International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-12, Mar 2019

RAODV Routing Protocol based Malicious Node Detection in MANET Environment

P. Karthikeyan, Assistant Professor, Department of Computer Science and Engineering, UCE, Anna University, Tiruchirappalli, India. karthiaut@gmail.com

Dr. J. Raja, Professor, Department of Electronics and Communication Engineering, Sri Sai Ram Engineering College, Chennai, India. rajajanakiraman@gmail.com

Abstract: Nowadays, the mobile ad hoc network is becoming increasingly popular in the research area. Because world necessity is to create user friendly environment, less cost, compatibility and without any disturbances to social environment. In that time wireless communication technology was born. The great communication achievement is possible through MANET, without base station and pre-existing setup help to reduce human interaction. These types of network are very useful in critical situations. Ad hoc environment all nodes are move freely. Here data communication is challenges. So many researchers suggested several techniques to solve them but it is need updation continuously due to recent types of attacks are very vulnerable to detect and prevent them using existing routing protocol with additional of some parameter are introduced to enhance detecting malicious activities. The proposed method Node's packet receive and send activities are monitored through efficient on demand basis. Ad-hoc On Demand Distance Vector (AODV) is used with addition of few new constraints. i.e., Reanalysis base AODV (RAODV) algorithm. The experimental show that the improve result of the proposed technique compare to the existing algorithm by using NS2 simulator.

***Keywords — Back truck base, Cluster, MANET, RAODV, Reanalysis, Secure Transmission, Trust rate*.**

I. INTRODUCTION

MANET is an ad hoc network which involves no support for infrastructure and wireless network to also start carrying packets of data between two nodes through radio communication shared medium. Source to destination data transmission stage so many nodes are participate as intermediate nodes [1]. Every node maintain neighbor nodes details. The intermediate nodes are need to monitor is very complicated because they are scatter (figure 1.) around the territory in ad hoc environment [2, 3]. The packets are transfer from source to destination in scatter nodes communication is so hard, because all are mobile nodes the intermediate nodes activities are monitor exactly is very difficult because node 'x' is near in distance d1 after few time period it may be move to distance d2. In that time node x knows activates of a node at distance d1 but does not know activities node at a distance d2.

Source to destination node data transfer operation using routing protocol [4, 5] they are classified into proactive routing, reactive routing and hybrid routing protocol. Proactive or table driven based approach define all nodes are continuously monitor and update to its routing table, it is relatively stable link network. Reactive or on demand based approach define all nodes are monitor by on demand basis.

Finally hybrid based approach define nodes activities are updated by using above two methods, it is based on inside of the cluster use proactive routing and outside of the cluster use reactive routing.

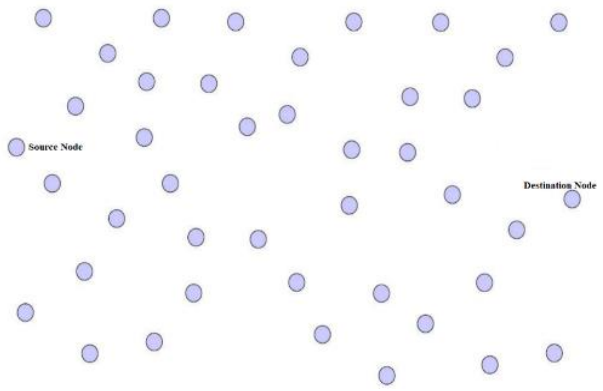


Figure 1. Nodes in MANET

Scatter nodes are arrange into isolate groups. They are called clusters. Node activities are monitor and controlled by head of the cluster it is present inside the group. It is responsible for monitor and control gate way nodes and normal nodes within territories. Gate way node is responsible for transfer data to another cluster's gate way node.

 DOI : 10.18231/2454-9150.2019.0186

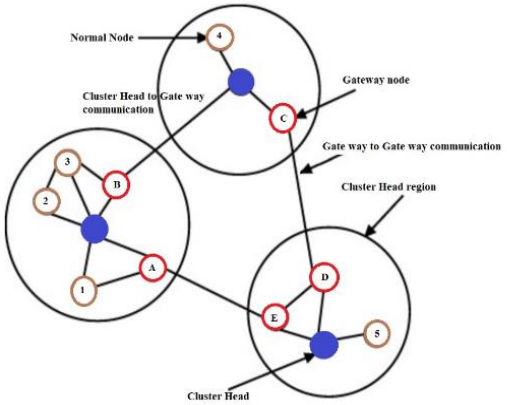


Figure 2. Cluster communication

II. PROBLEM STATEMENT

MANET is an important issue to consider where wireless nodes are coordinated in a wireless network without any predefined infrastructure and services. Securing MANETs is a key part of their deployment and use as MANET is often used in critical applications where truthfulness of data and communication is essential [6] Established wireless network solutions can be used to achieve a certain level of sophistication security. However, these solutions may always be sufficient, as the ad hoc network has its own security vulnerabilities that these solutions cannot be address. To acquire an adequate level of security in such a framework and security resolution need in malicious node detection. Efficient communication occurred in MANET need energy and power aware routing algorithm [7, 8].

III. RELATED WORK

In Mobile Ad - hoc data security architecture which an intrusion detection system (IDS), each node is examined [9, 10]. The node in the MANET with in its interaction range, which nodes are, gathers by IDS, the data transmit normal and abnormal behavior to its neighborhood predicated only on a processed host and new data. The theory of abuse detection which can correctly suit the sign of known attacks. A threat detection scheme for intrusion based on adjoining node's abnormal behavior [11].

Within its radio range, each node monitors particular traffic activity. All intrusions observed locally are kept in an investigation file. When local investigation data are collected, some algorithm can be used to correctly identify unresolved attacks from the collected data [12].

AODV is a reactive type of protocol. His technique is data forwarding hop - to - hop. So the intermediate mobile nodes transfer the data for the path and these intermediate nodes generate a reverse route to the destination [13] at the same time.

AODV[14] is based on a classical hop - by - hop forwarding method for short distance vector routing. When propagating RREQ messages, the route is developed by having left a backward route to the source at intermediate nodes and left a through route to the destination at intermediate nodes when transmitting the RREP packet to the source.

AODV protocol formed the wireless network routing between two nodes based on route tracking and route repairs [15]. In the route require system, RREQ message was broadcast to the target node in the form of flooding; the target node selectively choosing the first - received RREP and sent RREP data in the route response system. Since the node is hectic to find routines, the route was simple. In the routine maintenance and repair process, the damaged node would reject the anomaly packet and realize the source node to reattempt request message when transmitting RERR packets, which would cause the consequent packet to be postponed [16]; in order to remove the loopback precipitated by new commuting, local repair could cause the downstream node sent RREP to be discarded, which decreased the possibility of routing recovery process

The proposed scheme has been integrated by AODV protocol Perkins C et al. [17] have proposed some technique incorporated using Ad hoc Distance Vector routing protocol. It trace the path when it is required and packet has been transmit that route. However, in order to maintain routing data, AODV invents a very different method. It uses established tables of routing, one entryway per point of origin. AODV depended on routing table listings without source to disseminate routing a route reply message back to the first initiated node and then destination node got route data packets. Number order uses in AODV protocol to find the newness of routing data at each desired destination nodes and to completely reduced loops formation of routing. These arrangement numbers are passed by all data packets. AODV's important feature is the preservation in each node of timer-based statuses regarding the use of discrete routing table records. If not used freshly, a routing table record will finish. For each routing table registration, a set of instant precursor nodes is maintained, suggesting the set of adjacent nodes that use that invitation to route data streams. When the next - hop link terminate, these nodes will be alerted with route error packets. In turn, each antecedent node forward the route error to its own set of ancestors, effectually removing all paths through the damaged link. The broadcast of route faults in AODV can be abstractly imagined as a tree whose node is the root at the fact of defeat and all sources using the unsuccessful link as the leaves. AODV's benefit is that it create perfect communication traffic along present links. Also, the routing of distance vectors is simple and requires little memory.

The proposed a scheme used for recognizing misbehavior nodes [18]. Trust prediction method based on fuzzy system and discovering the malicious node. Two types of approaches are used here, they are compute current trust of node and historic trust. Secure routing protocol used to define the secure path. Predict the trustworthiness of node

 DOI : 10.18231/2454-9150.2019.0186

used first dynamic prediction model, it use historical activities. All nodes activities are monitored based on historical behavior, it evaluate present node activities. Malicious node identified and eliminated. Finally secure path based data packet broadcast through desired nodes.

The author suggested a method to identify the RREP node author's neighbor [19], i.e. the node suspected. Neighbor node is trained to monitor through doubted activity node for all the data sent. Neighbor node including of fcount and rcount holds two security values. While a neighbor node transfers any packet to the suspected node, the fcount counter will increase by 1. If the suspected node transfers a packet, the neighbor node will probably overhear it and the rcount will growth by 1. After receiving RREP from the source node, it sends packets to the route to check whether or not the node is malicious. Nearby node moves packets to suspect node until fcount reaches a threshold; if rcount is 0, then. The author of RREP will categorize and block the node as malicious.

An exclusive method to wormhole discovery was planned [20, 21]. The connection of the wormhole is analyzed by estimating the extreme E2E delay within the communication range between two nodes. The suggested system uses threshold limits to observe the connection of the wormhole without any different hardware being required. There are certainly independent routes on this scheme. Data gathering procedure is single time because with appreciation of coverage area we calculate most distance. This can offer us with the high time delay value that can occur between the two nodes while transmitting the data to the final node and sending the data down to the initiated node.

Gupta et al. [22] offered Real Time Monitoring AODV as a kind of new technique. It no lengthier introduces overhead. In addition, the neighboring node detects and prevents the use of real time observing from attacking the black hole. In immoral mode, the source node sends RREQ is monitored. Neighbor node Route Reply (RREP) i.e. suspected node is definitely used to detect malicious node. Two counters are used as fvalue and rvalue to take a monitor at malicious node. These are used to count the amount of packets sent and the wide variation of data packets obtained. Fvalue touches a threshold limit and value is 0 then node is measured malicious and dismissed from the community via INTNOT Packet broadcasting.

Detection, Prevention and Reactive AODV was recommended [23]. On this research, authors offered new method DPRAODV based MANET to secure black hole attack by notifying various nodes in the group. The node obtains the route reply packet first evaluates the value of arrangement number in its routing table in regular AODV. If its order number is improved than the routing table in one, this packet is recognized by route reply process. In this result, an additional checked is agreed whether or not the route reply arrangement variation is greater than the threshold limit. If it is greater than the threshold limit, the node is measured to be a misbehavior node and it affords the black inventory.

Bandwidth Control Management algorithm contains a bandwidth controller [24]. It determines a new flow that can be permitted without disturbing the previous flows. The bandwidth calculation algorithm is used to calculate the bandwidth. Multi priority admission and rate control protocol reduce the communication failure and choose different communication path from source to destination node. Wireless components are capable to distribute multimedia data from source to destination.

In this paper [25] the author has bandwidth evaluation is done by local accessible bandwidth and neighbourhood available bandwidth. Here the bandwidth computes for semi saturated, saturated and unsaturated network using MPARC. Here incoming packets from new route delay is not measured. In MANET mobility of the node changes its links hence it affects the available bandwidth.

The author [26] has separated the transportation to video, audio and data. To achieve Quality of Service in the chosen network finest path when link bandwidth deficiency. QoS involves two major fragments they are route detection and route preservation and retrieval.

Energy Harvesting in a Modified Opportunistic Routing Protocol [27], a different Tactic in Wireless Sensor Network. A similar type of message is delivered to multiple receivers, is called multicast. The broadcast is a simple way to data transmission in MANET. It consumes significant bandwidth and energy. The best solution is to use a multicast transmission in MANET. It prevents bandwidth wastage. Multicast routing protocol consists of three major categories they are proactive, reactive and hybrid multicast.

Bo Zhu, Member, IEEE, Sanjeev Setia, et al proposed a Localized Multicast approach [28] to avoid duplication attack in nodes. It is distributed to approach adept for data transformation and storage overheads in large networks. The position of information in a MANET where each node holds its position. Nearest node position is changing frequently in MANET, it is updated in Neighborhood node information. Local Server Update mechanism is to update Infrequent modifying its position information.

IV. PROPOSED WORK

On demand basis protocol, a better updation is required for the proposed Reanalysis base AODV (RAODV). Routing table contain Destination node, sequence number, Hop count, Next hop, Expiration Timeout and Node Trust Rate. Here Node Trust Rate contain two state '0' and '1'. '0' stand for not recommended this mean malicious node & '1' stands for recommended this mean normal node. Based

 DOI : 10.18231/2454-9150.2019.0186

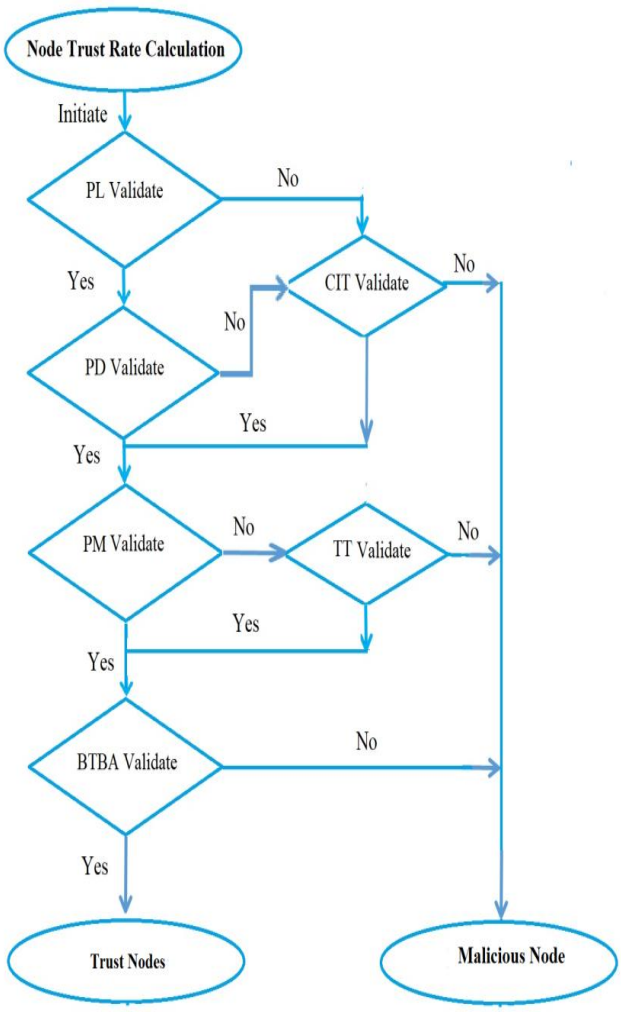
on current scenario lack of AODV protocol, a better protocol is needed in exiting routing protocol to prevent node's malicious activity, network delay and routing overhead. A new improved approach RAODV based on AODV was designed additionally add with trust node field. The proposed node trust rate calculated by state level technique this value is consider for the routing table efficient purpose.

Route establish:

The cluster based approach clearly route the packet from source to destination. Consider the figure 2. Cluster head know five node's (node1, node2, node3, nodeA and nodeB) characteristics based on past history. It is linked based on satisfied some parameters such as signal and battery level, packet drop, delay and misroute.

Node1 want to transmit data to node3 there is no problem because both nodes are present in the same cluster. Here node1 initiate to send packet to cluster head and cluster head verify his route table, if it is present than cluster head receive that data and send to appropriate destination node.

Node Trust rate Calculation:



Node Trust Rate Calculation

Now node1 wants to communicate node4, here node1 send data to node1's cluster head, it search in its table but not present after that data will be send to gate way node such as nodeB and nodeA. Gate way node, nodeB directly connected to cluster head, it contain node4 and nodeC, cluster head check on his table node4 is present if yes send to the destination otherwise it will be forward to gate way node.

Simultaneous process of the gate way nodeA send packet to the gate way node the it will reach to its cluster head, it check his routing table it is not present than sent to gate way nodeD and gate way node C receive and send to its cluster head finally reach the destination. The route reply sent by the node4 through its cluster head to nodeB and its cluster head, finally reach node1. The intermediate nodes are counted from destination to source is 4. Another route replay sent by the node4 to node1 the intermediate nodes are calculated from destination to source that is 8.

S-D path1 = {Node1}{Cluster Head, NodeB, Cluster Head} {Node4}

S-D path2 = {Node1} {Cluster Head, NodeA, NodeE, Cluster Head, NodeD, NodeC, Cluster Head} {Node4}

The RAODV protocol measure the distance between node1 to node4

Distance of Node1-4 = min{S-D path1, S-D path2} = S-D path1

Communication starts to S-D path1.
Malicious node detection technique:

Packet loss (PL):

$$PL = \sum_{k=0}^{n} \frac{PFN_{XK}}{PRN_{XK}}$$

PFN - packet forwarded to node x
PRN - packet receive to node x
PL value greater than 10% it will be analysis by following parameter

Channel idle time (CIT)
Node x size of the bandwidth at forward time T1 is measure
Node y size of the bandwidth at received time T2 is measure

$$CIT = \sum_{k=0}^{n} T_{K1} + T_{K2} \geq RPS$$

T1 & T2 - time period bandwidth size
RPS- required packet size

if bandwidth value greater && stable Link
  suspicious node
else
  normal node

Packet Delay (PD):

$$PD = \sum_{k=0}^{n} \frac{PST_K}{PRT_K}$$

 DOI : 10.18231/2454-9150.2019.0186

PST - packet sent time
PRT- packets receiving time
CIT = $\sum_{k=0}^{n} T_{K1} + T_{K2} \geq RPS$
T1 & T2 - time period bandwidth size
RPS- required packet size

if bandwidth value greater
suspicious node
else
normal node

Packet Misroute (PM):

$$PM = \sum_{k=0}^{n} PMR_{K2}$$

PMR - packet misroute
TT = BT - IT
TT – Total Time
BT - Busy Time
IT - Idle Time

Actual transfer node traffic rate is analysis it is busy or not.

if traffic value less
suspicious node
else
normal node

Node Trust Rate

$$NTR = Min\left\{\sum_{k=0}^{n} \frac{PFN_{XK}}{PRN_{XK}}, \sum_{k=0}^{n} \frac{PST_K}{PRT_K}, \sum_{k=0}^{n} PMR_{K2}\right\}$$

Back Track Base Reanalysis (BTBR):
Consider any one of clusters (figure 2.). Assume 10 packets transmission to inter cluster communication.

Table 1

Node name	CH
Received from ndoeC	10
Send ack. to nodeC	9
Ratio	9/10*100 = 90%

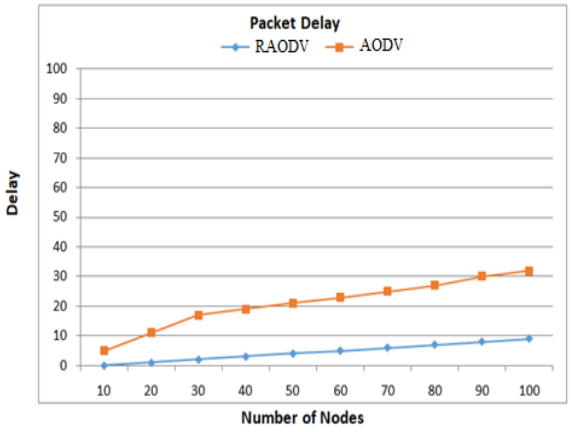
Table 2

Node name Node	4
Received from CH	9
Send ack. to nodeC	9
Ratio	9 / 9 * 100 = 100%

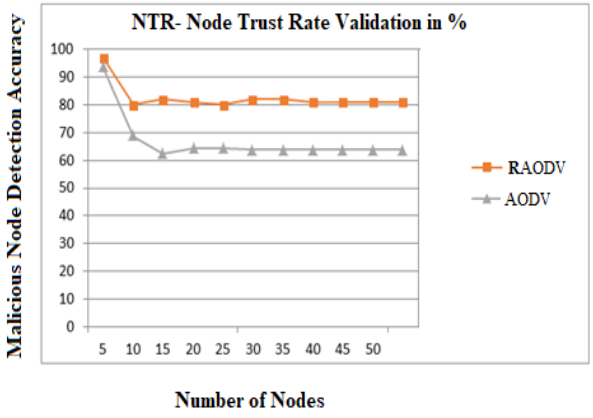
Here Table 2 result is 100% but it is really attain 50% behind that sense Node c sent 10 packets to Cluster head but cluster head send only 9 packets to node4 then node4 send 9 acknowledge packets. So total is tallied, but its actual check is needed, it drop one packet it will be analysis by the above parameters such as PL, PD and PM's and sub estimation evaluated. If it is satisfied above NTR condition, it is termed as normal behavior node.

V. RESULT AND ANALYLSIS

The simulation is based on NS2, starts with arrangement of cluster head and surrounded by normal and gate way nodes. The random interval time data generate in each node. Node trust rate calculation based all parameters are checked carefully. Every 1000ms results are calculated. The data delivery ratio increased compared with previously detected with minimal parameters approach.



The above graph representing the packet delivery ratio of RAODV. The orange color indicate packet delivery (in m/s) ratio of AODV. The blue color curves indicate improvement of packet delivery ratio in RAODV. It shows RAODV works better than previous AODV.



The above graph representing the Node Trust Rate validation through RAODV routing protocol. The grey color indicate packet delivery ratio of AODV. The orange color curves indicate improvement of Trust Rate validation in RAODV. It shows RAODV works 20% better than previous AODV.

Submission of a manuscript is not required for participation in a conference. Do not submit a reworked version of a paper you have submitted or published elsewhere. Do not publish "preliminary" data or results. The submitting author is responsible for obtaining agreement of all coauthors and any consent required from sponsors before submitting a paper. IJREAM strongly discourage courtesy authorship. It

 DOI : 10.18231/2454-9150.2019.0186

is the obligation of the authors to cite relevant prior work.

At least two reviews are required for every paper submitted. For conference-related papers, the decision to accept or reject a paper is made by the conference editors and publications committee; the recommendations of the referees are advisory only. Undecipherable English is a valid reason for rejection. Authors of rejected papers may revise and resubmit them to the TRANSACTIONS as regular papers, whereupon they will be reviewed by two new referees.

VI. CONCLUSION AND FUTURE WORK

The proposed RAODV protocol improves result compare with previous AODV protocol. RAODV uses the reanalysis the node parameters, it will use the whole activities of the nodes are observed. RAODV routing protocol reduce the delay, packet loss and routing overhead. Packet loss is evaluated and it reanalyzed through channel idle time, Packet delay is evaluated and it reanalyzed through channel idle time, Packet modification is evaluated and it reanalyzed through total time, finally Back Track Base Reanalysis method estimated the exact node though this method. Thus reanalysis method very helpful to avoid the mistake while monitoring the node and avoid trust node is noted as malicious node. Misbehavior of nodes are noticed by reanalysis is more efficient than the normal analysis process through primary parameters. As better result is gained, reanalysis of primary parameters such as packet loss, delay and misroute. Future work will be carried out in real time applications to check reliability which is compared with simulation result given in this work. If it attains desirable reliability, the further work will be carried out in cloud computing technologies.

REFERENCES

[1] Raji, V., and N. Mohan Kumar. "An effective stateless QoS routing for multimedia applications in MANET" International Journal of Wireless and Mobile Computing 7.5 (2014): 456-464.

[2] Rath, Mamata, et al. "Load balanced routing scheme for MANETs with power and delay optimisation" International Journal of Communication Networks and Distributed Systems19.4 (2017): 394-405.

[3] Singh, Tejpreet, Jaswinder Singh, and Sandeep Sharma. "Energy efficient secured routing protocol for MANETs" Wireless Networks Volume 23, Issue 4, pp. 1001–1009, May 2017.

[4] S. Kumar, R. K. Rathy and D. Pandey, "Traffic pattern based performance comparison of two reactive routing protocols for Ad hoc networks using NS2" 2nd IEEE International Conference on Computer Science and Information Technology, pp. 369-373, Aug. 2009

[5] Sanabani, M., R. Alsaqour, and S. Kurkushi. "A reverse and enhanced aodv routing protocol for manets" ARPN Journal of Engineering and Applied Sciences 9.2 (2014): 153-159.

[6] Alrajeh, Nabil Ali, and Jaime Lloret. "Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks" International Journal of Distributed Sensor Networks, ID 351047, October 2013.

[7] Ho, Yao Hua, Meng Chang Chen, and Han–Chieh Chao. "Congestion avoidance routing for MANETs" International Journal of Ad Hoc and Ubiquitous Computing, pp. 26-41, May 2014.

[8] Srinivasan, S., and S. P. Alampalayam. "Intrusion Detection Algorithm for MANET." International Journal of Information Security and Privacy (IJISP), pp. 36-49, August 2011.

[9] A. Partwardan, J. Parker, A. Joshi, M. Iorga, T. Karygiannis, "Secure routing and intrusion detection in ad-hoc networks", Third IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, pp. 8–12, March 2005.

[10] Alrajeh, Nabil Ali, Shafiullah Khan, and Bilal Shams. "Intrusion detection systems in wireless sensor networks: a review." International Journal of Distributed Sensor Networks, pp. 1-7, May 2013.

[11] Aljawarneh, Shadi, Monther Aldwairi, and Muneer Bani Yassein. "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model." Journal of Computational Science, pp.152-160, December 2018.

[12] Chitkara, M. and M.W. Ahmad, "Review on MANET: characteristics, challenges, imperatives and routing protocols", International Journal of Computer Science and Mobile Computing. Vol.3 Issue.2, pp. 432-7, February 2014.

[13] Sachin Dnyandeo Ubarhande, "Performance Evolution of AODV and DSR Routing Protocols in MANET Using NS2", International Journal of Scientific & Engineering Research Volume 3, Issue 5, May 2012.

[14] Marchang Ningrinla. "Light-weight trust-based routing protocol for mobile ad hoc networks. J IET Information Security", Volume 6, Issue 2, June 2012, pp.77 – 83, June 2012.

[15] Vipin Khandelwal, Dinesh Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs" International Journal of Advanced Research in Computer Engineering and Technology, Volume 2, Issue 4, April 2013.

[16] Butun, Ismail, Salvatore D. Morgera, and Ravi Sankar. "A survey of intrusion detection systems in wireless sensor networks." IEEE communications surveys & tutorials, Volume: 16 , Issue: 1 pp. 266-282, May 2013.

[17] Sharma, Vishal, et al. "Performance evaluation of reactive routing protocols in MANET networks using GSM based voice traffic applications", Optik-International Journal for Light and Electron Optics Volume 124, Issue 15, Pages 2013-2016, August 2013,

[18] Poongodi, T., and M. Karthikeyan. "Localized Secure Routing Architecture Against Cooperative Black Hole Attack

 DOI : 10.18231/2454-9150.2019.0186

in Mobile Ad Hoc Networks", Wireless Personal Communications, Volume 90, Issue 2, pp 1039–1050, September 2016.

[19] Xia H, Jia Z, Li X, Ju L, Sha EHM (2013) Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw 11(7):2096–2114

[20] Durgesh Kshirsagar, Ashwini Patil, "Black hole Attack Detection and Prevention by Real Time Monitoring" Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on 12-14 Dec. 2013

[21] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack in AODV Based Manet." International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (Printed): 1694-0814.

[22] Parvinder Kaur1. Dalveer Kaur2. Rajiv Mahajan3.Wormhole Attack Detection Technique in Mobile Ad Hoc Networks,Wireless Personal Communications November 2017, Volume 97, Issue 2, pp 2939–2950.

[23] Anurag Gupta, Kamlesh Rana, "Assessment of Various Attacks on AODV in Malicious Environment" 2015 1st International Conference on Next Generation Computing Technologies (NGCT2015) Dehradun, India, 4-5 September 2015.

[24] Basarkod, P. I., and S. S. Manvi. "Multiple Parameters based Approach to Estimate and width in Mobile Ad Hoc Networks." IJCSI (2011).

[25] Ali, Rabia, and Fareeha Zafar. "Bandwidth estimation in mobile ad-hoc network (MANET)." International Journal of Computer Science Issues (IJCSI) 8.5 (2011): 331.

[26] Mandhare, V. V., V. R. Thool, and R. R. Manthalkar. "QoS Routing enhancement using metaheuristic approach in mobile ad-hoc network." Computer Networks 110 (2016): 180-191.

[27] Singh, Debabrata, et al. "Energy Harvesting in a Modified Opportunistic Routing Protocol, a New Approach in Wireless Sensor Network." January 2018, Eighth International Joint Conference on Advances in Engineering and Technology - AET 2017

[28] Zhu, Bo, et al. "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks." IEEE Transactions on Mobile Computing 9.7 (2010): 913-926.

 DOI : 10.18231/2454-9150.2019.0186