RESEARCH TRENDS IN MANET

Dr. PRATIK GITE
Assistant Professor
Department of Computer Science & Engineering
IPS ACADEMY : INSTITUTE OF ENGINEERING & SCIENCE
Indore, Madhya Pradesh, INDIA

RESEARCH TRENDS IN MANET

ISBN-13: 978-93-87610-21-7
FIRST EDITION, SEPTEMBER 2018, INDIA

Printed & Published by:
VSRD Academic Publishing
A Division of Visual Soft India Private Limited

Printed & Bound in India

VSRD ACADEMIC PUBLISHING
A Division of Visual Soft (India) Pvt. Ltd.

REGISTERED OFFICE
154, Tezabmill Campus, Anwarganj, KANPUR – 208 003 (UP) (INDIA)
Mob.: +91 98999 36803 ||Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

MARKETING OFFICE (SOUTH INDIA)
340, First Floor, Adarsh Nagar, Oshiwara, Andheri(W), MUMBAI – 400 053 (MH) (INDIA)
Mob.: +91 99561 27040 || Web.: www.vsrdpublishing.com || Email: vsrdpublishing@gmail.com

FOREWORD

This research book meets the requirement of students of engineering, professional, research scholars of MANET and other courses. This book is useful to know the research trends in MANET.

"Research Trends in MANET" takes a thorough approach to introduce the basic concepts of the wireless mobile ad-hoc network. It covers the key features of wireless mobile ad-hoc network and advanced topics such as security issues in MANET, Applications of MANET, Features of MANET and simulation study of MANET ad various attacks.

The book is organized in a systematic way to cover various topics with numerous examples. The goal of this book is to make the students and research scholars to understand the concepts of wireless mobile ad-hoc network.

This book will help the students to understand the concepts of MANET in a simple and easy way. This book is for beginners who wish to know about introductory part of wireless mobile ad-hoc network. This book is written by assuming that the reader need not be an expert of Mobile Ad-hoc Network.

The book has been provided summary and review questions which will be useful to the reader of the book. While writing this book, I have worked actively with the matter of the book to ensure that the book is technically correct, although it is hoped all material in this book is accurate, the possibility exists that some omissions or errors may present. It will be grateful if I receive suggestions from the users of this book and if they communicate to me for any errors they discover. It will help me to improve the future editions of this book. Suggested improvements should be mail at pratikgite135@gmail.com.

✍ *Dr. Pratik Gite*

ABOUT THE AUTHOR

Destiny drew **Dr. Pratik Gite** towards the computer education in 2012. He has completed his B.E. and M.E. from RGPV University Bhopal (M.P.). He holds a Ph.D. in Wireless Mobile Ad-hoc Network from Pacific Academy of Higher Education & Research University, Udaipur, Rajasthan. He started his academics at LKCT Indore (MP).

Dr. Pratik Gite has a passion for writing computer engineering books. He is an expert of various computer technologies. He has worked with many computer programming languages and open source technologies. His areas of interest include Mobile Ad-hoc Network, Software Engineering, Computer Network, Basic Computer Engineering and Information Technology. His current affiliation includes Asst. Prof. at IES-IPS Academy, Indore (M.P.). His contribution includes active participation in various research projects and research papers (IEEE). He can be reached at pratikgite135@gmail.com.

ACKNOWLEDGEMENTS

I am grateful to Dr. Sanjay Thakur, Principal, L.K.C.T. Indore, for his encouragement and suggestions in carrying out this book.

I am very much thankful to Dr. Archana Keerti Chowdhary, Principal, IES-IPS Academy Indore, for her continuous motivation and advice for this book. I would like to express my gratitude to Dr. Namrata Tapaswi, H.O.D., Computer Science and Engineering, IES-IPS Academy Indore, for her valuable comments and support. I express my sincere thanks to Dr. Ashish Moyade for their help throughout completion of this book.

I am very much thankful to my parents Mr. Rajendra Gite and Mrs. Sunita Gite for their personal attention and care. I am grateful to my Elder Brothers Mr. Sandeep Gite and Mr. Kapil Gite for inspiring me for this book. I want to thank my wife Mrs. Rajeshwari Gite for her patience and motivation.

I like to remember the motivation initiated by my respected Father in Law Mr. Rameshwar Tare and Mother in Law Anusuiaya Tare.

I wish to thank faculty members of CSE department of IES-IPS Academy, Indore for their constant co-operation, directly inspiration and encouragement.

I deeply express my heartful thanks to the VSRD Academic Publishing (A Division of Visual Soft India Private Limited) for publishing this book in such a beautiful getup and well in time.

✍ *Dr. Pratik Gite*

KEY FEATURES

- *Easy language used for better understanding.*
- *Key concepts are mentioned at the beginning of each chapter.*
- *Each chapter contains summary and review questions.*
- *Reader friendly presentation for easy grasp.*
- *Thoroughly discussed the important topics of Information Technology.*
- *List of definitions for better understanding of technical terms.*
- *Topics are covered with real life examples.*
- *Technical terms are explained with pictorial presentation and screen shots.*
- *Includes notes and remarks for quick review.*
- *Some important points to be remembered are mentioned separately.*

Dedicated to

My Parents,
Wife, Brothers, My Son
Shivay
&
All Students, Research
Scholars
and
Teachers

ABBREVIATION

IEEE	*Institute of Electrical and Electronics Engineers*
LAN	*Local Area Network*
MAC	*Media Access Control*
NAM	*Network Animation Model*
MANET	*Mobile Ad-hoc Network*
QoS	*Quality of Service*
RREQ	*Route Request*
RREP	*Route Reply*
TCP	*Transmission Control Protocol*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
AODV	*Ad-hoc On-demand Distance Vector Routing Protocol*
DSR	*Dynamic Source Routing*
TCL	*Tool Command Language*
NS-2	*Network Simulator*

DEFINITIONS

Ad-hoc Network: Ad-hoc Networks are basically self organizing, self configuring and peer to peer multi-hop mobile wireless networks where information packets are transmitted in a stored and forward manner via through the intermediate nodes.

