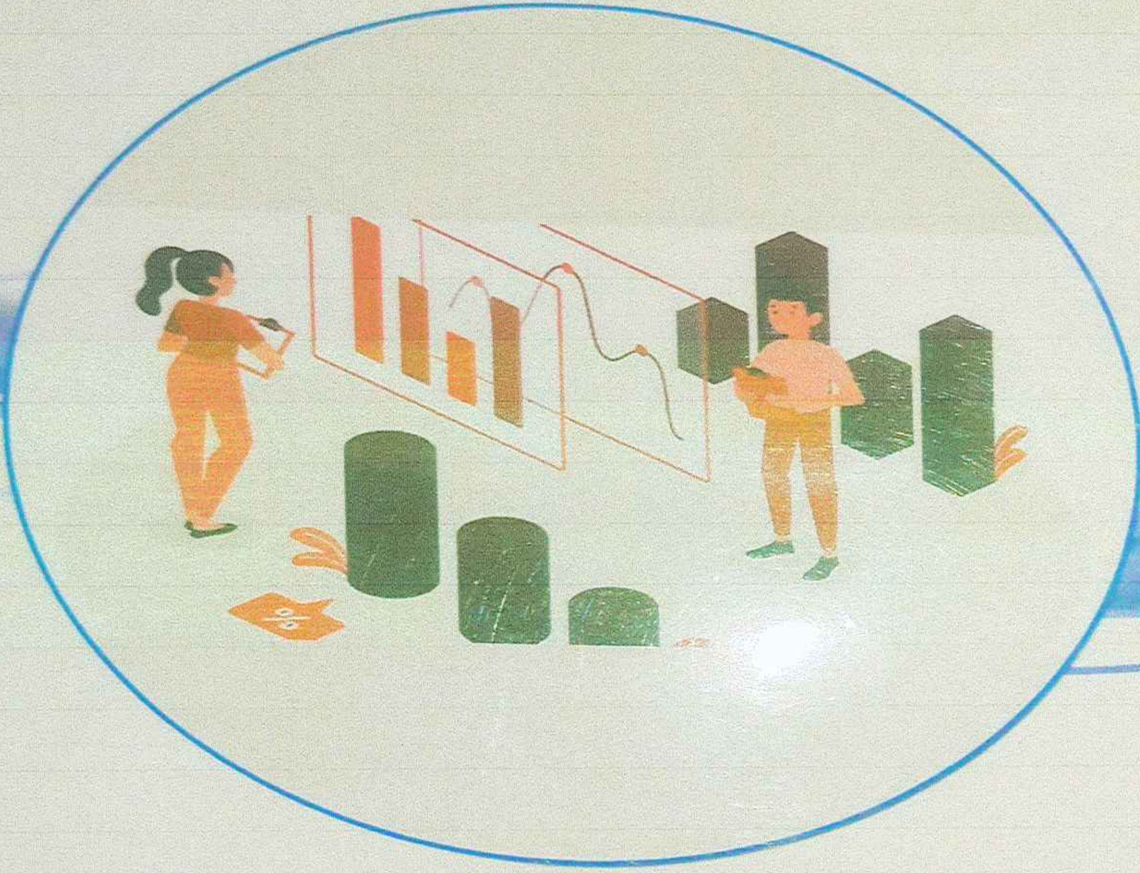
Research Methodology



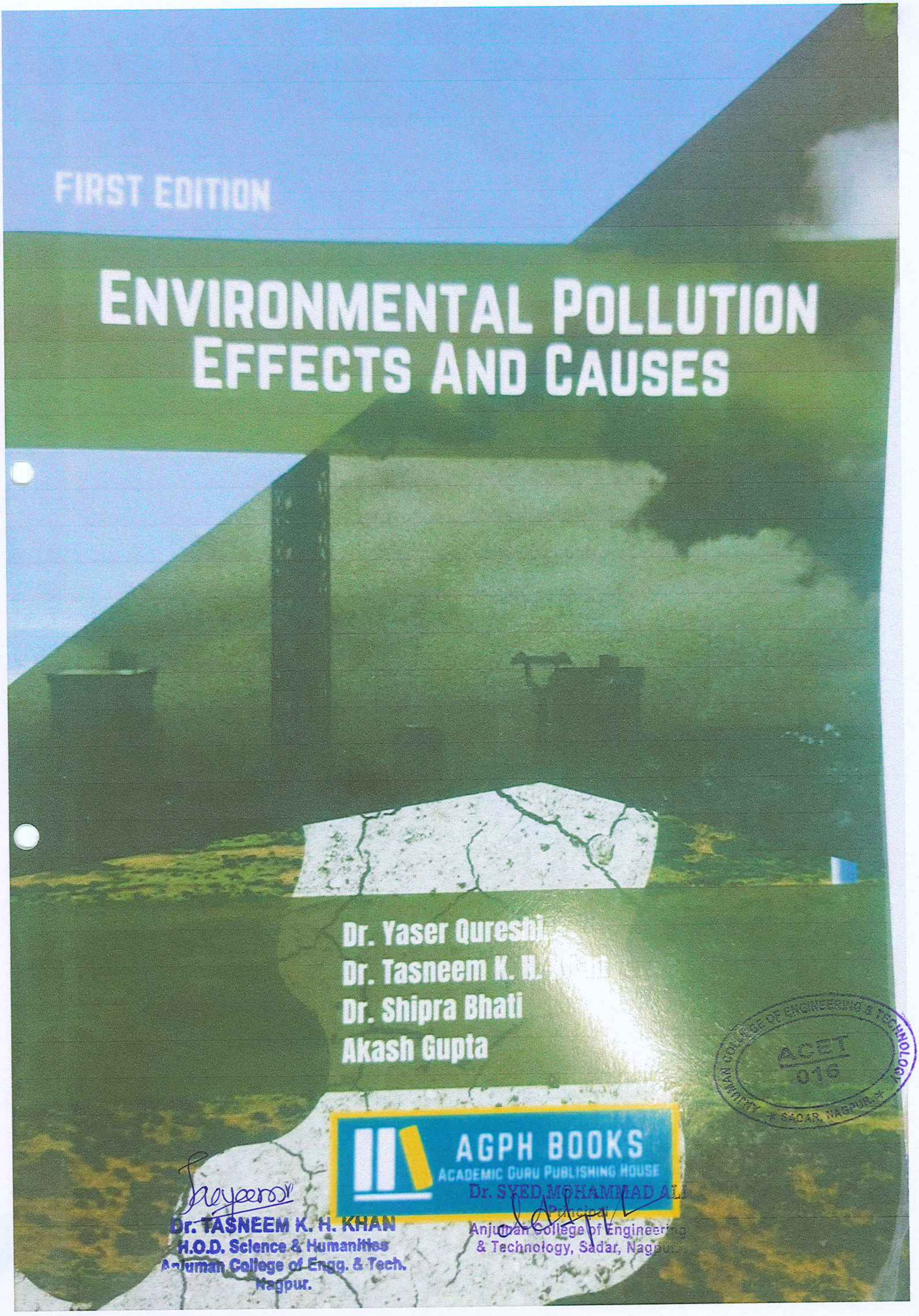
SIPH

Dr. Vikas Pradhan

Dr. Vilas J Kharat

Dr. Tasneem K. H. Khan

Dr. Aniket Bhagirath Jadhav

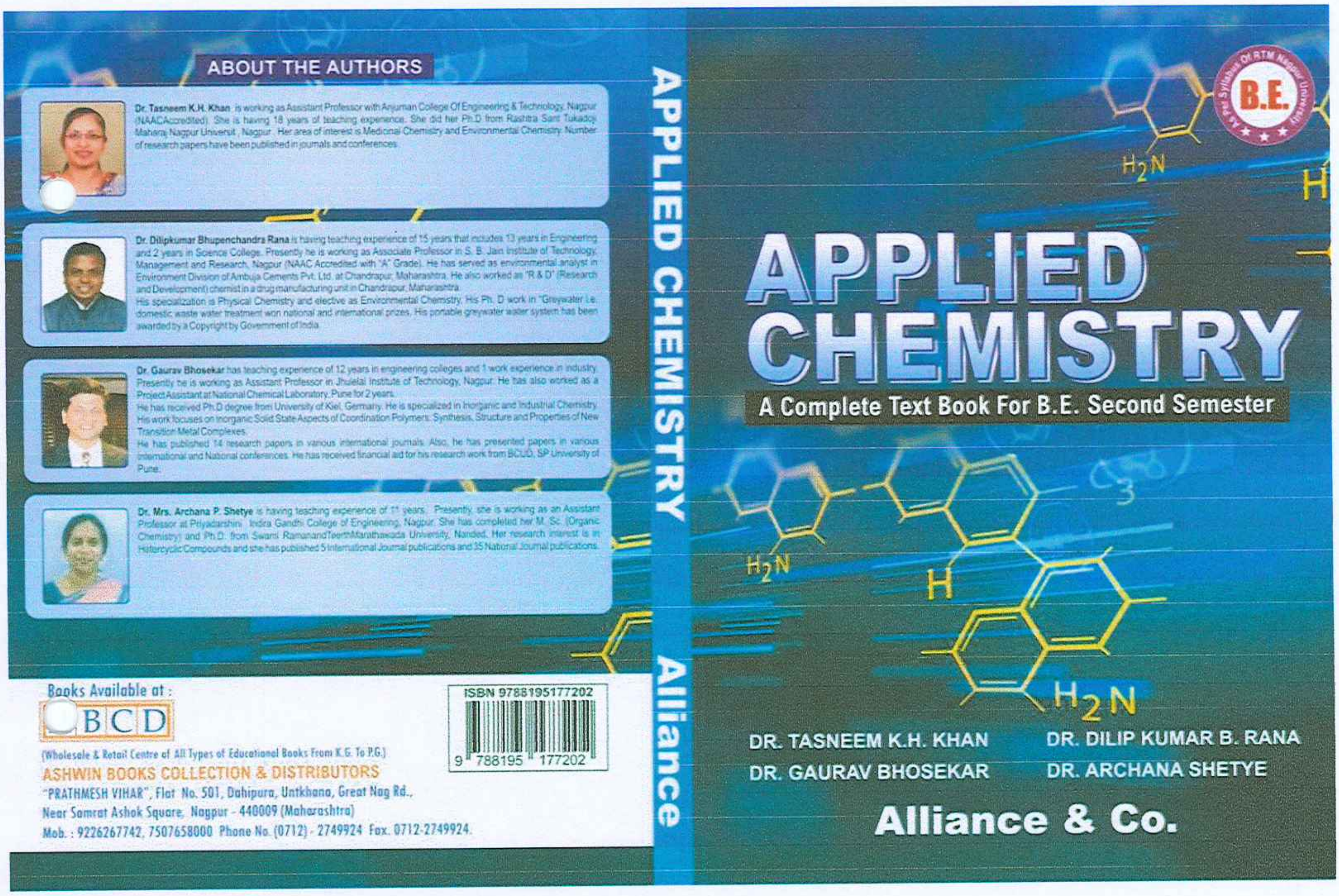


FIRST EDITION

ENVIRONMENTAL POLLUTION EFFECTS AND CAUSES

Dr. Yaser Qureshi
Dr. Tasneem K. H. Khan
Dr. Shipra Bhati
Akash Gupta

AGPH BOOKS
ACADEMIC GURU PUBLISHING HOUSE



ABOUT THE AUTHORS

Dr. Tasneem K.H. Khan is working as Assistant Professor with Anjuman College Of Engineering & Technology, Nagpur (NAACAccredited). She is having 18 years of teaching experience. She did her Ph.D from Rashtra Sant Tukadoji Maharaj Nagpur Universit , Nagpur . Her area of interest is Medicinal Chemistry and Environmental Chemistry. Number of research papers have been published in journals and conferences.

Dr. Dilipkumar Bhupenchandra Rana is having teaching experience of 15 years that includes 13 years in Engineering and 2 years in Science College. Presently he is working as Associate Professor in S. B. Jain Institute of Technology, Management and Research, Nagpur (NAAC Accredited with "A" Grade). He has served as environmental analyst in Environment Division of Ambuja Cements Pvt. Ltd. at Chandrapur, Maharashtra. He also worked as "R & D" (Research and Development) chemist in a drug manufacturing unit in Chandrapur, Maharashtra.

His specialization is Physical Chemistry and elective as Environmental Chemistry. His Ph. D work in "Greywater i.e. domestic waste water treatment won national and international prizes. His portable greywater water system has been awarded by a Copyright by Government of India.

Dr. Gaurav Bhosekar has teaching experience of 12 years in engineering colleges and 1 work experience in industry. Presently he is working as Assistant Professor in Jhulelal Institute of Technology, Nagpur. He has also worked as a Project Assistant at National Chemical Laboratory, Pune for 2 years.

He has received Ph.D degree from University of Kiel, Germany. He is specialized in Inorganic and Industrial Chemistry. His work focuses on Inorganic Solid State Aspects of Coordination Polymers: Synthesis, Structure and Properties of New Transition Metal Complexes.

He has published 14 research papers in various international journals. Also, he has presented papers in various international and National conferences. He has received financial aid for his research work from BCUD, SP University of Pune.

Dr. Mrs. Archana P. Shetye is having teaching experience of 11 years. Presently she is working as an Assistant Professor at Priyadarshini Indira Gandhi College of Engineering, Nagpur. She has completed her M. Sc. (Organic Chemistry) and Ph.D. from Swami RamanandTeerthMarathawada University, Nanded. Her research interest is in Hetercyclic Compounds and she has published 5 International Journal publications and 35 National Journal publications.

Books Available at :
BCD
(Wholesale & Retail Centre of All Types of Educational Books From K.G. To P.G.)
ASHWIN BOOKS COLLECTION & DISTRIBUTORS
"PRATHMESH VIHAR", Flat No. 501, Dahipura, Untkhana, Great Nag Rd.,
Near Samrat Ashok Square, Nagpur - 440009 (Maharashtra)
Mob. : 9226267742, 7507658000 Phone No. (0712) - 2749924 Fax. 0712-2749924.

ISBN 9788195177202
9 788195 177202

APPLIED CHEMISTRY

Alliance

APPLIED CHEMISTRY

A Complete Text Book For B.E. Second Semester

DR. TASNEEM K.H. KHAN
DR. DILIP KUMAR B. RANA
DR. GAURAV BHOSEKAR
DR. ARCHANA SHETYE

Alliance & Co.

Dr. TASNEEM K. H. KHAN
H.O.D. Science & Humanities
Anjuman College of Engg. & Tech.
Nagpur.

Dr. SYED MOHAMMAD ALI
Principal
Anjuman College of Engineering
& Technology, Sadar, Nagpur.

ANJUMAN COLLEGE OF ENGINEERING & TECHNOLOGY
ACET
016
★ SADAR, NAGPUR. ★

As per New Syllabus
(w.e.f. 2020-21)

B.E.

ENERGY AND ENVIRONMENT

(A Complete Text Book For BE. Sem I)

Tasneem

Dr. Tasneem K. H. Khan

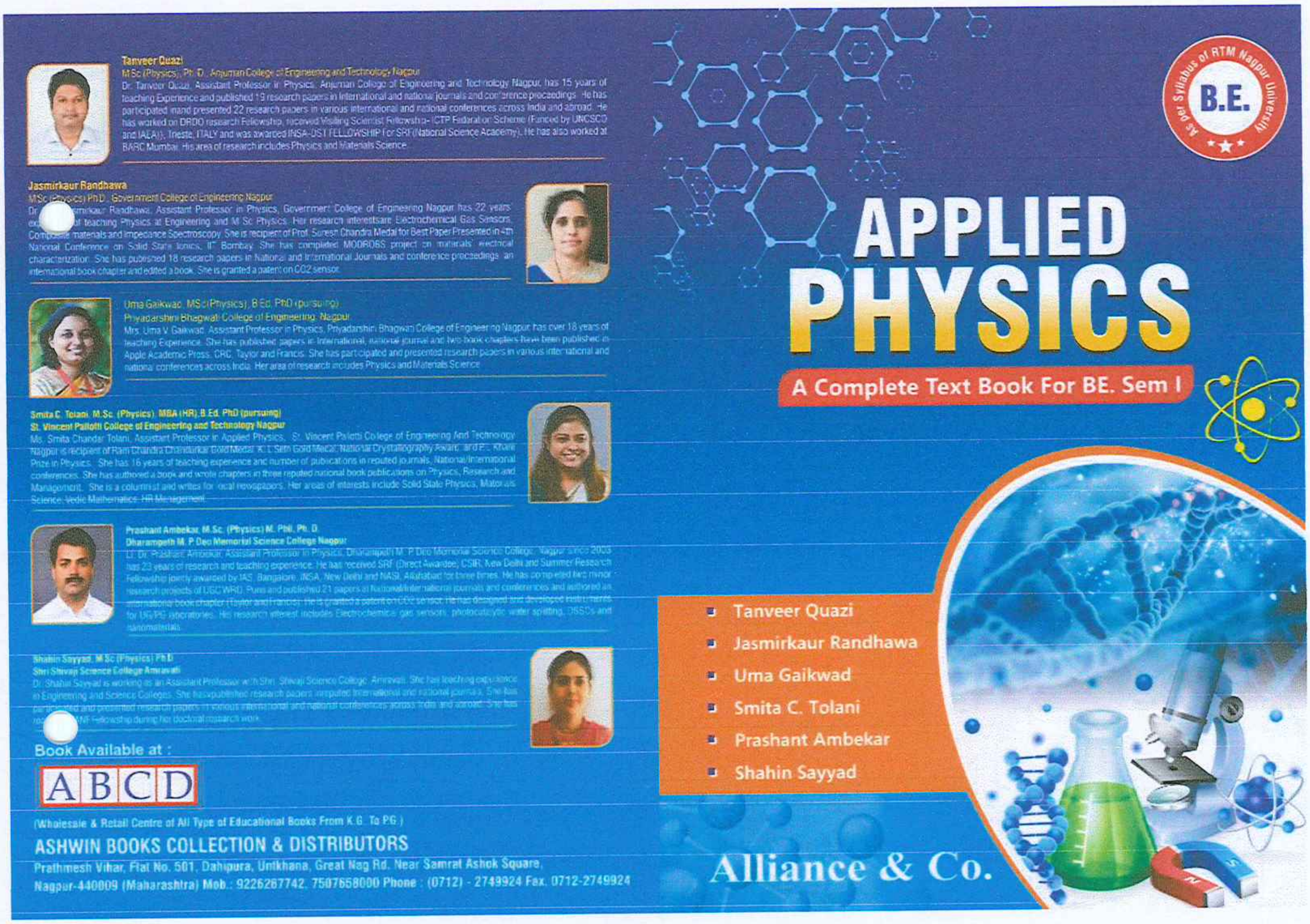
Dr. Dilip kumar B. Rana

Dr. Gaurav Bhosekar

Dr. Archana Shetye

Alliance & Co.

