International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

Security in DOA routing protocol for Mobile Adhoc Networks

Vanitha.M[1], Deepak.S[2] , Ayesha.N[3]
[1,2,3] *Department of Electronics and Communication Engineering, Sriram Engineering College*

Abstract— One of the most important requirements to establish communication among nodes in MANET (Mobile Adhoc Network) is cooperation of nodes among each other. In the presence of malicious nodes, this requirement may lead to serious security issues. In some cases such nodes may even disrupt the routing process. Hence preventing or detecting malicious nodes causing gray hole or collaborative black hole attacks is a challenge. Our paper attempts to solve this issue by implementing security using the Cooperative Bait Detection Scheme (CBDS) in DOA (DSR over AODV routing mechanism. This work integrates the merits of both proactive and reactive type of MANET routing protocols. DOA (DSR over AODV) is a hierarchical routing protocol developed from the combination of DSR and AODV routing protocols. It is used in environments where overcoming the routing issues that occur in MANETs due to increase in network size is necessary. Our CBDS method adopts a reverse tracing technique to help in achieving the expected solution.
Keywords— AODV, CBDS, DOA, DSR, MANET, Routing protocols.

I. INTRODUCTION

In the recent years, a rapid expansion in the field of mobile computing has been identified due to the proliferation of inexpensive, widely available wireless devices. Wireless ad-hoc network is a collection of mobile nodes in which communication takes place without the involvement or necessity of a centralized access point. MANETs are a type of wireless ad-hoc networks of autonomous topology. A wireless network is a rising technology that allows various users to access different services and information electronically without any need for wired links irrespective of their geographic position. Wireless networks fall into two categories: infrastructure based network and infrastructure less ad-hoc network.

A mobile host in an infrastructure network interacts with base station with in its communication range. During communication the mobile unit moves geographically and starts communicating with new base station. When it goes out of present base station range, it is known as handoff [1].

The characteristics of MANETs are: 1. Dynamic topologies 2. Bandwidth constrained 3. Energy constrained operation. Therefore the routing protocols used in wired networks are not well suited for this kind of dynamic environment. In MANET each node acts as a host a well as a router. When they discover and maintain routes to other nodes in the network it act as router. Such a network may be operate in a standalone fashion, or may be connected to larger internet.

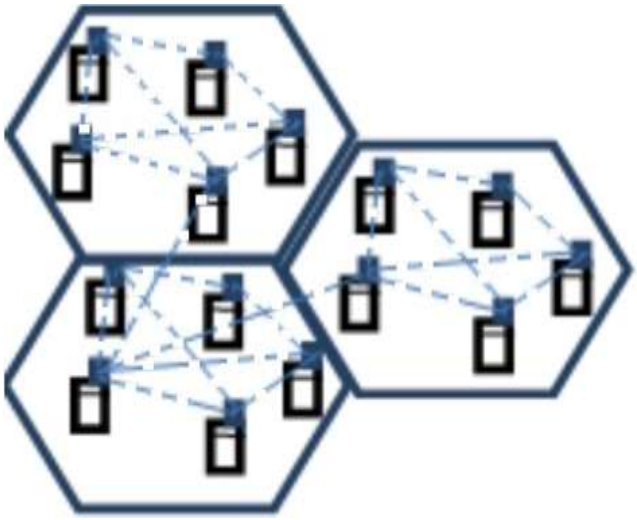

Figure 1. A Mobile Ad-hoc Network

1.1 Security issues in MANETs

Lack of Secure Boundaries-When it is compared with the clear line of defence in the wired network, there is no such clear secure boundary in the mobile ad hoc network.

Threats from Compromised nodes inside the Network-When it try to perform some malicious behaviour to make destruction to the links, it attacks the link place in their emphasis on the links between the nodes.

Lack of Centralized Management Facility- Ad hoc networks doesn't have a centralized management mechanism that may lead to vulnerable problems [2]and [3].

II. ROUTING PROTOCOLS

2.1 Adhoc On Demand Distance Vector (AODV)

AODV is an on-demand reactive protocol . It is an advanced DSDV. This protocol will be recognized only when it is required. This establishment is achieved by two phases: route discovery and route maintenance. The route will be discover only when source has a message to send . It will discover by first broadcast the request to all neighbor nodes as such every nodes will broadcast its request to every neighbor node until source get the reply message from the destination. In AODV all nodes are assigned a sequence number so that the message will be delivered to the destination along with that sequence number and by which path the message had reached. AODV will maintain a Time To Live (TTL) until that the path will be maintain to a particular destination if TTL is expired the path will be discarded.

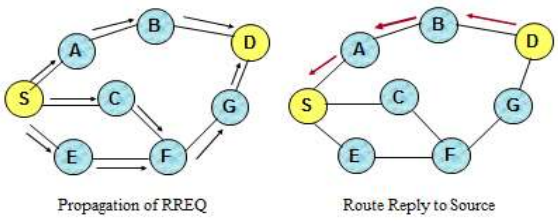

Figure 2. Route Discovery in AODV

During the message transfer if any link breakage occurs automatically from the failed node the route error message will be flooded all over the network . Then the message will be automatically choose the another shortest path route and will deliver to the destination. Since it is on-demand routing protocol the route won't be known early. So each transfer of intermediate nodes, the nodes information will be send back to source [4].

2.2 DSR

Dynamic Source Routing (DSR) is a source routing protocol for wireless mesh network. It uses source routing table at each intermediate device where all the routing information is maintained at mobile nodes. An optimum path between source and destination node is determined by route discovery.

Route maintenance mechanism ensures that the path established is optimum and also loop free according to change of condition of the network and if required a change of route can be opted. Route reply is generated only if the message has reached the destination node. To return the route reply the destination node should have route to the source node. If route to source node is in route cache of the transfer node the route is used for transfer of route reply from destination to source. If the path is not used in the route cache table it will use route record

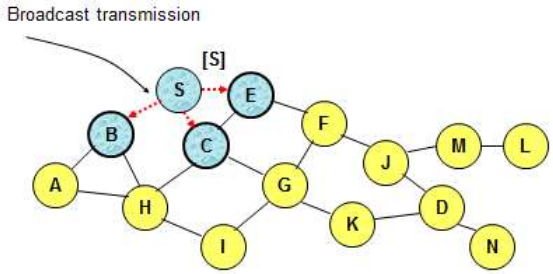

Figure 3. Route discovery in DSR

If any fault message is transmit by the node, then route maintenance will be initiated by node from the route cache . Again the route discovery will be initiated to determine the valuable path to transfer the message. In this above routing protocols have some advantages but has some disadvantages also in which DSR protocol will intimate destination about intermediate path details but it won't have that much efficiency in greater number of nodes. In AODV protocol will be somewhat efficiency in higher number of nodes but it won't send details about intermediate path to destination. In both routing protocol will face the scalability problem when number of nodes increase[5] .

III. RELATED WORK

We have undergone a literature survey about the various problems that occur due to the presence of malicious nodes in MANETs. Most of these solutions had dealt with the detection of a single malicious node and required much time and cost for detecting such black hole attacks. Also, some of these methods may require some special environment or criteria in order to operate.

In general, detection mechanisms can be grouped into two broad categories. 1) Proactive detection schemes are need to constantly detect or monitor nearby nodes. In these schemes, the overhead of detection is constantly created, and the resource are used for detection is constantly wasted , regardless of the existence of malicious nodes. Here the advantage is that prevention or avoiding an attack can be done in its initial stage itself. 2) Reactive detection schemes are those in which the destination node is triggered only when it detects decrease in packet delivery ratio. This is a two ACK scheme for the detection of routing misbehavior in MANETs. Here, two-hop acknowledgement packets are sent in a direction opposite to the routing path in order to indicate

successful delivery of the packets. A parameter named (RAck) is used to control the ratio of the received and acknowledged data packets.Our concept is a type of proactive schemes and so it produces additional routing overhead regardless of the existence of malicious nodes by implementing a prevention mechanism called best-effort fault-tolerant routing (BFTR). This scheme uses end-to-end acknowledgements for monitoring the quality of the routing path which is measured in terms of packet delivery ratio and delay determined by the destination node. If the behavior of the path deviates from the pre-defined one, the source node has to find an alternate new route. One of the demerits of BFTR is that even in the new route malicious nodes may still prevail. Hence repeated route discovery processes take place which may increase the significant routing overhead [7].

The motivation of choosing the proposed detection scheme is to attain the advantages of both reactive and proactive schemes in order to design a DSR-based routing scheme to be able to detect gray hole and black hole attacks in MANETs [8].

IV. PROPOSED WORK

In this paper we propose security in DOA protocol for mobile ad-hoc networks to attain a good trade-off in the routing overhead in order to overcome highly vulnerable black hole and grey hole routing attacks.

4.1 DOA (DSR OVER AODV)

DSR and AODV routing protocols belong to the classification under flat routing protocols where all the nodes in the network work with the same functionalities. They are suitable only for small sized networks with lesser number of nodes. When the size of the network increases they come across scalability problem due to routing overhead. To avoid the scalability problem, a hierarchical routing protocol, DOA is implemented from DSR and AODV for MANETs to make it suitable for any size of networks. DOA is implemented using the way point routing model. In hierarchy, a single route will be divided into many sub routes, which are called as segments. Each segment commences with start node and ends with end node. Start and end nodes are connected by means of forwarding nodes. Every two successive segments use the same way point node with start node as downstream segment and end node as upstream segment. This is Way Point Routing.

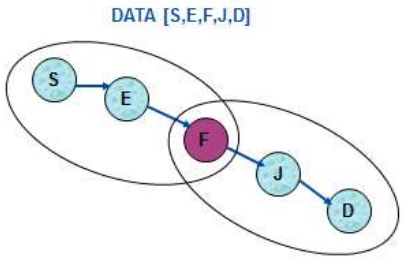

Figure 3. Way Point Routing in DOA

Way Point routing model is a 2 level routing model namely inter-segment routing (Global) and intra-segment routing (Local). The overall route from source to destination is called inter-segment routing. The routing within each segment is said to be known as intra-segment routing. Thus the DOA protocol can work in any situation either as DSR or AODV. For Inter-segment routing we use DSR and for Intra-segment routing we use AODV [9] and [10].

The noticeable merit of this method is that if a node fails or moves from a route it is sufficient to find a new segment for repairing the failed link, instead of finding the entire route. The remaining segments remain undisturbed. Thus the overhead in any network can be limited by using DOA routing.

4.2 CBDS (Co-operative Bait Detection Scheme)

The cooperative bait detection scheme (CBDS) aims to detect and prevent the malicious nodes that cause grayhole / blackhole attacks in MANETs. In this approach, the source node selects an adjacent node to find the bait destination address in order to force the malicious nodes to send a RREP message. Malicious nodes are detected and also prevented to participate in any routing operations by using a reverse tracing technique. When a significant decrease occurs in the packet delivery ratio, an alarm will be sent by the destination node back to the source node for triggering the detection mechanism once again [11].

CBDS scheme combines the merits of proactive detection scheme and the superiority of reactive response in the initial step and the subsequent steps respectively. This in turn reduces the resource wastage. CBDS works based on DSR. It can only identify the addresses of all nodes in any selected path between sources to destination. However, it is not necessary for a source node to identify the intermediate nodes that have the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP.

In this work, the source node sends its packets in the fake shortest path chosen by the malicious node that may later develop into a black hole attack. For this a HELLO message is added to the CBDS in order to help all nodes to identify their adjacent nodes in one hop. This helps in sending the bait address to lure the malicious nodes and to utilize the reverse tracing program of the CBDS to trace the exact addresses of malicious nodes. The baiting RREQ packets are like the original RREQ packets, only difference is that their destination address is the bait address [12].

V. SIMULATION ENVIRONMENT

This section deals with the simulation environment used for analyzing the performance of DSR over AODV (DOA). The simulation is performed using NS-2 which is a network simulator tool. This discrete event simulation software simulates events like sending, receiving, forwarding and dropping packets from source to destination respectively. The routing protocols for ad-hoc networks like AODV and DSR is supported in latest version of NS-2 2.35. The coding is written with ns-2 and Object Tool Command Language (OTCL). In our paper NS-2 works in Linux platform [FEDORA version 7]. This version is chosen because it offers a number of programming development tools which can be used with the simulation process. The simulation results are then viewed in an output trace file and later graphically visualized.

Table 1. Simulation Parameters

Protocols	DOA
Agent	TCP Agent
Simulation Area	1000x1000 m
Number of nodes	45
Transmission Range	150 m
MAC Layer Protocol	IEEE 802.11
Maximum Speed	100 m/s
Traffic Type	CBR

VI. PERFORMANCE ANALYSIS

We have undergone a detailed performance analysis with CBDS in DOA routing protocol. The parameters taken into consideration for analysis were Packet Delivery Ratio, Delay, end to end delay, control overhead, routing overhead and Throughput. These parameters were analyzed by varying speeds of different speeds of 5, 10, 15, 20 and 25 m/s for DOA routing protocols with

CBDS and graphical simulation results were obtained. Then these parameters were compared with DOA routing protocol with CBDS and without CBDS.

6.1 Packet Delivery Ratio

$$\text{Packet Delivery Ratio} = \frac{\text{No. of packets received}}{\text{No. of packets sent}} \times 100$$

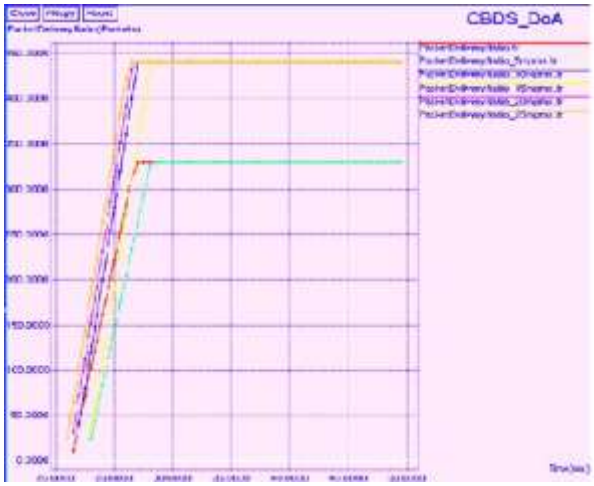

Figure 4. Packet Delivery vs Time

6.2 End-to-End Delay

$$\text{End-to-end Delay} = \frac{\text{Inter-arrival time between 1st and 2nd packet}}{\text{Total Data packet delivery time}}$$

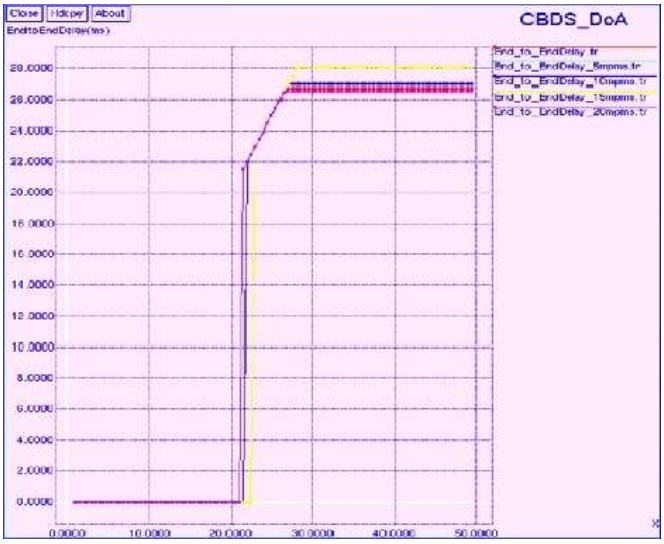

Figure 5. End to End Delay vs Time

6.3 Throughput

$$\text{Throughput} = \frac{\text{No. of packets received in bytes}}{\text{Time in seconds}}$$

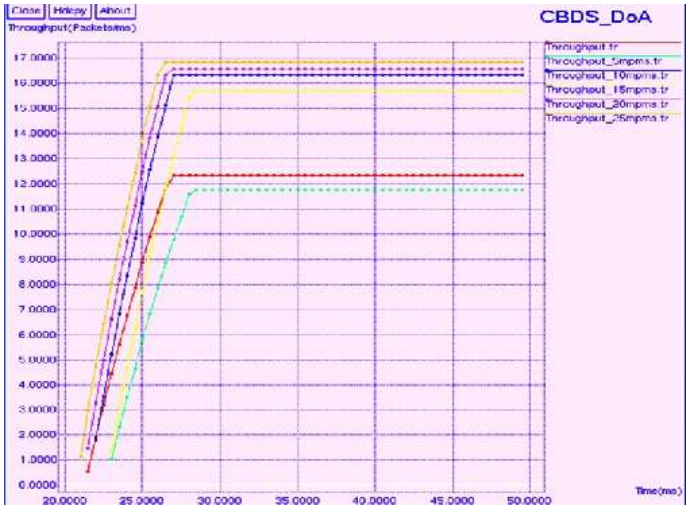

Figure 6. Throughput vs Time

6.4 Control Overhead

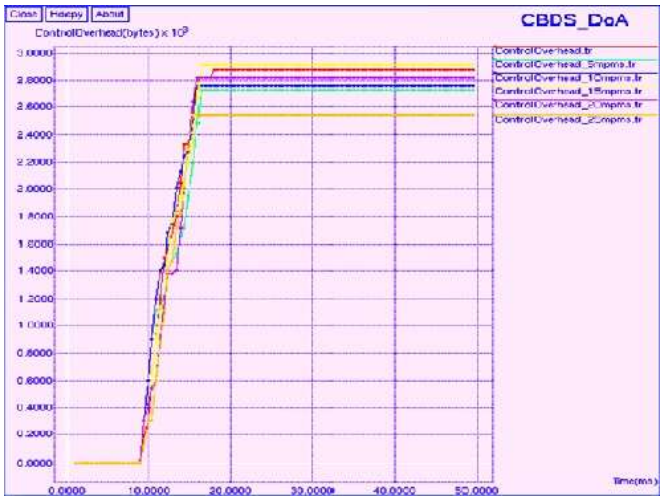

Figure 7. Control Overhead vs Time

6.5 Routing Overhead

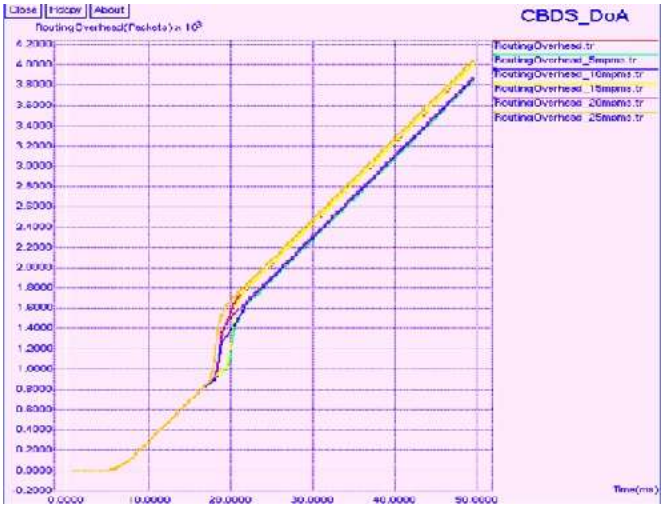

Figure 8. Routing Overhead vs Time

6.6 Comparison between DOA with CBDS and without CBDS

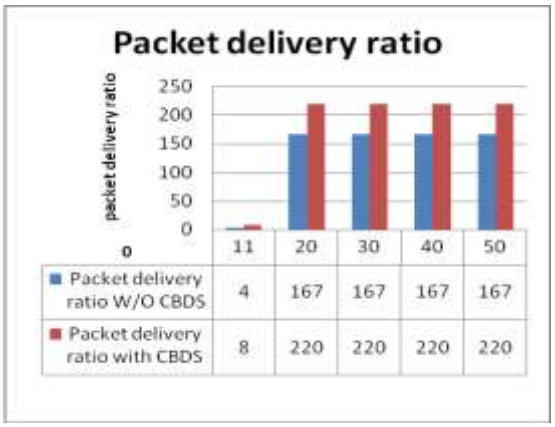

Figure 9. Packet Delivery vs Time

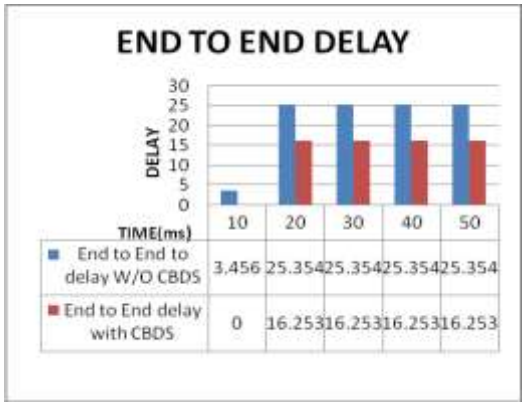

Figure 10. End to End Delay vs Time

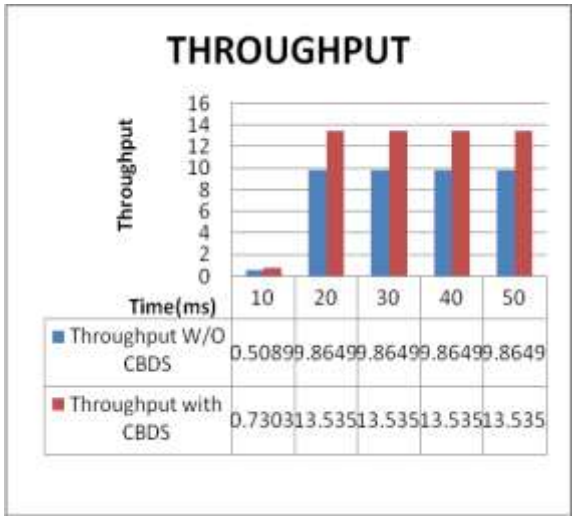

Figure 11. Throughput vs Time

Figure 12. Control Overhead vs Time

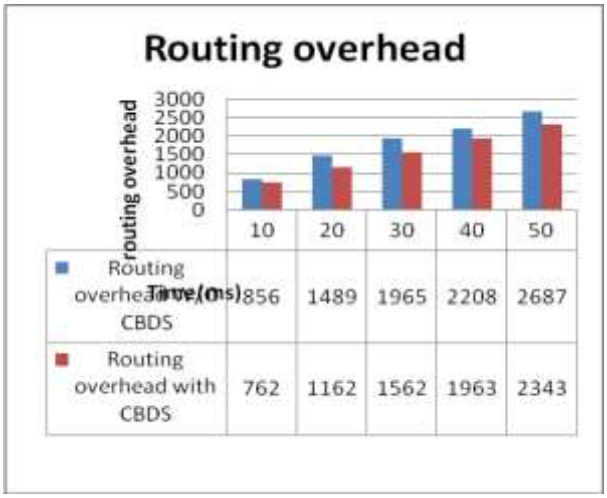

Figure 13. Routing Overhead vs Time

VII. CONCLUSION

In this paper we have established communication among all nodes in Mobile Adhoc Networks. Our CBDS algorithm implemented in DOA routing protocol has improved security in MANETs which has been proved from our results. Our work proves that DOA using CBBS algorithm improves security even in the presence of malicious nodes. We have overcome the routing issues that occur in MANETs due to increase in network size. By adopting a reverse tracing technique we have achieved the expected solution. Our future work is to concentrate on energy efficiency in such routing protocols.

REFERENCES

1. Rashmi, Dr. R Kanagavalli, Utilization of Energy from Attacks Using RSA Algorithm in Wireless Adhoc Sensor Networks, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 4, pp. 2853-2856, April 2015.
2. Sukhpreet Kaur ,Chandan Sharma, An Overview of Mobile Adhoc Network: Application, Challenges and Comparison of Routing Protocols, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 5, PP 07-11 May- Jun. 2013.
3. Jayraj Singh, Arunesh Singh, An Assessment of Frequently Adopted Unsecure Patterns in Mobile Adhoc Network: Requirement and Security Management Perspective, International Journal of Computer Applications, Vol. 24– Issue No.9, pp. 34-39, June 2011.
4. Dhari Ali, Mahmood, Rahul Johari, Application of Routing Metrics in Wireless Network, , International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 2, Issue 4, pp. 477-484, July 2013.

5. Konduri, Sucharitha, Dr.R.Latha, Performance Analysis of Routing Protocols in Mobile AD-HOC Networks (MANETs), IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Ver. IV, PP 12-17 (Jan. 2014).
6. T.Karpagam, Mr.S.Sivakumar, Enhanced Secure Data Transmission Using Key Distribution Scheme Shuffling Algorithm, International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) , Vol 17 Issue 2–September 2015.
7. V.Renugadevi, C.Saranya, P.Saranya, D.Arulanantham, Resisting Malicious and Packet Dropping Attacks in the Presence of Collisions in Wireless ADHOC Networks, International Journal for Research in Applied Science & Engineering Technology, Volume 3 Issue III, Page No. : 391-395, March 2015.
8. Kisantini, V.Sakthivel, Protecting Alongside Collaborative Attacks By Malevolent Knobs In Wsns: A Cooperative Bait Recognition Approach, D International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Volume 18 Issue 2, pp. 15-20, November 2015.
9. M. Vanitha, B. Parvathavarthini, An Enhanced DOA (DSR Over AODV) Protocol for Mobile Ad-Hoc Networks, International Review on Computers and Software, Vol. 8. No.6, pp. 1416-1426, January 2013.
10. M.Vanitha and Dr.B.Parvathavarthini, Performance Analysis of an Enhanced DOA for Mobile Ad-hoc Networks, IEEE International Conference on Smart Structures and Systems (ISSS-2013), pp.131-137, March 28th – 29th, 2013.
11. O.Akinlemi Olushola , K. Suresh Babu,Cooperative Bait Detection Scheme (CBDS) To Avoid the Collaborative Attacks of Nodes in MANET, International Journal of Scientific Engineering and Research (IJSER), Volume 3 Issue 4, pp.66-69, April 2015 .
12. A. Swarnalatha, R. Avudaiammal, M Beneto Nixon, Detection Of Collaborative Attacks In Manets Using Enhanced CBDS technique, National Level Technical Conference, Volume 1, No. 1, pp. 16-25, March 2015.

