DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4578

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# A HEURISTIC APPROACH TO SECURE MOBILE AD-HOC NETWORK

Arpita
M.tech(CSE),
DCRUST,India

Mr. Sanjeev Indora
A.P, CSE Dept.,
DCRUST ,India

***Abstract:*** An Ad Hoc[1] network is a gathering of wireless mobile nodes framing a transitory network without the aid of any centralized administration or standard support services. The topology of the ad hoc network may change rapidly and unexpectedly. One of the most problems encountered in these networks, is finding the optimization path between source and destination nodes within a specified time with minimum energy consumption. As energy and bandwidth is the main constrains in MANET so there is no requirement to pass the information through all nodes. Only the required nodes take part in communication. In this paper a swarm algorithm to find the optimal route is presented which automatically makes the network secure and more efficient. The proposed work is inspired by the path selection algorithm. The proposed work considers various parameters such as Distance, consumed energy, delay, time etc to solve routing problem. Simulation results are carried out for both algorithms using MATLAB. The results are shows in the graphical as well as in tabular forms.

***Keywords:*** Ad Hoc, MANET, AODV, route repairing, QOS etc

## 1. INTRODUCTION

Wireless networks[2] have become increasingly popular in the computing and communication industries, since their emergence in the '70s. This is predominantly true within the past decade, which has seen wireless networks evolve with the purpose of enabling better mobility. There are two variations of mobile wireless networks - the first is known as infrastructure network [3], i.e., a network with fixed and wired gateways and the second is infrastructure-less mobile network [4], better known as an Ad Hoc network. This has importantly two ways of functioning, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad Hoc connectivity where there is no Control Module. Ad Hoc networks don't rely upon fixed infrastructure with a specific end goal to do their functioning. The functioning method of such system remains stand alone, or might be appended with one or numerous focuses to give web and availability to cell networks.

## 2. SECURITY IN MANET

Mobile Ad Hoc Network (MANET) is not same as the traditional wired networks because of its portability, infrastructure less topology and the nonexistence of central authority in the network. Any framework that must be secured may have shortcomings or vulnerabilities, a few or all of which might be focused by an intruder. Henceforth, one way to deal with planning security [5] components for frameworks is to take a glance at the dangers that the framework faces and the attacks [6] conceivable given the vulnerabilities. The plan security mechanism should then guarantee that the framework is secure in the light of these dangers, assaults, and vulnerabilities. The mechanism must ensure that only authentic [7] user allowed the access of packets.

## 3. VULNERABILITIES

The vulnerabilities of MANETs are summarized as

- ***Wireless links***: Most importantly, the utilization of wireless connections make the system defenseless to malicious [8] activities, for example, overhearing and active illegal obstruction. Not at all like wired networks, intruders don't require tangible access to the system to do such assaults.
- ***Dynamic topology [9]***: Nodes in MANET can depart from system and stick with the set-up, and roam freely. Accordingly, the structure of network can vary very often. In this type of changing condition it is very difficult to distinguish between an ordinary conduct of set-up and a noxious conduct of set-up.
- ***Co-operativeness***: The algorithms for routing purpose in MANET hope for the nodes to be cooperative and non intruding. Therefore, by resisting the protocol basic requirements, the system functioning can be disturbed without much of a stretch by a noxious intruder.
- ***Lack of clear line of defense [10]:*** Assault origination in MANET may take from any possible direction as there is an absence of any optimal defense line. The isolation limit separating inner network from the outer network is not transparent in MANETs.
- ***Restricted resources:*** Resource restrictions [11] are another weakness. MANETs can have numerous gadgets. The distinctive figuring and constrained capacity of these gadgets may seek the attention of new assaults.

## 4. CONSTRAINS

MANETs have a need to progressively decide routing in light of accessibility or perceivability of nodes. MANETs additionally have nodes whose energy [12] preservation is exceptionally restricted. Regularly, they are battery prepared, with extremely constrained to no charging or substitution possible. Accordingly, while attempting to work typically preservation of energy is a large factor in designing and usage of MANETs.

Another restricted asset in MANETs is transmission capacity [10]. To adapt to the energy and transfer speed necessities, MANETs utilize gathering procedures, in which a few nodes perform particular capacities (like sending/handing-off sensor information), while all the more capable individuals perform more resource-intensive exercises( like information conglomeration, steering and so forth).

## 5. LITERATURE SURVEY

In year 2006, Shekhar H M P performed a work, "**Mobile Agents based Framework for Routing and Congestion Control in Mobile Ad Hoc Networks**". For Steering and clogging control the authors in this paper have presented a mobile agent based structure called MAFRC[13].

In year 2007, Vincent Borrel performed a work, **"Understanding the Wireless and Mobile Network Space: A Routing-Centered Classification".** For perceiving the suitable routing according to the network the researchers in this paper have focused on the categorization of mobile and wireless network.[14]

Alfredo Garcia performed a work, "**Rational Swarm Routing Protocol for Mobile Ad Hoc Wireless Networks"**. Wireless Mobile Ad Hoc networks (MANET) requires changing routing plans for adequate execution. Another dynamic routing plan in view of stigmergy is presented by the researchers in the paper.[15]

## 6. ROUTING PROTOCOLS

When the routing in wired set-up with stationary framework is contrasted with routing in mobile Ad Hoc network then some further issues and difficulties are confronted. There are a few surely understood conventions in the writing that have been particularly created to adapt to the confinements forced by ad hoc networking conditions. Routing is for the most part grouped into static routing and dynamic routing. Static routing is what keeps up a routing table. Dynamic routing alludes to the routing technique that being is learnt by an inside and outside routing convention. The cases for routing algorithm are:

a) **Reactive protocols[16]:** - Responsive conventions generally approached request driven receptive conventions. They are known as responsive conventions since, they don't begin course disclosure all alone, unless they are requested, when a source hub request to find a course. These traditions setup courses when asked.

   **AODV:** AODV[17] is the situation of receptive convention, when a hub wishes to start transmission with another hub in the system to which it has no course; AODV will give topology information to the hub. AODV use control messages to find a course to the goal hub in the system.

   **Proactive protocols [5]**: - Proactive directing conventions fill in as the other way around when diverged from responsive steering conventions. These traditions dependably keep up the revived topology of the system. Every hub in the system consider the other hub ahead of time, toward the day's end the whole system is known to each one of the hubs making that system. All the steering information is for the most part kept in tables.

b) **Hybrid protocols:** - Hybrid protocols [18] reprimand the characteristics of both responsive and proactive conventions, and solidify them together to hint at enhanced outcomes. Hybrid protocols segment the system into areas called zones which could be covering or non-covering depending upon the zone creation and organization algorithm used by a particular hybrid protocol.

TABLE1 Example of protocols

| Parameter | Network | Protocols | Examples |
|---|---|---|---|
| Response Time And Bandwidth | Ad hoc | Proactive protocols | Destination-sequenced Distance-Vector (DSDV) |
| | | | Optimized Link- State Routing (OLSR) |
| | | Reactive protocols | Ad Hoc On-Demand Distance-Vector (AODV) |
| | | | Dynamic Source Routing (DSR) |
| | | | Geography-based routing |
| | | | Cluster-based (or *hierarchical*) routing |
| Energy | Sensor | Network structure | Flat network routing |
| | | | Hierarchical network routing |
| | | | Location based routing |
| | | Protocol operation | Negotiation based routing |
| | | | Multi-path based routing |
| | | | Query based routing |
| | | | QoS based routing |
| | | | Coherent based routing |

## 7. PROBLEM STATEMENT

Energy and efficiency are dependably the primary worry in wireless Mobile network. A moving set up contains enormous measure of information out sending over the network. As a result there is more possibility of information loss over the network. Our work is described in same area. We proposed an algorithm to get the efficiency and the trustworthiness. In this work a successful maximally secured versatile system algorithm is displayed with the true objective that addresses the necessities of vitality capable framework issues for MANET. In this work we have united the Path Selection Routing nearby Swarm. The fundamental course will be recognized by the Path Selection calculation and if there emerge an event of any broken connection or assault up the course it will scan for the Alternate way using Swarm improvement.