Tasneem



Tanveer Quazi
M.Sc (Physics), Ph. D., Anjuman College of Engineering and Technology Nagpur
Dr. Tanveer Quazi, Assistant Professor in Physics, Anjuman College of Engineering and Technology Nagpur, has 15 years of teaching Experience and published 19 research papers in International and national journals and conference proceedings. He has participated inand presented 22 research papers in various international and national conferences across India and abroad. He has worked on DRDO research Fellowship, received Visiting Scientist Fellowship- ICTP Federation Scheme (Funded by UNCSCO and IAEA)), Trieste, ITALY and was awarded INSA-DST FELLOWSHIP For SRF(National Science Academy). He has also worked at BARC Mumbai. His area of research includes Physics and Materials Science.

Jasmirkaur Randhawa
M.Sc (Physics) Ph.D., Government College of Engineering Nagpur
Dr. Jasmirkaur Randhawa, Assistant Professor in Physics, Government College of Engineering Nagpur has 22 years experience of teaching Physics at Engineering and M.Sc Physics. Her research interestsare Electrochemical Gas Sensors, Composite materials and Impedance Spectroscopy. She is recipient of Prof. Suresh Chandra Medal for Best Paper Presented in 4th National Conference on Solid State Ionics, IIT Bombay. She has completed MODROBS project on materials' electrical characterization. She has pubished 18 research papers in National and International Journals and conference proceedings, an international book chapter and edited a book. She is granted a patent on CO2 sensor.

Uma Gaikwad, MSc(Physics), B.Ed, PhD (pursuing)
Priyadarshini Bhagwati College of Engineering, Nagpur
Mrs. Uma V. Gaikwad, Assistant Professor in Physics, Priyadarshini Bhagwati College of Engineering Nagpur has over 18 years of teaching Experience. She has published papers in International, national journal and two book chapters have been published in Apple Academic Press, CRC, Taylor and Francis. She has participated and presented research papers in various international and national conferences across India. Her area of research includes Physics and Materials Science.

Smita C. Tolani, M.Sc. (Physics), MBA (HR), B.Ed, PhD (pursuing)
St. Vincent Pallotti College of Engineering and Technology Nagpur
Ms. Smita Chandar Tolani, Assistant Professor in Applied Physics, St. Vincent Pallotti College of Engineering And Technology Nagpur is recipient of Ram Chandra Chandurkar Gold Medal, K. L. Seth Gold Medal, National Crystallography Award, and P. L. Khare Prize in Physics. She has 16 years of teaching experience and number of publications in reputed journals, National/International conferences. She has authored a book and wrote chapters in three reputed national book publications on Physics, Research and Management. She is a columnist and writes for local newspapers. Her areas of interests include Solid State Physics, Materials Science, Vedic Mathematics, HR Management.

Prashant Ambekar, M.Sc. (Physics) M. Phil, Ph. D.
Dharampeth M. P. Deo Memorial Science College Nagpur
Lt. Dr. Prashant Ambekar, Assistant Professor in Physics, Dharampeth M. P. Deo Memorial Science College, Nagpur since 2003 has 23 years of research and teaching experience. He has received SRF (Direct Awardee, CSIR, New Delhi and Summer Research Fellowship jointly awarded by IAS, Bangalore, INSA, New Delhi and NASI, Allahabad for three times. He has completed two minor research projects of UGC WRO, Pune and published 21 papers in National/International journals and conferences and authored an international book chapter (Taylor and Francis). He is granted a patent on CO2 sensor. He has designed and developed instruments for UG/PG laboratories. His research interest includes Electrochemical gas sensors, photocatalytic water splitting, DSSCs and nanomaterials.

Shahin Sayyad, M.Sc (Physics) Ph.D
Shri Shivaji Science College Amravati
Dr. Shahin Sayyad is working as an Assistant Professor with Shri. Shivaji Science College, Amravati. She has teaching experience in Engineering and Science Colleges. She hasxpublished research papers inreputed International and national journals. She has participated and presented research papers in various international and national conferences across India and abroad. She has received MANF Fellowship during her doctoral research work.

Book Available at :

ABCD

(Wholesale & Retail Centre of All Type of Educational Books From K.G. To P.G.)

ASHWIN BOOKS COLLECTION & DISTRIBUTORS
Prathmesh Vihar, Flat No. 501, Dahipura, Untkhana, Great Nag Rd. Near Samrat Ashok Square,
Nagpur-440009 (Maharashtra) Mob.: 9226267742, 7507658000 Phone : (0712) - 2749924 Fax. 0712-2749924

As per Syllabus of RTM Nagpur University
B.E.

APPLIED PHYSICS

A Complete Text Book For BE. Sem I

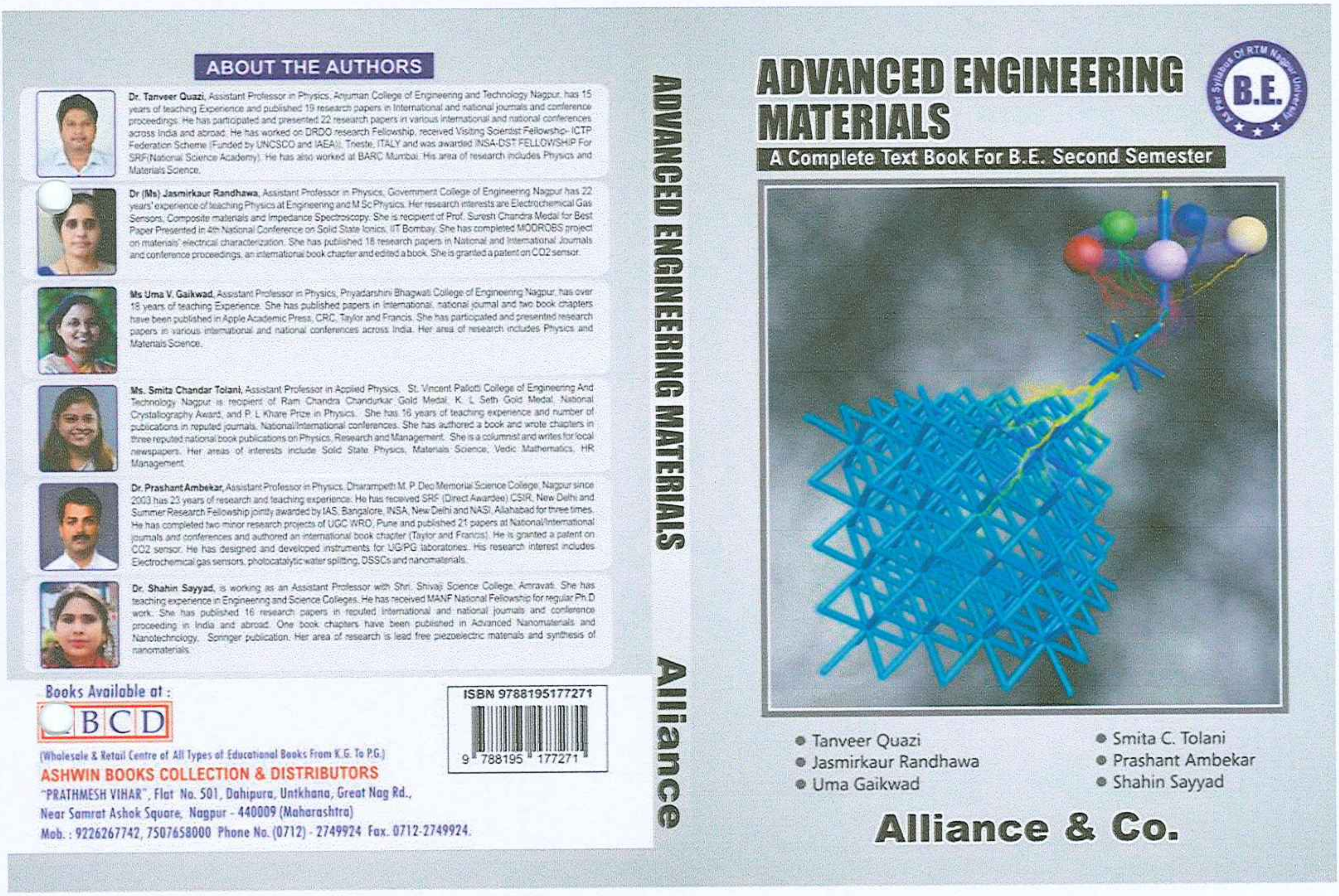
- Tanveer Quazi
- Jasmirkaur Randhawa
- Uma Gaikwad
- Smita C. Tolani
- Prashant Ambekar
- Shahin Sayyad

Alliance & Co.

Dr. TASNEEM K. H. KHAN
H.O.D. Science & Humanities
Anjuman College of Engg. & Tech.
Nagpur.

Dr. SYED MOHAMMAD ALI
Principal
Anjuman College of Engineering
& Technology, Sadar

ANJUMAN COLLEGE OF ENGINEERING & TECHNOLOGY
ACET
016
★ SADAR, NAGPUR ★



ABOUT THE AUTHORS

Dr. Tanveer Quazi, Assistant Professor in Physics, Anjuman College of Engineering and Technology Nagpur, has 15 years of teaching Experience and published 19 research papers in International and national journals and conference proceedings. He has participated and presented 22 research papers in various international and national conferences across India and abroad. He has worked on DRDO research Fellowship, received Visiting Scientist Fellowship- ICTP Federation Scheme (Funded by UNCSCO and IAEA)), Trieste, ITALY and was awarded INSA-DST FELLOWSHIP For SRF(National Science Academy). He has also worked at BARC Mumbai. His area of research includes Physics and Materials Science.

Dr (Ms) Jasmirkaur Randhawa, Assistant Professor in Physics, Government College of Engineering Nagpur has 22 years' experience of teaching Physics at Engineering and M Sc Physics. Her research interests are Electrochemical Gas Sensors, Composite materials and Impedance Spectroscopy. She is recipient of Prof. Suresh Chandra Medal for Best Paper Presented in 4th National Conference on Solid State Ionics, IIT Bombay. She has completed MODROBS project on materials' electrical characterization. She has published 18 research papers in National and International Journals and conference proceedings, an international book chapter and edited a book. She is granted a patent on CO2 sensor.

Ms Uma V. Gaikwad, Assistant Professor in Physics, Priyadarshini Bhagwati College of Engineering Nagpur, has over 18 years of teaching Experience. She has published papers in International, national journal and two book chapters have been published in Apple Academic Press, CRC, Taylor and Francis. She has participated and presented research papers in various international and national conferences across India. Her area of research includes Physics and Materials Science.

Ms. Smita Chandar Tolani, Assistant Professor in Applied Physics. St. Vincent Pallotti College of Engineering And Technology Nagpur is recipient of Ram Chandra Chandurkar Gold Medal, K. L Seth Gold Medal, National Crystallography Award, and P. L Khare Prize in Physics. She has 16 years of teaching experience and number of publications in reputed journals, National/International conferences. She has authored a book and wrote chapters in three reputed national book publications on Physics, Research and Management. She is a columnist and writes for local newspapers. Her areas of interests include Solid State Physics, Materials Science, Vedic Mathematics, HR Management.

Dr. Prashant Ambekar, Assistant Professor in Physics, Dharampeth M. P. Deo Memorial Science College, Nagpur since 2003 has 23 years of research and teaching experience. He has received SRF (Direct Awardee) CSIR, New Delhi and Summer Research Fellowship jointly awarded by IAS, Bangalore, INSA, New Delhi and NASI, Allahabad for three times. He has completed two minor research projects of UGC WRO, Pune and published 21 papers at National/International journals and conferences and authored an international book chapter (Taylor and Francis). He is granted a patent on CO2 sensor. He has designed and developed instruments for UG/PG laboratories. His research interest includes Electrochemical gas sensors, photocatalytic water splitting, DSSCs and nanomaterials.

Dr. Shahin Sayyad, is working as an Assistant Professor with Shri. Shivaji Science College, Amravati. She has teaching experience in Engineering and Science Colleges. He has received MANF National Fellowship for regular Ph.D work. She has published 16 research papers in reputed International and national journals and conference proceeding in India and abroad. One book chapters have been published in Advanced Nanomaterials and Nanotechnology, Springer publication. Her area of research is lead free piezoelectric materials and synthesis of nanomaterials.

ISBN 9788195177271
9 788195 177271

ADVANCED ENGINEERING MATERIALS

Alliance

ADVANCED ENGINEERING MATERIALS

As Per Syllabus Of RTM Nagpur University
B.E.

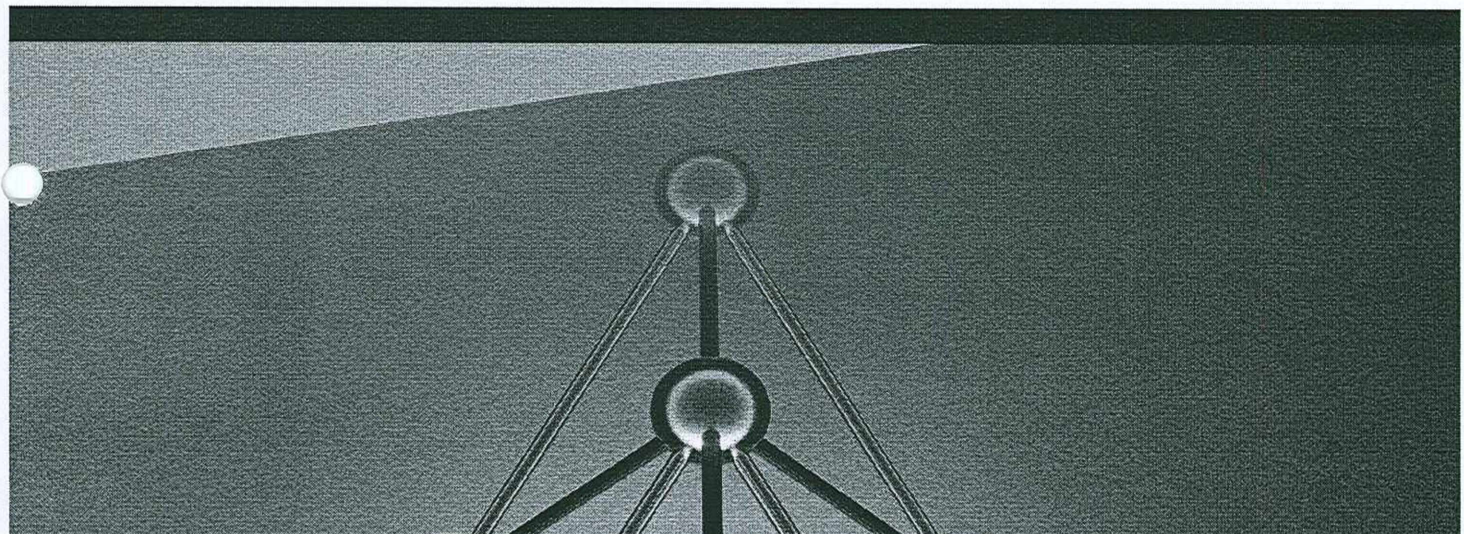
A Complete Text Book For B.E. Second Semester

- Tanveer Quazi
- Jasmirkaur Randhawa
- Uma Gaikwad
- Smita C. Tolani
- Prashant Ambekar
- Shahin Sayyad

Alliance & Co.

New Trends in Physical Science Research

Vol. 6



B P International

Contents

Chapter 5
Print ISBN: 978-93-5547-342-4, eBook ISBN: 978-93-5547-350-9

Effect of Glycine Dopant on FTIR Spectrum of Ammonium Dihydrogen Phosphate (ADP) Crystal Grown by Slow Evaporation, Rotation and SR Methods

A. Z. Khan [a*ϖ] and Z. S. Khan [bϖ]

DOI: 10.9734/bpi/ntpsr/v6/2314A

ABSTRACT

Diverse molar concentrations of Ammonium Dihydrogen Phosphate crystals doped with Glycine (GADP) have been generated using different processes, including slow evaporation, rotation, and Sankaranarayanan - Ramasamy (SR) procedures. ADP crystals have found many applications in Non-linear optics, electro-optics, and transducer devices. On the developed GADP crystals, the Fourier Transform Infrared (FTIR) researches have been widely examined. The extra peaks in the FTIR spectrum that correspond to the functional groups of Glycine reveal the interaction between ADP and the dopant. The presence of all functional groups in the substance is confirmed by FTIR's standard spectrum statistics. When compared to the conventional slow evaporation method created Glycine doped ADP crystals, the spectra for ADP crystals doped with Glycine grown by Rotation and SR procedures had identical peaks with minimal variance.

Keywords: Evaporation, crystal growth, electro-optics, ADP Crystals

1. INTRODUCTION

In material science and engineering, crystal growth is a fundamental concept. The vast majority of crystal growth research has focused on practical approaches rather than hypothetical exploration. For the manufacture of greater efficiency PV cells for surrogate energy, advancements in crystal formation are critical. For initial data acquisition and devices utilized for practical purposes such as ICs and sensors, crystals of the necessary diameter and precision are required. Adding small previously prepared crystals to the prepared solutions provides nucleating sites. A single seed crystal would result in a larger crystal [1-2]. Depending on the phase conversion method, techniques of crystal growth can be classified as growth from solid, vapour, melt and solution [3]. The various methods of solution growth are studied by many researchers [4]. As the crystal growth is conceded at the room temperature, the structural impurities in the crystals grown by solution method are quite less [5].

