International Journal of Control Theory and Applications

ISSN : 0974-5572

© **International Science Press**

Volume 10 • Number 30 • 2017

Detection of Malicious Nodes using Intelligent Authorization Agent for Clustering in MANETs

A. Aranganathan[a] and C.D. Suriyakala[b]

[a]Research Scholar, Sathyabama University, chennai
E-mail: a_aranganathan@yahoo.com
[b]Professor, Dept.of ECE, SNGCE, Kerala
E-mail: drcdsk@yahoo.in

Abstract: Mobile adhoc networks consisting of collection of nodes. MANET does not rely on any fixed infrastructure. It is among one of the main research areas and it has grown drastically through the past several years. The lack of a centralized monitoring point makes it vulnerable to many network attacks. Mobile adhoc networks may moves in any path from source to destination node and frequently changing topology. The motivation of the adhoc networks is to decide by own with neighboring nodes and communicate it to other networks. Many intrusion detection systems have been found to prevent these attacks. Cluster Head (CH) plays a major role in wireless networks.CH selection is based on many factors like node density, mobility, geographical location and energy. It acts as a special mobile node which can communicates with other cluster head through gateway nodes. But these cluster heads can get attacked by the intruders. In the proposed system, using Intelligent Authorized Agent based Detection (IAAD) for the detecting purpose. IAAD has proved the improved performance in terms of packet delivery ratio, throughput in AODV based clustering routing protocol using *ns*2.

Keywords: *Cluster Head, AODV, intelligent authorization agents, MANETs.*

1. INTRODUCTION

MANET is a self-configuring infrastructure consists of mobile nodes connected by wireless links. It has the properties of no infrastructure deployment and has no centralized control management. Mobile nodes play as host as well as routing network in many cases. It is naturally in autonomous condition. Many of the nodes are free to move in any other directions with different cycles. Mobile ad-hoc networks are used for wireless security operations, rescue operations. Some of the features of adhoc networks are as follows

1. **Node movement:** Mobile nodes are movable from anywhere within the limited area. It makes a dynamic topological environment. Nodes may share the information via unidirectional and bidirectional way and also speed may varies depends upon the type of applications.
2. **Energy conservation :** Mostly nodes are battery operated device to must share the data packets within the time period for conserving efficient energy. So that the optimizing the energy conservation is important. So MAC layer plays a vital role in mobile ad-hoc networks.

3. **Bandwidth limitation:** Only limited bandwidth is available for each node. Due to less stability, capacity and reliability of nodes in wireless networks compares to wired networks.

4. **Security:** There is a possibility of attacks which makes disrupting the network performance. Some of the attacks like packet dropping attack, eavesdropping and wormhole attack are to be monitored carefully. So as to design efficient routing protocol with improved security against malicious attacks.

   Mobile ad-hoc networks ranging from small scale to large scale networks that are collaborative and distributed computing, military applications, emergency operations. But it some efficient algorithms for determining scheduling and routing functions.

1.1. Clustering in MANETS

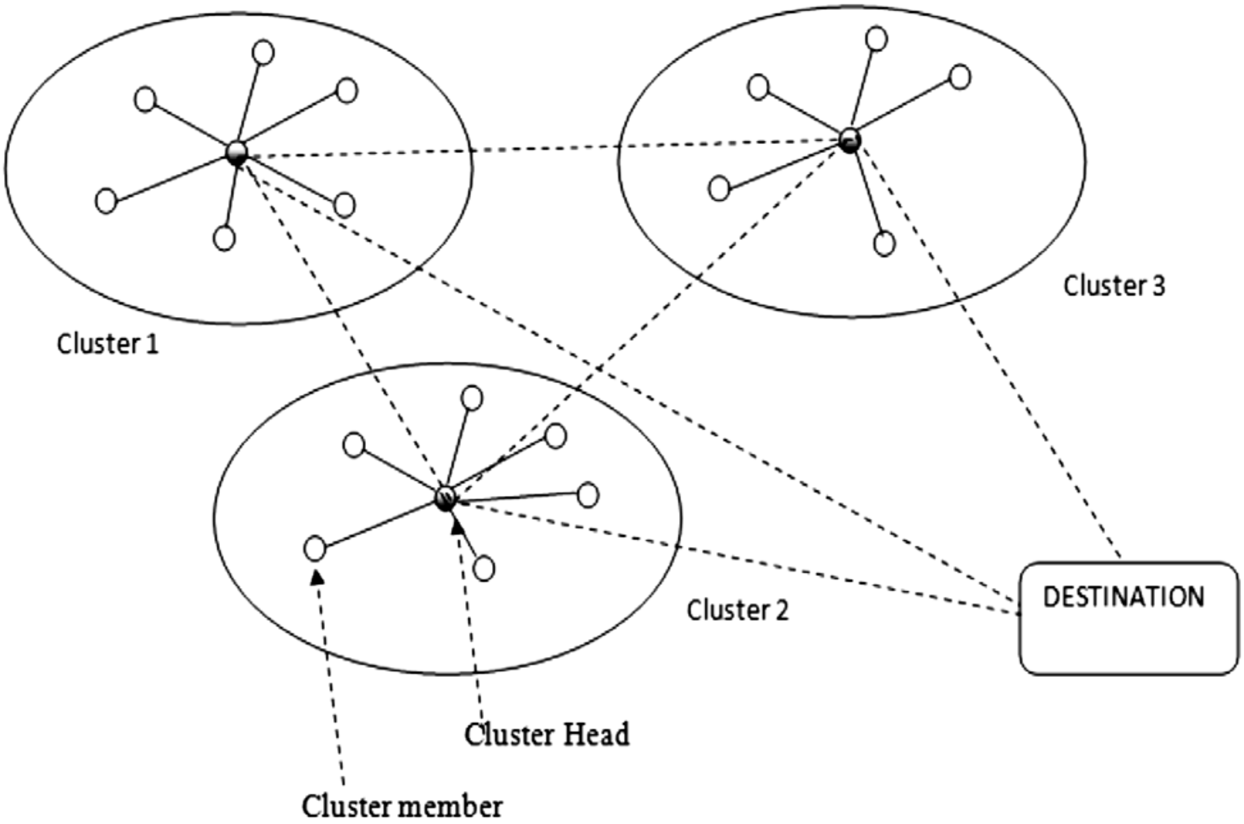

Figure 1: Cluster formation

------- Inter- cluster communication

——— Intra-cluster communication

In a clustering scheme, mobile nodes are divided into many groups to form a cluster. Each mobile node in a cluster has a different behavior from other clusters. Under the category of cluster formation, mobile nodes are assigned by different names called cluster member, cluster head (CH), gateway. Clustering is a hierarchical network is used to divide the entire network into many small networks with some number of member nodes. Every cluster has one special node which creates the member nodes known as Cluster Head. Many member nodes can directly communicate with single cluster head through gateways. Member nodes can transfer the information packets to the neighboring cluster Head.

1.2. Denial of Service attacks in MANETs

The main motive of Dos attack is memory, storage space or CPU of the service provider. It means that the malicious nodes continuously sending of unwanted data packets to the legitimate nodes to make heavy load traffic called flooding attack. Malicious nodes consume more energy of all the neighboring nodes to degrade the performance of networks.

Malicious nodes performs many types of attacks namely, blackhole attack, grayhole attack, wormhole attack, route disruption attack. Blackhole attack is to drop all the received data packets from legitimate nodes where grayhole attacks drops few data packets only. Wormhole attack is dangerous attack which acts as a tunneling that means there are two malicious nodes are dropping the data packets between the source and the destination without the knowledge of any legitimate node. Rout disruption attack send forged routing packets for creating routing loop without reaching to the destinations. It consumes more energy and bandwidth.

2. RELATED WORK

1. Authors Proposed four modules of mobile agent namely registration, service, detection and prevention module. During the network deployment, all the nodes including cluster head and cluster member should be registered with Mobile agent through registration module. Each node to get acceptance from Service agreement for required applications. During entire network deployment, intrusion detection module is used to monitor the each packet routed by cluster head. Then prevention module for securing the data packets with application ID. If ID does not match or exceeding packet length, CH drops the packets. A threshold packet length is predefined for detecting misbehavior nodes. Drawback is that heavy overload due to MA with multiple functions leads to error and also cost of deployment is high.
2. Author's proposed specialized intrusion detection system by agents for detecting malicious nodes against black hole attack. Sender node which creates mobile agent and it can transmit data through forward path to the destination node. Mobile agent calculates data transmission called throughput. If there is no malicious node present in the network, the network proceeds the next process by transferring the data packets from cluster head to the neighboring cluster head Otherwise, it assumes that there is a intruder present in the network.
3. Fault tolerance based model using secure agents mainly used for increasing fault tolerance and reduces the nodes failure using mobile agents and also compared with some existing security approaches were discussed in this paper.
4. This paper proposed IDS architecture with mobile agent mechanism. It has four types of agents namely, network monitoring agent, host monitoring, decision making agent and action agent.

   Many of the nodes are grouped into cluster, one cluster head will be selected for each cluster. In cluster networks, node monitoring selection algorithms have been proposed with network monitoring agent and host monitoring agent used for preserving battery power and monitoring each node in mobile adhoc networks. Decision making agent is used to collect the intruders and make necessary decisions about intrusions. Action agent is to responsible for avoiding intrusions.
5. Authors implemented lightweight agent for minimizing the functionality .Compared to heavyweight agents, lightweight agents are small size, simple, update and also upgrade. These agents for detecting intrusion activities.

   AODV (Ad Hoc On demand Distance Vector) is popular routing protocol in MANETs [6]. Using on demand basis with route discovery and maintenance process when the network topology is in dynamic nature. The advantage of this protocol has low memory overhead. In AODV-Clustering approach , there are many designing goals for improving the performance of gradualness, cooperate with AODV in hierarchical routing protocol for selecting cluster head selection and quick route discovery and route repairing mechanism.

3. PROPOSED SYSTEM:

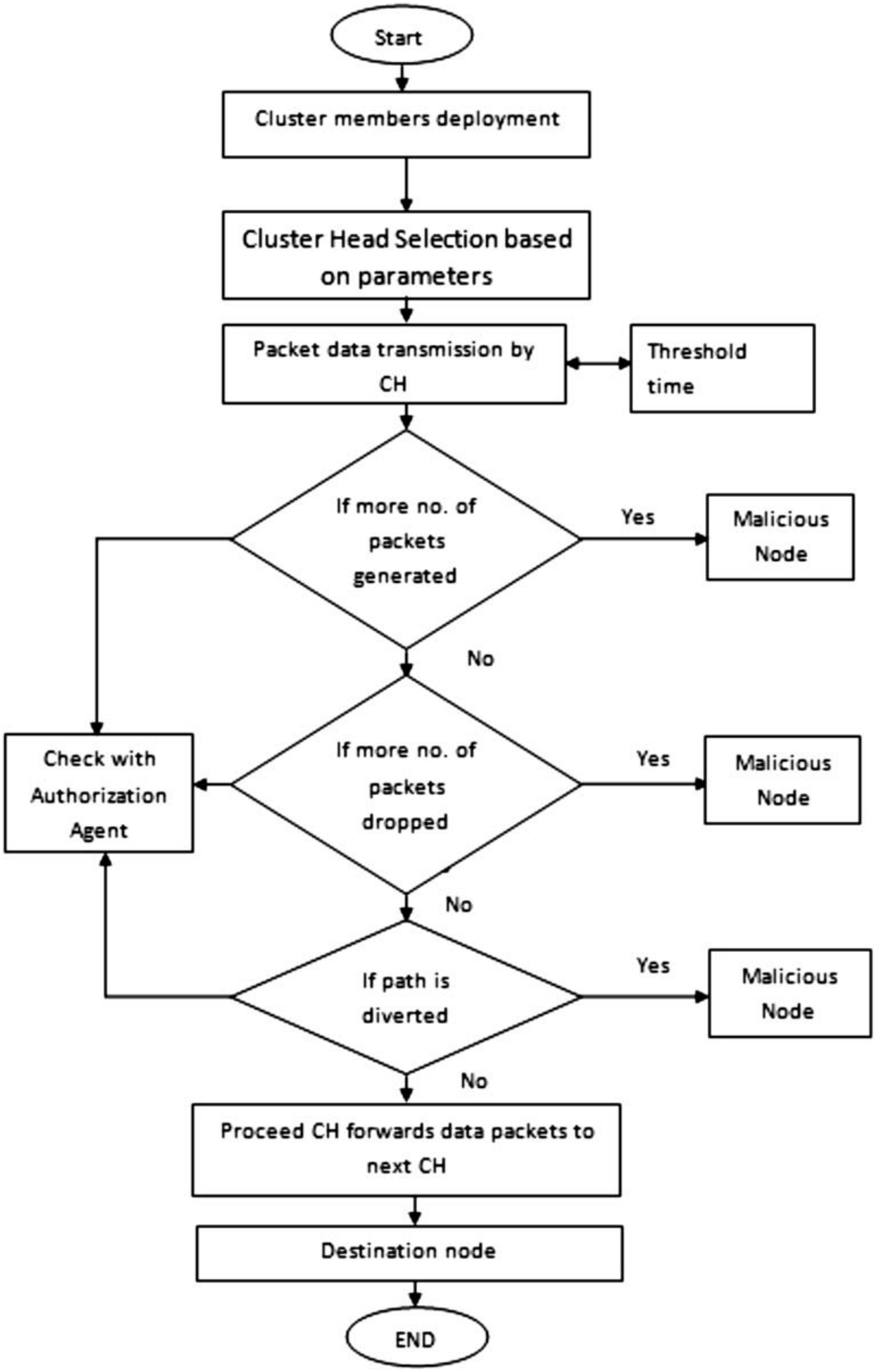
Start
Cluster members deployment
Cluster Head Selection based on parameters
Packet data transmission by CH
Threshold time
If more no. of packets generated
Yes
Malicious Node
No
Check with Authorization Agent
If more no. of packets dropped
Yes
Malicious Node
No
If path is diverted
Yes
Malicious Node
No
Proceed CH forwards data packets to next CH
Destination node
END

Figure 2: Flowchart for Proposed Intelligent Authorized Agent based Detection System

There are many methodologies for selecting cluster head procedure namely identifier based clustering, connectivity based clustering, mobility aware clustering, low maintenance cost clustering, power aware clustering. In the proposed scheme, cluster head selection based on the parameters like cluster ID, distance and residual energy of the node. The entire network is divided into form clusters.Clusted Head can be elected based on the above parameters. Authorization agent has been introduced for authenticating the cluster member information with threshold time of 10 seconds. If the threshold time exceeds, it can be considered as a malicious nodes. After electing the CH, data packets can be transmitted to the neighbor through routing protocol to reach the destination. During the transmission, there are three possibility of malicious attacks can occurs

1. More number of data packets generated at a specific time period
2. More number of data packets are dropped and
3. Path may be diverted

   Otherwise data packets can be forwarded to the neighborhood cluster head to reach the destination by routing procedure of AODV protocol.

4. SIMULATION PARAMETERS

Table 1
Simulation parameter Table

Parameter	*Value*
Simulator and Version	Ns -2.34
Number of Nodes	100
Channel	Wireless channel
MAC Type	802.11 MAC layer
Routing Protocol	AODV
Traffic model	Constant Bit Rate
Packet size	512 Kbps
Threshold time	10 sec
Antenna	Omni directional

4.1. Results and Discussions

Simulation parameter and its values are given in the table 4.1. There are two performance metrics of throughput and packet delivery ratio of existing [12] (modified AODV approach) and proposed (intelligent authorization agent based approach) are analyzed.

1. **Throuhput:** The total number of data packets transmitted to the total number of data packets received at a time. In fig 4.1 there is an improvement in the throughput of agent based system with time period when compares with existing system [12].
2. **Packet Delivery Ratio:** It is nothing but total numbers of data packets are successfully delivered to the total number of data packets sent by a source node. Hence the packet delivery ratio can be improved by a proposed system with speed.

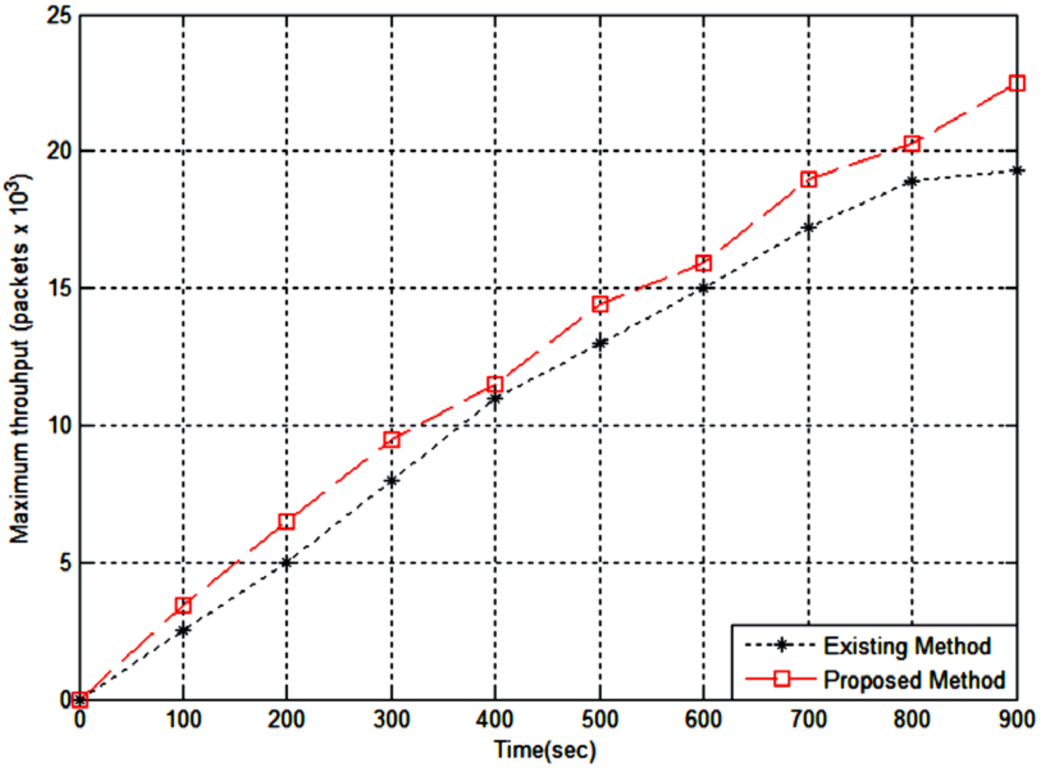

Figure 3: Time verses maximum throughput

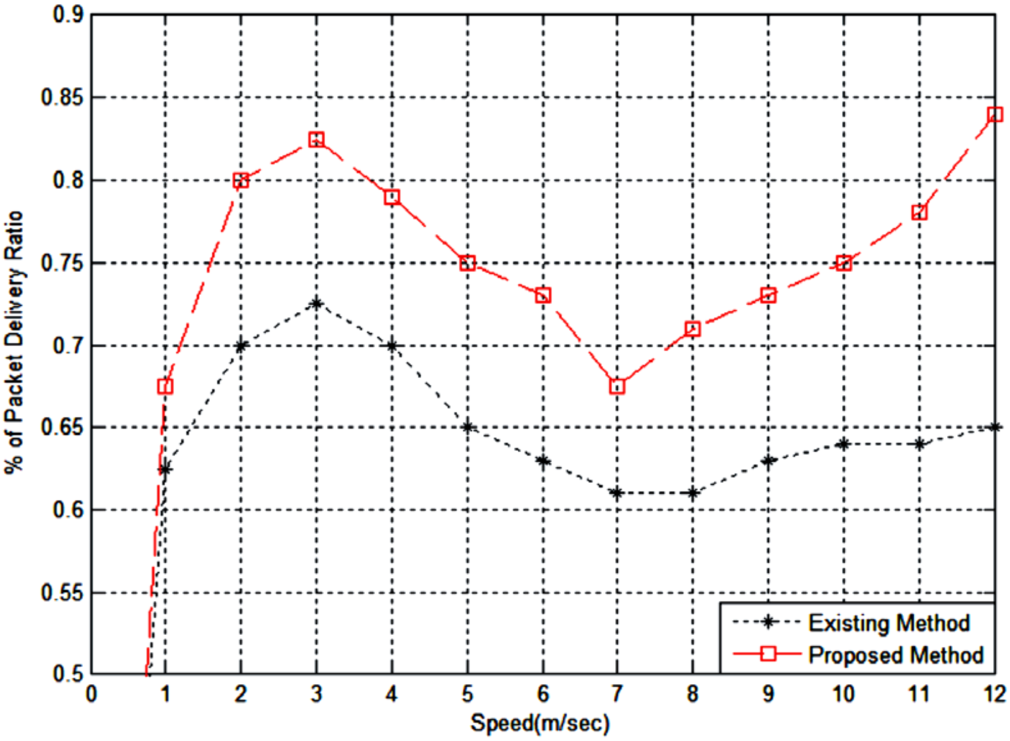

Figure 4: Speed verses % of packet delivery ratio

5. CONCLUSION AND FUTURE WORK

Denial of service attack is very dangerous in routing protocol AODV. In the existing approach, there are many algorithms proposed using agent based detection algorithms against malicious attacks. The proposed authorization agent based system is successfully implemented authenticated nodes in the networks with improved performance metrics of packet delivery ratio, packet loss rate, end to end delay and throughput against malicious nodes in mobile adhoc networks. In future, every node can be secure with security key for preventing unauthorized nodes (malicious nodes) in the networks.

REFERENCES

[1] Binod Kumar Pattanayak and, Mamata Rath, “a mobile agent based intrusion detection system architecture for mobile ad hoc networks” , Journal of Computer Science 10 (6): 970-975, 2014, ISSN: 1549-3636, 2014 Science Publications, pp-970-975.

[2] Debdutta Barman Roy, Rituparna Chaki, “BAIDS: Detection of Blackhole Attack in MANET by Specialized Mobile Agent”, International Journal of Computer Applications (0975 – 8887) Volume 40– No.13, February 2012, pp 1-6.

[3] Cansin Turguner, Computer Engg. Dept., Turkish Air Force Acad., Istanbul, Turkey, ” Secure data dissemination in MANETs by means of mobile agents”, IEEE Communications (COMM), 2014 10th International Conference , 28th July 2014.

[4] Oleg Kachirski, Ratan Guha,School of Computer Science, University of Central Florida, Orlando, FL 32816, U.S.A., “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks”, Proceedings of the IEEE Workshop on Knowledge Media Networking. 2002.

[5] G. Helmer, J. Wong, V. Honavar, L, Miller, “Lightweight Agents for Intrusion Detection”, Technical Report, Dept. of Computer Science, Iowa State University, 2000.

[6] ZHENG Kai, WANG Neng, LIU Ai-fang,Dept.of compuer,East china Normal University,Shanghai,China, “A new AODV based clustering routing protocol”, IEEE international conference on wireless communications, networking and mobile computing, 2005,pp 682-685.

[7] JANE y. Yu and peter h. J. Chong, Nanyang Technological university, “A survey of clustering schemes for mobile ad hoc networks”, IEEE communication surveys,first quarter, volume 7, NO.1, 2005.

[8] Hu Y.C, A. Perrig; “A Survey of Secure Wireless Ad Hoc Routing”; Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

[9] Jane Y.Yu ,Peter H.J.Chong, “A Survey of clustering schemes for Mobile ad hoc Networks”, IEEE communications and surveys,Vol.7,IssueNo.1,pp.32- 47,2005.

[10] Perkins C.E, Ad Hoc Networking, Addison-Wesley, 2001.

[11] Belding E.M -Royer, “Hierarchical Routing in Ad Hoc Mobile Networks,” Wireless Commun. and Mobile Comp., vol. 2 Issue No. 5, pp.515–32, and 2002.

[12] Sanjay K. Dhurandher, Issaac Woungang, Raveena Mathur, Prashanth Khurana“A Modified AODV against Single and Collaborative Black Hole Attacks in MANETs”, IEEE international conference on Advanced Information Networking and Applications Workshops (WAINA), 25-28 march 2013.