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, Open 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 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **4767 Cities** in **180 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We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications;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 entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it 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 their inclusion of 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	:
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	:

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 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) **Abstract alone 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 manuscript, within two days of 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 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 **bold typed**, **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 italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain 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.
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 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 range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **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, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should 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: 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 are supposed to follow Harvard Style of Referencing. **Also check to make sure 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 italics. 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 after 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

A SURVEY ON TRUSTBASED SECURE AODV IN MANET: A LITERATURE REVIEW

V.VALLINAYAGI
HEAD
DEPARTMENT OF COMPUTER SCIENCE
SRI SARADA COLLEGE FOR WOMEN
TIRUNELVELI

ABSTRACT

A mobile Adhoc network is a collection of wireless mobile nodes forming a temporary network without using any centralized access points, infrastructure or centralized Administration. Data transmission between the two nodes in Manet may require multiple hops as Nodes transmission range is limited. Mobility of the different nodes makes the situation even more Complicated. These nodes are often vulnerable to failure thus making mobile adhoc networks Open to threats and attacks. Routing is always the most significant part for any network. One way is to transplant ordinary mechanisms in common networks with some improvement While the other way is to find some other factors such as trust to achieve the objective. This paper gives you a survey on trust in manet.

KEYWORDS

aodv, manet, network, trustbased, simulation, routing.

1. INTRODUCTION

In Aodv the network is silent until connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message and record the node that they heard it from creating an explosion of temporary routes back to the needy node. When a node receives such message and already has a route to the needy node. it sends a message backwards through a temporary route to a requesting node. The needy node then begins using the route that has the least number of hops through other nodes unused entries in the routing tables are recycled after time. When a link fails a routing Error is passed back to a transmitting node and the process repeats.

Much of the complexity of the protocol is to lower the number of message to conserve the capacity of the network. For example, each request for a route has sequence number nodes use this sequence numbers so they do not repeat route request that they have already passed on. Another such feature is that if a route request has time to live number that limits how many times they can transmitted. Another such feature is that if a route request fails another route request may not be send until twice as much time has passed as the timeout of the previous route request. The advantage of AODV is that it creates no extra traffic for communication along existing links. Also distance vectors routing is simple and does not require much memory to calculation. However, AODV requires more time to establish a connection and the initial communication a to establish a connector and the initial communication to establish a route is heavier than some other approaches.

2. WHAT IS TRUST?

As an important concept in network security, trust is interpreted as a set of relations among agents participating in the network activities. These relations are founded on the proof generated by the prior interactions of entities in a protocol. As a general rule if these interactions have been true to the protocol, then trust will accumulate between these entities. Trust has also been defined as the degree of belief about the behavior of other entities (or agents). Establishing trust relationships among participating nodes is vital to facilitate collaborative optimization of system metrics. Trust and security are two tightly interdependent concepts that cannot be desegregated. For example, cryptography is a means to implement security but it is highly dependent on trusted key exchange. Similarly, trusted key exchange cannot take place without requisite security services in place. It is because of this inter-reliance that both these terms are used interchangeably when Defining a secure system.

2.1 PROPERTIES OF TRUST

In the context of a social network viewpoint, there are three main properties of trust: transitivity, asymmetry, and personalization. Firstly, trust is not perfectly transitive in a mathematical sense i.e., if A trusts B, and B trusts C, it does not guarantee that A trusts C. Secondly, trust is not essentially symmetric which means that it is not identical in both directions. A classic case of asymmetry of trust can be observed in the relations between supervisors and employees. Thirdly, trust is Intrinsically an individual outlook. For example, a particular entity will be contrarily evaluated by two people.

2.2 CHARACTERISTICS OF TRUST IN MANETs

In MANETs, the theory of trust is to be defined with caution because of the distinctive features of MANETs and the intrinsic fickleness of the wireless medium. The main characteristics of trust in MANETs are given below:

1. The existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed. Therefore, a decision method to determine trust against an entity should be wholly distributed.
2. Trust should be gauged without too much computation and communication load in a very customizable manner, while also capturing the complexities of the trust relationship.
3. A trust decision framework should not work under the assumption that all nodes are cooperative for MANETs. In an environment that is restricted of resources, selfishness is prone to be rampant over collaboration. For example, to save battery life or computational power.
4. Trust is not static, it is dynamic.
5. Trust is subjective.
6. Trust is not inevitably transitive. The fact that A trusts B and B trusts C does not mean that A trusts C.
7. Trust is asymmetric and not essentially reciprocal.
8. Trust is dependent on context. A could trust B as a wine expert but not as a car fixer. Likewise, in MANETs, if a specific task entails high computational power, a node with high computational power is considered as trusted; while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

2.3 SECURITY FLAWS OF AODV

Malicious nodes can perform many attacks just by not following AODV rules since AODV has no security mechanisms.

A malicious node M can carry out the following attacks (among many others) against AODV:

1. Impersonate a node S by forging a RREQ with its address as the originator address.
2. When forwarding a RREQ generated by S to discover a route to D, decrease the hop count field to increase the chances of being in the route path between S and D so it can evaluate the communication between them. A variation of this is to increment the destination sequence number to make the other nodes assume that this is a 'fresher' route.
3. Impersonate a node D by forging a RREP with its address as a destination address.
4. Impersonate a node by forging a RREP that claims that the node is the destination and, to add to the impact of the attack, claims to be a network leader of the subnet SN with a big sequence number and send it to its neighbors. Thus it will become (at least locally) a black hole for the whole subnet SN.
5. By not forward certain RREQs and RREPs selectively, not responding to certain RREPs and not forwarding certain data messages. This kind of attack is particularly hard to even detect because transmission errors have similar effect.

6. Forge an RERR message by pretending it as the node S and sending it to its neighbor D. The RERR message has a very high destination sequence number dsn for one of the remote destinations (U). This might cause D to update the destination sequence number corresponding to U with the value dsn and, therefore, future route discoveries performed by D to take a route to U will fail (because U's destination sequence number will be much smaller than the one stored in D's routing table).
7. In accordance with the existing AODV draft, the originator of a RREQ can put a much bigger destination sequence number than the actual one. Additionally, sequence numbers wraparound when arriving at the maximum permissible field size value. This facilitates a very easy attack in where an attacker is able to set the sequence number of a node to any desired value by just sending Two RREQ messages to the node.

3. LITERATURE REVIEW

TRUST BASED SECURE AODV IN MANET

The performance of Adhoc on demand vector protocols has been modified by including the source route accumulation feature. The node may assist and trust each other in forwarding packets from one node to other. However, this implied trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. Trusted on this trust model we design trusted routing protocols using trusted frameworks and intrusion detection system.We extend the routing table and routing messages of AODV with trust information which can be updated directly through monitoring in the neighbourhood, so the computation is reduced and trustworthiness of the routing procedure can be guaranteed as well. Through simulation we can see that the bud nodes are clearly separated from the good nodes. The performance of AODV and TAODV under different environments were achieved.

ST-AODV QOS ASSERTION MANET ROUTING BASED ON THE TRUSTED AODV

In this paper a trusted ST_AODV protocol is proposed that identifies the nodes that drops packets during data transmission. Trust value for each node is calculated to spot the untrustworthy nods in the path during routing. A node is declared as a trustworthy node if its trust value is greater than the threshold value thus resulting in the trust worthy manet routing. This scheme has a good development on Qos parameter like pdr and delay also has provided trustworthy routing.

TRUSTED ON DEMAND ROUTING PROTOCOLS BASED ON AGENTS FOR MOBILE ADHOC NETWORKS

In this paper a new protocol based on self-monitoring and following the dynamic source routing algorithm is presented. THEREFORE, security is more important Trust routing protocols are one means security. ATDSR depends on self-monitoring of each node to find out its trust value. The advantages of ATDSR Are examined and it is compared with other techniques.

TRUST BASED ROUTING USING DOMINATING SET APPROACH IN WIRELESS ADHOC NETWORK

Some protocols are designed from scratch so as to incorporate security solution and some are designed to provide security measures into the existing protocols. some protocols require each node to have high memory capacity as they store large tables using for stored security information. A new trust based routing protocols is proposed which overcome the above mentioned limitation.

AN ENHANCEMENT SCENARIO OF ROUTING PROTOCOLS SCHEME USING TAODV PROTOCOL AND FUZZY LOGIC

This paper has highlighted, the effect of malicious nodes on Performance of Ad-hoc networks is presented and importance of using trust levels to improve the reliability and performance Ad-hoc networks. Evaluating trust levels between nodes of Ad-hoc networks poses a big challenge due to the lack of infrastructure in Ad-hoc networks. To overcome this limitation a new approach based on fuzzy trust algorithm is proposed to facilitate the evaluation of trust levels between nodes of Ad-hoc networks. Simulation and experimental results collected after applying the TAODV approach show significant improvements in the performance and the reliability and Reduce the Packet dropped rate with reference to Time. Ad-hoc networks in the presence of malicious nodes. However, a number of further investigation could be conducted to extend this approach. User make many trust–based decisions on a Sub conscious level.

TRIUMF: TRUST-BASED ROUTINE PROTOCOL WITH CONTROLLED DEGREE OF SELFISHNESS FOR SECURING MANET AGAINST PACKET DROPPING ATTACK

In this paper we proposed a general solution to packet dropping misbehaviour in mobile ad hoc networks. The solution allows monitoring, detecting, and isolating of the droppers in short time without using promiscuous listning, and can differentiate between selfish and malicious nodes. In our trust routing protocol, nodes can cooperate together to perform trusted routing behaviours according to the trust relationship among them; to route around the misbehaving node. With the trust value threshold, nodes can flexiby decide whether its neighbour is a malicious node or not according to the value of certainty factor. In the future we will simulate the proposed trust routing protocol to show the results and effectiveness of our solutions, and compare it with existing trust based routing protocols like TAODV, TWOACK, and TDSR protocols. A detailed simulation evaluation will be conducted in terms of Routing Packet Overhead, Security Analysis, Mean Time to detect dropper node, Overall Network Throughput, and Average Latency. Also we will study the situation when there is more than one malicious node in the route from the source and destination, with asymmetry of communication link in both directions.

TRUST BASED ROUTING ALGORITHMS FOR MOBILE AD-HOC NETWORK

Mobile Ad-hoc networks (MANETs) has many challenges due to its dynamic nature. Some of the major challenges are number of malicious nodes detected, number of hopes, route discovery time and packet loss.

Routing algorithms namely DMR, TMR and MTMR have their own way in order to establish the trust and transmit packet securely. But message trust based multipath routing protocol proved to be best in terms of number of malicious nodes detected, number of hops, to discovery time and packet loss.

In future we plan to implement the secure routing protocols such as the ARIADNE and ARAN and compare them with the trust based routing protocols. The system handles only text as message for data packets. In future it can be enhanced to include multimedia packets.

RESEARCH AND IMPROVEMENT OF AODV PROTOCOL IN AD-HOC NETWORK

This research has been contributed by JIAO Wen-Cheng, et al.. There are two processes in AODV protocol routing find and routing maintenance. AODV protocol uses the method of hop-by-hop routing to transmit packets. Wormhole attack is a special attack method aimed at Ad hoc network. Based on the analysis of AODV protocol and the attack conditions of wormhole attack, the process and algorithm aimed at wormhole attack are researched.

ENHANCING THE SECURITY OF THE AODV-S ROUTING PROTOCOL

This research has been contributed by Prakash Veeraraghavan, et al.. Security is the major issue in Ad-hoc network. Protocols of MANET do not offer protection against various type of attack. Thus the do not offer any immunity. AODV-s is the modified version of AODV protocol by immune to various type of attacks. It also provides solutions of Dos attack when the hope count modified in it. Outcome of this research it successfully various type of attack which increases the network performance. In future he would like to work on mobility prediction methods.

MODIFIED ROUTING ALGORITHM FOR AODV IN CONSTRAINED CONDITIONS

This research has been contributed by Prakash Veeraraghavan, et al. In MANET AODV exhibits abnormal behaviour due to the high mobility of nodes in the network. The proposed work is aimed at performance improvement in internet connectivity by applying local congestion methods in routing protocols.

Outcome of this research increases packet\delivery ratio even in constrained conditions in satisfactory level and also improvement of network load and end to end delay has achieved.

PERFORMANCE COMPARISON AND EVALUATION OF AODV, OLSR, AND SBR IN MOBILE AD-HOC NETWORKS

This Research has been contributed by Alexander Klein, et al. In this paper various proactive routing protocols has been compared like SBR, AODV, and OLSR in various mobile scenarios with different traffic pattern.

This protocols are compared on the basis of reliability and routing overhead. Outcome of this research source SBR achieve high end to end reliability without frequent end to end roite calculations. Future directions of research is to increase the reliability without increasing the routing overhead.

PROPOSED WORK TO DECREASE THE ROUTING OVERHEAD

AODV enhanced local repair is Motivated by the issues identified in local repair. Aodv which uses to broadcast locally to repair the route. In trusted Aodv rout repair by unicast mechanism instead of broad cast. Trusted route aodv is modified by sending route error message towards the source by the help of RREP to report the route failure.

So that routing congestion will decrease and propogation delay will reduce. We know that until it sends the route packet it never stops the data sending. If it has a trust worthy node and pick by the route, then it leads to decrease the congestion an d delay.

CONCLUSION

In this paper we have done survey of all the paper published in AODV in futures we would like to improve this protocol by removing one of the drawbacks of AODV that is routing overhead by our proposed methodology and research work. As described in this paper, significant research has already been performed in the area of congestion and security. However, a number of issues still Remain unresolved or not completely addressed.

Additionally, the proposed solution is in most cases not tested in real environment Therefore, future studies should rather be devoted to real implementations than just simulation. Only such an approach can ultimately verify a protocol's usefulness in future Ad-hoc network.

REFERENCES

1. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, 2000, pp. 255–265.
2. S. Buchegger and J.-Y. LeBoudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc Networks)," In Proceedings of the 3rd ACM International Symposium on Mobile and Ad Hoc Networking & Computing (MobiHoc 2002), pp. 226–236, Lausanne, Switzerland, June 2002.
3. X. Li, M. R. Lyu, J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks". In the Proceedings of IEEE Aerospace Conference (IEEEAC) 2004, pp. 1286-1295.
4. M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in Proceedings of ACM Workshop on Wireless Security (WiSe '02). Atlanta, USA: ACM Press, September 2002, pp. 1–10. [Online] Available: http://doi.acm.org/10.1145/570681.570682.
5. K. Balakrishnan, J. Deng, and P.K. Varshney. "Twoack: preventing selfishness in mobile ad hoc networks,". In The IEEE Wireless Communication and Networking Conference (WCNC'05), pp. 2137-2142, New Orleans, LA, USA, March, 2005

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