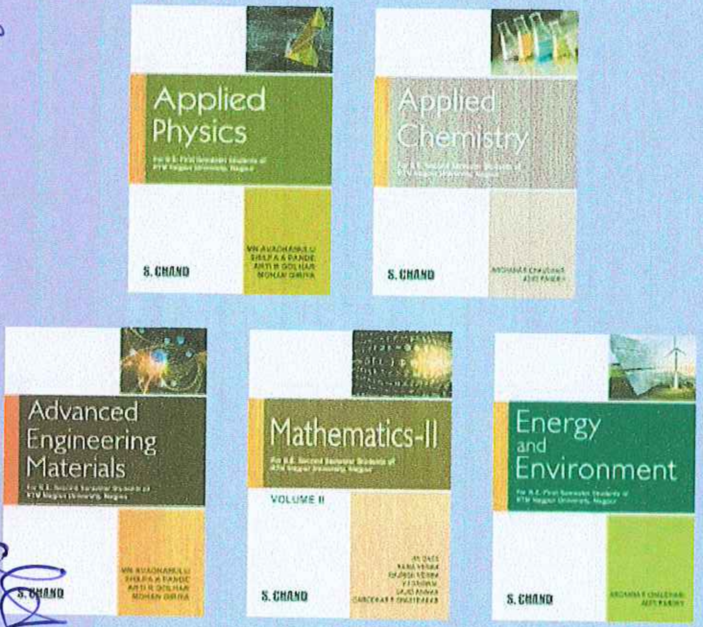
Ammonium Dihydrogen Phosphate crystals have been extensively used as the 2nd, 3rd and 4th harmonic generators for different laser applications which require short pulses of laser. ADP crystals have found many applications in Non-linear optics, electro-optics, and transducer devices. It is also used as Monochromator in X-ray fluorescence investigation. Numerous researchers have studied properties of pure and doped Ammonium dihydrogen phosphate crystals [6-7]. Amino acids with various molar concentrations have been used as an additive to grow ADP crystals [8]. Glycine (NH_2CH_2COOH) is considered to be the simplest amino acid among the 20 protein amino acids. In this research module; we have used amino acid Glycine as an additive in ADP in different

[ϖ] *Assistant Professor,*
[a] *Yeshwantrao Chavan College of Engineering, Nagpur, India.*
[b] *Anjuman College of Engineering & Technology, Nagpur, India.*
**Corresponding author: E-mail: arsalazamirkhan@gmail.com;*

Mathematics-I

VOLUME I

OTHER IMPORTANT BOOKS



S. CHAND PUBLISHING
A division of S Chand And Company Limited
(ISO 9001 Certified Company)
E-mail: info@schandpublishing.com
Customer care (toll free) No.: 1800-1031926

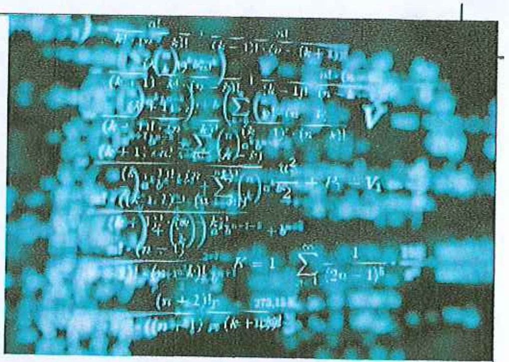
Buy books online @
https://schandpublishing.com

9 789355 012933
0122
₹ 306.00

Mathematics-I
VOLUME I

DASS • VERMA • VERMA
DAGWAL • ANWAR • SHASTRAKAR

S. CHAND
TECHNICAL



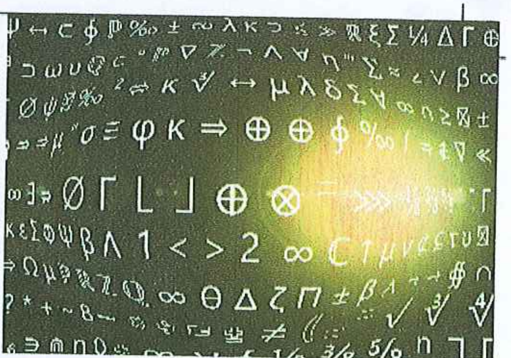
Mathematics-I

For B.E. First Semester Students of
RTM Nagpur University, Nagpur

VOLUME I

S. CHAND

HK DASS
RAMA VERMA
RAJNISH VERMA
VJ DAGWAL
SAJID ANWAR
DAMODHAR F SHASTRAKAR



Mathematics-II

For B.E. Second Semester Students of
RTM Nagpur University, Nagpur

VOLUME II

HK DASS
RAMA VERMA
RAJNISH VERMA
VJ DAGWAL
SAJID ANWAR
DAMODHAR F SHASTRAKAR

S. CHAND

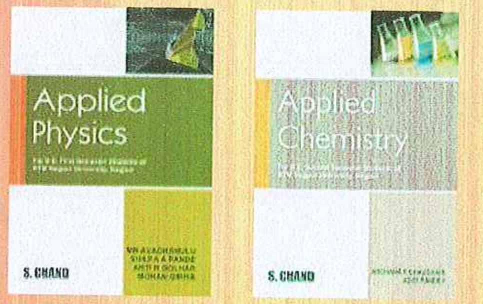
Mathematics-II
VOLUME II

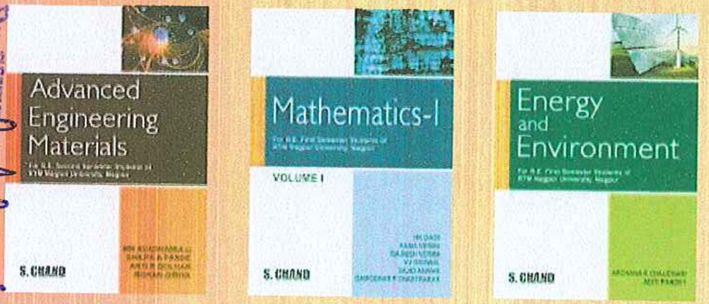
DASS • VERMA • VERMA
DAGWAL • ANWAR • SHASTRAKAR

S. CHAND
TECHNICAL

Mathematics-II
VOLUME II

OTHER IMPORTANT BOOKS





S. CHAND PUBLISHING
A division of S Chand And Company Limited
(ISO 9001 Certified Company)
E-mail: info@schandpublishing.com
Customer care (toll free) No.: 1800-1031926

9 789355 012012
0122
₹ 295.00

A TEXTBOOK ON

INDIAN CULTURE & CONSTITUTION

As Per Syllabus Of RTM Nagpur University
B.E.
★ ★ ★

A Complete Text Book For B.E. Second Semester

Dr. Mrs. Nawaz F. Khan

Alliance & Co.

ABOUT THE AUTHORS

Dr. Nawaz F. Khan is presently working as an Associate Professor in Anjuman College of Engineering & Technology. She is having 26 years of academic experience. She is Ph.D., M.Phil. and Post Graduate in Sociology, Economics and Management. She has authored books on Social Sciences and Humanities. This book is an attempt to help students update their knowledge towards Indian Culture and Constitution

Books Available at :

A|B|C|D

(Wholesale & Retail Centre of All Types of Educational Books From K.G. To P.G.)

ASHWIN BOOKS COLLECTION & DISTRIBUTORS
"PRATHMESH VIHAR", Flat No. 501, Dahipura, Untkhana, Great Nag Rd.,
Near Samrat Ashok Square, Nagpur - 440009 (Maharashtra)
Mob. : 9226267742, 7507658000 Phone No. (0712) - 2749924 Fax. 0712-2749924.

ISBN 9789391322410
9 789391 322410

BHAGEERATHI BAI NARAYANA RAO MAANAY EDUCATIONAL INSTITUTIONS • BANGALORE •

Vidyayāmruthamashnuthe

B. N. M. Institute of Technology

IEEE
Advancing Technology
for Humanity

An Autonomous Institution under VTU.

iciitcee

Certificate

Prof./Mr./Mrs. Iram Nausheen *of* SAGE University

presented a paper entitled Performance Analysis of Efficiently trusted AODV serving Security in MANET under Blackhole Attack Using Genetic Algorithm

in the IEEE International Conference on ***"Intelligent and Innovative Technologies in Computing, Electrical and Electronics"*** *organized by* ***Department of Electronics and Communication Engineering,*** *BNMIT Bengaluru during 27th & 28th January 2023.*

P.A. Vijaya	Krishnamurthy G.N.		T.J. Rama
Dr. P. A. Vijaya	**Dr. Krishnamurthy G. N.**	**Dr. S. Y. Kulkarni**	**Prof. T. J. Ramamurthy**
General Chair, IITCEE	Principal	Additional Director	Director

ACCREDITED WITH GRADE A NAAC

NBA NATIONAL BOARD OF ACCREDITATION

nirf 201-250 Band

ARIIA ATAL RANKING OF INSTITUTIONS ON INNOVATION ACHIEVEMENTS

INSTITUTION'S INNOVATION COUNCIL (Ministry of HRD Initiative) ★★★★

QS I·GAUGE INDIAN COLLEGE RATING DIAMOND

2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) | 978-1-6654-9260-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/IITCEE57236.2023.10091046

Performance Analysis of Efficiently trusted AODV serving Security in MANET under Blackhole Attack Using Genetic Algorithm

Iram Nausheen[1]
Department of Electronics & Communication,SAGE University,Indore,India
iramnausheen@gmail.com

Dr.Akhilesh Upadhyay[2]
Department of Electronics & Communication,SAGE University,Indore,India
akhileshupadhyay@gmail.com

Abstract— The mobile nodes or systems in mobile ad hoc networks wirelessly transmit binary data. The topology of the network is dynamic. Therefore, because of the network's wireless nature, sensitive data is vulnerable to uninvited external attackers, sometimes known as data theft or loss by an attacking or malicious node For the network to operate more efficiently and to preserve safe connectivity, these hostile nodes must be identified. A trust based routing protocol is proposed here with genetic algorithm to identify the attack in MANET using AODV protocol. The performance analysis is made using NS2 simulator with AODV under attack and with proposed trusted algorithm(ETSAODV) using GA under blackhole attack. In terms of network lifetime and characteristics like throughput and packet delivery ratio in simulation, it maximises the network's performance.

Keywords— Mobile Ad-hoc Network (MANET), Security attacks, Routing protocols, AODV,GA

I. INTRODUCTION

The mobile ad hoc network (MANET) technology has a very high level of device-to-device communication dependability. Every MANET node employs an ad hoc connectionless routing system that allows data transmission to other nodes. Data is transmitted to the target, which may be in text or audio format. The server under scrutiny however has a dependable ad hoc wireless connection is necessary for communication. Every node performs two functions: hosts and routers. These wireless hosts are mobile and there is no pre-existing infrastructure. However in MANET's security is weak and could easily hacked. The capacity to dynamically build communication routes distinguishes ad hoc networks from conventional wired networks as a significant advantage. Additionally, while connected, the nodes can roam by the network at will [2]. It has a self-organized topology, meaning that routes between nodes may possibly comprise several hops, and node mobility may result in a change in the routes. Also appropriate for temporary requirements, and it can be tailored to cover certain locations when establishing a confectioned infra of network is impractical. Therefore, it finds fields of application such as disaster management, fly and vehicular communication monitoring forecasts. A straightforward MANET mobility with a destination that is outside the source node's range is shown in Figure 1. Mobility frequently causes routing paths to be interrupted; therefore maintaining constant network connectivity is a difficult task. A packet is sent forth by a group of portable devices operating between two i.e. source and destination nodes. After getting the RREQ, each intermediate node repeatedly examines the minimalist route to the target. In MANETs, the connection between nodes is supported by the paths propagating packets propagated in network are done using the routing protocols AODV, DSR , DSDV . As seen in Figure 1, more nodes assist in forwarding the packet coz of the significant separation distance between the origin and target nodes. The communication model used in many research studies posits that the nodes in between can assist in carrying traffic by exchange of information and control packets based on trust[7]. MANET is highly prone to security threats since lack of mechanism for validating legitimate packets.

Various forms of attacks can easily penetrate into the network shown in figure 2. produces significant network performance degradation. Security assaults in MANET can be classified into two categories: passive attacks and active attacks, depending on a number of factors. Former is as an theft of info and traffic analysis, are used to collect information from a network.

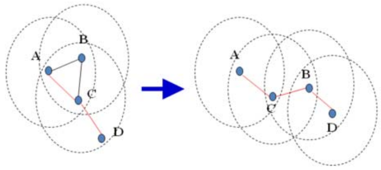


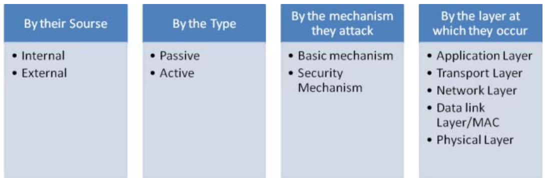
Figure.1. Node Mobility featuring in Mobile Ad-hoc Network.

Indeed, here attackers obtain data transferred in a network without disturbing the network's functionality or altering the data exchanged. Active assaults, on the other hand, involve attackers duplicating, modifying, and deleting shared data. External and internal threats are the two types of above discussed attacks that could be categorized. As opposed to outside assaults, which are carried out by unapproved nodes

978-1-6654-9260-7/23/$31.00 ©2023 IEEE

that participate in the environment, internal attacks are carried out by permitted network nodes. Network layer assaults are an example of a different category of attacks that pertain to protocol stacks. There are multiple security vulnerabilities to MANET depending on the features of different OSI reference models of communication layer. Examples of attacks that contribute significantly to DoS assaults include wormhole, sinkhole, grey, and black hole attacks [6]. The Black Hole attack in MANET is the main subject of this article when routing is carried out using the selected AODV as the base route selection protocol for the analysis. because it performs better than the other protocols in a number of crucial and desired aspects. Because AODV lacks a validated technique to check for real packets, information can be lost if an evil behaviour like a black hole takes place.

Attacking the Black Hole [11], In order to trick the target node into believing it has a genuine minimal path, the attacker node fabricates and disseminates bogus routing information. A fake route is produced when the errant node responds to the requesting node before the genuine node, as demonstrated in the work of Kolade [1].



By their Sourse	By the Type	By the mechanism they attack	By the layer at which they occur
• Internal • External	• Passive • Active	• Basic mechanism • Security Mechanism	• Application Layer • Transport Layer • Network Layer • Data link Layer/MAC • Physical Layer

Figure 2. Wider Classification of Attacks in MANET

Then packets can't reach to the destination. The malicious node broadcasts fake routing updates causing packet drops network performance will be poor. Moreover, when more no. of such nodes cooperate with one another with same malicious characteristics or different then network performance can be worsen. A collaborative Black Hole attack is what this is called. AODV's vulnerability is primarily coz of the lack of a validation method of detection of malicious nodes. For improving the security different studies being done for demand-based routing protocol [16]. The performance of the network hasn't improved much as a result of several of the suggested solutions. Because the schemes ignore the dynamic characteristics of MANETs, this occurs. Previous researchers found it difficult to build a fixed and route-optimization protocol because of these difficulties. Any packets sent through the malicious node are then discarded. This study aims to investigate the response of an effective AODV routing system in a MANET to a black hole impact. Because it satisfies on-demand routing characteristics, the AODV protocol was chosen. It also has the ability to route unicast and multicast traffic. The following is a description of the paper's structure. Basic operation of black hole attack in Section II with an outline of the AODV routing protocol. Section III goes through the security mitigation that has been done in earlier related work. Section IV is Methodology that has been proposed .The simulation is introduced in Section V and the findings and performance analysis are discussed. The job is completed in Section VI.

II. OVERVIEW OF AODV & BLACKHOLE OPERATION

A. AODV Route Request

The AODV protocol based on the reactive distance vector principle in routing because nodes are not required to keep up path to inactive communicating destination , and it enables wireless nodes to react to connection interruptions and the timely changing network topology. Each route entry in AODV use a destination sequence number to ensure freedom from loops. Route discovery and route maintenance are the two key stages of AODV functioning. Once a source node is identified, the path discovery process starts when it communicates with its neighbors by broadcasting a Route Request (RREQ) packet to all of them. This is how a source node initiates the path discovery process. In order to fulfill the RREQ, each neighbor either sends a route reply packet (RREP) back to the source or resends the RREQ to its own neighbors after adding a hop. Specific RREP is issued to the affected source nodes when mobility is observe in source and intermediate nodes. The necessary node chooses the route based on the packet carrying the highest sequence number in order to maintain a fresh path. Hello messages sent on a regular basis can be used to maintain symmetric links and identify link faults. [3].

B. Black Hole Attack

As it is carried out by a single node or a group of nodes in the MANET, this attack has the potential to seriously deteriorate[14]. On sender request, a black hole node running the AODV protocol seems to have the highest sequence number across all routes to destinations. The black node sends back an RREP with the largest sequence number that appears to be from an actual target or from a node with a sufficiently new path to the destination in response to the source node broadcasting an RREQ packet. Other inbound RREP packets are discarded by the source because it thinks the destination is hidden behind a malicious node. Once the source receives the RREP packet, it sends data packets to the black hole node in the hope that they will reach their destination. The data packet is eventually discarded and not passed along to the intended location seen in Figure 3. Let node 6 be the destination and source 1 be a source which send REEQ messages. Adjacent nodes 2, 5, and 4 are able to receive RREQ broadcasts from node 1. Although there is no viable route. When Node M receives the request packet,RREP is sent to destination 6. Let's say the malicious node M's RREP message arrives first. The initiator node discards RREP messages from other neighbors, including those from the real destination node, and changes the routing state information table for new routes to a specific target node.

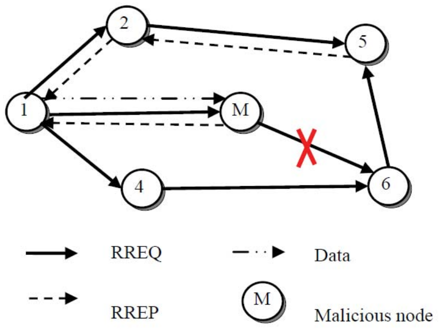


Figure 3. Blackhole Attack in AODV

In anticipation of the data reaching the targeted destination node, the source transmitting packets to malicious node as soon as it records the route. However, the errant node removes all packets of data in place of passing them on to the following next hop (as part of a black hole attack).

III. RELATED WORK

[13]The SAODV routing protocol is comparatively safe over default AODV, according to experimental investigation. It primarily addresses the issue of whether AODV is at risk of black hole attacks as SAODV. The primary operating principle of SAODV is split into a route detection and maintenance phase, and is quite known to that of AODV. The procedure for route finding is where they diverge the most. By exchanging random integers, SAODV speeds up the routing of directly verifying the target node. The process of checking the target node increases directly by exchanging random numbers in SAODV. [14] For overcoming security flaws related to this protocol as well as the actual AODV protocol, a more dependable MANET routing protocol termed BP-AODV has been developed. Additionally, BPAODV can defend against coordinated black hole assaults started during routing as well as potential black hole attacks during forwarding. By utilizing chaotic map capabilities and expanding AODV protocol capabilities, BP-AODV was created. The BP-AODV protocol, which can effectively thwart these attacks launched by hostile malicious nodes throughout the process, is demonstrated by experimental results to be more better than the SAODV protocol. The outcomes also demonstrate that BP-AODV can offer effective defense against black hole assaults that take place throughout the transfer procedure. Additionally, it makes use of chaotic maps to guard against coordinated black hole assaults launched by two hostile nodes. [15] An evolutionary self-coordinated trust scheme (ESCT) that uses trust-level data to secure against a variations of routing disruption threats and imitates the way people think. In this strategy, mobile nodes communicate trust details and use their own cognitive judgment to examine the received trust information. In order to eliminate malignant entities, each node's perception evolves dynamically. The most alluring aspect of ESCT is that even an internal attacker who understands how the security mechanism functions cannot put the system at risk. In several routing interruption attack scenarios, the effectiveness of ESCT methods is assessed in this white paper. The ESCT technique pushups the adaptability and assures effective routing in the presence of disruption caused by attackers within MANET.

IV. PROPOSED WORK

To lessen the effects of black hole assaults, the suggested effort relies on trust-based computing using genetic algorithm. Source node send CBR (constant bit rate) data packets forwarded, then source node maintains a packet list and when again forwarded via intermediate node towards destination then trust value is incremented and removes intermediate CBR from packet list. If source node does not observe intermediate node to transfer CBR till threshold then it treats it to be malicious node by setting trust value to zero. This is accomplished with the use of a genetic algorithm, a form of soft computing that makes use of the principles of evolution and selection. The fitness of the node as determined by GA affects packet routing. The fitness function uses node distance to calculate fitness value. The protocol begins with the deployment of nodes, following which the network's nodes' hop counts are all initialised. After identifying the event, the node collects data from nearby nodes within the transmission radius. A packet is routed to the fittest node using Genetic Algorithm, which is chosen from the group of nodes based on distance. Fitness value shown in equation (1) and the distance among two nodes is calculated with distance equation (2).

$$Fitness = dist(i,j)+dist(j,bs) \quad \ldots\ldots\ldots\ldots\ldots(1)$$

$$dist(i,j)=\sqrt{}(x1-x)2+(y1-y)^{2} \quad \ldots\ldots\ldots\ldots.(2)$$

where bs is the base station and i, j are parent nodes.

