*International Journal of Engineering Research and Development*
***e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com*
*Volume 3, Issue 7 (September 2012), PP. 27-32*

# IDS for Detection and Prevention of Dynamic mobile node positioning based on Logical Distance Measures

Subburaj.V[1], Dr. K.Chitra[2]

*[1]Ph. D Research Scholar, Manonmaniam Sundaranar University, Tirunelveli & Assistant Professor, Department of MCA, Thiagarajar School of Management, Madurai, Tamilnadu, India*
*[2]Assistant Professor, Department of Computer Science, Government Arts College, Melur, Sivagangai Dist, Tamilnadu, India*

***Abstract*—Mobile network has a highest level of vulnerability since mobile networks are liable to attack due to its transparent location. The Adhoc nature posses structure less property due to its dynamic nature which paves way for multiple ways of attacks. Implementing IDS is a tedious process and one among them is Worm Hole attack which really challenges researchers to provide solution for preventing it. This Worm hole also referred as relay attack. This work focus on to eradicate worm hole using wormeros measure and black hole attack using RREP strategy by detecting it and measuring the node distance by changing the node structure rapidly. Preciously prevention of Worm hole attack works well when the neighboring nodes lies in a minimal distance. To extend the transmission each mobile node depends on the other nodes of same zone or network. Generally distance deals with mobile data transmission and it's been affected by the relay attack (Worm Hole attack) where distance is directly proportional to data and its relay. In this work our scheme focused to trace the node based on its location, its structure and node arrangements to fight against attack. The nodes locations were evaluated using DV-hop propagation method. This work will never oblige on network founding and its operations.***

***Keywords*—IDS, Security breaches, Node Location, Wormeros, relay attack, Node vulnerability**

## I. INTRODUCTION

IDS are an enormous threat in every networking concept. Hence ADHOC is not an exception for this. One among the IDS security breech is Worm Hole Attack. This Worm hole attack focuses on Relay transmission of data. The data from one mobile node moves among each and every mobile node of the same network group. Now the issues arises how to get the mobile node location and its neighbouring nodes. Due to the social networking and the immense GIS space makes it much more complicate.

This attack makes the major threat in Denial of Service which happens if the nodes are distributed for data transmission. The purpose of dealing these issues with DENIAL OF SERVICES is that mobile node always depends on the nearby nodes for its transmission. The IDS were implemented so far focus on the various attacks and in order to make it wider it dealt with an attack affects the other. This present work focuses on the demerits of efficient data transmissions between mobile nodes due to Intrusion of Worm hole. The MANET was establishing by the mobile sensor where each and every mobile node act as a sensor. This role of sensor is to identify the mobile node, deploy the transmission and to identify the other mobile nodes in the network. Now the issues come in the form of threat. The main issues of threat come in the form of Worm Hole attack which is very difficult to stop. The Worm hole attack also referred as relay attack where it will provide relay access for a transaction and removing the worm hole attacked nodes from the network makes the transmission inconsistent. Though the node is attacked by worm hole it will act as back bone for the data transmission. On the other end, Black Hole attack is a kind of thread which provide false path for data transmission. These two attacks persuade DENIAL OF SERVICES to the legitimate nodes.

For a success transmissions within the mobile nodes there will be a starting and as well as ending point for mobile nodes which normally sets the ADHOC boundary. The boundary region of the nodes works along with the routing protocols like AODV, DSR. These protocols ensure the data transmission but it will not sense the boundary where it focuses only the mobile nodes which fall within the boundary. The boundary hence forth determined by the GRID Space [1]. Grid space provides the boundary and landmark to the Mobile node. This landmark can be either in Grid or in GPS enhanced. The trade off between Grid and GPS is the landmark of limited or maximized boundary conditions. The node available within the boundary has start node which would be always the initial position of the node and the end node which is off termination node. This node positioning differs based on Grid or GPS.

