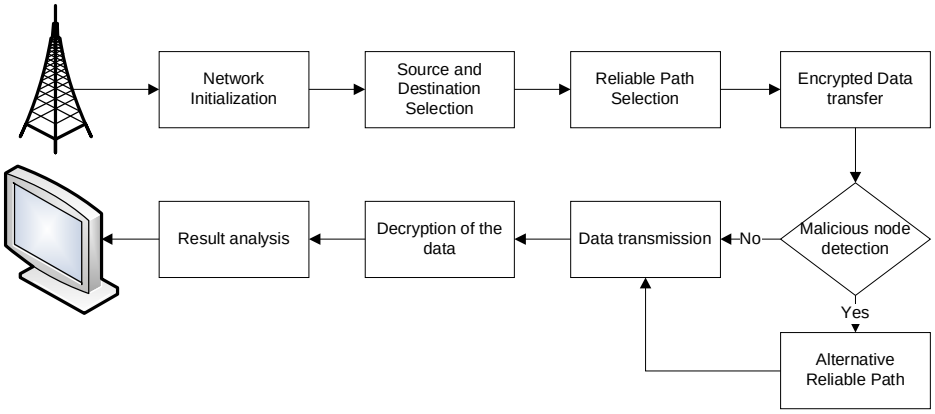


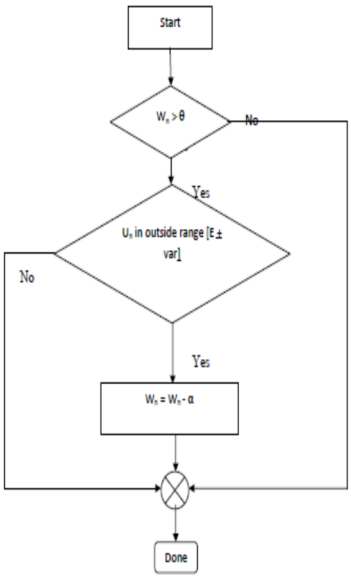
Fig 2: System Architecture

The System begins with network initialization, and by using greedy forwarding algorithm a reliable path is selected between source and destination. The sensed data is encrypted by using BLOWFISH algorithm to increase the security and avoid the data failure from malicious attack. Although any malicious node is found in between the path , it is identified by its properties and a reliable, uninfected ,suitable path is selected and whole incoming traffic is diverted towards destination using using that path by adapting VBR approach.

A. Identification Of Infected Node

In this paper, we proposed a novel Weight Trustesd Evaluation based algorithm for the detection of malicious SNs in WSNs. Here,. The basic idea is that a weight representing the reliability of a node is assigned to each SN in the cluster. Since malicious nodes usually report falsified information to disrupt the network, if a node sends incorrect information, the FN gradually decreases the

weight of the node and detect the node as a malicious node when its weight value becomes lower than a threshold. In addition, a weight recovery mechanism is incorporated in the algorithm to recover the weight of a node whose weight is accidentally decreased.



Malicious nodes are assumed to arbitrarily modify their readings without being easily detected. To monitor their behavior we define confidence level of a sensor node to represent its reliability in form of WEIGHTS, measuring its past behavior in reporting sensor readings. For a grid with *n* sensor nodes, N1……N*n*, the cluster head maintains w1…..w*n*, as their weights (confidence levels), respectively, where, (0 < wi < 1), and updates them each time a decision on the correctness of their reports is made. Initially all the weights are set to 1. At the time the weight reaches a *predefined lower bound (θ)*, the corresponding node is determined to be malicious and logically isolated thereafter. If the value(Un) lies outside the range [E + var] and [E – var] it is treated as false value and hence the weight of the node sending this data is reduced by a value 'α', where 'α' is called *weight depreciating factor*.

$$Wn = \begin{cases} Wn - \alpha, & \text{if}(Un > [E + var] \text{ or } Un < [E - var] \\ Wn, & \text{elsewise} \end{cases}$$

If the data sent by a node (Nn), Un is outside the acceptable range the nodes weight is reduced by a factor α. The initial condition of Wn > θ is done so that the procedure is applicable only to nodes which are above threshold θ. Once θ is reached the node is termed as malicious and is removed from network. No data coming from that SN is taken into consideration. The procedure is executed for each SN and for each transmission the weight reduction is performed so that once 'Wn' reaches 'θ', it is declared malicious.

B. By Passed Routing

1) Voting Based Routing Approach: The multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. While most prior research focused on using multipath routing to improve reliability.