The route request, route answer, and data packet are utilized to determine the trust information. Get the confidence values and stop communicating that node if network permits it and the trust value is trusted. This way minimizes errors at the link or node level while maximizing network end-to-end connectivity. Using an energy-efficient neighbor node selection technique, a number of different pathways are built from the source to destinations. It creates a suitable path that satisfies the delay requirement and provides effective load balancing at the node between the source and destination. Simulation findings show that the proposed protocol performs better than the state-of-the-art ones in terms of throughput, routing overhead, packet delivery ratio, and average end-to-end time. Signal intensity, queue length, drain rate, and delay metrics are now included in a variety of ways in AODV's route finding process. The protocol finds a trustworthy route between source and target based on the received signal strength by balancing at each node (queue length and drain rate) before figuring out the route between source and destination. The source node can maintain connectivity by establishing a number of links between it and the destination multipath routing Data transmission errors and delays brought on by route disconnections can be minimized by using multipath routing protocol. In the steps below the communication started initially by updating the neighbour table by sending RREQ then Source and Target is detected then nodes start to receive response RREP then Response incremented and trust value check is obtained with GA classification attacker is detected and data is received by the node by making a viable rescue path avoiding attacker node in the communication from source to destination. Process flow of proposed protocol is as follows:

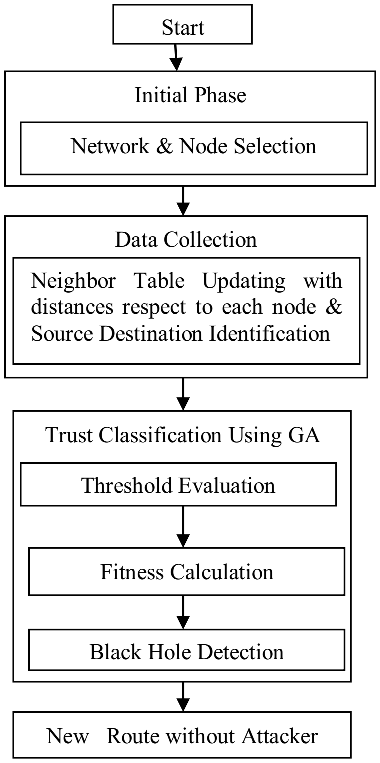

Start
Initial Phase
Network & Node Selection
Data Collection
Neighbor Table Updating with distances respect to each node & Source Destination Identification
Trust Classification Using GA
Threshold Evaluation
Fitness Calculation
Black Hole Detection
New Route without Attacker

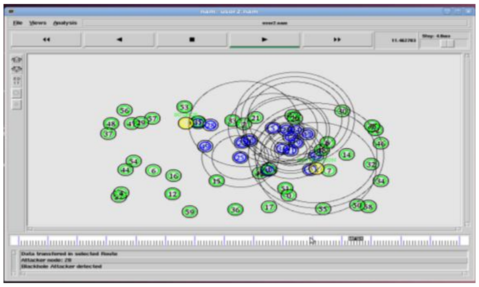
Figure 4. Flowchart

V. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

Based on the parameters listed in Table 1, the simulation experiment is run in the network simulator NS2. Figure 3 shows the basic operation of a black hole node, while Figure 4 shows the sequence of steps taken in the proposed one. In general, this attack shows a difference in drop of packets when there is a false updates. The trust levels are calculated and the best path is chosen here. In this experiment, a known number of malicious nodes are added, and data is gathered at the specific rogue node. As a result, Table 2 displays a comparative result to highlight the effectiveness of MANET in the face of malicious node attack. Between the source and target in Figure 5 the secured path marked in blue color and source and destination is marked in yellow color is shown, then attacker detection is made and seen in Figure 6 . where that node turned red which was earlier under secured path. Hence with ETSAODV that node becomes idle for any further communication as the fitness value is not supported. So other nodes are used via another path marked under blue color as shown below and hence the freshness of data can be maintained using multipath routing.

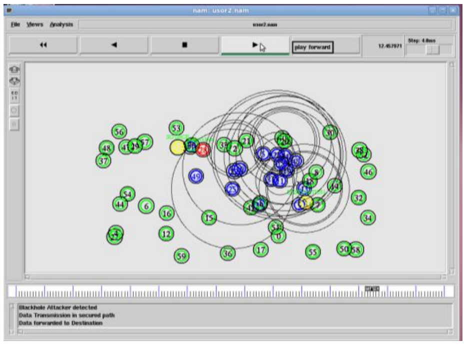
Table 1: Simulation Parameters

Parameters	Value
Topology size	1000 x 700 m
Routing Protocol	AODV
Channel Type	Wireless channel
Simulation time	15s
Number of nodes	0 to 59
Radio propagation model	Two ray model
Transport type	IEEE 802.11
Antenna model	Omni Antenna
Traffic model	CBR
WLAN standard	IEEE 802.11b
Data rate	11,2 & 1 Mbps
Interface Queue type	Drop Tail/ Pri Queue
Initial Energy for nodes	10J



Data transferred in selected Route
Attacker node: 28
Blackhole Attacker detected

Figure 5. Route Selection between Source and Destination



Blackhole Attacker detected
Data Transmission in secured path
Data forwarded to Destination

Figure 6. Blackhole Attacker detected

Table 2. Performance parameters under blackhole scenario

Performance parameters	**AODV under multipath environment**	**Proposed Efficient and Trusted AODV**
Generated Data	4348	4348
Received Data	3529	3629
Data Delivery Ratio	73.0474	81.1264
Average Delay	0.0638091	0.0425394
Throughput Ratio	56.8146	73.0474
Network Lifetime Ratio	48.6871	64.9161
Packet Loss Ratio	24.3435	16.229

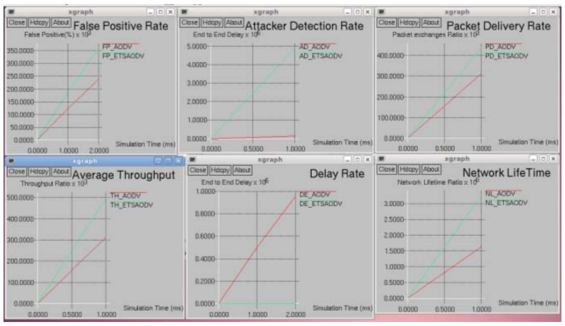


Figure7. Comparison Results

VI. CONCLUSION AND FUTURE WORK

Based on different characteristics like throughput, network lifetime, and packet delivery ratio, AODV's performance under a black hole attack is analysed, and a proposed study with a trust categorization technique utilising GA is presented. An improvement is observed with the simulation results where the attacker's made the data packets lost by node that travel across the path during a black hole strike, resulting in poor network performance with lower packet delivery rates. Additionally, the throughput drastically decreases when a malicious node is found in the network. Because the majority of packets sent do not reach their intended location in normal AODV. Attacks from black holes have little impact on packet ratio as we kept the no. of blackhole limited. A comparison of the performance of ETSAODV and other on-demand routing protocols in attack scenarios will be made in future study, along with a model and analysis of how black hole attacks and other network layer attacks (gray hole and wormhole attacks) effect networks.

REFERENCES

[1] A.T. Kolade, M.F. Zuhairi, H. Dao, and S. Khan, "Bait Request Algorithm to Mitigate Black Hole Attacks in Mobile Ad Hoc Networks," in Journal of Computer Science and Network Security, vol. 16, No. 5, 2016.

[2] K. S. Patel and J. Shah, "Study the Effect of Packet Drop Attack in AODV Routing and MANET and Detection of Such Node in MANET," in Proceedings of International Conference on ICT for Sustainable Development, 2016.

[3] R. Datta and N. Marchang, Security for mobile ad hoc networks. Elsevier Inc., 2012.

[4] A. Yasin and M. Abu Zant, “Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique,” Wirel. Commun.Mob. Comput., vol. 2018, 2018.

[5] Z. A. Zardari et al., “A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs,” Futur. Internet, vol. 11, no. 3, 2019.

[6] A. Nadeem and M. P. Howarth, “A survey of manet intrusion detection & prevention approaches for network layer attacks,” IEEE Commun. Surv. Tutorials, vol. 15, no. 4, pp. 2027–2045, 2013.

[7] C. Perkins, E. Belding-Royer and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” Network Working Group, The Internet Society, RF3561, 2003. E. Perkins, E. M. Belding-Royer, and S. R. Das, ―Ad Hoc On Demand Distance Vector Routing‖: IETF RFC 3561, July 2003.

[8] 8. Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, “Performance analysis of ad-hoc networks under black hole attacks”.Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.

[9] Govind Sharma, Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE).

[10] V. M. Agrawal and H. Chauhan, "An Overview of security issues in Mobile Ad hoc Networks," International Journal of Computer Engineering and Sciences Vol. 1, 2015.

[11] P. Chahal, et al., "Comparative Analysis of Various Attacks on MANET," International Journal of Computer Applications, vol. 111, 2015.

[12] S. Kumar and M. Soni, "Cooperative Intrusion Detection Technique against Blackhole and DoS Attacks in MANET," International Journal of Engineering & Technology, vol. 7, 2015.

[13] Songbai Lu, Longxuan Li,” SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack”, 2009 International Conference on Computational Intelligence and Security

[14] Aly M. El-Semary, Hossam Diab ,“BP-AODV: Blackhole Protected AODVRouting Protocol for MANETs based on Chaotic Map” DOI 10.1109/ACCESS.2019.2928804, IEEE Access 2019.

[15] RuoJun Cai,Xue Jun Li,andPeter Han Joo Chong “An Evolutionary Self-Cooperative Trust Scheme against Routing Disruptions in MANETs”, DOI 10.1109/TMC.2018.2828814, IEEE Transactions on Mobile Computing 2018.

[16] Dhama, S., Sharma, S. and Saini, M., 2016, March. “Black hole attack detection and prevention mechanism for mobile ad-hoc networks”. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 2993-2996). IEEE.

2023 IEEE Sponsored Third International Conference on

Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT 2023)

Third Edition

05 - 06, January 2023 | Bhilai, Chhattisgarh, India | www.icaect.com

Sponsored by

IEEE
Advancing Technology for Humanity

23CHEC 2007
Peer Reviewed

CERTIFICATE

This certificate is presented to

Iram Nausheen

Department of Electronics & Communication,
SAGE University,
Indore, India

for presenting the research paper entitled "ETSAODV: An Efficient and Trusted Secure AODV with Performance Analysis for MANETS suffering Blackhole Attack" in the 2023 IEEE Sponsored Third International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT 2023) held at the Department of Electrical and Electronics Engineering, Shri Shankaracharya Technical Campus (SSTC), Bhilai, Chhattisgarh, India during 05 - 06, January 2023.

Dr. Shimpy Ralhan
Conference Chair

Dr. P. B. Deshmukh
General Chair

Ms. Jaya Mishra
President, SGES

Promotional Partner
DILIGENTEC SOLUTIONS

Organized by

ज्ञानदेव तु कैवल्यम्

Electrical and Electronics Engineering
Shri Shankaracharya Technical Campus (SSTC)
Bhilai, Chhattisgarh, INDIA

An Efficient & Secure Approach under Multiple Attack Prone MANET

Iram Nausheen[1]
Department of Electronics & Communication,SAGE University,Indore,India
iramnausheen@gmail.com

Akhilesh Upadhyay[2]
Department of Electronics & Communication,SAGE University,Indore,India
akhileshupadhyay@gmail.com

2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) | 978-1-6654-7467-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSSIT55814.2023.10061008

***Abstract*— Security or secure communication is the most difficult problem in MANETs because of its many shortcomings. The lack of authorization functionality, the lack of infrastructure in the network environment, and dynamically random node movement are a few of the flaws or distinctive characteristics that make MANETs susceptible to various attacks. Due to energy limitations brought on by nodes' mobility, the network uses power inefficiently and experiences battery issues. This leads to a requirement for improved security effectiveness. Multiple attacks have a more severe effect on MANETs than a single targeted attack. There have been numerous types of secure algorithms and protocols developed as a result of the rising demand for MANET usage, but there are still no fully secure protocols that make communication easy. This study now presents an approach to detect multiple attacks blackhole, grayhole and wormhole attacks on MANETs.**

Keywords*— *Mobile Ad-hoc Network (MANET), Security attacks, Routing protocols, AODV (Ad-hoc On-demand Distance Vector)

I. INTRODUCTION

Ad-hoc networks are composed of a group of independent nodes that are able to join or leave the network at any time. These nodes are self-managed and have a dynamic topology. They are set up in a decentralized fashion, which means they are independent of any established infrastructure, capable of modelling communication networks, and have no central authority. Packets routed from one node to another imply that all nodes in the network must have mutual trust since each node in the network participates in traffic routing or acts as a routing mediator. Mobile ad hoc networks' moderate bandwidth and limited battery capacity are two features that make routing more difficult. Numerous attack kinds target the network, hence the need for security protocols is essential. In order to combat some of the threats, numerous security measures had previously been devised. However, collaborative attacks are launched by a specific quality and two or more attacks coordinate and deployed concurrently in the network. The nodes facilitate this connectivity with the aid of several routing protocols created by acclaimed MANET working group, such as AODV(Ad-hoc On-demand Distance Vector), DSR, DSDV, etc. because they have the capacity to route the data packets directly. Despite this, none of these security methods addresses security vulnerabilities in a satisfactory manner. Routing protocols are affected by two main sources of attacks. One originates from nodes outside the network, and the other from infected or compromised nodes that therein. While an attacker can send out outdated information, change routing information, and put too much strain on the system to prevent the protocol from working properly. Routing protocols are necessary for selecting routes in network nodes or transmitting routing information between them. In a similar vein, MANETs routing protocols are also created to provide security characteristics for non-antagonistic networks. This adheres to the conventional methodology whereby a protocol is designed first, then security considerations are added subsequently. As the use of MANETs becomes more and more popular each day, a method has been developed for making the AODV more secure to use under collaborative attack. There various strategies for dealing with attacks. For instance, while Blackhole and Grayhole attacks can coexist, Wormhole attacks cannot coexist with DoS because DoS attacks require lower bandwidth whereas Wormhole attacks require rapid connections. This paper's remaining section is thoughtfully structured as: A brief summary of earlier works is provided in part II. The proposed method is put into practice in III. Graphical result analysis and the simulation environment are covered in IV. The portion V represent conclusion and future scope of the work.

II. RELATED WORK

Attack from a wormhole [1] In ad hoc networks, a compromised node collaborates with an external attacker to create a network bypass. They could fool the source node into winning the route discovery process by constructing this shortcut, and then they could start the interception attacks. In order to find the quickest way between the source and the destination node, packets from these two conspiring attackers are often transported using wired connections.[3] The wormhole nodes may also permanently prevent the establishment of alternative routes if they continually maintain the fake routes. Therefore, participation in network operations is restricted for the intermediary nodes situated along the forbidden paths. Attacks involving black holes: In these attacks, the malicious nodes work together with all the nodes in their immediate vicinity to attract all the routing packets to them [4]. Malevolent nodes could carry out black hole attacks by convincing neighboring nodes that they are the best route to the target locations, similar to wormhole assaults [5]. But in contrast to wormhole attacks, which involved numerous attackers working together to target a single nearby node, black hole assaults only involve one attacker, who poses a threat to every node in the vicinity. [6]

In contrast to a black hole attack, a gray hole attack makes use of a malicious node that, while initially benign, has the potential to turn malevolent in the future[7]. A trust-based security solution cannot identify harmful nodes before they become malicious nodes due to their abnormal behaviour. The packets arriving from or intended for a particular node may be dropped by a grey hole, which may otherwise forward all packets to that node[8]. Another variant of this attack involves a node that initially acts maliciously before returning to regular behaviour[9]. A node may occasionally combine the characteristics of the aforementioned assaults. In comparison to black hole attacks, grey hole attacks are more challenging to identify and prevent because of the grey hole's unpredictable behaviour. Cooperative grey hole attacks against AODV might be feasible, just like with black holes.[10].

El-Semary & Diab[11]: A proposed routing protocol called BPAODV (Black-hole Protected AODV) provides defence against both cooperative and black hole assaults. Better than Secure AODV and AODV in attack-free and black hole attack network scenarios. Cai et al. [12]: To defend against internal attacks like black hole and grey hole attacks, the proposed Evolutionary Self-Cooperative Trust (ESCT) strategy with DSR comprises self- and cooperative detection schemes. Yasin & AbuZant[13]: The suggested Timer-based bait strategy with AODV offers isolation and detection of both solitary and group black-hole attacks. Hazra & Setua[14]: Here trust is context sensitive in AODV (CST-AODV) to defend the network against black hole attacks by different levels of trust computations. Nadeem & Howarth [15]: provides a thorough analysis of different attack types and the defense mechanisms needed for attack detection and mitigation. Bhalsagar et. al. [16]: The impact of several malicious attacks, on some established protocols, such as the AODV, DSDV, and DSR protocols is covered in this study. Additionally, it illustrates how a trust-based system can be used to counteract the negative impacts of rogue nodes in a network. Because there is no fixed, centralised infrastructure, the network topology is dynamic, there is little physical protection for nodes, there is no certification authority, and the nature of the transmission medium is open, security in mobile ad hoc networks (MANETs) is difficult to achieve and only gets harder. The majority of the routing protocols in use today trust all mobile nodes without taking security into account. Security issues include routing and data forwarding, medium access, key management, and intrusion detection systems (IDSs). Recent studies have concentrated on security-related issues and suggested security measures for protocols and applications. From the above literature we would try to overcome the identified Research gaps that there is no single algorithm is available for security mechanism which can protect MANETS from more than two attacks at a time. Another gap found was that Single Blackhole, Multiple Blackhole and Cooperative Blackholes attacks, Grayhole attacks and advanced versions of these attacks need to opt enhanced way of routing and optimization which is not available in earlier works.

III. PROPOSED WORK

Each node monitors its neighbour during the first phase of initialization to determine if it send the packet to the following node or not. If a node exhibits any questionable activity, the trust mechanism is employed to determine whether or not the node is malevolent. The proposed protocol allows load balancing based on queue length and drain rate during the second stage, which helps to ease node congestion. The protocol also uses the received signal strength measure to identify the stable path, reducing the frequency of connection failures brought on by a dynamic network architecture. In terms of the latency metric, it guarantees quality of service (QoS). Once the fitness function and the trust classification representation have been established, a GA starts by initializing a population of solutions and then improves it by repeatedly using the mutation, crossover, inversion, and selection operations. There are three stages in the algorithm flow: discovery, stable, and execution. The detailed step in process of developing the efficient and secure way in MANET is shown in pseudo code in below Table1 and 2.