Clustering: The clusters in the Ad-hoc networks are initially created when the eligible wireless nodes are discovering each other.

Wireless Sensor Network: A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions.

Routing: Routing is the way to find best suitable path from source to destination for packet forwarding from one end to another end.

Simulation: Simulation can be defined as "reproduction of essential features of something as an aid to study or training". In simulation, we can construct a mathematical model to reproduce the characteristics of a phenomenon, system or process often using a computer in order to get information or solve problems.

Network Simulator: Network Simulator (NS) is a discrete event and object oriented simulator targeted for networking researches. It provides substantial support for simulation of TCP, UDP, routing and multicast routing protocols over wired and wireless network [21]. NS-2 is written in C++ and Object Tool Command Language (OTCL) where C++ for data per packet events and OTCL are used for periodic or triggered event.

Tool Command Language: Tool Command Language (TCL) is a high-level interpreted scripting language which is basically useful for build the simulation scenario and configures the system.

Trace File Analysis: NS-2 simulation generates results in the form of trace files [21]. Trace file is the file which consists of the complete packet flow information of a network. It shows the complete packet flow information about the transmission related to packet Id, type of packet used etc.

Network Animator: Network Animator is used for the visualization of network topology. NS-2 includes a Network Animator called Network Animation Model (NAM) which draws a picture of the network topology and as the simulation time increases, the visual view of packets moving around the network can be seen

AWK Programming: AWK Programming is used for extracting data from a complex trace files and produces a well formatted data file in context of user point of view.

Throughput: It is the amount of data transferred over the period of time, measured in bytes/second or bits/second (bps).

Packet Delivery Ratio: It is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source node. It can be calculated in terms of percentage (%).

Routing Overheads: It is the total amount of control data packets generated by each routing protocols throughout the duration of simulation experiment .

Packet Dropped: The number of data packets that are not successfully sent to the destination. Basically it is define as the number of packets drop to the total number of packet generated during the simulation time. Lower the packet drop, lower would be the delay in the network [26].

Public Key Infrastructure: Public Key Infrastructure is a technology used in modern security mechanisms on the internet. It covers a cryptographic system including encryption, asymmetric key cryptography, message digest and digital signature.

Cryptography: Art and science of achieving security by encoding messages to make them non-readable is known as cryptography.

Cryptanalysis: The technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

Cryptology: A combination of cryptography and cryptanalysis is known as cryptology.

Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text or clear text.

Cipher text: When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.

Encryption Algorithm: Step by step procedure to convert plaintext into cipher text and vice versa is known as encryption algorithm.

Key: Stream of bit used in cryptographic algorithm for encryption and decryption is called as a key.

Encryption: The process of encoding plain text message into cipher text message is called as encryption.

Decryption: The process of decoding cipher text message into plain text message is called decryption.

Brute force attack: Brute force attack is a method of defeating a cryptographic scheme by trying a large or all possible number of

possibilities.

Symmetric Key Cryptography: In Symmetric Key Cryptography, only one key (same key) is used for both encryption and decryption. Both the parties (sender and receiver) agree upon the key before any transmission begins.

Asymmetric Key Cryptography: It Asymmetric Key Cryptography, a key pair (Two different Keys), is used i.e. one key is used for encryption and only the other corresponding key is used for decryption.

Threat: Any potential event or act that could cause injury to employee or assets.

Risk: The chance of a vulnerability being exploited.

Vulnerability: A cause to security that could permit a threat to make injury.

Digital Signature: A digital signature is used to authenticate the sender of the message and to check the integrity of the message, i.e. that it has not been altered in transit.

Digital Certificate: Digital certificate is a document such as our passport or driving license. It is basically a computer file such as ABC.cer and is certified by a trusted agency called certification Authority (CA).

Secure Socket Layer (SSL): It is an internet protocol used for exchange of information between browser & server developed by Netscape Corporation.

Secure Electronic Transaction (SET): The Secure Electronic Transaction (SET) is an open encryption and security specification that is designed for protecting credit card transactions on the Internet.

Cyber Law: Cyber Law is the law governing computers and the Internet.

Cyber stalking: Cyber stalking is a criminal offense with use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization.

Defamation: The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person.

Hacking: Hacking is the practice of modifying the features of a computer system, in order to accomplish a goal outside of the creator's original purpose.

Hacker: A hacker is a person who tries to gain un-authorized access to your computer.

Cracker: A hacker expert at accessing password-protected computers, files, and networks is known as "crackers."

Spam: Spam is any kind of unwanted email sent in bulk by companies

Information theft: Information theft or identity theft is a crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity in order to make transactions or purchases.

Denial of Service (DoS): An attack, in which an attacker attempts to prevent legitimate users from accessing information or services, is known as Denial of Service attack.

Logic Bomb: Logic bomb is a malware that is triggered by a response to an event, such as launching an application or when a specific date/time is reached.

Passive Attack: A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it.

Active Attack: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks.

External Attack: External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

Internal Attacks: Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult

CONTENTS