This work focus on the mobile node landmark based on GPS and also provides security measures for the attack like Worm hole and Black hole which invokes Denial of Services (DOS). The landmark referred as Mobile boundary gives the number of mobile nodes within the boundary. The node in the landmark gives the source point of access. This paper were split up in to Problem statement, Definition, MAODDP routing protocol, DV Hop propagation method, GPS Location

### A. Problem Statement

The era of gadgets and the increasing usage of mobile technology, also gave rise to the security issues which are the problems to be stated here. The IDS places a vital role in preserving the mobile node location. In this paper we have addressed location based access of mobile nodes which measures the node distance in GPS mode. The way GPS dealt with this paper gives vast boundary of access. In order to detect Worm hole attack, AODV routing protocol is used and in order to prevent Worm hole attack DV-Hop propagation method is used. The need of DV-Hop propagation method which gives the node position in the provided GPS space and it also considered as the landmark.

### B. Problem Definition

MANET is the area affected by series of thread and among all notable threat are worm hole and black hole attack. There are few strategy exists to get rid of these attack issues. In this paper we have proposed the combination factor of detection and prevention of attack which makes the system as IDS. If the sensor is made as IDS it will protect itself and as well as the other mobile node of a network. We have incorporated the concept of WORMEROS [2] which will detect worm hole and black hole attacks. In the Fig. 1 X and Y will communicate with S and D and make them think it's also a part of network. This X and Y were used act as a tunnel to send the pack and it becomes the part of network. The Back Bone Network (BN) works towards black hole attack and remaining other will work towards Worm hole attack.

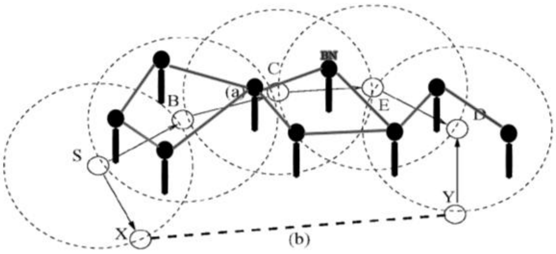


***Fig. 1*** Worm hole and Black hole attack

Setting up wormhole is very ease and detecting is very tough. The transceivers were placed on different location by the attackers which will tent to behave like legitimate nodes. Tracing these worm holes with in legitimate nodes is a tough ask. In this paper we have incorporate the concept of DV-Hop which gives the node location information and the position of node in GPS space. The usage of DV-Hop will get rid of Worm hole attack and subsequently the black hole were eradicated using RREP concept discuss by Deng et. al. [3]. In his paper when the node starts its transmission it will check the nearby node for authentication to sent data through the node. This concept will work in both proactive and reactive protocol. Further this will enable Selective Forwarding of data packets from one mobile node to another.

## II. REVIEW OF LITERATURE

Packet Leashes concept [4] were the first one to detect work hole attack. The solutions dealt with these concepts are Geo leashes and temporal leashes were both works with GPS for tracing the location and to sync with packet data transmission. The need for sync is to provide packet time duration and once time exceeds the data transmission is terminated or expired. This also works to check Time To Live (TTL) of packet duration. Directional antenna concept of Hu and Evans[5] deals with the special hardware to measure accurate distance to establish versatile speed for data transmission. Another conceptual research work comes from Eriksson which deals with True Line [6] depends on the RTS-CTS-Data-ACK mechanism of IEEE 802.11MAC protocol to defend against wormhole attacks. In this solution the nodes have a time constraint to authenticate each other and thus wormhole attacks are prevented.

The work of Deng and Wei Li [7] has proposed an algorithm to detect black hole attack in mobile adhoc networks. This work focus on to detect black hole attack by receiving RREP packet and to check whether all nodes in the network receives it. This concept of RREP will not entertain malicious node and thus black hole attack is revert back and avoided. The work of S.Ramaswamy [8] has proposed an algorithm to detect and prevent co-operative black hole attacks in ad hoc network. This concept works with mutual concern of nodes and to enrich trust relationship between the nodes, and hence it cannot tackle black hole attacks. Besides due to intensive cross checking, the algorithm takes more time to complete, even when the network is not under attack.

## III. ROUTING AND SECURITY IN MANET

The routing scenario in Manet leads to the number of security issues. Since there is no predefined feature in mobile nodes like routers, transmission range moreover it is not possible to adapt like traditional wired networks. The build in nature of mobile nodes will keep on moving and changing irrespective of the network. The routing protocols used in MANET were broadly classified in to Reactive and Proactive protocols. The Reactive protocols deals with the algorithm like DSDV. Such algorithm works with table driven approach. In order to focus on high latency routing and selective flooding the later will work. The work of DSDV [9] works with table driven approach where nodes will be placed in a position and based on the location the data transmission were done. Implementing DSDV it has pros and cons. *Dynamic Source Routing* (DSR) uses routing from one node to another in the network in the same network. The starting node or the source code has the entire path history of its deliverables. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms: Route Discovery and Route Maintenance.

This paper focus on Mobile Adhoc On-Demand Data Delivery Protocol MAODDP [10] which provides services based on the node request. The selective forwarding of data packets were implemented based on the initiation of the service from MAODDP. This protocol works with Geocasting protocol since it works with GPS landmark. The security issues arrives in the form of Black hole and Worm hole attack which when initiated at the moment when MAODDP starts it routing paradigm. The architecture of Wormeros [2] plays vital role in eradication of worm hole attack which prevails in the network and to prevent the impact of black hole attack in the network the concept of RREP packets were implemented. The work of

RREP is to identify the mobile node neighbor for maintaining authenticity. The work of MAODDP algorithm in this issue is making the routing data transformation from one mobile node to another. In this work we have adapted the use of MAODDP along with RREP to eradicate the above mentioned issues i.e. Worm hole and Black hole.

The MAODDP initiates its function based on DV-Hop method which uses to identify the mobile location in the mentioned GPS land space. The idea is to propagate the mobile nodes using DV-hop propagation method. To get the landmark of the mobile nodes, DV-hop uses classification distance vector routing by which exact mobile distance were known according to the landmark.

$$ci = \frac{\sum\sqrt{(Xi-Xj)^2+(Yi-Y}}{\sum_h i} \quad \text{i} \quad \neq j, all\ landmark \qquad [1]$$

Each and every node gets update from the mobile nodes about the landmark of each neighbour in the specified GPS landmark. Using the above mentioned formulae the closest mobile node and its distance were noted along with the TTL of every packet. If there is a variation in timing if affects the TTL and further it leads to security issues. The usage of MAODDP algorithm is to provide security based on the mobile nodes location and as well as to its neighbouring nodes. The impact of DV-hop[11] propagation method is used to identify the Worm hole in the said network based on the location. The triangular method in DV-hop leads to the third stage to find the closest neighbour. The below mentioned result were adopted from Dragos Niculescu and Badri Nath work on DV-Hop propagation.

Suppose considering node with coordinates (x,y):
(x1, y1) = coordinates of the first closest landmark
d1 = distance from first landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)

(x2, y2) = coordinates of the second closest landmark
d2 = distance from second landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)

(x3, y3) = coordinates of the third closest landmark
d3 = distance from third landmark obtained from product of no. of hops and correction factor (of landmark nearest to node)

Using the equation of a circle, the systems of equations are:

$$(x - x1)^2 + (y - y1)^2 = d1^2$$
$$(x - x2)^2 + (y - y2)^2 = d2^2$$
$$(x - x3)^2 + (y - y3)^2 = d3^2$$

Subtracting one equation from the rest:

$$2x(x2 - x1) + 2y(y2 - y1) = d1^2 - d2^2 + x2^2 - x1^2 + y2^2 - y1^2$$
$$2x(x3 - x1) + 2y(y3 - y1) = d1^2 - d3^2 + x3^2 - x1^2 + y3^2 - y1^2$$

Let $A = d1^2 - d2^2 + x2^2 - x1^2 + y2^2 - y1^2$
$B = d1^2 - d3^2 + x3^2 - x1^2 + y3^2 - y1^2$

Thus,

$$2x(x2 - x1) + 2y(y2 - y1) = A$$
$$2x(x3 - x1) + 2y(y3 - y1) = B$$

Reducing the above equations:

$$y = \frac{A(x3 - x1) - B(x2 - x1)}{2[ (y2 - y1)(x3 - x1) - (y3 - y1)(x2 - x1)]}$$

$$x = \frac{[A - 2y(y2 - y1)]}{2(x2 - x1)} \qquad [2]$$

With the assistance of the formulae, mobile node and its nearest neighbour were noted and they were subjected to work in IDS platform to avoid security issues. The results thus received were subjected to MAODDP which will provide network transmission along with the security measures. The value of x has the value of nearest neighbour. To continue further the value of x along with MAODDP protocol will provide the efficient way for data transmission.

$$T= X \quad MAODDP + RREP \qquad [3]$$

In above mentioned formulae the Variable T is the transmission which is approximately works with MAODDP and RREP for initiating the successful packet transmission. The work of Dragos Niculescu et. al.[11] focus on Grid based sensor network which calculates the nodes location using DV-Hop. In this work, a worm hole is simulated and the results were published based on Network. It uses DSR protocols for implementation in the said network. The parameters used in the network deals with Grid range, number of nodes, size, landmark nodes, worm hole start and end points. In this study we have implemented in ns2 mobility pack using MAODDP routing protocol with the following parameters. GPS landmark, number of nodes, number of nodes in said GPS zone, Worm hole start and end point, Black hole attack tracer using RREP. The implementation of GPS will initiate by sending hello packet using MAODDP routing protocol among the nodes in the said zone. Once the hello packets were send to a node, it will start propagating this message to the neighbouring nodes. This flow will repeat until the destination node is reached. During the Hello Packet transmission the delay is measure based on the node distance to find the possibility of attack and the acknowledgement were received using RREP. The distance of each and every nodes and the network structure will change drastically. Due to this dynamic change in node position and network structure, the result will not be same. There may be few variation occurred in terms of result.

## A. Measuring the Attack

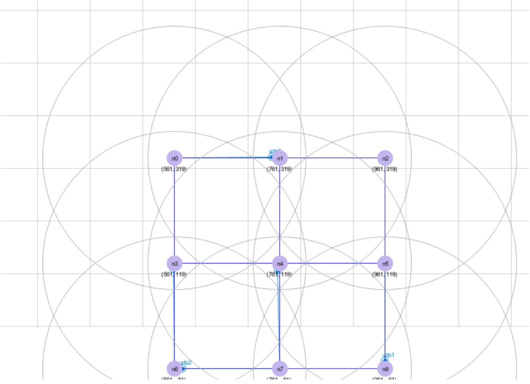


*Fig 2.* **Node arrangement in Grid Space**

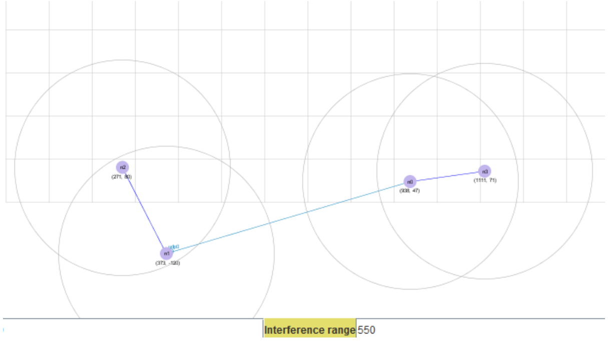
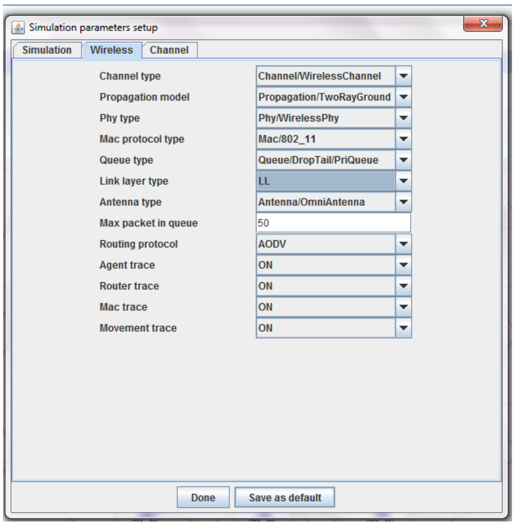


*Fig 3.* **Node setup with interference range**



| | |
|---|---|
| Channel type | Channel/WirelessChannel |
| Propagation model | Propagation/TwoRayGround |
| Phy type | Phy/WirelessPhy |
| Mac protocol type | Mac/802_11 |
| Queue type | Queue/DropTail/PriQueue |
| Link layer type | LL |
| Antenna type | Antenna/OmniAntenna |
| Max packet in queue | 50 |
| Routing protocol | AODV |
| Agent trace | ON |
| Router trace | ON |
| Mac trace | ON |
| Movement trace | ON |

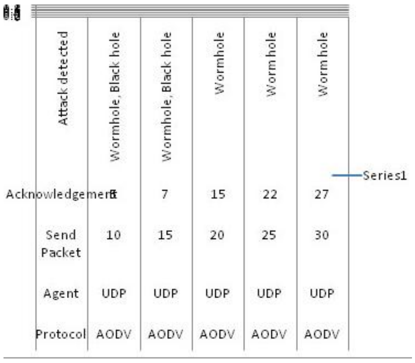
*Fig 4.* **Simulation setup**

In the above mentioned Fig 2, the nodes were displayed in the form of grid and the number of nodes used was 9 (3 x 3). The waypoint movement of the nodes were given by above mentioned simulation result. The node to be started with is n1 and it will keep on sending the Hello packet till it reaches n9. Each and every node were works with the simulation worm hole attack detection and with RREP to detect black hole attack. The node displayed in the grid also shows its locations. The attack were measured based on the node location which are already mentioned in the Grid simulation. Using the node location with DV-hop propagation, their positions were calculated and thus invoke the hello packet to the nodes. This strategy was applied to each and every node until the destination node is reached.

In the Fig 3 it consists of 4 node starting from no to n3 with the interference range with GPS space. It uses agent type UDP for simulation wireless scenario. In the above mentioned network model the attack is measure based on the interference range by which the node location is calculated. The interference range provides the range of access of the mobile nodes by which the attack possibilities are limited. This range will further provide the duration of packet transmission. When there is data transmission between mobile nodes the time is calculated and attack is measured. If the time taken is maximized, then the nodes were unable to generate RREP. If there is no acknowledgement in the form of RREP then node will sense the attack (black hole) and it will discontinue its transmission. The link further will be disabled where the data transmission is not possible and avoids worm hole attack. In this format the distance were measured and the location using DV-Hop using for formulae 2 and 3.

**B. Simulation result**

The results were shown below deals with the comparison of the routing protocol with 100 mobile nodes. The work focuses on traceability of the worm hole and black hole attack. This work was the results derived using NS2 simulator for mobility pack.



| | | | | | |
|---|---|---|---|---|---|
| Attack detected | Wormhole, Black hole | Wormhole, Black hole | Wormhole | Worm hole | Worm hole |
| Acknowledgement | 5 | 7 | 15 | 22 | 27 |
| Send Packet | 10 | 15 | 20 | 25 | 30 |
| Agent | UDP | UDP | UDP | UDP | UDP |
| Protocol | AODV | AODV | AODV | AODV | AODV |

*Fig 5.* **Attack notification with AODV**

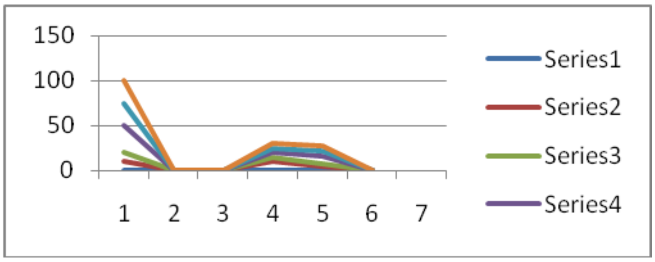
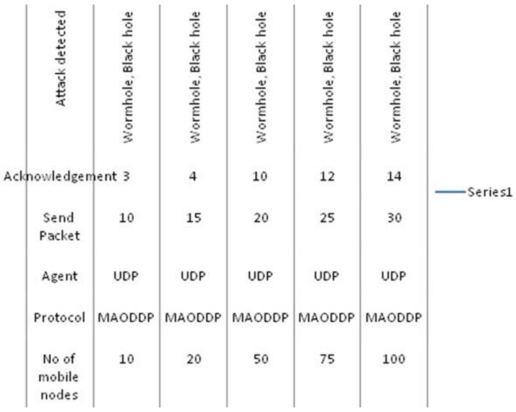


***Fig 6:*** **Sample Graph shows the Worm hole and Black hole attack using AODV**



| | | | | | |
|---|---|---|---|---|---|
| Attack detected | Wormhole, Black hole | Wormhole, Black hole | Wormhole, Black hole | Wormhole, Black hole | Wormhole, Black hole |
| Acknowledgement | 3 | 4 | 10 | 12 | 14 |
| Send Packet | 10 | 15 | 20 | 25 | 30 |
| Agent | UDP | UDP | UDP | UDP | UDP |
| Protocol | MAODDP | MAODDP | MAODDP | MAODDP | MAODDP |
| No of mobile nodes | 10 | 20 | 50 | 75 | 100 |

*Fig 7.* **Attack notification using MAODDP protocol**

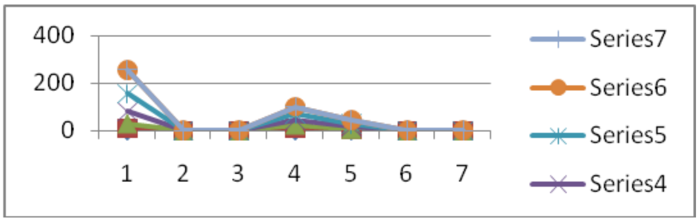


***Fig 8.*** **Sample Graph shows the Worm hole and Black hole attack using MAODDP protocol**

The above results show the comparison between AODV and MAODDP to explore the attack. The impact of the above mentioned result for AODV which will explore Worm hole attack when acknowledgment happens in less time. As the acknowledgment increases in time only worm hole attack can be traced and it fails to trace black hole attack. The proposed MAODDP routing protocol produce result for tracing both worm hole and black hole attack. Since the acknowledgement time was limited it can produce result for both worm and black hole attack.

## IV. CONCLUSIONS

In this work the usage of AODV and MAODDP protocols were used to trace worm hole and black hole attack. In order to trace black hole attack that will be missed out by few nodes if the times taken for acknowledge increases. Despite using AODV protocol will eradicate worm hole attack and further tracing black hole attack leads to failure due to lack in time for acknowledgement. To trace both attack and to create an IDS, MAODDP routing protocol were used. The impact of MAODDP routing protocol will detect and prevent both the attack. Increase the acknowledgement timing will increase RREP and thus Black hole attack is prevented and to find the lack in transmission leads to detection of black hole attack. To eradicate Worm hole attack in the network, efficient data transmission were done among nodes based on node position location using landmark will detect worm hole attack and simulating the result based on efficient data transmission will eradicate worm hole attack. Thus this system will act as efficient IDS to detect and remove the attack in the mobile nodes.

## ACKNOWLEDGMENT

I would like to extend my sincere gratitude to my guide and for those who encourage me in accomplish this research work. I would also extend my appreciation to my students of MCA, Thiagarajar School of Management, Madurai for their interest and hard work extended in my research work.

## REFERENCES

[1]. “Location determination Algorithms for Distributed Wireless Sensor Networks”, Manika Sethia, Priti Mahale, Sonal Sheth, 2008

[2]. Hai Vu, Ajay Kulkarni, Kamil Sarac, and Neeraj Mittal, “WORMEROS: A New Framework for Defending against Wormhole Attacks onWireless Ad Hoc Networks”, Springer 2008

[3]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, ”Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[4]. Capkun, S., Butty´an, L., Hubaux, J.P.: SECTOR: secure tracking of node encounters in multihop wireless networks. In: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 21–32 (October 2003)

[5]. Hu, L., Evans, D.: Using Directional Antennas to Prevent Wormhole Attacks. In: Network and Distributed System Security Symposium (February 2003)

[6]. Eriksson, J., Krishnamurthy, S.V., Faloutsos, M.: Truelink: A practical countermeasure to the wormhole attack in wireless networks. In: Proceedings of IEEE ICNP, pp. 75–84 (November 2006)

[7]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, ”Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magzine, vol. 40, pp. 70-75, 2002

[8]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575

[9]. C. E. PERKINS, P. BHAGWAT Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234–244.

[10]. H.Bakht: Theory of Centralization for Routing in Mobile Ad-hoc Network, Annals Computer Science Series, 9th Tomb, 2nd Fasc, 2011

[11]. “DV Based Positioning in Ad Hoc Networks”, Dragos Niculescu and BadriNath, 2002.