Bharath
INSTITUTE OF HIGHER EDUCATION AND RESEARCH
(Declared as Deemed-to-be University under section 3 of UGC Act, 1956)
(Vide Notification No. F.9-5/2000 - U.3, Ministry of Human Resource Development, Govt. of India, dated 4th July 2002)
Accredited by NAAC
NATIONAL ASSESSMENT AND ACCREDITATION COUNCIL
Phone : 044-22290742 / 22290125 . Telefax : 044-22293886
Website : www.bharathuniv.ac.in
173, Agaram Road, Selaiyur, Tambaram,
Chennai - 600 073. Tamil Nadu.

Ref No.SMS-2018-O-08 Date: 17/04/2019

TO

Mrs. N. Priya,

Asst. Professor/CSE,

BIHER.

Thro: Concern Head of the Department

Greetings!!!

We are happy to announce that the Research Advisory Committee has approved your proposal for Seed Money Scheme-2018 which was presented by you. You are requested to complete the proposal and send the progress report to the Dean Research in the prescribed time period.

Title of the Project: A Novel and Efficient technique for Enhancing the Energy of WSNs

Seed Money Amount: Rs.1, 00,000/- (Rupees One Lakh Only)

Approved on: 17/04/2019

Payment details:

Voucher No.08 **Dated: 19/04/2019**

With Regards

Dean-Research 17/04/2019

Bharath University

SELAIYUR, CHENNAI - 600 073, TAMIL NADU, INDIA.

CASH / PAYMENT VOUCHER

Date 19/04/19

V.No.: 08

Debit _____ Amount

Rs. 1,00,000/-

PAID TO Mrs. N. Priya

RUPEES One lakh only

TOWARDS Seed Money Scheme - 2018

Authorised by **Finance Manager** **Cashier/Accountant** **Payee's Signature**

PROPOSAL SUBMISSION

1. **Details of Principal Investigator**

Name	: N.Priya
Designation	: Assistant Professor
Highest Qualifications	: M.E
Department	: Computer Science and Engineering
E-mail	: priya.cse@bharathuniv.ac.in
Contact no	: 9944052990
Date of Joining	: 17.9.2012

2. **Details of Co - Principal Investigator**

Name	: Dr. C.Rajabhushanam
Designation	: Professor
Highest Qualifications	: Ph.D
Department	: Computer Science and Engineering
E-mail	: rajabhushanamc.cse@bharathuniv.ac.in
Contact no	: 9445159354
Date of Joining	: 26.09.2015

Technical Details

1. Introduction

Wireless Sensor Networks (WSNs) are one of the most widely used technologies in our daily lives. The attractive feature of WSN is that the users communicate in a free, open environment. The open nature of WSN makes it very prone to the malicious attacks. One of the most frequently used attacks is the Denial of Service (DoS) attack otherwise known as a jamming attack. Jamming attacks floods the transmission channels by constantly sending useless packets and disrupts the communication process between legitimate nodes. This type of attack blocks the on-going communication and also reduces the lifetime of the network by exhausting the energy of the sensor nodes. DoS attacks can be performed at all layers of the network. Being the lowest and the first layer, the physical layer is attacked more by the jammers.

Payment for network resources, pushback, strong authentication and identification of traffic are some of the mechanisms to prevent the jamming attacks in a WSN. Therefore guarding against DoS attacks is a critical component of any security system but there is lack of research for preventing such attacks.

The depth-based routing protocols, examined in this work. In DBR(Depth-Based Routing) and EEDBR(Energy-Efficient Depth-Based Routing), stability period quickly ends due to unnecessary data forwarding and high load on low depth nodes, and a sharp instability period due to the fast energy consumption of medium-depth nodes. In AMCTD, the substantial pocket loss is due to distant transmissions of medium-depth nodes and which is not suitable for data-sensitive applications. The AMCTD's performance is better than DBR and EEDBR, respectively; however, deficiencies do exist. To overcome the deficiencies observed, an Improved Adaptive Mobility of Courier hubs in Threshold-Optimized Depth Based Routing (iAMCTD) is recommended.

2. Review of status of Research and Development in the subject

Shazana Md *et al.* (2014) proposes rapid advances of WSNs in supporting various kinds of applications are motivating the researchers to perform extensive research on the routing protocols. In this paper, we have presented a review on design

requirements and challenges of secure routing techniques for WSNs. We have contributed our categorization and critical comparisons of the noteworthy protocols, which should fill the void in this particular niche area. Furthermore, analysis of the security context design issues offers the basic guideline to develop proper mechanisms to combat the security infringements. Open issues are provided in order to stimulate more research interests in those interesting areas.

Opeyemi Osanaiye *et al.* (2018) says DoS attack, in its different forms, is detrimental to the availability of resources and services of WSN. It disrupts the monitoring and sensing function of WSN by directing malformed packets towards the target node to deplete its energy and resources. In this paper, we first present the areas where WSN can be deployed, such as terrestrial, underground, underwater, mobile and multimedia. The three main network structure of WSN; flat-based, cluster-based and hierarchical-based network topology was also discussed before presenting a taxonomy of the different forms of DoS attacks targeting different layers of the WSN. A corresponding taxonomy was also presented for DoS defence in WSN, by categorizing the proposed approaches according to the technique used, defence network structure and their deployment location. A comparative summary of the different defence techniques was presented together with the different IDS deployment location, which is dependent on the network structure. Anomaly-based detection and sensor node IDS deployment were identified as the most popular detection technique and deployment location proposed. Finally, the drawbacks of suggested techniques were highlighted and possible solutions were proposed.

W Al-Sakib Khan Pathan *et al.* (2006) finds a large portion of the attacks against security in wireless sensor networks are brought about by the inclusion of false data by the compromised nodes inside the system. For protecting the consideration of false reports by compromised nodes, a method is required for distinguishing false reports. Be that as it may, growing such a discovery component and making it effectively speaks to an extraordinary research test. Once more, guaranteeing all-encompassing security in a wireless sensor network is a noteworthy research issue. A considerable lot of the present proposed security plans depend on explicit system

models. As there is an absence of consolidated exertion to take a typical model to guarantee security for each layer, in future however the security instruments turn out to be settled for every individual layer, joining every one of the systems together to make them work in a joint effort with one another will cause a hard research test. Regardless of whether all-encompassing security could be guaranteed for remote sensor organizes, the cost-adequacy and vitality effectiveness to utilize such components could, in any case, present incredible research test in the coming days.

Hymlin Rose and Jayasree (2017) concluded that the new technique proposed is very simple and as it is a clustering approach if any node is identified as the malicious node, the communication is altered to the other grouping by arranging a new cluster leaving the malicious node. Therefore the transmission is not been disrupted. Thus the spreading code which has been used for receiving the acknowledgement, if mismatched with the receiver, it also identifies that node as the malicious node and stops transmission through that node. The performance metric is analyzed based on the Packet Delivery Ratio (PDR), and it shows that, if the malicious node present is increased, the PDR decreases and vice versa.

Raja Waseem Anwar *et al.* (2014) Wireless sensor network is a standout amongst the most developing innovation for detecting and playing out the distinctive assignments. Such systems are gainful in numerous fields, for example, emergencies, health monitoring, environmental control, military, industries and these systems inclined to malevolent clients' and physical attacks because of radio scope of the system, un-confided in transmission, unattended nature and get to effectively. Security is a key necessity for these systems. In this paper, our focal point of consideration is on physical attacks and issues in Wireless sensor networks. Through this survey, effectively distinguish the reason and abilities of the assailants. Further, we talk about understood methodologies of security identification against physical attacks.

Mini Sharma *et al.* (2017) survey of various attacks along with their countermeasures in sensor networks is presented. The requirement for security in WSNs is of utmost importance because it is susceptible to various types of attacks.

WSNs is vulnerable to attacks because of its dynamic nature, resource-constrained nodes and large network scales. The paper also presents a detailed survey on IEEE 802.15.4 standard attacks and their countermeasures.

Javaid *et al.* (2014) proposed routing metrics such as Expected Transmission Count (ETX) and Minimum Delay (MD), which are also used in localization-free routing protocols. Another efficient scheme, Reliable and Energy-efficient Routing Protocol for underwater wireless sensor networks (RERP2R) (Wahid *et al.* 2010) employ the routing metric based on the physical distances between the sensor nodes and exercise it to achieve higher throughput in UWSNs.

Adaptive Mobility of Courier nodes in Threshold-optimized DBR (AMCTD) (Jafri *et al.* 2013) employs courier nodes to improve stability period and network throughput. It attempts to confiscate a coverage hole problem, which is necessary for data-sensitive applications. Improved Adaptive Mobility of Courier nodes in Threshold-Optimized DBR (IAMCTD) (Jafri *et al.* 2013) is an enhanced version of AMCTD. It devises efficient forwarding function to minimize the deficiencies of AMCTD and also implements on-demand data routing.

2.1 International Status: NIL

2.2 National Status: NIL

3. Progress/achievement so far,

a) Reference papers were collected.

b) Literature survey was studied.

c) Proposal work has been started in WSNs based on Jamming attacks.

4. Work Plan:

4.1 Methodology:

The main Objectives of the proposed work are as follows:

- To enhance the energy of WSNs by creating a shortest route between nodes. To save energy in all of the clustering WSNs.

- To reduce transmission loss in WSNs.
- To reduce packet loss in WSNs.
- To reduce the delay in transmission of data in WSNs.

Block Diagram:

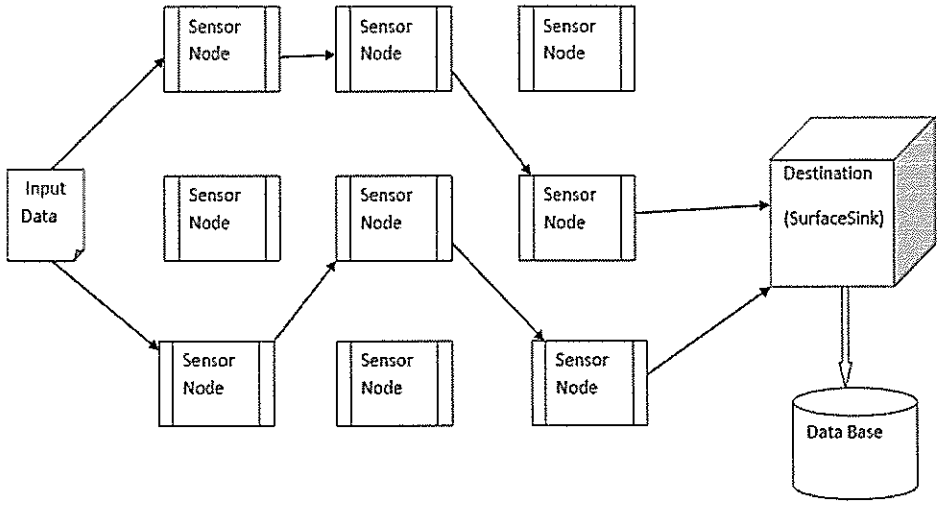


Figure 1 : Proposed System Architecture

- The proposed protocol performs on-demand data routing as the nodes react immediately to sudden and drastic changes considering the value of sensed attribute The sensor nodes, transmit control packets after every 100 rounds for the computation of network density at the surface sink, which is additionally used to succeed the deviation in the mobility patterns of courier nodes and depth-thresholds.

- The data packet format of our system is shown in Figure 2 which consists of sender ID, packet sequence number, depth information, and payload.

Sender ID	Packet sequence number	Depth	Payload....

Figure 2: Data packet format

- The proposed iAMCTD technique deploy the network of 225 nodes using arbitrary topology. The transmission range of sensor node is 100 meters, following the physical features of the underwater acoustic modem. The network compared with proposed iAMCTD and DBR. For simulation 15000 nodes have been deployed randomly.

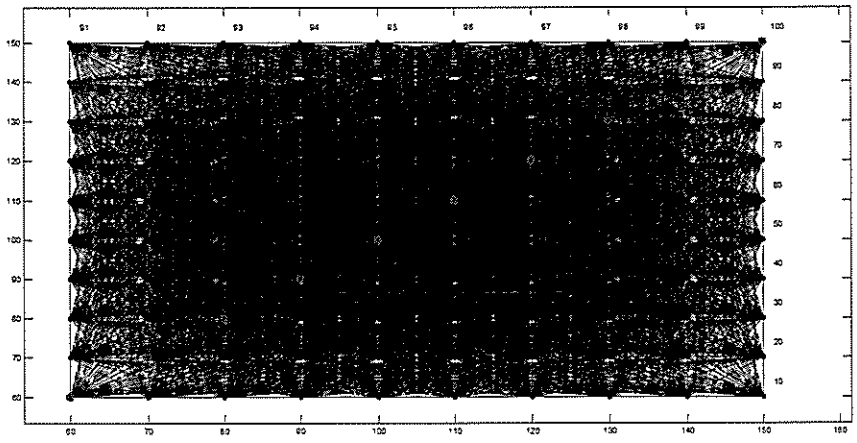
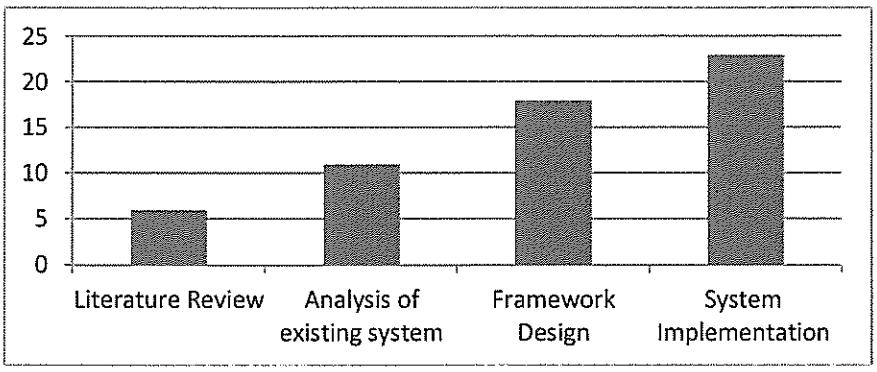


Figure 3: Proposed Square grid 100 node WSN network

- In iAMCTD, the efficient movement of courier nodes minimizes end-to-end delay and decreases the energy consumption of low-depth nodes in rare conditions.
- Implementation of threshold-optimized data forwarding is an inventive process for on-demand routing and removes forwarding of unnecessary data in the network.

4.2 Time Schedule of activities giving milestones through BAR diagram. Work plan (including detailed methodology and time schedule)

Sl.No	Activity Milestone	1rd Year		2nd Year	
1.	Literature Review	1-6			
2.	Analysis of existing system		7-12		
3.	Framework Design			13-18	
4.	System Implementation				19-24



4.3 Expected outcome within the time period of Seed Money Scheme

a) Prototype framework design can be implemented within the time period of Seed Money Scheme.

b) Real time implementation of proposed work can be done within the time Period of Seed Money Scheme.

5. Suggested Plan of action stating the name of funding agency where the project will be communicated for financial support within the time period of project.

Nil

6. Bibliography: Nil

7. List of Projects submitted/implemented by the investigators (Separate for PI and Co-PI)

Nil

7.1 Details of Projects submitted to various funding agencies:

Sl. No	Title	Cost in Lakhs	Month of Submission	Role as PI/Co-PI	Agency	Status
	NA	NA	NA	NA	NA	NA

7.2 Details of Projects under implementation:

Sl. No	Title	Cost in Lakhs	Duration	Role as PI/Co-PI	Agency
	NA	NA	NA	NA	NA

7.3 Details of Projects completed during the last 5 years

Sl. No	Title	Cost in Lakhs	Duration	Role as PI/Co-PI	Agency
	NA	NA	NA	NA	NA

8. List of publications published by the investigators, if any:

a) Co-Principal Investigator

S.No	Author names	Title of paper	Name of Journal	Vol (issue)	Page no.	Year
1.	Rangaswamy, K. Dr.Rajabhushanam,C.	Practical Congestion Control Scheme with hop-by-hop Control in Wireless Sensor Networks	International Journal of Future Generation Communication and Networking	12(5)	197-205	2018
2.	Rangaswamy, K. Dr. Rajabhushanam,C.	Implementing EDGE: a Greedy Algorithm for Diminishing the Drop and Delay in Wireless Sensor Networks	Journal of Advanced Research in Dynamical and Control Systems	10 (15)	615-623	2018
3.	Harikrishna,T., Rajabhushanam,C., Michael,G., Kavitha, R	Liver disorder prognosis with apache spark random forest and gradient booster algorithms	International Journal of Innovative Technology and Exploring Engineering	8(9)	615-620	2018
4.	Krishna, T.H., Rajabhushanam, C., Jayapriya, D., Deivasigamani, S	A scalable and fault tolerant health risk predictor using big data process systems	International Journal of Innovative Technology and Exploring Engineering	8(9)	609-614	2018

b) Principal Investigator

S.No	Author names	Title of paper	Name of Journal	Vol (issue)	Page no.	Year
1	Priya, N., Sridhar, J., Sriram, M	Ecommerce Transaction Security Challenges and Prevention Methods - New Approach	Journal of Chemical and Pharmaceutical Sciences	9(3)	S66 - S68	2016

2	Priya, N., Sridhar,J., Sriram, M.	Vehicular cloud computing security issues and solutions	Journal of Chemical and Pharmaceutical Sciences	9(2)	E424 - E427	2016
3	Priya, N., Sridhar,J., Sriram, M.	Mobile large data storage security in cloud computing environment-a new approach	Journal of Chemical and Pharmaceutical Sciences	9(2)	E420 - E423	2016

9. Budget

Sl.No	Equipment	Quantity	Amount in INR
1	Processor: Intel® Core™ i3 CPU, Hard Disk: 400 GB and RAM: 4 GB Operating system: Windows XP / Windows 7/Windows 8. Language : Java 1.7 Front-end Tool : Net Beans IDE Backend Tool : MySQL Other Tools/SW : MATLAB, NS2	1	60,000
2	Consumables(Book, CD,USB, Paper, Stationeries, Research Journals)	As per requirement	30,000
3	Travel support for the purpose of research work.	-	5,000
4	Contingency	-	2,500
5	Others	-	2,500
	Total		**1,00,000**

10. Name of at least two subject experts from the Institute and one from the outside Institute with their contact details

a) Dr.KP.Kaliyamurthie - Professor, Dept. of CSE, BIHER, Chennai- 600073

b) Dr.Baskar - Professor, Dept. of CSE, SRM Institute of Science and Technology, Kattankulathur, Chennai- 603203

CERTIFICATE FROM THE INVESTIGATOR

Project Title: **A Novel and Efficient technique for Enhancing the Energy of WSNs**

It is certified that

1. I do hereby agree to submit a complete proposal for financial support to the external funding agency within the time period of SMS-2018.
2. I undertake that spare time on equipment procured in the project will be made available to other users.
3. I agree to submit a certificate from Institutional Bio safety Committee, if the project involves the utilization of genetically engineered organisms. I also declare that while conducting experiments, the Bio safety Guidelines of Department of Biotechnology, Department of Health Research, GOI would be followed in to.
4. I agree to submit ethical clearance certificate from the concerned ethical trails/experiments/exchange of committee, if the project involves field specimens, human & animal materials etc.
5. I agree to abide by the terms and conditions of SMS-2018, BIHER, and Chennai.

Name and signature of
Principal Investigator
(MS. N. PRIYA)

Name and signature of
Co-Principal Investigator
DR. C. RAJABHUSHANAM

Date : 15.03.2019
Place : Chennai - 73

Forwarded by Head of the Department

Signature of the Head

PROJECT EVALUATION FORMAT

Recommendation Sheet

Name of the Principal Investigator	N.Priya
Name of the Co-Investigator	Dr.C.Rajabhushanam
Name of the Department	Computer Science and Engineering
Title of the Project	**A Novel and Efficient technique for Enhancing the Energy of WSNs**
Recommendation of the evaluation committee	— Recommended —
Financial allocation recommended	Rs. 100,000 —

Sl.No	Equipment	Quantity	Amount in INR
1	Processor: Intel® Core™ i3 CPU, Hard Disk: 400 GB and RAM: 4 GB Operating system: Windows XP / Windows 7/Windows 8. Language : Java 1.7 Front-endTool : Net Beans IDE BackendTool : MySQL Other Tools/SW : MATLAB, NS2	1	60,000
2	Consumables(Book, CD,USB, Paper, Stationeries, Research Journals)	As per requirement	30,000
3	Travel support for the purpose of research work.	-	5,000
4	Contingency	-	2,500
5	Others	-	2,500
	Total		**1,00,000**

Name and Signature of the Research Advisory Committee members with date

(Dr. P. Nageenchandran)

Internal Quality Assurance Cell IQAC Saveetha Chennai-77