[Optimal route] = algorithm (N, Src, Dst)

Step1: Input

Node, Source, Destination

Step 2: define the transmission Range

Step 3: Apply greedy Method and calculate the distance using Euclidian distance formula

Dist =

In the Euclidean plane, if p = (p1, p2) and q = (q1, q2) then the distance is given by

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

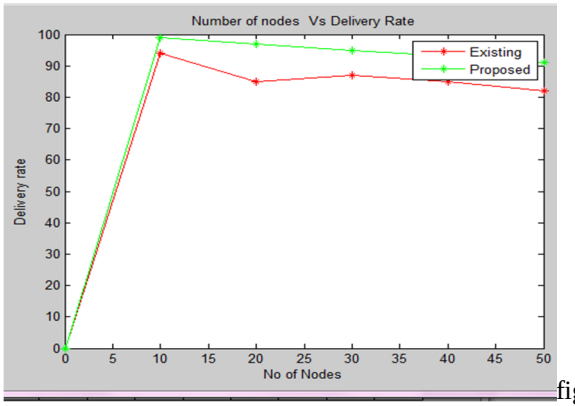
$$d(\mathbf{p},\mathbf{q}) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2}.$$

Step 4: Calculating and displaying initial energy of the nodes
Step5: check if the dest lies within the Range? 1:0
Update source and destination location
Step 6: if dest dist <= transmission_range
Update the source and routers
Step7: Finding the nodes distance, which are all within the transmission range
And update in range Nodes _dist.
Step 8 : elect the node within transmission range which is near to Destination based on the threshold value
If dist < threshold
Threshold = dist
Src = Next Src
Go to step5

IV. EXPERIMENTAL EVALUATION

In this section, we evaluate the performance of the proposed approach through MATLAB simulations using some predefined

metrics. To rate the performance , we compare the performance of our result with the existing GAR approach using configuration setup shown in table 1.Our simulation is based on a configuration where 20 nodes are randomly scattered in a monitored region. The sensor nodes perform continuous information sensing while sending periodic updates to the sink node.



fig(a)

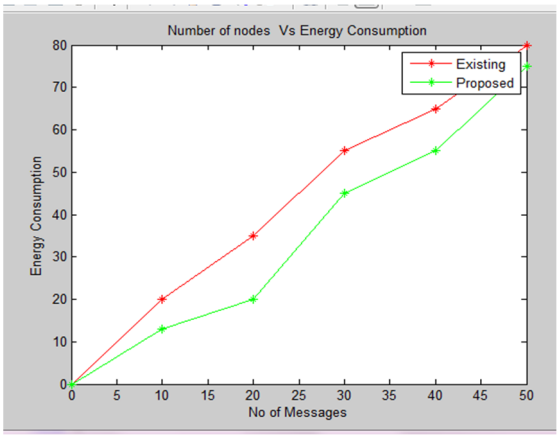


fig (b)

Graph shows the Result analysis of both existing Rolling ball algorithm and proposed Voting Based Routing approach.fig a) Packet Delivery Rate b) Energy consumption

Packet Delivery ratio(PDR) the ratio of the packets that are successfully delivered to destinations. In existing BOUNDHOLE, GAR approaches PDR rate has been reduced due to wrong selection of exit node where as our proposed VBR approach has high PDR since there is a proper selection of alternative path with low energy expenditure.