### 7.1 The presented work is divided in two main stages:

- In first stage, the path selection algorithm will be defined over the network.
- Then the swarm will be implemented to find an optimal route.

Since, the mobile ad hoc networks are more inclined to experience the ill effects of the noxious practices than the traditional wired networks. In the proposed work we will find out all possible routes and will calculate their fitness. By considering a threshold value some broken path may be repaired and considered for transmission. The work further will improve QOS of the system.

### 7.2 Parameters Used

- Throughput Analysis
- Time Delay
- Energy
- Distance

The description of the Swarm idea is displayed here

- At uniform time intervals any node s(Source) is chosen to send information to some target node d.
- Each forward Swarm chooses the next hop node utilizing the routing table data. The following node chose relies on upon some arbitrary plan. If all nodes are already went by, then a uniform determination will be executed.
- If the chosen hub is some assault or intruder node or it is not at present accessible. The forward Swarm holds to turn out the low need priority node from the queue.
- Delay will be analyzed on any distinguished non visited node.
- In case of detection of any cycle the swarm is forced to turn on the visited node.
- A backward swarm is generated to trade all its memory on the achievement of target node.
- Same route as forward swarm is used by the Backward Swarm.

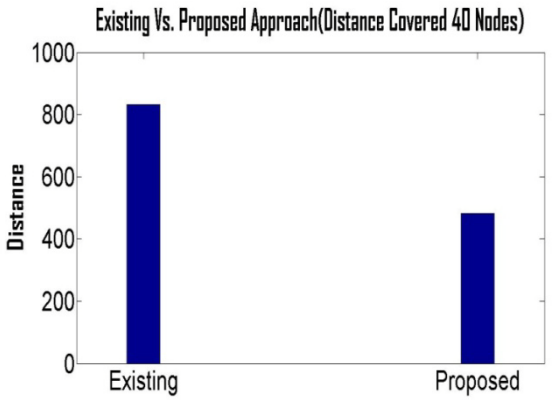
## 8. SIMULATION

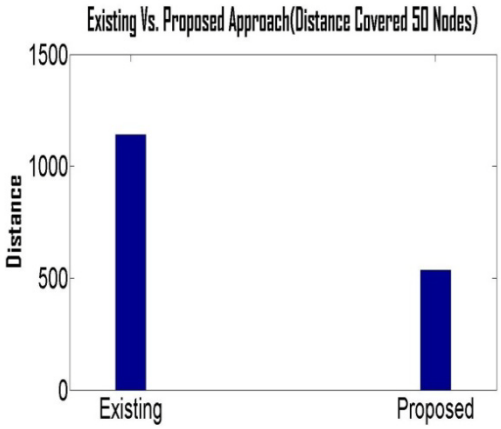
The simulation studies involve the deterministic, network topology with different nodes. The proposed Algorithm is implemented with MATLAB. Below table shows the numeric values obtained using the two different approaches.

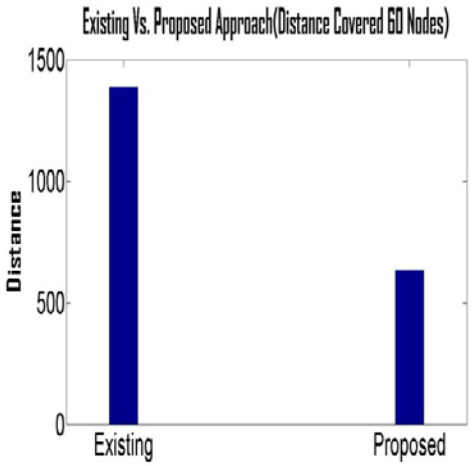
**TABLE2: DISTANCE ANALYSIS**

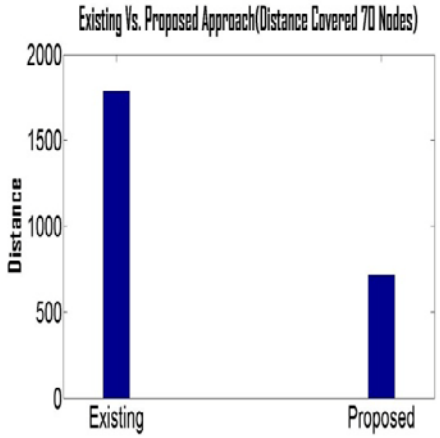
| **No of Nodes** | 40 | 50 | 60 | 70 | 80 |
|---|---|---|---|---|---|
| **(EXISTING WORK) Sum of distance** | 831.5202 | 1.1418e+003 | 1.3874e+003 | 1.7840e+003 | 2.0953e+003 |
| **(PROPOSED WORK) Sum of distance** | 482.0894 | 534.1621 | 632.8761 | 718.3171 | 810.1708 |

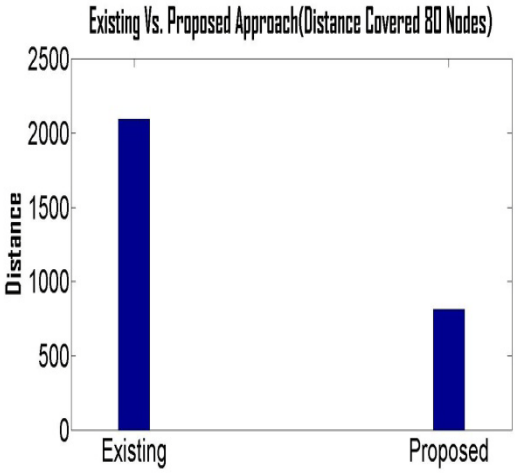
### 8.1GRAPHS



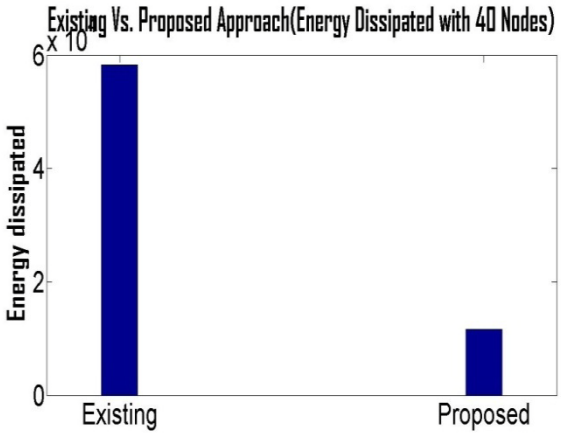



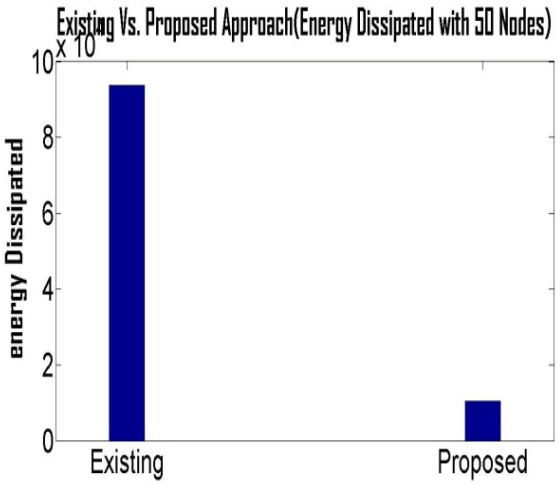



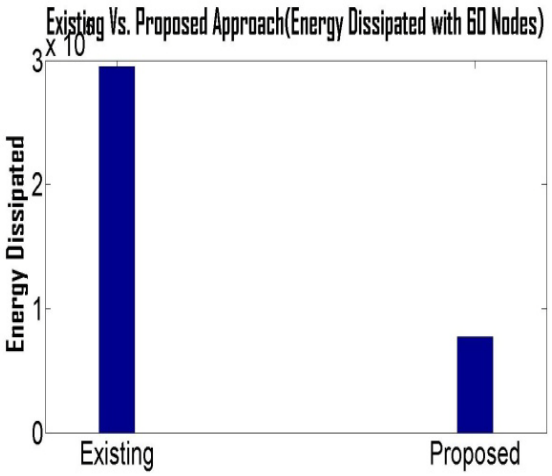



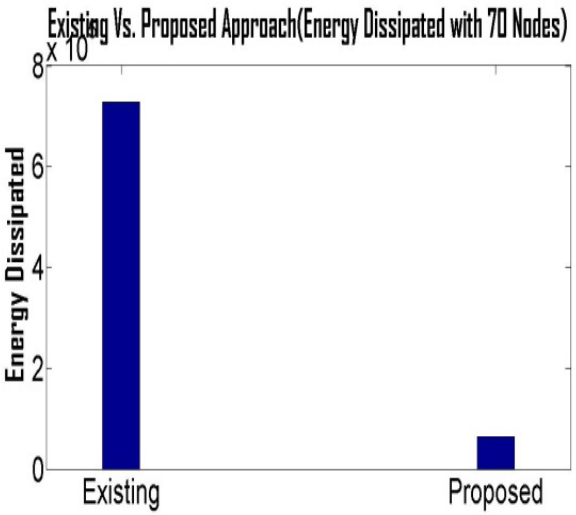
### 8.2 TABLE3: ENERGY ANALYSIS

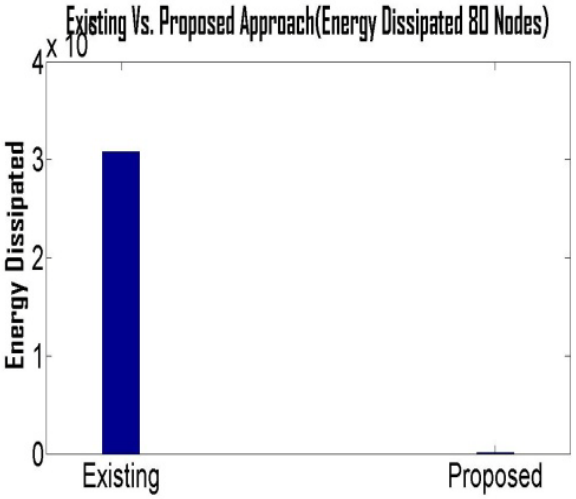
| No of Nodes | 40 | 50 | 60 | 70 | 80 |
|---|---|---|---|---|---|
| (EXISTING WORK) Consumed Energy | 5.8291e+004 | 9.3650e+004 | 2.9477e+005 | 7.2686e+005 | 3.0841e+006 |
| (PROPOSED WORK) Consumed Energy | 1.1571e+004 | 1.0438e+004 | 7.7387e+004 | 6.5113e+004 | 1.4750e+004 |



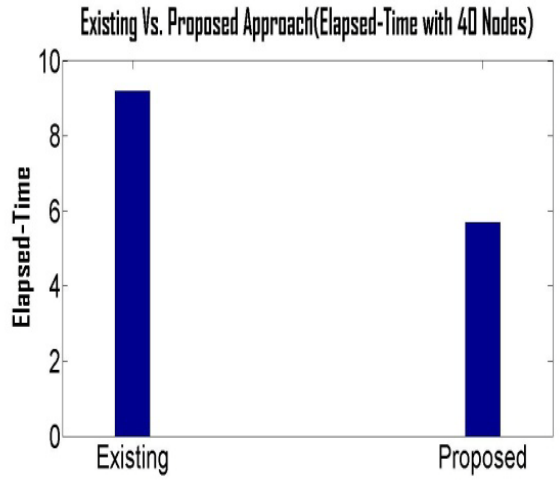



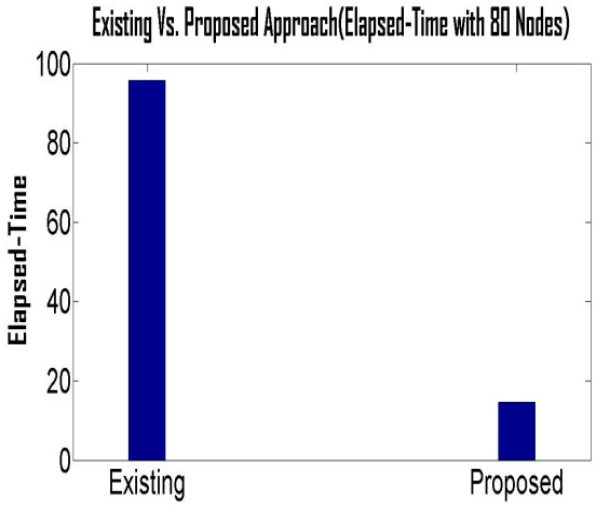



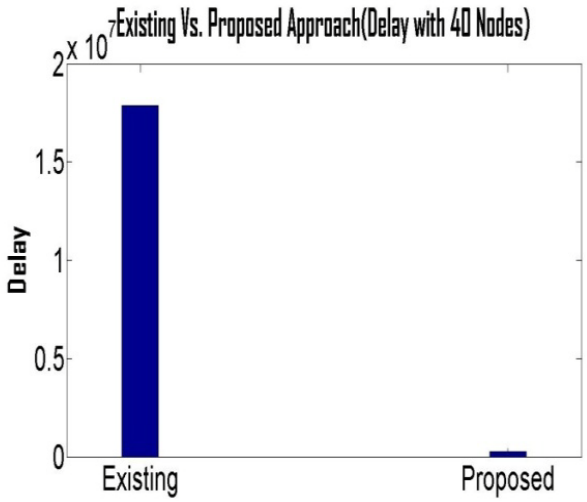



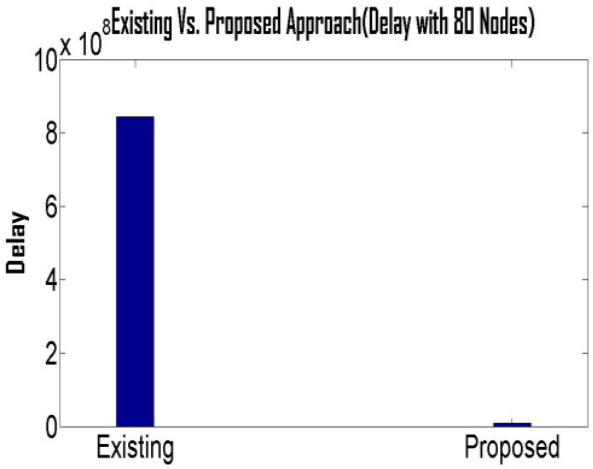

### 8.3 TABLE4: TIME & DELAY ANALYSIS

| No of Nodes | 40 | 50 | 60 | 70 | 80 |
|---|---|---|---|---|---|
| (EXISTING) Time(sec) | 9.195183 | 14.867682 | 27.887024 | 49.961416 | 95.682297 |
| (PROPOSED) Time(sec) | 5.700278 | 6.02 | 8.52 | 12.69 | 14.66 |
| (EXISTING) Delay | 1.7885e+007 | 3.9670e+007 | 8.2989e+007 | 3.9834e+008 | 8.4416e+008 |
| Proposed (Delay) | 2.7672e+005 | 2.5819e+005 | 2.8117e+006 | 5.3532e+006 | 8.1897e+006 |




We can see, in figures, as the data is transferred from a congestion free path, the overall energy consumed, Elapsed time, cost etc while performing the transmission is reduced as compared to the existing approach.

## 9. CONCLUSION & FUTURE SCOPE

In the present work, we have characterized a Swarm based heuristic enhanced secure routing way to deal with exchange information from congestion free and assault safe route. Generally, the briefest course is the most cherished zone for the intruders to play out the interference, hence the showed proposal won't cover any hub that is having the higher probability of the interruption or the blockage. As the correspondence will be performed over a clog free way, the vitality and the delay over the system will be diminished. The presented proposal is appealing regarding vitality and the time and furthermore gives a trustworthy course over the system. The results acquired demonstrate that the approach has upgraded the system trust quality and the vitality

In this present work, swarm is used as the advancement and safe course generation algorithm. In future, some other advancement limits can be used for the way development, like PSO[19], ACO[20].

## REFERENCES

[1] Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (Eds.), "Mobile ad hoc networking. John Wiley & Sons",2004.

[2] Ganz, Aura, Zvi Ganz, and Kitti Wongthavarawat,"Multimedia Wireless Networks: Technologies, Standards and QoS", Pearson Education, 2003.

[3] Zimmerman, Rae, "Social implications of infrastructure network interactions." Journal of Urban Technology 8.3 (2001): 97-119.

[4] Saadawi, Tarek, and Osama Hussein, "Routing method for mobile infrastructureless network." U.S. Patent No. 6,940,832. 6 Sep. 2005.

[5] Sogani, P., & Jain, D. A.,"A Study on Security Issues in Mobile Ad Hoc Networks", IJIACS ISSN, 2015, 2347-8616 (vol. 4).

[6] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Rushing attacks and defense in wireless ad hoc network routing protocols." Proceedings of the 2nd ACM workshop on Wireless security. ACM, 2003.

[7] Lee, Kyu-Hwan, et al, "Routing based authentication for mobile ad hoc network in home environment", Proceedings of the 2nd international conference on Ubiquitous information management and communication. ACM, 2008.

[8] Saffarian, Mohsen, and Matei Ciobanu Morogan, "A novel protocol to prevent malicious nodes from misdirecting forward ants in AntNet algorithm", Proceedings of the 2008 ACM symposium on Applied computing. ACM, 2008.

[9] Johnson, David B., and David A. Maltz, "Dynamic source routing in ad hoc wireless networks", Mobile computing (1996): 153-181.

[10] Hunter, Andrew M., Jeffrey G. Andrews, and Steven Weber, "Transmission capacity of ad hoc networks with spatial diversity", IEEE Transactions on Wireless Communications 7.12 (2008): 5058-5071.

[11] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu, "Mobile ad hoc networking: imperatives and challenges" , Ad hoc networks 1.1 (2003): 13-64.

[12] Goldsmith, Andrea J., and Stephen B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks", IEEE wireless communications 9.4 (2002): 8-27.

[13] Shekhar H M P, "Mobile Agents based Framework for Routing and Congestion Control in Mobile Ad Hoc Networks", CoNEXT'06, December 4–7, 2006, Lisboa, Portugal. © 2006 ACM 1-59593-456-1/ 06/ 0012

[14] Vincent Borrel, "Understanding the Wireless and Mobile Network Space: A Routing-Centered Classification", CHANTS'07, September 14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-737-7/07/0009

[15] Alfredo Garcia, "Rational Swarm Routing Protocol for Mobile Ad Hoc Wireless Networks", ICPS'08, July 6–10, 2008, Sorrento, Italy. ACM 978-1-60558-135-4/08/07

[16] Abolhasan, Mehran, Tadeusz Wysocki, and Eryk Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Ad hoc networks 2.1 (2004): 1-22.

[17] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das, "Ad hoc on-demand distance vector (AODV) routing", No. RFC 3561. 2003.

[2] Nacer Hamani, "An ACO/MAS joint approach to manage communications in wireless sensor networks", MEDES 2009 October 27-30, 2009, Lyon, France ACM 978-1-60558-829-2/09/0010

[18] Khaleel Ur Rahman Khan, "An Efficient Integrated Routing Protocol for Interconnecting Mobile Ad Hoc Networks and the Internet", International Conference on Advances in Computing, Communication and Control (ICAC3'09) ICAC3'09, January 23–24, 2009, Mumbai, Maharashtra, India. ACM 978-1-60558-351-8

[19] C D'Souza, "Implementation of Particle Swarm Optimization Based Methodology for Node Placement in Wireless Sensor Networks",International Conference and Workshop on Emerging Trends in Technology (ICWET 2011) – TCET, Mumbai, India ICWET'11, February 25–26, 2011, Mumbai, Maharashtra, India. ACM 978-1-4503-0449-8/11/02

[20] Mohsen Saffarian, "A Novel Protocol to Prevent Malicious Nodes from Misdirecting Forward Ants in AntNet Algorithm", SAC'08, March 16-20, 2008, Fortaleza, Ceará, Brazil. ACM 978-1-59593-753-7/08/0003