Table 1. State of Route discovery, steady

```
Pseudo Code 1:
Initialization:
M: MANET with mobile nodes
S: source point belongs to M
R: receiver point belongs to M
I: intermediate nodes belongs to M
Sid: source Id
Rid: receiver Id
Iid: intermediate Id
rp: AODV route packet
bh: normal, abnormal
ti: trust is 1
tth: trust threshold value (0.6)
tj: trust value
En: energy of node
Eth: energy threshold
Pi: problematic nodes, abnormal (BH,GH,WH)
Output: tj, En, route
Route discovery(S, R, route)
S produce route (rp, sequence no, Sid, Rid)
S broadcast above packet to search R node
if I in range and Iid = Rid and En ≥ Eth then
Assign ti to Intermediate node
send rp to next position hop
else if Iid == Rid and En ≥ Eth , route ≥ 1 then
Select shortest route
Send acknowledgement to S
Call Steady state ();
end if
Steady state(Intermediateid, route Pi)
Examine nodes 0 to 8 seconds
```

```
Activate route $P_i$
while live path discovered do
    All routes watch activity of neighbor
    Path trust calculation
    $t_j = t_i + (forward/ receive)$
    if $t_j < t_{th}$ then
        Send info to $b_h$ module
        Comparing header with $b_h$(normal, abnormal)
        if header is abnormal then
            Calculate average $t_j$ over all $P_i$
            $t_j = t_{jn1} + t_{jn2} .... t_{jnm}$/number of $P_i$ nodes
            if $t_j < t_{th}$ then
                Send block message to I node
                Call local route repair module
                Re-establish path
            else
                I is normal behavior
                Call execution state ()
            end if
            I is normal behavior
            Call execution state ()
        end if
        Update trust $t_j$
        I is normal behavior
        Call execution state ()
    end if
end while
```

The logic path is found as shown in pseudocode that the AODV packet is forwarded till the check on the intermediate node is made by updating the neighbor table. And if it is not same as that of destination id then it is assigned the trust value 1 to that intermediate node and take next hop for packet and if the condition of id is equal then shortest route is selected, and source node is acknowledged that now the transmission between source and node can be made. Then the steady state is reached where active route with the trusted nodes between the source and destination is identified. If any abnormal activity under the attacker effect is observed, then block that intermediate node from the trusted route and a route repair and new updated route is established. From the flowchart in figure1 there is an initialization phase where the neighbor table is updated after sending the beacon messages, here the calculated distance with each neighbor node is jotted then the observation of the nodes is carried to see the trust values using genetic classification for calculating the fitness function the threshold value for making decisions and the acknowledgements (ACKs) from data link and TCP layer are taken into consideration to revive these values from the stage of queue scheduling phase as can be seen in the diagram.

TABLE 2. EXECUTION STATE

```
PseudoCode 2 :

Initialization:
$E_n$: Node Energy
$E_{nold}$ : previous interval Energy
$E_{nnew}$: current Energy
$E_{th}$: threshold energy (10 joules)
$t_j$ : current trust
$t_{jold}$ : previous trust
Output: Info sent, received, Energy consumed,
    AvgDelay, NetworkLifetimeRatio.
Execution state ($S_{id}$, $R_{id}$, $I_{id}$, $P_i$)
Examine trusted route node.
$P_i$ active mode
Calculate $t_j$, $E_n$ in every packet base
if $E_n \geq E_{th}$ and $t_j \geq t_{th}$ then
    Send info by found route
    $P_i$ watch I node
    $E_{nnew} = E_{nold} - E_n$ per packet
    $t_j = t_{jold}$ (plus/minus)(forward/receive)
    if $P_i$ finds $t_j < t_{th}$ then
        Steady state ();
    else if $P_i$ finds $t_j > t_{th}$ and $E_{nnew} < E_{th}$ then
        Selected route repair ();
    else
        Trust path found Source to Destination
    end if
    Execute newpath for alternate route
end if
```

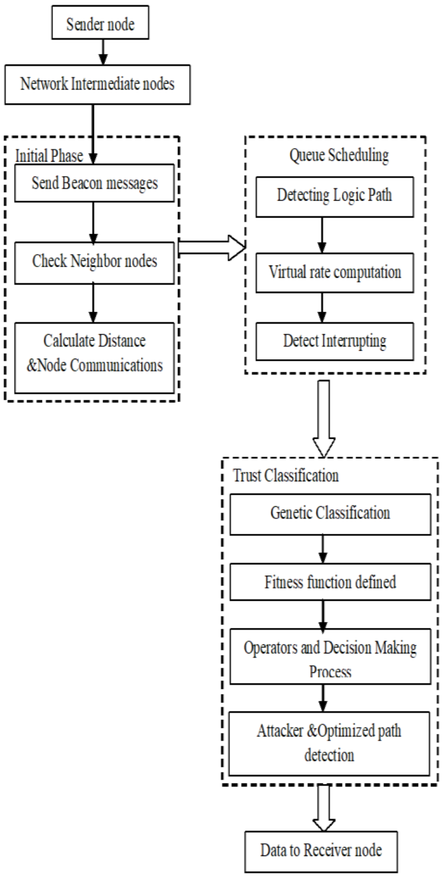
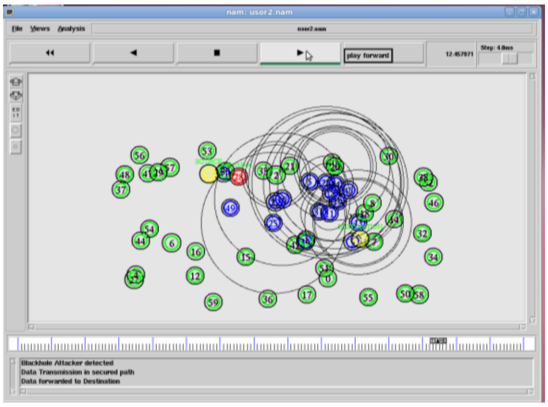


Figure 1. Flowchart

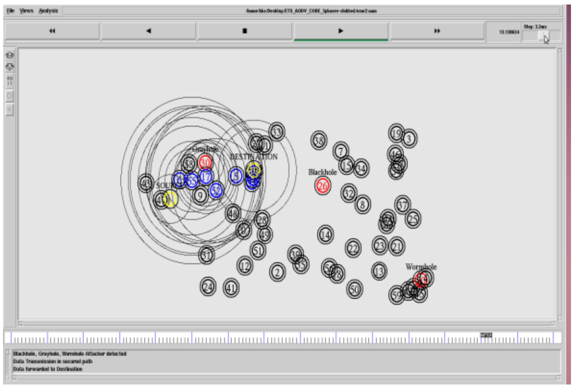
IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

Observant parameters listed in Table 3, the simulation experiment is run in the network simulator NS2. Figure 2 shows the basic operation under a black hole node, while Figure 1 shows the sequence of steps taken in the proposed one and explained in section III. In general, this attack shows a difference in drop of packets when there is a false update. The trust levels are calculated, and the best path is chosen here. In this experiment, three scenarios are considered where MANET under single blackhole as shown in figure 2. It is observed that the attacker node is when discovered is marked in red and no participating via a trusted path marked in blue color. Then under three attacks BH, GH, WH single nodes only are shown in figure 3 in MANET in the second scenario where the attacker nodes are marked in red and are not made to participate in the communication between source and destination. In third Scenario the double Attackers are observed that is two BH, two GH and two WH attackers in MANET and performance is calculated. As a result, Table 4 displays a comparative result with the existing AODV and the proposed work under three scenarios to highlight the effectiveness of work in MANET in the face of malicious node attack. Between the source and target in the secured path marked in blue color which are the trusted nodes and source, and destination is marked in yellow color, attackers are shown in red color is shown. Performance comparisons of these were made with the existing AODV protocol in Table 4. Where it is observed that the data delivery ratio is improved with the proposed work by 14% and average delay is reduced further, and throughput is improved from 56 to 77. Packet losses are reduced from 24 to 17 all are noted in Table 4 below.



Blackhole Attacker detected
Data Transmission in secured path
Data forwarded to Destination

Figure 2. Scenario1: Single Blackhole Attacker detected

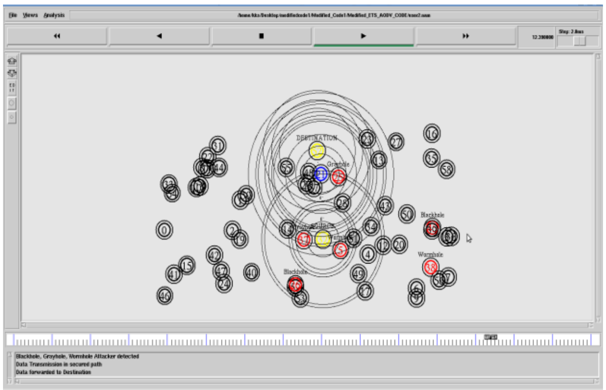


Blackhole, Grayhole, Wormhole Attacker detected
Data Transmission in secured path
Data forwarded to Destination

Figure 3. Scenario 2: Route Selection between Source and Destination and Single BH,GH,WH Attacker detected

TABLE 3: SIMULATION VALUES& PARAMETERS

Parameters	Value
Channel Type	Wireless channel
Routing Protocol	AODV
Topology size	1000 x 700 m
Simulation time	15s
Number of nodes	0 to 59
Radio propagation model	Two ray model
Transport type	IEEE 802.11
Antenna model	Omni Antenna
Traffic model	CBR
WLAN standard	IEEE 802.11b
Data rate	11,2 & 1 Mbps
Interface Queue type	Drop Tail/ Pri Queue
Initial Energy for nodes	10J



Blackhole, Grayhole, Wormhole Attacker detected
Data Transmission in secured path
Data forwarded to Destination

Figure 4. Scenario 3: Route Selection between Source and Destination and Double BH,GH,WH Attacker detected

TABLE 4. PERFORMANCE PARAMETERS UNDER DIFFERENT SCENARIO

Performance parameters	Existing AODV Under multipath environment	Proposed Efficient and Trusted AODV under single BH	Proposed Efficient and Trusted AODV under single BH,GH,WH	Proposed Efficient and Trusted AODV under Double BH,GH,WH
Generated Data	4348	4362	4395	4340
Received Data	3529	3873	3871	3818
Data Delivery Ratio	73.0474	86.4574	85.763	85.6287
Average Delay	0.0638091	0.00777535	0.0339366	0.0128044
Throughput Ratio	56.8146	77.8473	77.2218	77.1014
Network Lifetime Ratio	48.6871	69.1818	68.626	68.5188
Packet Loss Ratio	24.3435	17.2954	17.1565	17.1297

V. CONCLUSION AND FUTURE WORK

The performance of AODV and proposed efficient and trusted AODV under black hole, grey hole, and wormhole attacks is examined based on several factors like packet sent and received, throughput, network lifetime, and packet delivery ratio. In a proposed study a trust categorization technique is presented. An improvement is observed with the simulation results when there is no prevention scheme and when scheme under the multiple attackers made. Furthermore, when a rogue node is discovered in the network, throughput is severely reduced with no prevention scheme. Due to the fact that most sent packets in AODV do not arrive at their intended location. Attacks from black holes, grayhole and wormhole have little impact on packet ratio as we kept the no. of BH, GH, and WH limited. A comparison of the performance of proposed work and other on-demand routing protocols in attack scenarios may be made in future study and accuracy can be improved by applying Artificial intelligence schemes.

REFERENCES

[1]. Johnny Wong, Xia Wang ,An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks, Computer Software and Applications Conference, Annual International ,:July 2007

[2]. Abdel-Azim, M., Salah, H.E.D. and Eissa, M.E., 2018. "IDS Against Black-Hole Attack for MANET". IJ Network Security, 20(3), pp.585-592.

[3]. N. Marchang, R. Datta, and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684–1695, Feb 2017.

[4]. Songbai Lu,Lingyan Jia,Kwok-Yan Lam,Longxuan Li, SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack, International Conference on Computational Intelligence and Security, 2009.

[5]. Iram Nausheen,Dr.Akhilesh Upadhyay" A Survey on MANETs: Entrusted Security Challenges," in International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 48 – 58.

[6]. Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedroil : Black Hole Attack Injection in Ad hoc Networks www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf.

[7] Aldaej, A. and Ahamad, T., 2016. "AAODV (aggrandized ad hoc on demand vector): a detection and prevention technique for MANETs". International Journal of Advanced Computer Science and Applications (IJACSA), 7(10), p.2016.

[8]. Ozcelik, M.M., Irmak, E. and Ozdemir, S., 2017, May. "A hybrid trust based intrusion detection system for wireless sensor networks". In 2017 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.

[9]. Vishnu K Amos J Paul , Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks International Journal of Advanced Engineering Technology E-ISSN .0976-3945 IJAET/Vol.III/ Issue I/January-March, 2012/383-388.

[10] Sukla Banerjee : Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks, International Journal of Computer Applications, Number 22 -Article 8,2010

[11]. El-Semary, A. M., Diab, H.: BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map. IEEE Access 7, 95197 – 95211 (2019).

[12]. Cai, R. J., Li, X. J., Chong, P. H. J.: An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs. IEEE Transactions on Mobile Computing 18(1), 42 – 55 (2019).

[13]. Yasin, A., AbuZant, M.: Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 1-10 (2018).

[14]. Hazra, S., Setua, S. K.: BlackHole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network. Advanced Computing, Networking and Informatics 2, 59-66 (2014)

[15]. Nadeem, A., Howarth, M. P.: A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. IEEE Communications Surveys & Tutorials 15(4), 2027 – 2045 (2013).

[16]. Bhalsagar S. S., Chawhan, M. D., Suryawanshi, Y., Taksande, V. K.: Performance Evaluation Of Routing Protocol Under Black hole Attack In Manet And Suggested Security Enhancement Mechanisms. International Journal of Innovative Technology and Exploring Engineering 8(5), 1–7 (2019).

Wesleyan Journal of Research

An International Research Journal

ISSN : 0975 - 1386

CERTIFICATE OF PUBLICATION

This is to certify that

Iram Nausheen

Electronics and Communication , SAGE UNIVERSITY, Indore, M.P, India,

for the paper entitled

A REVIEW ON ROUTING PROTOCOL ISSUES IN MANETS

Volume No. 14 No. 2(I) : **2021**

in

Wesleyan Journal of Research

ISSN : 0975 – 1386

UGC Care Approved, Peer Reviewed and Referred Journal

Editor in Chief
Dr Fatik Baran Mandal

A REVIEW ON ROUTING PROTOCOL ISSUES IN MANETS

Iram Nausheen Electronics and Communication , SAGE UNIVERSITY, Indore, M.P, India,
Dr.Akhilesh Upadhyay Electronics and Communication , SAGE UNIVERSITY, Indore, M.P,
akhileshupadhyay@gmail.com ;; iramnausheen@gmail.com

ABSTRACT

MANET stands for Mobile Ad-hoc Network known for its wireless and infrastructure-less network through which devices can communicate with one another with the assistance of nodes with none centralized infra. In this, all the nodes are liberal to move and may easily enter or leave the network which cause change in structure of network. To accommodate the changing topology special routing algorithms are needed to form communication successful. There's no single protocol that matches all networks perfectly. The protocols need to be chosen consistent with network characteristics, such because the mobility of the nodes, density and size. In MANET, the nodes also function as routers that discover and maintain routes to other nodes within the network. Establishing an optimal and efficient route between the communicating nodes is the first concern of the routing protocols of MANET. Any attack in routing phase may disrupt the general communication and the whole network can be stuck. Therefore security in network layer plays a crucial role to take care of security of the entire network. Routing Protocols are the set of rules which governs the way of message packet from source to destination which facilitate communication in mobile ad-hoc network. It's used for efficiency in performance between nodes effortlessly. The routing protocols in MANET are accomplished to handle a number of nodes with restricted resources. The choice of routing protocol exist in MANET which is chosen by taking count on the performance of network. This paper we've done a comparison analysis of varied Routing protocol issues with reference to Routing Approaches, Routing structure, Route selection, Routing table, Route maintenance, Operation of protocols, Strength, Weakness and security issues in them.

KEYWORDS Mobile Ad-hoc Network(MANET), Security attacks, Routing protocols.

1 Introduction

In the absence of centralized administration, MANET eliminates the utilization of a tough and fast framework for communication by creating multi hop wireless communication network with the help of intermediary mobile nodes between the source and destination [1]. The benefits of the MANET during the war, medical emergency, natural disasters, space exploration and crisis response attract researcher attention towards enhancement of secure and efficient communication protocols for MANET [2,3]. The subsequent essential characteristics of MANET are:

1. Dynamic topology
2. Bandwidth and wireless link capacity
3. Limited security
4. Multi-hop communications
5. Energy constrained nodes

Because of these characteristics of MANET, various challenging issues arise in practical applications and implementation.

Fig.1. Mobile Ad-hoc Network

The following list of challenges shows the inefficiencies and limitations that need to be dealt during a MANET environment [4]:

1) Limited wireless transmission range: In wireless networks the radio band are going to be limited and therefore the data rates it offers are much lesser than what a wired network. This needs the routing protocols in wireless networks to use the bandwidth during a finest way by keeping the overhead as low as possible. Especially in MANET's due to frequent changes in topology, maintaining the topological information at every node involves more control over head, which in turn results in more bandwidth wastage [5].

2) Broadcast nature of the wireless medium: Such a nature of the radio channel is that in which transmissions made by a node are received by all nodes within its direct transmission range. When a node is receiving data, no other node in its neighborhood, except sender, should transmit. A node should get access to the shared medium only .Its transmissions don't affect any ongoing session. Even the network is susceptible to hidden terminal problem and broadcast storms [5]. The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of these nodes that aren't within the direct transmission range of the source, but are within the transmission range of the destination. [5].

3) Packet losses due to transmission errors: In unplanned wireless networks great deal of packet loss due to factors like high bit error rate (BER) within the wireless channel, increased collisions due to the presence of hidden points, presence of interference, unidirectional links and mobility of nodes results into path breaks [5].

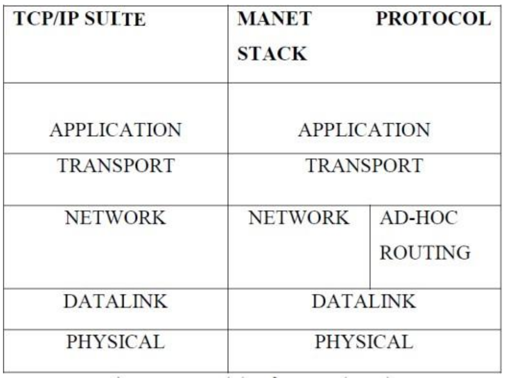
4) Mobility-induced route changes: The topology in ad- hoc wireless network is extremely dynamic due to the movement of nodes. So the current communication session suffers frequent path breaks. This situation some time results to change the route frequently. Communication in an ad-hoc network is not completely stable hence running conventional protocols for MANET's over a high loss rate will degrade its performance. However, with high error rate, it's very difficult to deliver a packet to its destination.

5) Battery constraints: This is often one among the limited resources that form a serious constraint for the nodes in an ad hoc network. Since battery capacity is fixed, hence node is extremely energy constrained. So, conservation of processing power and power-aware routing must be taken care of.

6) Potentially frequent network partitions: The randomly moving nodes in an ad hoc network can cause network partitions. In major cases, the intermediate nodes are the one which are highly suffering from this partitioning. Ease of snooping on wireless transmissions arise security issues. The radio channel used for ad hoc networks is broadcast in nature and is shared by all the nodes within the network to transmit data by a node which is further received by all the nodes within its direct transmission range. So an attacker can easily snoop the info being transmitted within the network [5].

1.1 Mobile Ad hoc Network Communication Architecture: Protocol Stack

This section briefs about the Protocol stack of the mobile ad hoc network. This provides a whole depiction and helps to know mobile ad hoc network. Figure 1.2 shows the protocol stack which contains five layers: physical layer, link layer, network layer, transport layer and application layer. it's almost like TCP/IP protocol suite. In this fig. TCP/IP suite illustration is on left and the MANET protocol stack is shown in right side. The main differentiating point between these two protocol stack is in network layer. The mobile nodes (hosts and routers) use an ad hoc routing protocol to route packets. In the physical and link layer, mobile nodes run protocol that has been designed for wireless channel. Some options are the IEEE standard for wireless LAN, IEEE 802.11, the European ETSI stands for top speed wireless LAN, [6] and eventually an industry approach towards wireless personal area network, i.e. wireless LAN at a honest small range, Bluetooth.



TCP/IP SUITE	MANET PROTOCOL STACK	
APPLICATION	APPLICATION	
TRANSPORT	TRANSPORT	
NETWORK	NETWORK	AD-HOC ROUTING
DATALINK	DATALINK	
PHYSICAL	PHYSICAL	

Fig1.2 Models of Protocol Stack

2. Routing Protocols In MANETs

Routing Schemes in MANETs are classified into Reactive, Proactive and Hybrid category on the idea of mode of operation. Further classification is due to network structure and classes identified are Flat, Hierarchical and site or geographical based.

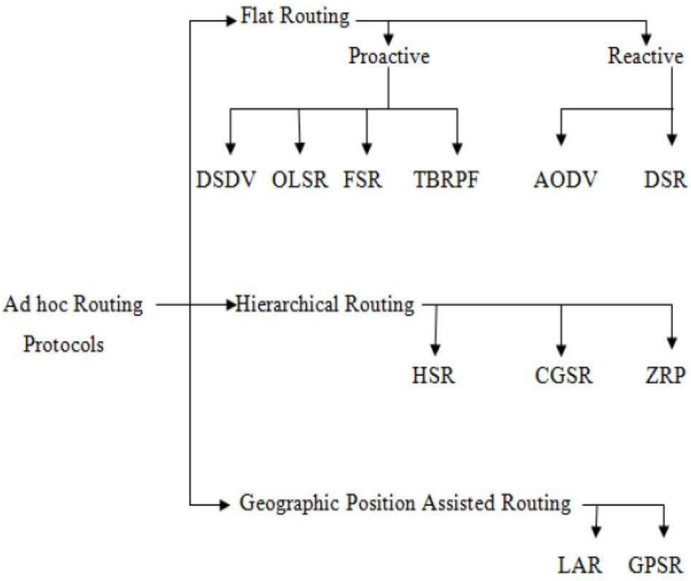
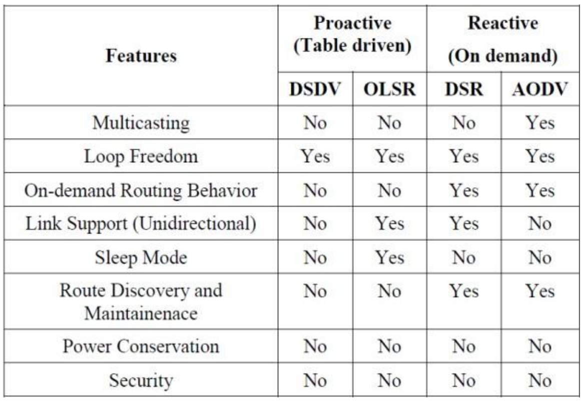


Fig.2. Classification of routing protocols in MANETs.



Features	Proactive (Table driven)		Reactive (On demand)	
	DSDV	OLSR	DSR	AODV
Multicasting	No	No	No	Yes
Loop Freedom	Yes	Yes	Yes	Yes
On-demand Routing Behavior	No	No	Yes	Yes
Link Support (Unidirectional)	No	Yes	Yes	No
Sleep Mode	No	Yes	No	No
Route Discovery and Maintainenace	No	No	Yes	Yes
Power Conservation	No	No	No	No
Security	No	No	No	No

Table.1.Features of Routing Protocols[7]

Figure 2, shows the classification of various routing protocols in MANETs.

2.1.a. Proactive Routing Protocol

Every node continuously maintains complete routing information of the network in proactive routing scheme. This is often achieved by continuously supplying information to the network and periodically set with network status information to seek out any possible change in topology. Routing protocols like Link State Routing (LSR) protocol ia based on open shortest path first and the Distance Vector Routing Protocol which uses enhanced version of Bellman-Ford algorithm are not suitable to be used in mobile environment. Destination Sequenced Distance Vector Routing Protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm [8].Examples of Proactive routing protocols are:

- Destination Sequenced Distance Vector Routing (DSDV).
- Optimized Link State Routing (OLSR).
- Fish-eye State Routing (FSR).
- Topology Broadcast Based on Reverse Path Forwarding (TBRPF).

2.1.b. Reactive Routing Protocol

In reactive routing protocol each node maintains information of only active paths to the destination nodes. A route search is required for each new destination therefore the communication overhead is reduced at the expense of delay toward route .Examples of Reactive routing protocols are:

- Ad hoc On-demand Distance Vector Routing (AODV).
- Dynamic Source Routing (DSR).

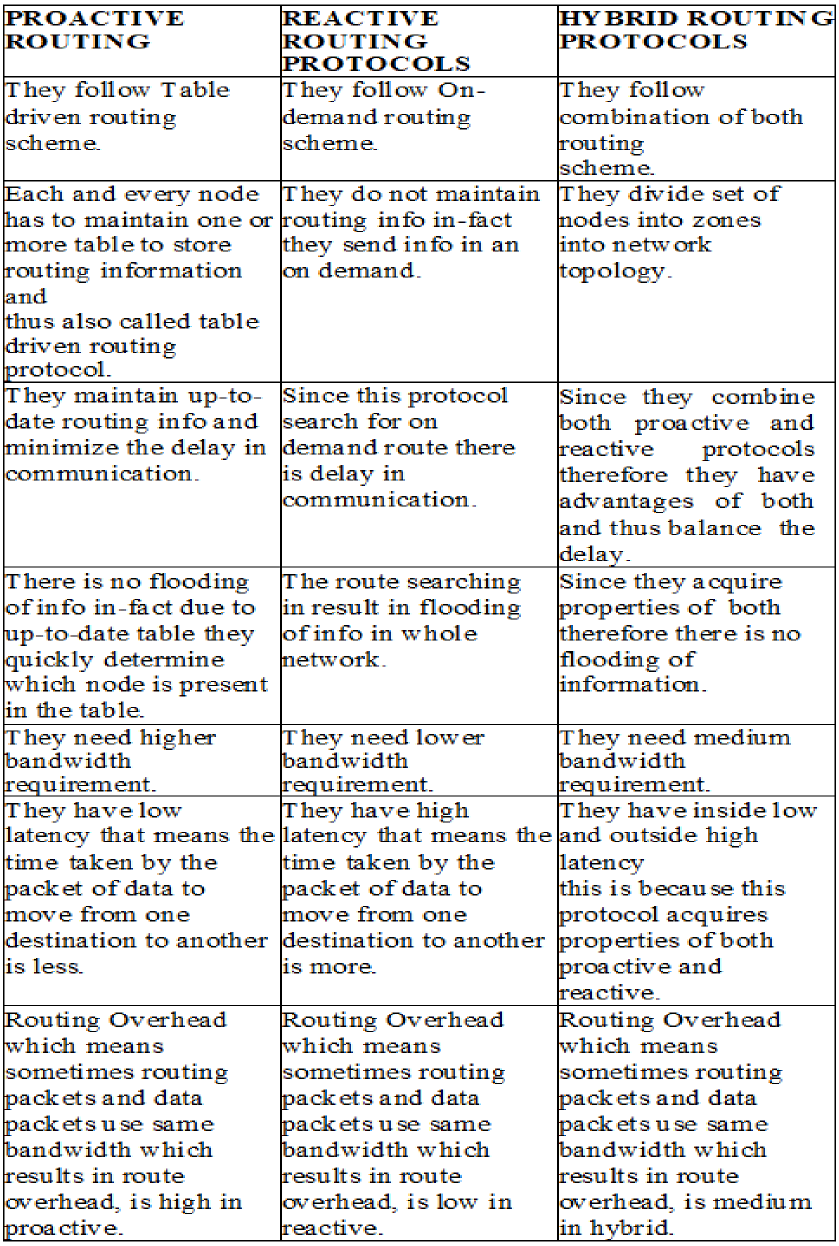
2.2 Hierarchical Routing

Because the size of wireless network increases, the flat routing protocols will produced more overhead within the network. Rapidly changing wireless network topology may shatter active route and cause successive route search [9]. At this point to overcome such situation Hierarchical Routing could also be used for MANETS. Examples of Hierarchical routing protocol are:

➢ Cluster head-Gateway Switch Routing (CGSR).

➢ Zone Routing Protocol (ZRP).

➢ Hierarchical State Routing (HSR).



PROACTIVE ROUTING	REACTIVE ROUTING PROTOCOLS	HYBRID ROUTING PROTOCOLS
They follow Table driven routing scheme.	They follow On-demand routing scheme.	They follow combination of both routing scheme.
Each and every node has to maintain one or more table to store routing information and thus also called table driven routing protocol.	They do not maintain routing info in-fact they send info in an on demand.	They divide set of nodes into zones into network topology.
They maintain up-to-date routing info and minimize the delay in communication.	Since this protocol search for on demand route there is delay in communication.	Since they combine both proactive and reactive protocols therefore they have advantages of both and thus balance the delay.
There is no flooding of info in-fact due to up-to-date table they quickly determine which node is present in the table.	The route searching in result in flooding of info in whole network.	Since they acquire properties of both therefore there is no flooding of information.
They need higher bandwidth requirement.	They need lower bandwidth requirement.	They need medium bandwidth requirement.
They have low latency that means the time taken by the packet of data to move from one destination to another is less.	They have high latency that means the time taken by the packet of data to move from one destination to another is more.	They have inside low and outside high latency this is because this protocol acquires properties of both proactive and reactive.
Routing Overhead which means sometimes routing packets and data packets use same bandwidth which results in route overhead, is high in proactive.	Routing Overhead which means sometimes routing packets and data packets use same bandwidth which results in route overhead, is low in reactive.	Routing Overhead which means sometimes routing packets and data packets use same bandwidth which results in route overhead, is medium in hybrid.

Table.2.Comparision table of Routing Protocols[10]

3. MANET Routing Protocol Performance Issues

Above is a comparison table of classification of routing protocol, there is a requirement of both qualitative and quantitative metrics with which we will measure its suitability and performance. These metrics are always considered to be independent of any given routing protocol [11].

The following list shows a number of the desirable qualitative characteristics of MANET routing protocols [11]:

1) Distributed operation: An Ad-hoc wireless network is totally distributed in nature, since nodes possesses to realize quick access to the acquired channel. The use of any centralized control or routing approach in such networks will consume great deal of bandwidth.

2) Loop-freedom: Avoids some problems like, a compact amount of packets spinning around within the network for random time periods. Unplanned solutions like TTL (Time to Live) values can bind the matter, but a more structured and well-formed approach is typically desirable because it always leads to better overall performance.

3) Demand-based operation: The dynamic topologies will cause the routing algorithm adapt to the traffic pattern on a requirement or need basis, rather than assuming a consistent

traffic distribution within the network (and maintaining routing between all nodes in the least times). If this is being dealt carefully, the network energy and bandwidth resources are utilized more efficiently, at the worth of increased route discovery delay.

4) Proactive operation: This is often vital property for a demand-based operation. Intrinsically in certain contexts, an extra additional latency demand-based operation incurs may not be acceptable. For such cases, if the bandwidth and energy resources of the network allows, then a proactive operation is desirable.

5) Security: If the ad hoc network lacks some sort of network-level or link-layer security, a MANET routing protocol are going to get more susceptiblility towards different sort of malicious attacks. It can be simple attack like snooping network traffic, transmissions replay, manipulation of the packet headers, and redirecting the routing messages, within an Ad-hoc wireless network with none appropriate security provisions. While a number of these concerns do exists during a wireless infrastructures and routing protocols and also many counter measures against the malicious attacks [12, 13, 14] as well, but maintaining the physical security of the transmission media is difficult in MANETS. Enough security protection is required to regulate the disruption of modification of protocol operation. This seems to be somewhat orthogonal to any particular routing protocol approach, e.g. through the appliance of IP Security techniques.

6) Sleep period operation: Nodes of a MANET will stop transmitting and/or receiving (even receiving requires power) for arbitrary time periods, when the energy conservation or another need to be inactive. An Ad-hoc routing protocol should be ready to accommodate such sleep periods with none adverse effects. So as to realise this characteristic it may require a close coupling with the link-layer protocol through a standardized interface.

7) Unidirectional link support: As per the routing algorithm design, bidirectional links will function well than unidirectional links. Sometimes, sufficient number of bidirectional links were present so that the use of unidirectional links is of limited importance. However, it's more considered in certain situations, where a pair of unidirectional links (in opposite directions) form the only bidirectional connection between two ad hoc regions.

The following list shows a number of the quantitative metrics which will be used to measure the performance of any routing protocol [12].

1. End-to-end delay and data throughput : Statistical measures of data routing performance based upon means, variances, distributions are important to deal with this. These are the measures of a routing policy's effectiveness for an ad-hoc network.
2. Route Acquisition Time: A specific form of external end-to-end delay measurement of particular concern with "on demand" routing algorithms is that the time required establishing route(s) when requested.
3. Percentage Out-of-Order Delivery: An external measure of connectionless routing performance of particular concern layer protocols, like TCP which prefer in-order delivery.
4. Efficiency: If data routing effectiveness is the external measure of a policy's performance, efficiency is the internal measure of its success.

To attain a given level of data routing performance, two different policies can expend differing amounts of overhead, counting on their internal efficiency. Protocol efficiency may or may indirectly affect data routing performance. If control and data traffic must share an equivalent channel, and therefore the channel's capacity is restricted, then excessive control traffic often impacts data routing performance.

It's useful to trace several ratios that illuminate the interior efficiency of a protocol in doing its job:

* Average number of data bits transmitted/data bit delivered--this will be thought of as a measure of the bit efficiency of delivering data within the network. Obliquely, it also

gives the standard hop count taken by data packets.

* Average number of control bits transmitted by data bit delivered—is equal to the measure of bit efficiency of the protocol in expending control overhead to delivery data. It should be notable that this could include not only the bits within the routing control packets, but also the bits within the header of the data packets or anything that's not data is control overhead, and can be counted within the control portion of the algorithm.

* Average number of control and data packets transmitted by data packet delivered—is rather than measuring pure algorithmic efficiency in terms of bit count, this tries to capture a protocol's channel access efficiency. As the cost of channel access is high in contention-based link layers.

Additionally, to the networking context where during a protocol performance is measured. Different network parameters that change often consistent with the applications used include [11]:

- Network size—this is that the measurement taken because the number of nodes within the network.
- Network connectivity—this is that the measurement of the typical degree of a node, successively gives the typical number of neighbors of a node within the network.
- Topological rate of change—this gives the measure of the speed with which a topology keeps changing.
- Capacity of a link –This is that the measure of effective link speed in bits/second, when it accounts for losses thanks to multiple accesses, coding, framing, etc.
- Unidirectional links—this provides the measure of the success of a protocol performance as a function of the unidirectional links present.
- Traffic patterns—this gives the measure of the effectiveness of a protocol in adapting to dynamic, non-uniform or short interval traffic patterns.
- Mobility—this gives the measure of the various circumstances, to seek out out whether the temporal and spatial topological correlation relevant to the performance of a routing protocol or not. Thereby it also helps find out most appropriate model for simulation of nodes mobility during a MANET.
- Fraction and frequency of sleeping nodes—this gives the measure of the protocol performance within the presence of sleeping and awakening nodes within the network. When wide selection of networking scenarios in MANETS are considered like small, collaborative, Ad-hoc groups to larger mobile, multihop networks, a protocol should function most effectively over this a good range of networks.

4. CONCLUSION AND FUTURE SCOPE

MANETs possesses several networking opportunities that require to be intrigued. Due to the various challenging tradeoffs for MANETS, sometimes each different set of performance issues requires new protocols for network control. The protocol for MANET should also confine account of scarcity of bandwidth and energy related constraints and work well to live the goodness of the network performance. This paper discusses protocol performance issues that highlight performance parameters which will help to market meaningful comparisons and assessments of protocol performance. This recognizes the suitability to use the right routing protocol for particular network or particular application.

In Ad-hoc routing protocols, nodes exchange information with one another about the topology, because the nodes also are routers. This fact is additionally a crucial weakness because a compromised node could give bad information to redirect traffic or just stop it.

Although it are often said that routing protocols are very fragile in term of security. This paper provide an outline of the causes of problems with Ad-hoc routing protocols. This clear idea about routing protocol issues will led to the right selection of routing protocol or necessary changes are often made accordingly at the network layer for security measures.

REFERENCES

[1] Sarangapani, J. Wireless Ad Hoc and Sensor Networks Protocols, Performance, and Control. CRC Press, Taylor & FrancisGroup,USA,(2007).514p.doi:https://doi.org/10.1201/9781420015317.

[2] Auon, M.A. & Wang, X. Cross-Layer Designs for Energy-Efficient Wireless Ad-hoc Networks, Energy Management in Wireless Cellular and Ad-hoc Networks. Studies in Systems, Decision and Control, Springer, Cham, (2016), 50, 147-168.

[3] Zuo, J.; Dong, C.; Ng, S.X.; Yang, L.L. & Hanzo, L. Cross-Layer Aided Energy-Efficient Routing Design for AdHoc Networks. IEEE ommunications Surveys & Tutorials,(2015),17(3),1214–1238.

[4] A. K. Gupta, & S. Prakash , "Secure communication in cluster-based ad hoc networks: a
review," In Next- Generation Networks, Springer, Singapore, 2018, pp.537-545).

[5] Iram Nausheen,Dr.Akhilesh Upadhyay" A Survey on MANETs: Entrusted Security Challenges," in International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 48 – 58.

[6] S. Corson and J. Macker, "RFC 2501 - Mobile Ad HocNetworking (MANET): Routing Protocol Pe", Network Working Group, Request for Comments: 2501, University of Maryland, Naval Research Laboratory, JAN 1999.

[7] Chawda, K. & Gorana, D. A survey of Energy Efficient Routing Protocol in MANET. In Proceedings of the IEEE Sponsored 2nd International Conference on Electronics And Communication System, 2015,953–957.

[8] Ankur Khetrapal, "Routing techniques for Mobile Ad Hoc Networks Classification and Qualitative/Quantitative Analysis",2006, pp 1-7.

[9] Puneet Kamal, Rajeev Sharma,Abhishek Gupta "Comparative Analysis of Attacks and Countermeasure in MANET"IJCSN-International Journal of Computer Science and Network, Volume 8,Issue 2, April 2019 ISSN (Online) : 2277-5420.

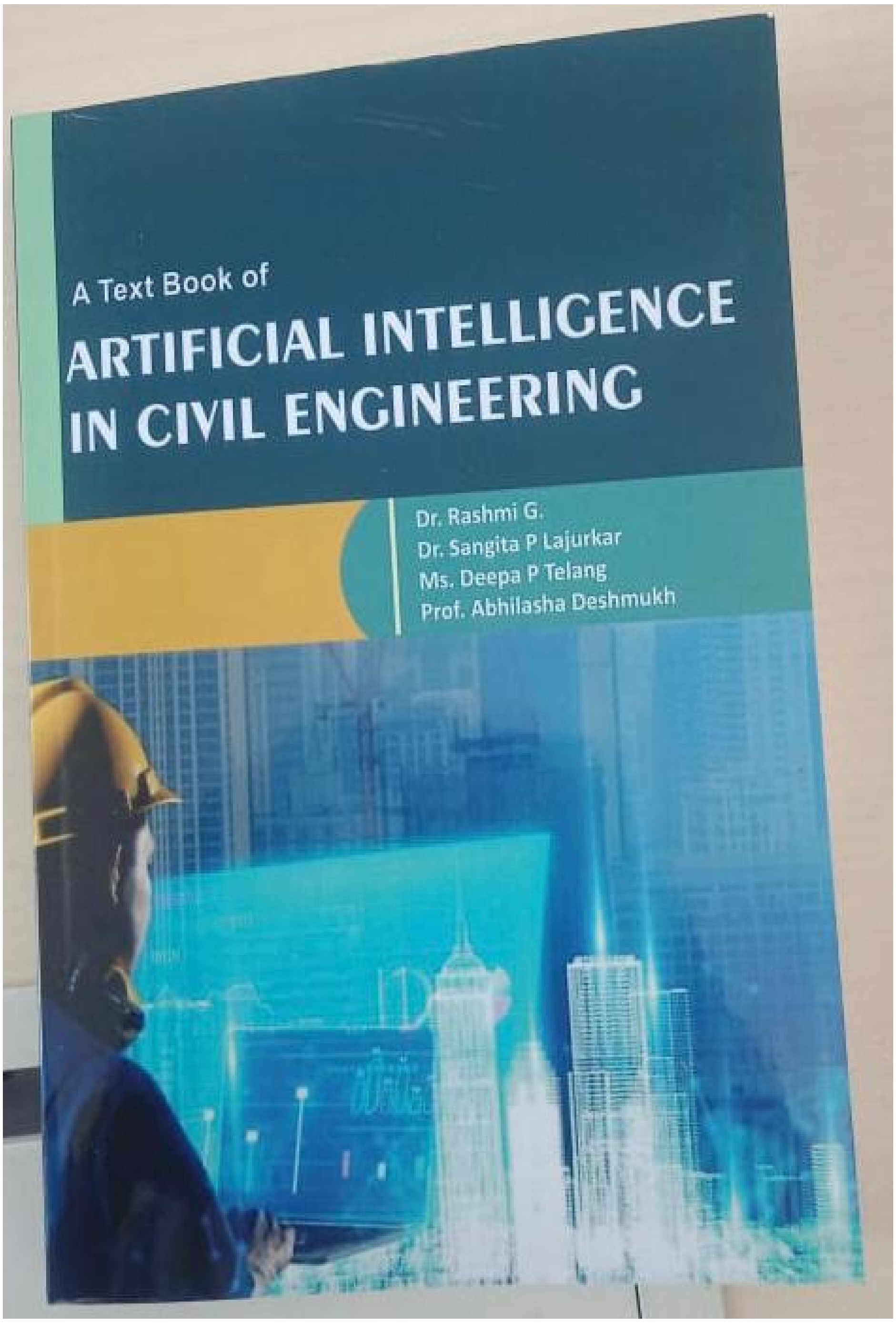
[10] Kritika Lamba, Aprajita Rawat, Shelja Sharma' Dr.Prateek Jain,"An Analysis based on Comparative Study of Routing Protocols in MANET"International Journal of Engineering Research & Technology (IJERT)ISSN: 2278-0181 Vol. 7 Issue 09, September-2018.

[11] Syeda kausar Fatima, Dr. Syeda Gauhar Fatima, Dr. Syed Abdul Sattar, Syed Mohd Ali"Mobile adhoc networks security challenges: a Survey" International Journal of Advanced Research in Engineering and Technology (IJARET)Volume 10, Issue 2, March-April 2019, pp. 224-237.

[12] G. S. Mamatha1 and Dr. S. C. Sharma Analyzing The Manet Variations,Challenges, Capacity And Protocol Issues International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[13] Muhammad Saleem Khan, Qasim Khan Jadoon, and Majid I. Khan "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks". Springer-Verlag Berlin Heidelberg 2015.

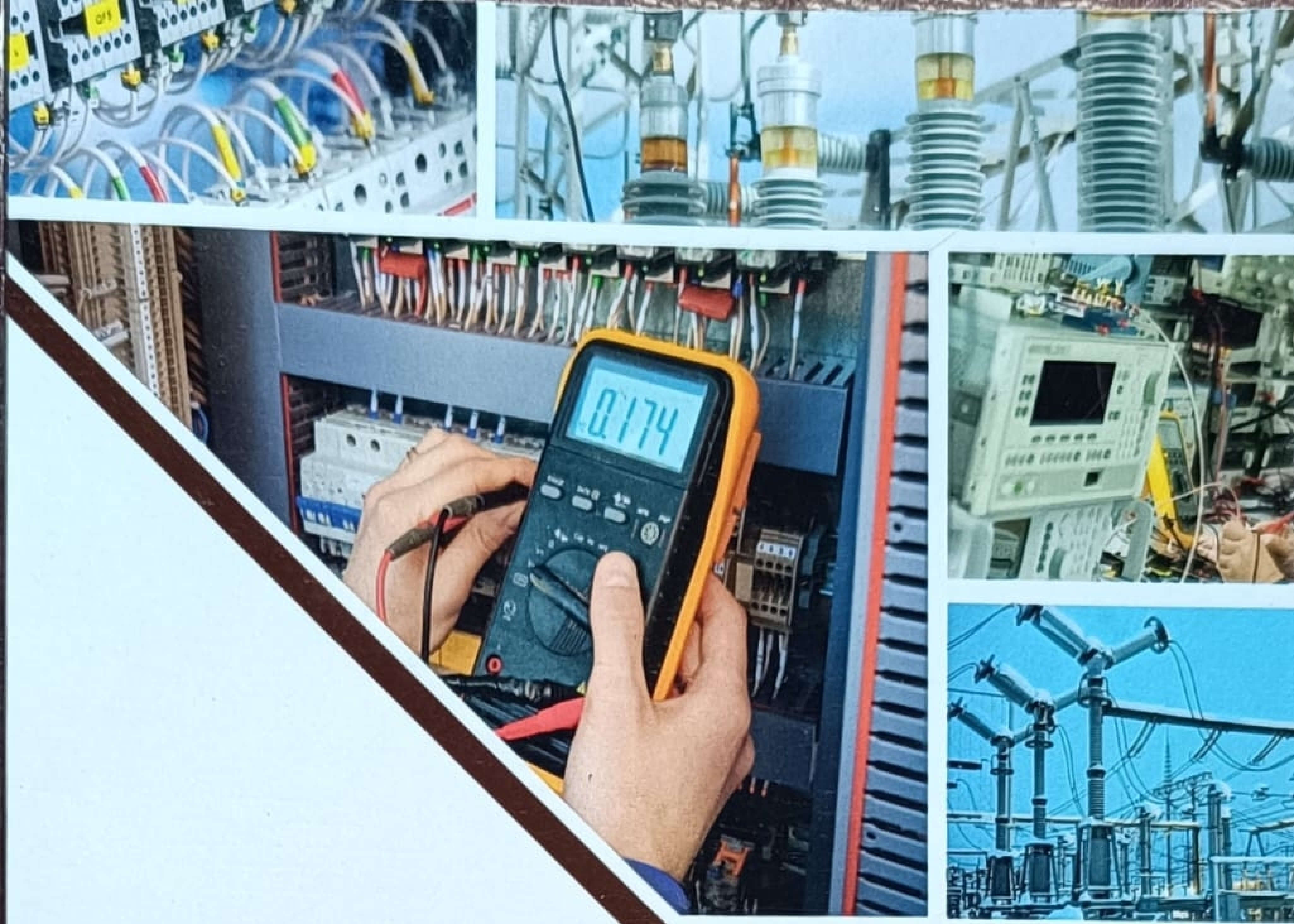
[14] Manish Devendra Chawhan, Ausaf Umar Khan and Bhumika Neole" A Survey on Cross Layer Framework based Energy Efficient Routing Protocols of Manets" International Journal of Future Generation Communication and Networking Vol. 13, No. 1, (2020), pp. 1125-1135 .



A Text Book of

ARTIFICIAL INTELLIGENCE IN CIVIL ENGINEERING

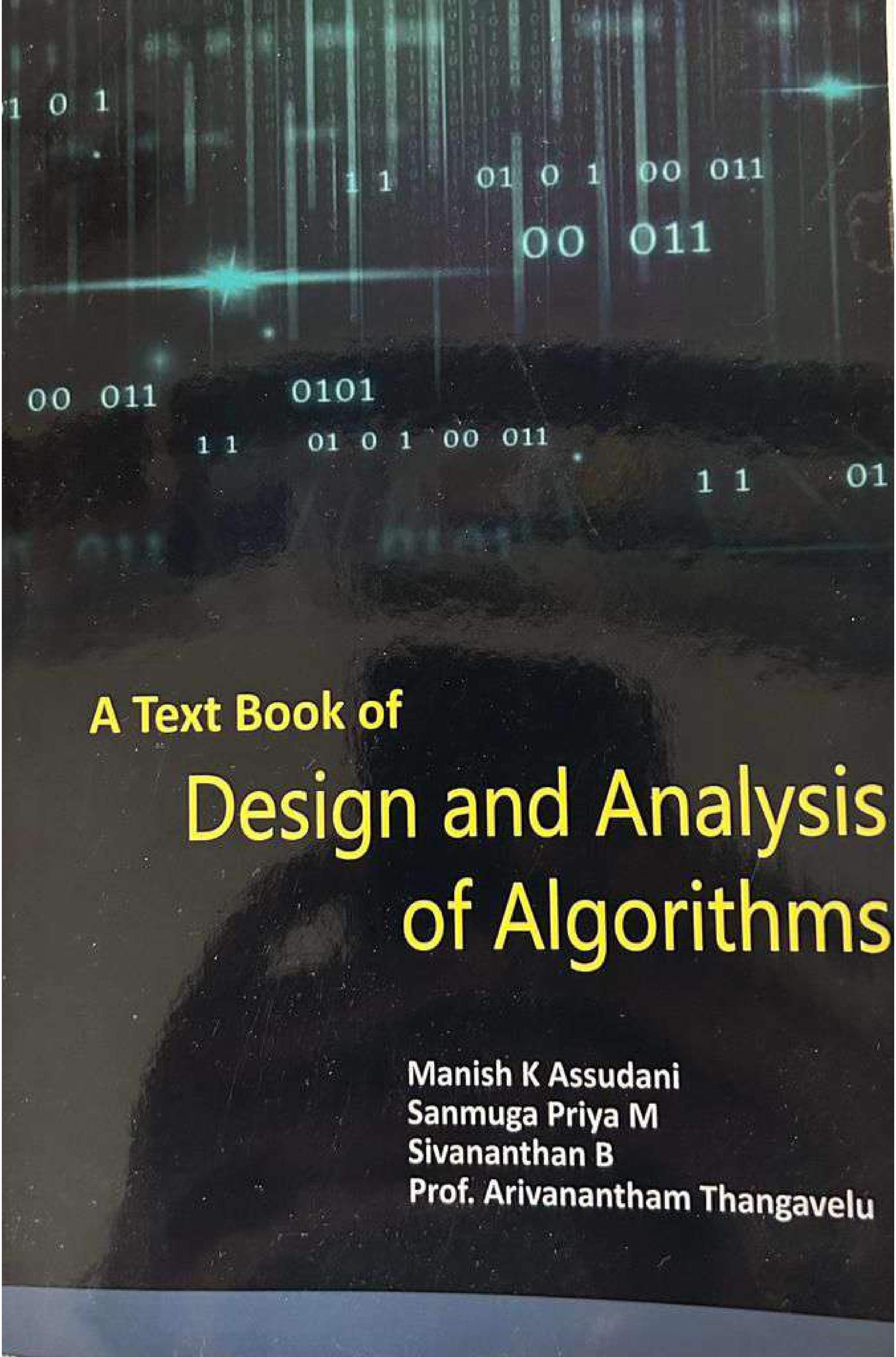
Dr. Rashmi G.
Dr. Sangita P Lajurkar
Ms. Deepa P Telang
Prof. Abhilasha Deshmukh



A Text Book of

Fundamentals of Electrical Engineering

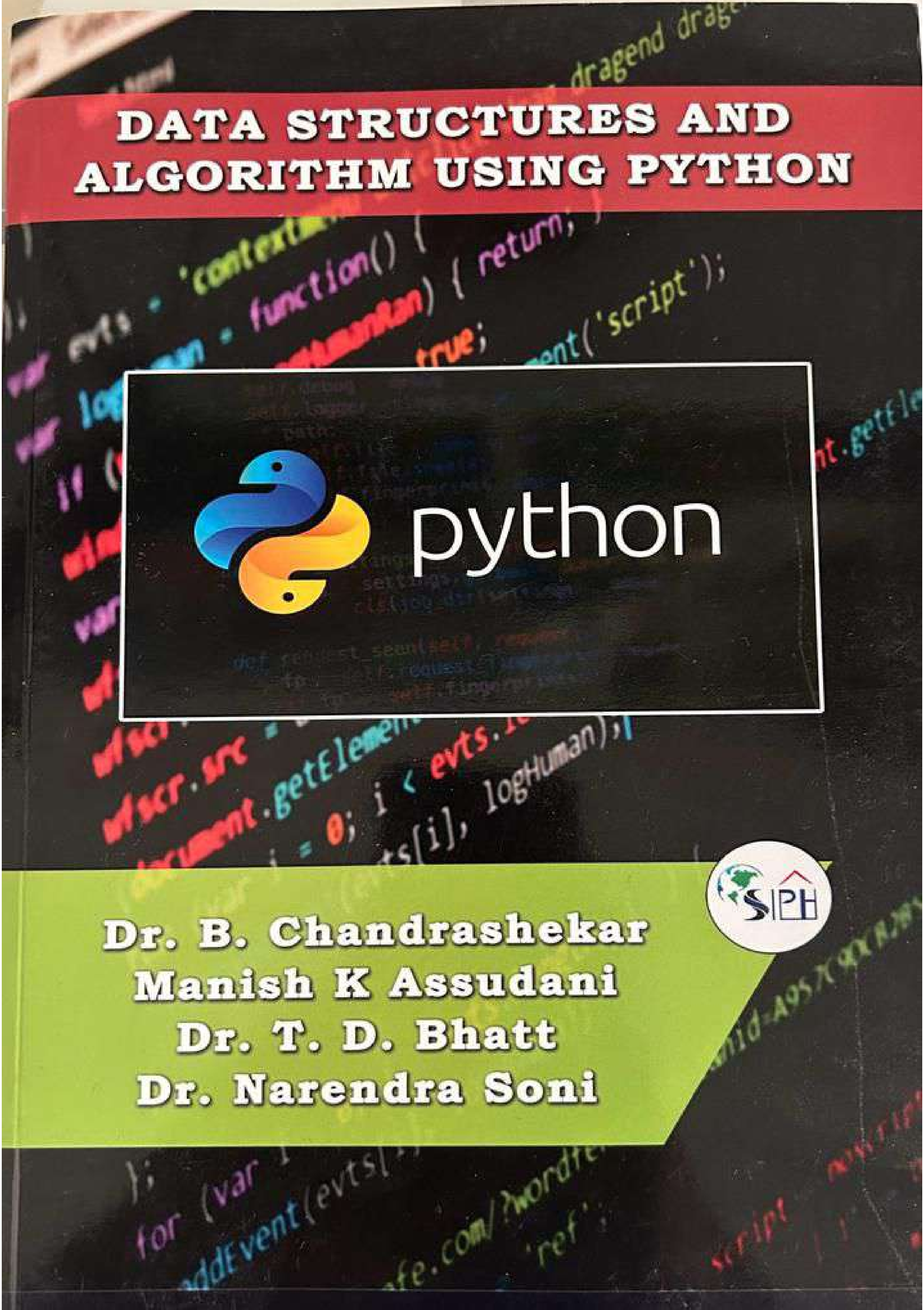
Dr. J.Latha
Prof. Najma Nasreen Siddiqui
Mr. A.S. Vigneshwar
Dr. S.Sathish Kumar



A Text Book of

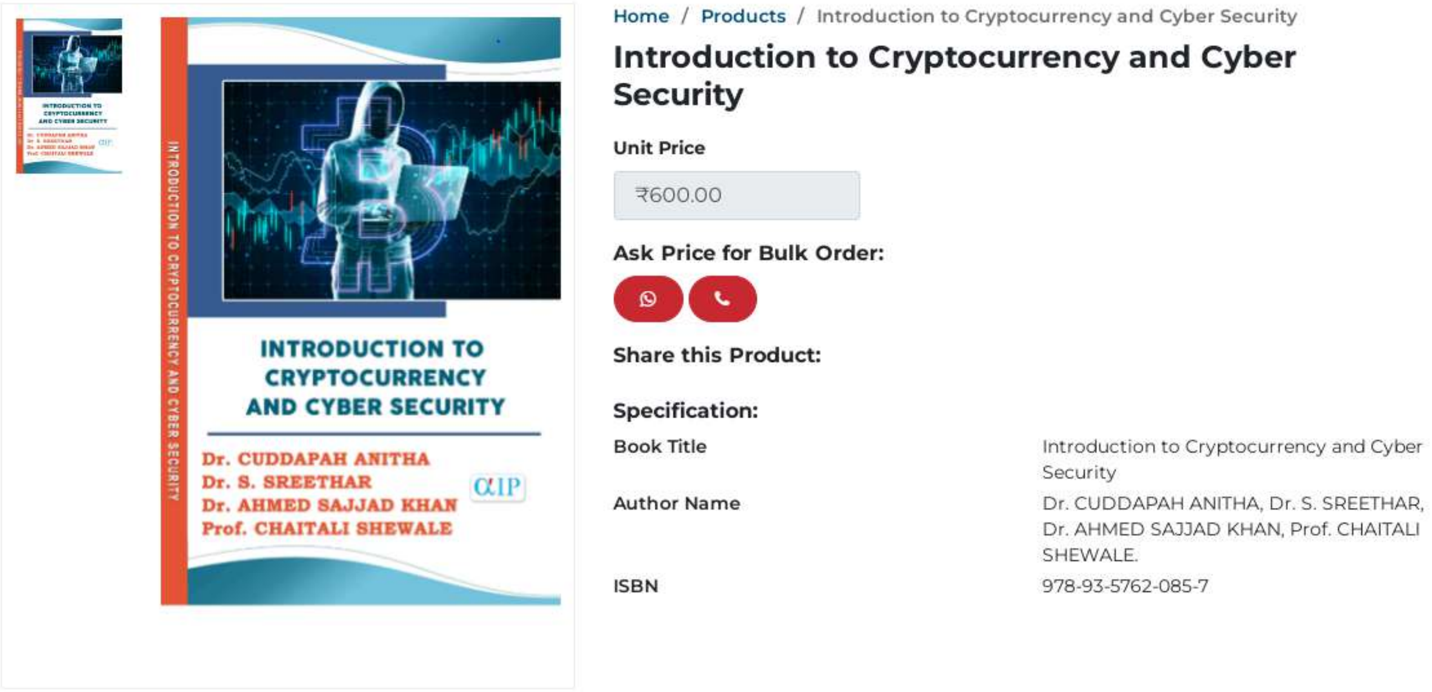
Design and Analysis of Algorithms

Manish K Assudani
Sanmuga Priya M
Sivananthan B
Prof. Arivanantham Thangavelu



DATA STRUCTURES AND ALGORITHM USING PYTHON

Dr. B. Chandrashekar
Manish K Assudani
Dr. T. D. Bhatt
Dr. Narendra Soni



INTRODUCTION TO CRYPTOCURRENCY AND CYBER SECURITY
INTRODUCTION TO CRYPTOCURRENCY AND CYBER SECURITY
Dr. CUDDAPAH ANITHA
Dr. S. SREETHAR
Dr. AHMED SAJJAD KHAN
Prof. CHAITALI SHEWALE
αIP

Home / Products / Introduction to Cryptocurrency and Cyber Security

Introduction to Cryptocurrency and Cyber Security

Unit Price

₹600.00

Ask Price for Bulk Order:

☎

Share this Product:

Specification:

Book Title	Introduction to Cryptocurrency and Cyber Security
Author Name	Dr. CUDDAPAH ANITHA, Dr. S. SREETHAR, Dr. AHMED SAJJAD KHAN, Prof. CHAITALI SHEWALE.
ISBN	978-93-5762-085-7

ICDAM-2023

LONDON METROPOLITAN UNIVERSITY

THE KARKONOSZE UNIVERSITY OF APPLIED SCIENCES

Springer

POLITÉCNICO DE PORTALEGRE
Escola Superior de Tecnologia e Gestão

BPIT
Bhagwan Parshuram Institute of Technology

INTERNATIONAL CONFERENCE ON DATA ANALYTICS & MANAGEMENT (ICDAM-2023)

Certificate

This is to certify that **Prof. /Dr. / Mr. / Ms.** Ahmed Sajjad Khan is a presenter/co-author of the paper titled **ML.Net based experiments for diagnosing Laryngitis & Chordektomie using SVD and Result** presented at the **4th International Conference on Data Analytics and Management (ICDAM-2023)**, organized jointly by London Metropolitan University, London, UK in association with the Karkonosze University of Applied Sciences, Jelenia Gora, Poland, Europe, Politécnico de Portalegre, Portugal, Europe and BPIT, GGSIPU, Delhi on **23rd – 24th June 2023**.

Prof. (Dr.) Bal Virdee
London Metropolitan University, UK
General Chair

Prof. Sérgio Duarte Correia
Politécnico de Portalegre, Portugal
Publication Chair

3.3.3 Number of books and chapters in edited volumes/books published and papers published in national/ international conference proceedings per tea

Sl. No.	Name of the teacher	Title of the book/chapters published	Title of the paper	Title of the proceedings of the conference	Name of the conference	National / International	Year of publication	ISBN/ISSN number of the proceeding	Affiliating Institute at the time of publication	Name of the publisher
1	Dr akash langde		Experimental investigations of carbon dioxide (CO2) removal through physical adsorption using carbonaceous adsorbents: A Review	AIP CONFERENCE PROCEDINGS	International Conference on Innovations in Science, Hybrid Materials and Vibration Analysis	international	2023	0094-243X	ANJUMAN COLLEGE OF ENGINERING AND TECHNOLOGY	AIP
2	A P GANORKAR		Experimental investigations of carbon dioxide (CO2) removal through physical adsorption using carbonaceous	AIP CONFERENCE PROCEDINGS	International Conference on Innovations in Science, Hybrid Materials and Vibration Analysis	international	2023	0094-243X	ANJUMAN COLLEGE OF ENGINERING AND TECHNOLOGY	AIP
3	Dr akash langde	SOUND ASSISTED FLUIDIZATION					2023	97789391322106.00		alliance and company

ATUL P. GANORKAR
Assistant Professor (MEC
Anjuman College of Eng
& Technology, Sadar, Nag

Dr. Namrata Lotia
Head of Mechinical Engineering Department
Anjuman College of Engineering & Techn.
Sadar, Nagpur.

4	Dr M Shakebuddin	SOUND ASSISTED FLUIDIZATION					2023	97789391322106.00	ANJUMAN COLLEGE OF ENGINERING AND TECHNOLOGY	alliance and company
5	Dr Nafees Khan	SOUND ASSISTED FLUIDIZATION					2023	97789391322106.00	ANJUMAN COLLEGE OF ENGINERING AND TECHNOLOGY	alliance and company

ATUL P. GANORKAR
Assistant Professor (MEC
Anjuman College of Eng
& Technology, Sadar, Nag

Dr. Namrata Lotia
Head of Mechinical Engineering Department
Anjuman College of Engineering & Techn.
Sadar, Nagpur.

RESEARCH ASSOCIATION OF MASTERS OF ENGINEERING

CERTIFICATE OF PARTICIPATION

This is to certify that

Akash Langde

has successfully participated the paper entitled

Experimental investigations of carbon dioxide (CO2) removal through physical adsorption using carbonaceous adsorbents: A Review

In the International Conference on Innovations in Science, Hybrid Materials and Vibration Analysis

IC-ISHVA 2022

held on 16-17 July 2022

DR. K. S. RAMBHAD
CONVENER

DR. J. D. KENE
CONVENER

DR. R. H. GAJGHAT
CONVENER

DR. M. A. KUMBHALKAR
CONFERENCE CHAIR

RESEARCH ASSOCIATION OF MASTERS OF ENGINEERING

AIP Publishing

CERTIFICATE OF PRESENTATION

This is to certify that

Atul Ganorkar

has successfully presented the paper entitled

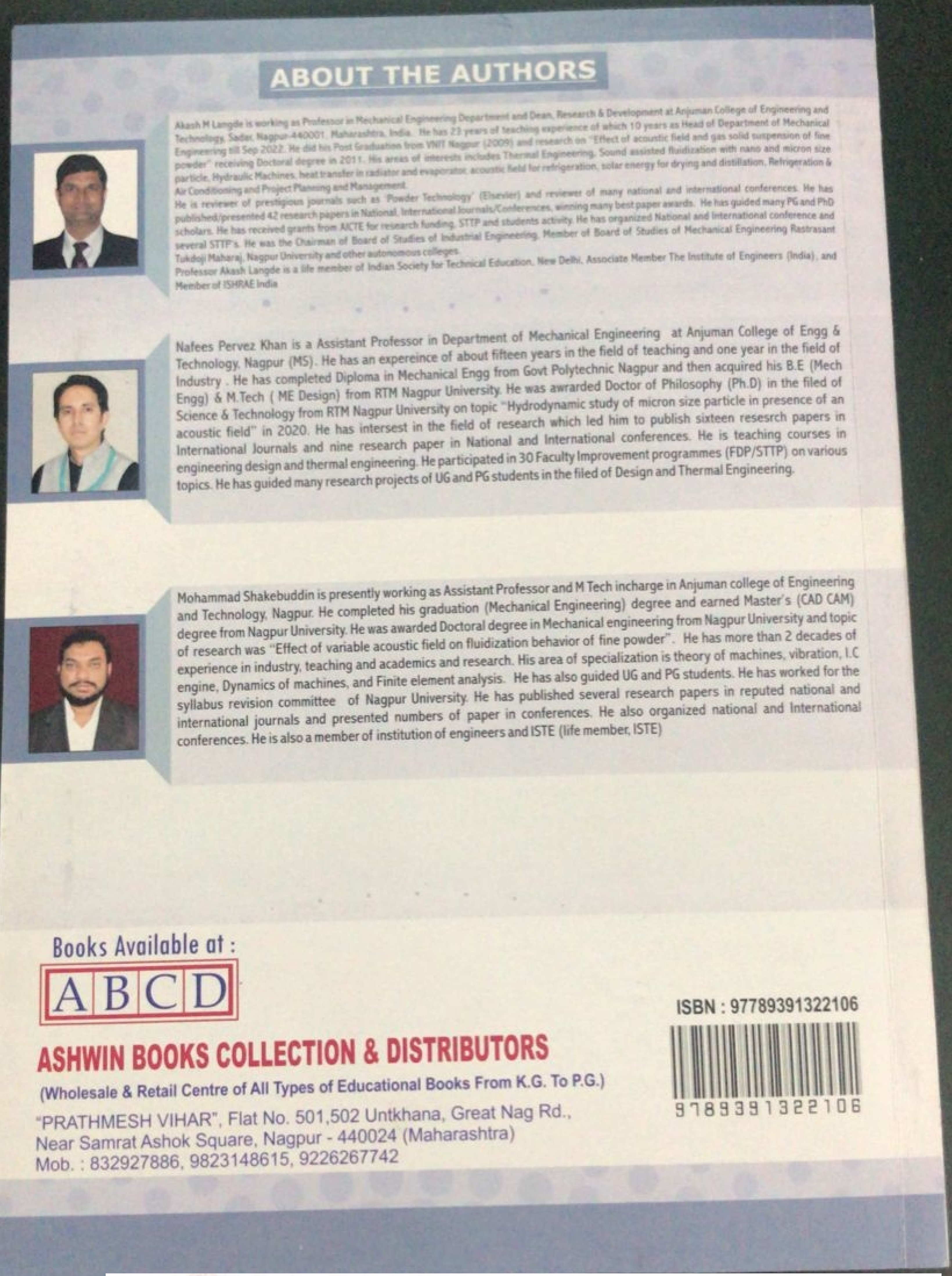
Experimental investigations of carbon dioxide (CO2) removal through physical adsorption using carbonaceous adsorbents: A Review

In the International Conference on Innovations in Science, Hybrid Materials and Vibration Analysis

IC-ISHVA 2022

held on 16-17 July 2022

DR. K. S. RAMBHAD CONVENER	DR. J. D. KENE CONVENER	DR. R. H. GAJGHAT CONVENER	DR. M. A. KUMBHALKAR CONFERENCE CHAIR



ABOUT THE AUTHORS

Akash M Langde is working as Professor in Mechanical Engineering Department and Dean, Research & Development at Anjuman College of Engineering and
Technology, Sadar, Nagpur-440001. Maharashtra, India. He has 23 years of teaching experience of which 10 years as Head of Department of Mechanical
Engineering till Sep 2022. He did his Post Graduation from VNIT Nagpur (2009) and research on "Effect of acoustic field and gas solid suspension of fine
powder" receiving Doctoral degree in 2011. His areas of interests includes Thermal Engineering, Sound assisted fluidization with nano and micron size
particle, Hydraulic Machines, heat transfer in radiator and evaporator, acoustic field for refrigeration, solar energy for drying and distillation, Refrigeration &
Air Conditioning and Project Planning and Management.
He is reviewer of prestigious journals such as 'Powder Technology' (Elsevier) and reviewer of many national and international conferences. He has
published/presented 42 research papers in National, International Journals/Conferences, winning many best paper awards. He has guided many PG and PhD
scholars. He has received grants from AICTE for research funding, STTP and students activity. He has organized National and International conference and
several STTP's. He was the Chairman of Board of Studies of Industrial Engineering, Member of Board of Studies of Mechanical Engineering Rastrasant
Tukdoji Maharaj, Nagpur University and other autonomous colleges.
Professor Akash Langde is a life member of Indian Society for Technical Education, New Delhi, Associate Member The Institute of Engineers (India), and
Member of ISHRAE India

Nafees Pervez Khan is a Assistant Professor in Department of Mechanical Engineering at Anjuman College of Engg & Technology, Nagpur (MS). He has an expereince of about fifteen years in the field of teaching and one year in the field of Industry . He has completed Diploma in Mechanical Engg from Govt Polytechnic Nagpur and then acquired his B.E (Mech Engg) & M.Tech (ME Design) from RTM Nagpur University. He was awrarded Doctor of Philosophy (Ph.D) in the filed of Science & Technology from RTM Nagpur University on topic "Hydrodynamic study of micron size particle in presence of an acoustic field" in 2020. He has intersest in the field of research which led him to publish sixteen resesrch papers in International Journals and nine research paper in National and International conferences. He is teaching courses in engineering design and thermal engineering. He participated in 30 Faculty Improvement programmes (FDP/STTP) on various topics. He has guided many research projects of UG and PG students in the filed of Design and Thermal Engineering.

Mohammad Shakebuddin is presently working as Assistant Professor and M Tech incharge in Anjuman college of Engineering and Technology, Nagpur. He completed his graduation (Mechanical Engineering) degree and earned Master's (CAD CAM) degree from Nagpur University. He was awarded Doctoral degree in Mechanical engineering from Nagpur University and topic of research was "Effect of variable acoustic field on fluidization behavior of fine powder". He has more than 2 decades of experience in industry, teaching and academics and research. His area of specialization is theory of machines, vibration, I.C engine, Dynamics of machines, and Finite element analysis. He has also guided UG and PG students. He has worked for the syllabus revision committee of Nagpur University. He has published several research papers in reputed national and international journals and presented numbers of paper in conferences. He also organized national and International conferences. He is also a member of institution of engineers and ISTE (life member, ISTE)

Books Available at :

ABCD

ASHWIN BOOKS COLLECTION & DISTRIBUTORS

(Wholesale & Retail Centre of All Types of Educational Books From K.G. To P.G.)

"PRATHMESH VIHAR", Flat No. 501,502 Untkhana, Great Nag Rd.,
Near Samrat Ashok Square, Nagpur - 440024 (Maharashtra)
Mob. : 832927886, 9823148615, 9226267742

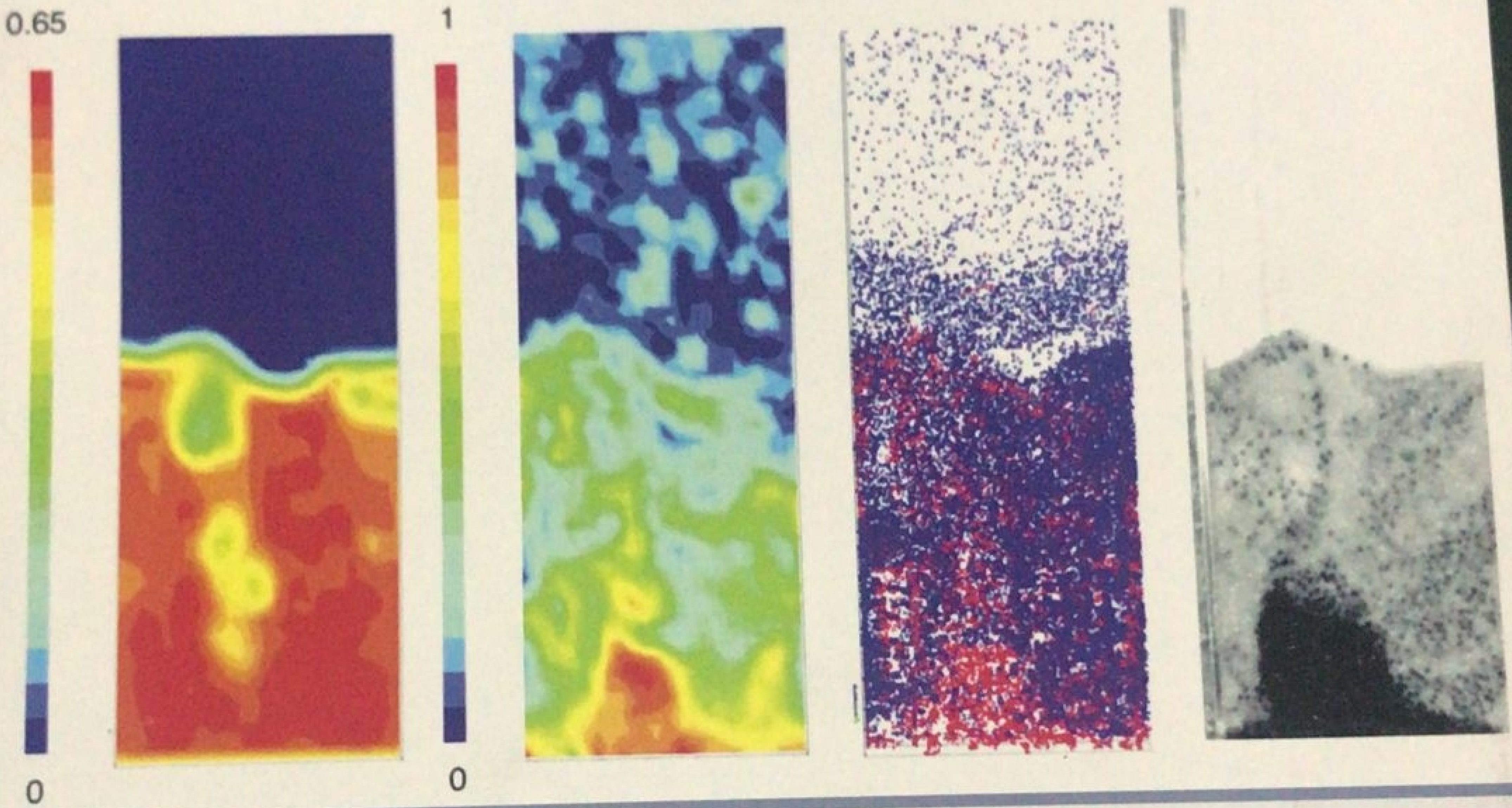
ISBN : 97789391322106

9789391322106

ATUL P. GANORKAR
Assistant Professor (MEC
Anjuman College of Eng
& Technology, Sadar, Nag

Dr. Namrata Lotia
Head of Mechinical Engineering Department
Anjuman College of Engineering & Techn.
Sadar, Nagpur.

SOUND ASSISTED FLUIDIZATION



Dr. Akash Langde
Dr.Nafees P.Khan
Dr. M.Shakebuddin

Alliance & Co.
A revolutionary attempt in educational books for all Indian universities & autonomous institutions...

• Maharashtra • Chhattisgarh • Gujrat • Madhya Pradesh • Tamilnadu • Karnataka • Andhra Pradesh • Punja