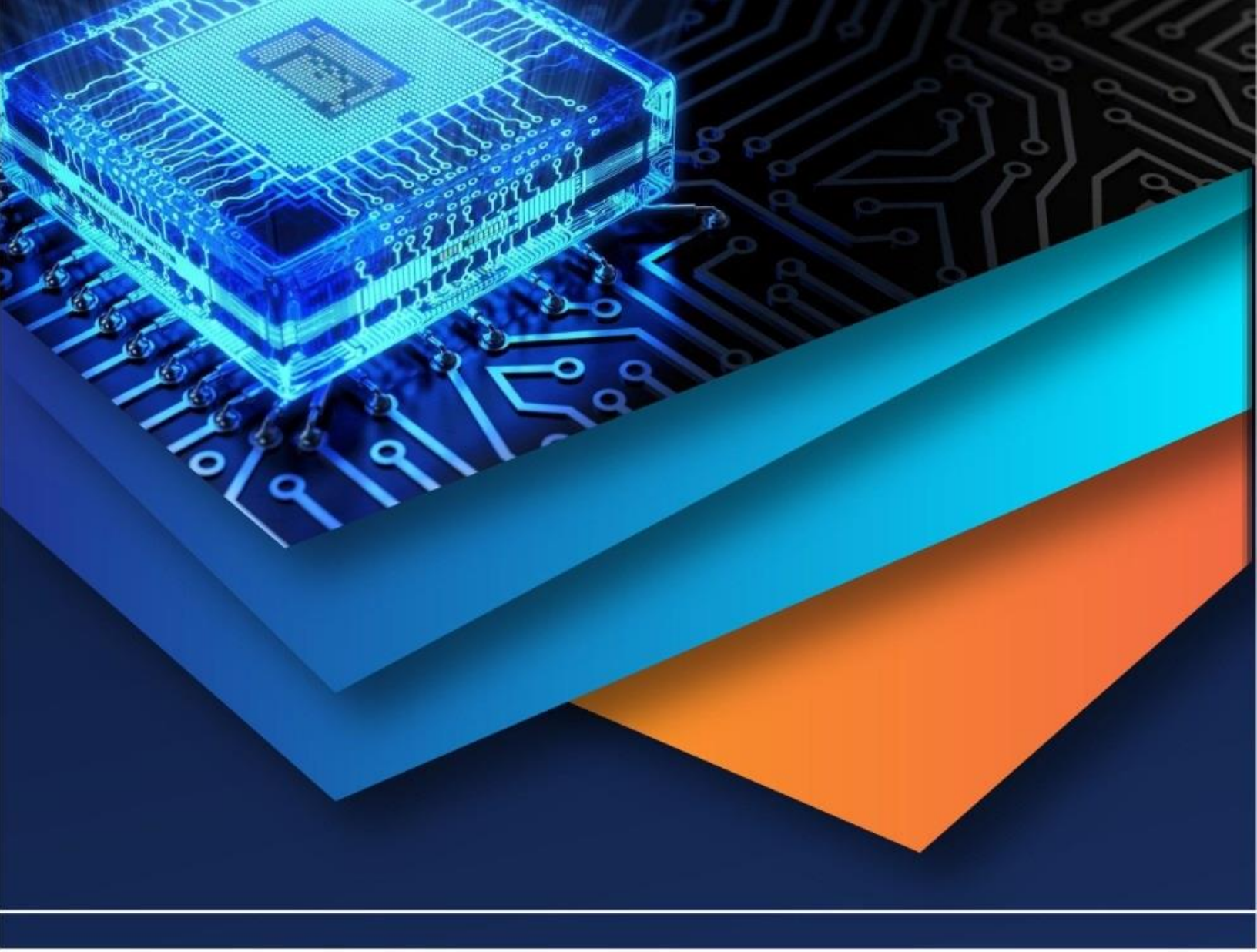
Energy Consumption The percentage of energy consumed for overall simulation as the no of messages transmission occurs between source and destination.we investigated that existing GAR approach has consumed high consumption in sparse network, where as our approach BPR has decreased amount of energy because of less number of hops.

V. CONCLUSION

In this paper , we have studied our Proposed architecture of By passing infected node has effectively improves the over all performance of the system. The infected area are detected using WTE approach and that path is bypassed using VBR approach. With this approach we have solved local minima(void problem), false boundary detection,malicious attack. The proposed system has greatly help to define the next forward node and mitigate the aforesaid problems.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a Survey", International journal on Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.
[2] Ameer Ahmed,Mohamad Younis "A Survey on Clustering Algorithms for Wireless Sensor Networks", International journal on Computer Communications, vol. 30, no. 5, pp. 2826-2841, 2007.
[3] Sohail Jabbar , Ayesha Ejaz Butt, Najam us Sahar and Abid Ali Minhas "Threshold Based Load Balancing protocol for Energy Efficient Routing in WSN" 13th International Conference on Advanced Communication Technology ,no.5,pp 196 - 201 , 2011
[4] A. Abdulla, H. Nishiyama, J. Yang, N. Ansari, and N. Kato, "HYMN: A novel hybrid multi-hop routing algorithm to improve the longevity of wsns," IEEE Transactions on Wireless Communications, vol. 11, no. 7, pp. 2531–2541, July 2012.
[5] N Yakob,I Khalil, H.Kumarage , "By-passing Infected Areas in Wireless Sensor Networks using BPR",IEEE Transcations Computer Networks, 0018-9340 2013.
[6] M. Ahmadi Livani and M. Abadi, "An energy-efficient anomaly detection approach for wireless sensor networks," in IST: 5th International Symposium on Telecommunications, 2010, pp. 243–248.
[7] N. Ahmed, S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey," SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 2, pp. 4–18, Apr. 2005.
[8] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
[9] N. Arad and Y. Shavitt, "Minimizing recovery state in geographic ad hoc routing," IEEE Transactions on Mobile Computing,vol. 8, no. 2, pp. 203–217, 2009.
[10] Ashwini and P. A. S, "Information dissemination between nodes of different intersections intersection in city environment using hop greedy routing protocol (BAHG)," International Journal of Ethics in Engineering and Management Education, vol. 1, no. 4, pp. 232–236, April 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY