INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Google Scholar, Indian Citation Index (ICI), J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 (2012) & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **5833 Cities** in **193 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to the recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript titled '_____' for likely publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published anywhere in any language fully or partly, nor it is under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to inclusion of their names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation/Post*	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

* i.e. Alumnus (Male Alumni), Alumna (Female Alumni), Student, Research Scholar (M. Phil), Research Scholar (Ph. D.), JRF, Research Assistant, Assistant Lecturer, Lecturer, Senior Lecturer, Junior Assistant Professor, Assistant Professor, Senior Assistant Professor, Co-ordinator, Reader, Associate Professor, Professor, Head, Vice-Principal, Dy. Director, Principal, Director, Dean, President, Vice Chancellor, Industry Designation **etc**. ***The qualification of author is not acceptable for the purpose***.

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of the mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) Only the **Abstract will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty-four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of the manuscript, within two days of its submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except on the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be typed in **bold letters**, **centered** and **fully capitalised**.
3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.
4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.
5. **ABSTRACT:** Abstract should be in **fully Italic printing**, ranging between **150** to **300 words**. The abstract must be informative and elucidating the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.
6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations etc.
7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aea-web.org/econlit/jelCodes.php. However, mentioning of JEL Code is not mandatory.
8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical***, ***spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.
9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.
11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably be in ***2000 to 5000 WORDS***, But the limits can vary depending on the nature of the manuscript.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self-explained, and the **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, left aligned with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word may be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section e.g. Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they may follow Harvard Style of Referencing. **Also check to ensure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc., in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italic printing. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders before the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SURVEY ON DIFFERENT TECHNIQUE FOR DETECTION AND RECOVERY OF MISBEHAVING NODE IN MANET

M.SUMATHI
RESEARCH SCHOLAR
PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE
GOVERNMENT ARTS COLLEGE
DHARMAPURI

Dr. M. GUNASEKARAN
HEAD
PG & RESEARCH DEPARTMENT OF COMPUTER SCIENCE
GOVERNMENT ARTS COLLEGE
DHARMAPURI

ABSTRACT

A Self-ruling collection of mobile nodes communicating with each other with the help of wireless links either in a direct or indirect manner or rely on other mobile nodes is referred as MANET. The communication link may have some trouble conducted by the misbehaving nodes. Misbehaving nodes may degrade the performance of the overall network. In this paper, we studied the common communication routing protocols in MANET and detection techniques. As from the study, some of the nodes available in the communication link and refused to cooperate in packet transmission are called selfish nodes. A selfish node may give priority to battery power saving.

KEYWORDS

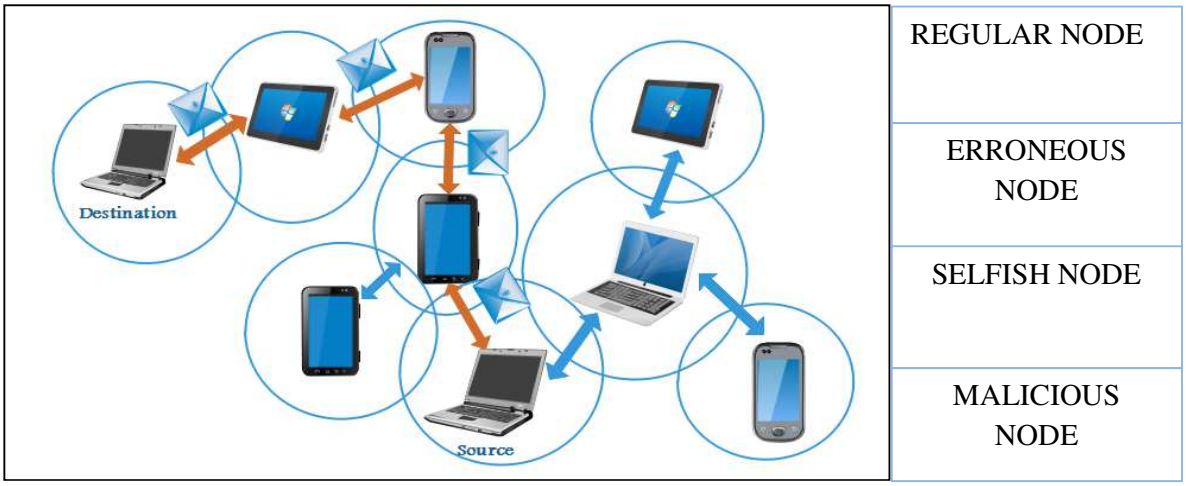
MANET, ad-hoc network, routing protocols, misbehavior detection.

1. INTRODUCTION

Mobile Ad-hoc network is a network which includes mobile nodes (laptop, personal digital Assistants (PDAs) and wireless phones) with the uniqueness of self-organization and self-configuration which allow it to form a new network quickly. [1] A node may be capable of communicate with other nodes far away with the teamwork of intermediate nodes, forwarding the packets to the destination. In this multi-hop communication, each node acts as both host and router.

A variety of literature investigated that MANET possesses 4 kinds of nodes viz. i) regular node, ii) erroneous node, iii) selfish node, and iv) malicious node. A regular node is the one which is paying attention to set up communication with any other node for the purpose of forwarding a data packet. Erroneous node is the one with circuitry issues and faulty hardware design that potentially poses as a trouble for security protocols as well as for permitting reliable communication. While selfish node has a tendency to refuse to onward the data packet to the destined nodes in order to shop its resources, at the same time as malicious nodes usually keep dangerous intention to disrupt the traffic and steal the exclusive information. Fig 1. Suggests the communication model and node classification in MANET. [2]

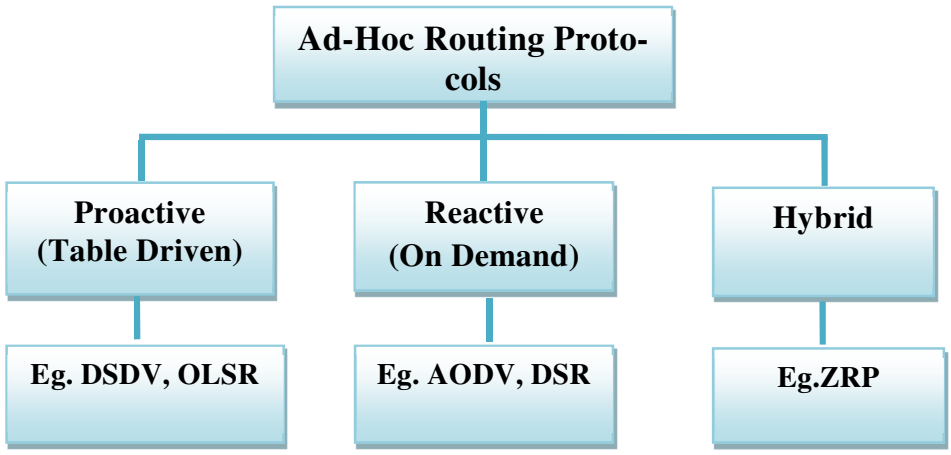
FIG. 1: TYPES OF NODES IN MANET



2. STUDY ON AD-HOC ROUTING PROTOCOLS

The routing protocols are of these categories, which include proactive routing protocols, reactive routing protocols and hybrid routing protocols with respect to the routing topology used in MANET. The below Fig.2 mentions the primary classification of Ad-hoc Routing Protocol with examples. [3]

FIG 2. ROUTING PROTOCOLS



2.1 Proactive (Table Driven) Protocols

In table-driven routing protocols, each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network.

2.1.1 (DSDV) Protocol

In this protocol, every mobile node within the network maintains a routing table listing all other nodes it has known both directly and through some neighbors. Each node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. In conjunction with those details, the table also maintains track of the subsequent hop neighbor to reach the destination node. The main contribution of the algorithm was to solve the routing loop trouble. [4]

2.1.2 (OLSR) Routing Protocol

OLSR is the table driven, proactive routing protocol designed for mobile ad-hoc networks. It exchanges routing information periodically and has path immediately available while wished. The OLSR protocol achieves optimization by way of determining for each node of the network a minimum subset of neighbors, referred to as Multi Point Relays (MPR) which is able to reach all 2-hop neighbors of the node. Usually, two kinds of routing messages are used a hello message and a Topology control (TC) message. Hello, messages are exchanged locally through neighbor nodes and aren't forwarded further to different nodes. In OLSR, only MPR nodes are answerable for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, every node can examine the partial network topology and can build a route to each node within the network. This message is used for route calculation.

Ex: Proposed SR-OLSR protocol was able to detect numerous attacks and mitigate the identical without affecting the best of service (QoS).

2.2 Reactive (On-demand) Protocols

These protocols take a lazy method to routing. The assessment of table-driven routing protocols, no longer all routes are maintained at each node as an alternative, the routes are created as and whilst required. While a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid until the destination is reachable or until the route is no longer wished

2.2.1 Ad-Hoc On-demand Distance Vector (AODV)

AODV makes use of sequence numbers and routing beacons from DSDV but plays route discovery by the usage of on-demand route requests (RREQ); the same method as the DSR protocol. AODV is distinct to DSR in that it makes use of distance vector routing; this requires each node within the route to holding a temporary routing table for the duration of the communication. AODV has improved upon the DSR route request process the usage of an expanding ring search mechanism based upon incrementing time-to-live (TTL) up prevent immoderate RREQ flooding. Nodes inside an active route record the sender's address, sequence numbers and source/destination IP address within their routing tables, this information is utilized by route reply (RREP) updated construct opposite paths. AODV deals with node mobility the usage of sequence numbers up to date identify and discard outdated routes, this is blended with route errors (RERR) messages which can be sent while damaged links are detected, RERR packets travel up upstream updated the source informing nodes up to date delete the damaged links and trigger new route discovery if alternative routes aren't up-to-date.

2.2.2 Dynamic Source Routing (DSR)

The reactive DSR Protocol turned in up updated advanced via operation of the DSR protocol is damaged in up stages; route discovery phase and route maintenance phase, these phases are triggered on demand while a packet wishes to route. Route discovery phase floods the network with route requests if a suitable route is not available up on the route. DSR makes use of a source routing method up-to-date generate a complete route to the destination, this could then be updated temporarily in nodes route cache. DSR addresses mobility troubles through using packet acknowledgments; failure up to date receive an acknowledgment causes packets up to date be buffered and route error messages to be sent to all upstream nodes. Route error messages cause the route maintenance phase which removes wrong routes from the route cache and undertakes a new route discovery segment.

2.3 Hybrid Protocols

Hybrid routing is a mixture of the Proactive and Reactive routing protocol.

2.3.1 ZRP (zone routing protocol)

The zone Routing Protocol (ZRP) describes that takes gain of this truth and divides the entire network into overlapping zones of variable size. It makes use of proactive protocols for locating region neighbors (right away sending hello messages) as well as reactive protocols for routing functions among distinctive zones (a route is only established if wanted). Every node may additionally define its personal zone length, whereby the zone size is defined as the wide variety of hops to the zone perimeter. As an instance, the zone length may additionally depend upon signal strength, to be had power, a reliability of various nodes and so on. Even as ZRP isn't a very distinct protocol, it affords a framework for other protocols. To begin with, a node needs to find out its neighborhood which will be capable of building a zone and determine the perimeter nodes. [4]

3. EMPIRICAL STUDY ON MISBEHAVING NODES

Those nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy along with CPU strength, battery and additionally bandwidth for retransmitting the data of other nodes and they reserve them only for themselves. The original AODV and DSR routing algorithms can be changed to detect such selfish nodes. [5]

3.1 Node Misbehavior

A node is marked as a misbehaving node when it avails from the network but it refuses to collaborate due to some motives. Those motives can be categorized into two primary kinds: honest and malicious reasons. The honest reasons are associated with collisions, channel errors and buffer overflow, even as the black hole, wormhole, and collision attacks are examples of the malicious attack. Such misbehaving movements bring about low packet delivery ratio and high packet delivery time, which in turn affects the overall performance of the MANET. Misbehaving nodes have 3 exclusive activities, which might be all described as misbehaving

actions. Inside the first type, the node participates with network's nodes in routing discovery and maintenance operation, but, it refuses to forward the data packet. in the second type, the node does not make a contribution in both the routing lookup and data packet transmission. When the nodes switch its behaviors among the primary and second types, the third kind of misbehaving moves is presented. "Misbehavior" refers to a node that doesn't behave in a proper way and has an unusual behavior. In other phrases, if the behavior of node deviates from its specification or set of behaviors than the node is stated to be misbehaving [6]. Misbehavior takes place in following approaches:

- Delay Packets
- Drop Acknowledgements
- Delay Acknowledgements
- Drop packets and alter routing information
- Don't forward packet to keep its own resources
- Forward control packets while losing data packets. There can be numerous types of misbehavior. Some of them are indexed underneath:

➢ **Failed / Malfunctioned:** A node malfunctions due to hardware and software program problems, weather, radio channel, link breakdown, unintentional physical harm.

➢ **Selfish:** selfish nodes have passive misbehavior. It does not intend to without delay damage other nodes and does not cooperate. It saves battery life for very own communication. A selfish node is unwilling to spend CPU cycles and to be had network bandwidth to forward packets.

➢ **Malicious:** Malicious nodes have active misbehavior. It deliberately damages other nodes and interrupts network operations. A malicious node may drop the packets, modify the routing information. it is able to deliver priority to battery power saving.[7]

4. COMPARATIVE STUDY ON VARIOUS ALGORITHMS FOR DETECTING MISBEHAVIOR

1. Reputation-based selfishness prevention techniques for mobile ad-hoc networks

Alberto Rodriguez-Mayol et.al., [8] proposed a three detection approach that improves the ability of selfishness prevention protocol to discover selfish nodes and to increase the variety of valid routes. Those three techniques are RAM (Reset Activity Mode), WM (warming mode) & RFM (reset failure mode).The research of proposed strategies is applied with team & Marti's protocol.

2. Detection & REAction to timeout MAC layer Misbehavior (DREAM)

Lei Guang, Chadi Assi et.al., [9] proposed mechanism that identifies the malicious nodes the use of a set of monitoring and reaction techniques. It makes use of stage reaction, the primary stage is for reaction and the second degree is of punishment that could improve the network overall performance. This gadget gives the excessive accuracy in identifying misbehaved nodes. The first reaction system is very powerful to mitigate the misbehaving impact and enhance network overall performance.

3. Watch dog/ Pathrater method

Kachirski O et.al., [10] the method identifies misbehaving node through eavesdropping at the transmission of the subsequent hop. Whilst a node forwards packets, Watchdog verifies whether the subsequent node within the route forwards the packets or not. If the subsequent node refuses to forward the packets, then it is referred to as misbehavior. The advantages of Watchdog mechanism is that it may discover misbehaving nodes not in forwarding level but also in the level of connection. In other phrases, it identifies nodes no longer only in the link layer but additionally inside the network layer. Implementation of Watchdog is especially easy. Kachirski O et al., proposed the technique calculates "path metric" for every path. Like Watchdog, each node runs Pathrater. The node maintains a degree of other nodes identified in the network. The path metric which is collected from past experience can be calculated by combining the node rating with link reliability. After calculating the path metric for all reachable paths, the path with the highest metric can be chosen by the pathrater.

4. Ex.Watchdog Technique

Nasser and Chen et.al., [11] proposed techniques to identify IDS called Ex.Watchdog which is actually an extension of Watchdog. It also detects intrusion from malicious nodes and reports this data to the response system. The main feature of the proposed system is the ability to detect malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then it proceeds to protect the network. So, Ex.Watchdog solves the fatal problem of Watchdog.

5. Record and Trust-Based Detection (RTBD) Technique

Senthil Kumar Subramanian et.al., [12] proposed a technique in which every node maintains global trust state for all nodes which is recorded in trust table. The selfish nodes are detected based on their trust value and predefined threshold for selfishness, their neighbors can use this information to avoid working with them, either for data forwarding, data aggregation, or any other cooperative function

6. Cooperative Bait Detection Scheme (CBDS)

In Jian-Ming Chang et.al., [13] proposed Cooperative Bait Detection Scheme (CBDS) which is able to detect and prevent malicious nodes launching cooperative black hole attacks. It integrates with the proactive and reactive defense architectures and the source node randomly cooperates with a stochastic adjacent node.

7. Token-Based Umpiring Technique (TBUT)

Jeba Kumar Mohan Singh Pappaji Josh Kumar et.al., [14] proposed a unified approach for detecting and elimination selfish nodes in MANETs using TBUT. It is the token based umpiring technique where every node needs a token to participate in the network and the neighboring nodes act as an umpire. Umpire nodes will monitor the behavior of the nodes and detect if any node is misbehaving. It is very efficient with reduced detection time and less overhead.

8. Secure Objective Reputation-based Incentive (SORI) scheme

Qu He et.al., [15] present a Secure Objective Reputation-based Incentive (SORI) scheme to encourage packet forwarding and discipline selfish nodes. This scheme consists of three components. First, neighbor monitoring component monitors packet forwarding behavior of the neighbor nodes and a Neighbor Node List (NNL) which consists of details for all the neighbors of a node is maintained by each node. Second Reputation Propagation is built a record of reputation by using the NNL and shared this reputation with all nodes to identify the selfish node. Finally, a punishment scheme is used by punishment component to penalize selfish nodes. The unique feature of this scheme is that.

9. TWO ACK and S-TWO ACK schemes

Kashyap Balakrishnan et.al., [16] TWOACK and S-TWOACK, which can be easily added-on to source routing protocols such as the DSR protocol. The schemes detect selfish nodes (links) so that other nodes may avoid them in future route selections, with the aim of overall improvement in end-to-end packet delivery ratio.

10. Observation-based Cooperation Enforcement (OCEAN) scheme

Bansal et.al., [17] OCEAN scheme for malicious node detection that is based on direct observations. In which rating of the node is depend on the behavior of the node. If the node behavior is positive then the rating of the node increased otherwise if the observed behavior is negative the rating of a node is decreased by more value than that is used for increment. If the rating of a node decreases beyond faulty threshold then it is added to the faulty list. This list is broadcasting to be used as the list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on the faulty list or not. Also used a chance mechanism which removes the node from the faulty list after an idle period with its rating remaining unchanged.

11. A Collaborative selfish node detection and incentive mechanism for opportunistic networks (SENSE) technique

Ciobanu et.al., [18] proposed SENSE that provides the selfish node detection by using community-based and context-based information of node. By using intensive mechanism it will appreciate the node to participate in the network. Use the altruism value to get the selfishness of node. It uses the home-cell community model for mobility model.

12. Fully Selfish Node Detection, Deletion and Secure Replica Allocation over MANET

N.Muthumalathi et.al., [19] proposed a selfish node detection method and novel replica allocation techniques to handle the selfish replica allocation appropriately. Selfish replica allocation technique reduces communication cost and secure hill cipher algorithm to provide security in replica data.

13. New Replication allocation technique

N.R.Suganya et.al., [20] proposed selfish node detection method and novel replica allocation techniques handle the selfish replica allocation properly. In our method the each node computes credit risk information on other associated nodes individually to appraise the degree of selfishness.

14. A novel technique for tracing the malicious nodes in the mobile ad-hoc network based on noise errors in different frequency bandwidths

Karjee, J et.al., [21] proposed a scanning procedure and security measures for the multi- hop wireless network after diagnosing the abnormal behavior of malicious node and verifying the physical presence of attack strategy in the wireless network. The model has not been validated for major routing issues like interference, asymmetric links channel capacity and effects of noise, etc. have not been taken into account. Furthermore, the work seems to be done on the assumption that selfish nodes never exist in MANET system.

15. Enhanced Adaptive Acknowledgement (EAACK)

K.Chinthanai chelvan et.al., [22] proposed EAACK (Enhanced Adaptive Acknowledgement) method designed for MANET was proposed for intrusion detection. EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.

TABLE 1: COMPARATIVE STUDY ON MISBEHAVIOR DETECTION ALGORITHMS

Misbehavior Detection Techniques / Misbehaviors	Authors	Proposal	Result
1. Reputation-based selfishness prevention techniques for mobile ad-hoc networks (Selfishness)	Alberto Rodriguez-Mayol&J. Gozalvez,	Three detection techniques, RAM (reset activity mode), WM (warming mode) & RFM (reset failure mode) may use to improve the ability of selfishness prevention protocol to detect selfish nodes and to increase the number of valid routes.	• Reduce the no of incorrect selfish accusations, • Increase the availability of safe multi-hop routes • Improving the final packet delivery ratio
2. DREAM-Detection & Reaction to Timeout MAC layer Misbehavior (Malicious Behavior)	Lei Guang, ChadiAssi, &Yinghua Ye	A Proposed mechanism that identifies the malicious nodes using a set of monitoring and reaction procedures.	• Achieves high accuracy in identifying misbehaved nodes. • First reaction system is very effective in mitigating the misbehavior effect and improve the network performance (e.g., throughput and delays)
3. Watch dog/ Pathrater Technique (Malicious Behavior)	Sergio Marti, T.J. Giuli, Kevin Lai, & Mary Baker	Watchdog technique to detects malicious node by overhearing next node's transmission. Pathrater helps to route protocols to avoid these nodes.	• Increase throughput by 17% in a network with moderate mobility, • Increases the ratio of overhead transmissions to data transmissions from the standard routing protocol's 9% to 17%. • Watchdog and pathrater can increase network throughput by 27%, • Improves the percentage of overhead transmissions from 12% to 24%.
4. Ex. Watchdog Technique (Malicious Behavior)	N. Nasser, & Yunfeng Chen	Ex-Watchdog intrusion detection system is an extension of Watchdog System whose function is to detect intrusion from malicious nodes and reports this information to the response system.	• Decreases the overhead greatly, • It does not increase the throughput obviously
5. RTDB: Record and Trust-Based Detection Technique (Selfishness)	Senthilkumar Subramaniyan, William Johnson,&KarthikeyanSubramaniyan	The selfish no desire detected based on their trust value and the predefined threshold for selfishness, their neighbors can use this information to avoid working with them, either for data forwarding, data aggregation, or any other cooperative function.	• Enhances the performance of MANET. • It improves the PDR and detection ratio. • It diminishes the overhead, latency, and packet dropping ratio. • Competently detects the selfish nodes in MANET
6. Cooperative Bait Detection Scheme (CBDS) (Malicious Behavior)	Jian-Ming Chang, Po-Chun TsouHan-Chieh Chao,&Han-Chieh Chao	Cooperative Bait Detection Scheme (CBDS) which is able to detect and prevent malicious nodes launching cooperative black hole attacks.	• CBDS presents good performance better packet delivery ratio • Not much overhead to network overhead under malicious node attack.
7. TBUT (Token-based umpiring technique) (Selfishness)	Jebakumar Mohan Singh PappajiJosh Kumar,AyyaswamyKathirvel, NamaskaramKirubakaran, PerumalSivaraman&MuthusamySubramaniam	A unified approach for detecting and elimination selfish nodes in MANETs using TBUT. it is the token based umpiring technique where every node needs a token to participate in the network and the neighboring nodes act as an umpire.	• To evaluate the performance of TBUT in the presence of 30% selfish nodes and have compared it with ETUS routing protocols. • TBUT significantly improves the performance of ETUS in all metrics, packet delivery ratio, and control overhead.
8. Secure Objective Reputation-based Incentive (SORI) scheme(Selfishness)	Qi He, Dapeng Wu & Pradeep Khosla	A (SORI) scheme to encourage packet forwarding and discipline selfish nodes	• Successfully identifies the selfish nodes and punish them accordingly.
9. TWO ACK / S-TWO ACK Scheme (Selfishness)	KashyapBalakrishnan, Jing Deng, Pramod & K. Varshney	The schemes detect selfish nodes (links) so that other node may avoid them in future route selections, with the aim of overall improvement in end-to-end packet delivery ratio.	• TWOACK scheme improves the end to-end packet delivery ratio from around 70% to almost 90% while increasing the overhead 4% to 7%. • S-TWOACK scheme, which is a derivative of the TWOACK scheme, achieves almost the same performance improvement.
10. Observation-based Cooperation Enforcement scheme (Selfishness)	Sorav Bansal & Mary Baker	OCEAN attempts to mitigate selfish routing behavior in ad hoc networks. The general idea is to punish nodes for their selfish behavior, by rejecting their traffic, in the hopes that this threat will act as a deterrent.	• Compared to such reputation schemes, OCEAN is more sensitive to the tuning of some parameters, • it fails to punish misbehaving nodes as severely, it performs almost as well, and sometimes even better, across a wide range of degrees of mobility

11. A Collaborative selfish node detection and incentive mechanism for opportunistic networks (SENSE)(Selfishness)	Ciobanu, Radu-Ioan, Ciprian Dobre, Mihai Dascălu, Ştefan Trăuşan-Matu, & Valentin Cristea.	SENSE that provides the selfish node detection by using community- based and context- based information of the node.	• Use the unselfishness value to get the selfishness of node. • It uses the home-cell community model for mobility model.
12. Fully Selfish Node Detection, Deletion and Secure Replica Allocation over MANET (Selfishness)	Muthumalathi & Dr.M.Mohamed Raseen,	An approach which stated that Selfish node may not share its memory space to store a copy for the profits of other nodes.	• Every node count credit risk information on another node individually to measure the amount of selfishness. • Selfish allocation schemes reduce communication cost and secure hill cipher algorithm to provide security in replica data.
13. New replication allocation technique (Selfishness)	N.R.Suganya, & S.Madhu Priya	Observe the impact of selfish nodes in a mobile ad hoc network which is termed as selfish replica allocation.	• Selfish node detection method and novel replica allocation techniques handle the selfish replica allocation properly.
14. A novel technique for tracing the malicious nodes in the mobile ad-hoc network based on noise errors in different frequency bandwidths. (Malicious Behavior)	Karjee & Banerjee,	Investigation and Mathematical analysis based upon the detection of a malicious node with attack modeling.	• Diagnosing the abnormal behavior of malicious node • Verifying the physical presence of attack strategy in the wireless network.
15. Enhanced Adaptive Acknowledgement (EAACK) method (Malicious Behaviour)	K.Chinthanaichelvan, T.Sangeetha, V.Prabakaran,&D.Saravanan	EAACK demonstrates higher malicious-behavior-detection rates in certain circumstances while does not greatly affect the network performances.	• Positive performance against Watchdog in the cases of receiver collision and false misbehavior report has been demonstrated

From the above Table.1, we examine which type of algorithms handling which type of misbehavior in MANET, accomplished that the MANET nodes most commonly behaves like Selfish nodes.

5. CONCLUSION

Now a day's, researcher's consideration on MANET, due to their open medium and wide distribution of nodes make MANET vulnerable to misbehavior issues. Misbehaviors of nodes are classified primarily as selfish nodes and malicious nodes. In this paper, we have analyzed the most common MANET routing protocols, misbehaviors of a MANET nodes and detection techniques that involved in misbehaving node detection. Hence I concluded that the most common problem in MANET is a selfish node. The Selfish behavior of a node affects the throughput of the network.

REFERENCES

1. Sagar Padiya, Rakesh Pandit and Sachin Patel, "Survey of Innovated Techniques to Detect Selfish Nodes In MANET" (IJCNWMC) Vol.3, Issue1, Mar 2013, pp221-230
2. Burhan U1 Islam Khan, Rashidah F. Olanrewaju, Farhat Anwar and Asadullah Shah, "Manifestation and Mitigation of Node Misbehavior In Ad-hoc Networks", WULFENIA Journal Klagenfurt, Austria Volume 2, No.3: Mar -2014
3. Manoj Kumar Khinchi, Dr. Bharat Bhushan, "Investigation on MANET Routing Protocols and Quality of Services Management Issues", International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 04 | Apr-2016
4. Anto Ramya. S. I, "Destination Sequenced – Distance Vector Algorithm" International Journal of Computer Science and Engineering (IJCSE), Nov-2015
5. Lilu Odedra, Ashish Revar, and Munindra H. Lunagaria, "Detection and Prevention of Selfish Attack in MANET using Dynamic Learning" IOSR Journal of Computer Engineering (IOSR-JCE), Volume 18, Issue 3, Ver. V May-Jun- 2016, PP 54-61
6. Farid Bin Beshr, Ahmed Bin Ishaq, Saeed Aljabri, and Tarek R. Sheltami, "A Guard Node (GN) based Technique against Misbehaving Nodes in MANET" Journal of Ubiquitous Systems & Pervasive Networks, Journal of Ubiquitous Systems & Pervasive Networks Volume 7, No. 1 2016 pp. 13-17
7. Lilu Odedra, Ashish Revar, and Munindra H. Lunagaria, "Comparative Analysis of Prevention and Detection Policies for Selfish Behaviour in MANET" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February- 2016
8. Alberto Rodriguez-Mayol, J. Gozalvez, "Reputation-based selfishness prevention techniques for mobile ad-hoc networks." Telecommunication Systems 57, no. 2 2014
9. Lei Guang, Chadi Assi, Yinghua Ye, "DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks." Computer communications 2007
10. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Proceedings of the 6th Annual International Conference, August- 2000.
11. Nasser.N, Yunfeng Chen, "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network", in ICC 2007
12. Senthi kumar Subramaniyan, William Johnson, Karthikeyan Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique", EURASIP Journal on Wireless Communications and Networking 2014.
13. Jian-Ming Chang, Po-Chun Tsou Han-Chieh Chao, Han-Chieh Chao, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture," IEEE 2011.
14. Jebakumar Mohan Singh Pappaji Josh Kumar, Ayyaswamy Kathirvel, Namaskaram Kirubakaran, Perumal Sivaraman and Muthusamy Subramaniam, "A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT", EURASIP Journal on Wireless Communications and Networking, 2015.
15. Qi He, Dapeng Wu,Pradeep Khosla, "SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks", ResearchGate, April-2004.
16. Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", IEEE 2005.
17. Sora Bansal, Mary Baker, "OCEAN: Observation based cooperation enforcement in ad hoc networks", Technical Report, Stanford University, July-2003.
18. Ciobanu, Radu-Ioan, Ciprian Dobre, Mihai Dascălu, Ştefan Trăuşan-Matu, and Valentin Cristea, "SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks." Journal of Network and Computer Applications 41 (2014): 240-249
19. Muthumalathi.N, Mohamed Raseen.M, "Fully Selfish Node Detection, Deletion And Secure Replica Allocation Over Manet", International Conference on Current Trends in Engineering and Technology, ICCTET'13,July-2013.
20. Suganya.N.R, Madhu.S Priya, "Detecting Selfish Nodes in a MANET through Fragmentation in Distributed Environment", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, No 6, June-2013
21. Karjee and Banerjee, "Tracing the abnormal behavior of malicious nodes in MANET. In Wireless Communications, Networking and Mobile Computing", WiCOM'08. 4th International Conference on (pp. 1-7). IEEE. October- 2008
22. Chinthanai Chelvan.K, Sangeetha.T, Prabakaran.V, Saravanan.D, "EAACK-A Secure Intrusion Detection System for MANET", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2014

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue, as well as on the journal as a whole, on our e-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our e-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward to an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals