Defense Strategy Using Trust Based Model to Mitigate Active Attacks in DSR Based MANET

N. Bhalaji[1], Dr. A. Shanmugam[2]
[1]Research Scholar, Anna University of Technology, Coimbatore (Bhalaji.80@gmail.com)
[2]Principal, Bannari Amman Institute of Technology

***Abstract*—An ad hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Research in wireless indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks. This paper analyses the black hole and cooperative black hole attack which is one of the new and possible attack in adhoc networks. A black hole is a type of attack that can be easily employed against routing in mobile adhoc networks. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. Our solution discovers the secure route between source and destination by identifying and isolating black hole nodes. In this paper, via simulation, we evaluate the proposed solution and compare it with standard DSR protocol in terms of throughput, Packet delivery ratio and latency. We have conducted extensive experiments using the network simulator-2 to validate our research.**

***Index terms*—Trust based routing, secured routing, blackhole attack, Cooperative blackhole attack, adhoc networks, DSR protocol**

I. INTRODUCTION

MANET is multihop infrastructure less network which is characterized by dynamic topology due to node mobility, limited channel bandwidth and limited battery power of nodes. Since mobile nodes in Mobile ad hoc network can move arbitrarily the topology may change frequently at unpredictable times. Transmission and reception parameters may Also impact the topology. The routing algorithm must react quickly to topological changes as per the degree of trust of a node or a complete path between a source and a destination pair. Nodes in Mobile ad hoc network communicate over wireless links. Therefore efficient calculation of trust is a major issue in mobile ad hoc networks because an ad hoc network depends on cooperative and trusting nature of its nodes. As the nodes are dynamic the number of nodes in route selection is always changing thus the degree of trust also keep changing. Survival of ad hoc networks depends on cooperative and trusting nature of its nodes.

Black hole Attack: A black hole attack [1] is a kind of denial of service attack where a malicious node can attract all packets by falsely claiming a fresh route to the destination and absorb them without forwarding them to the destination.

Cooperative Black hole attack: It is a type of attack in which blackhole nodes act in a group [2] [3]. For example when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to the one of its team mates B2 in the next hop, as depicted in fig. 1.

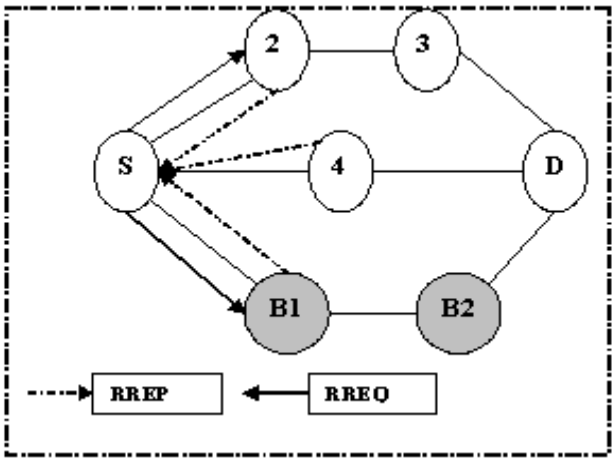

Fig.1.Attack scenario

II. RELATED WORK

Ramaswamy et al. [3] proposed a solution to defending against the cooperative black hole attacks. But no simulations or performance evaluations have been done. Ramaswamy et al. studied multiple black hole attacks on mobile ad hoc networks. However, they only considered multiple black holes, in which there is no collaboration between these black hole nodes. In this paper, we evaluate the performance of the proposed scheme in defending against the collaborative black hole attack.

In DPRAODV [4], they have designed a novel method to detect black hole attack: DPRAODV, which isolates that malicious node from the network. The agent stores the Destination sequence number of incoming

doi:10.4304/jait.2.2.92-98

route reply packets (RREPs) in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval as in [5].the solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than the one in routing table. DPRAODV does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet.

P. Agrawal et al [6] proposed a technique for detecting chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc network. In this technique initially a backbone network of strong nodes (capable of tuning its antenna to short (normal) as well as to long ranges) is established over the ad hoc network. Each strong node is assumed to be a trustful one. These trustful strong nodes detect the regular nodes (having low power antenna) if they act maliciously. With the assistance of the backbone network of strong nodes, the source and the destination nodes carry out an end-to-end checking to determine whether the data packets have reached the destination or not. If the checking results in a failure then the backbone network initiates a protocol for detecting the malicious nodes. For detecting malicious node strong node associated with source node broadcast a find chain message to the network containing the id of the node replied to RREQ. On receiving find chain message strong node associated with destination node Initialize a list GrayHole Chain to contain the id of the node replied to RREQ. It then instructs all the neighbors of that node to vote for the next node to which it is forwarding packets. If the next node id is null then the node is a black hole node. Then the GrayHole removal process is terminated and a broadcast message is sent across the network to alert all other nodes about the nodes in GrayHole Chain to be considered as malicious. Else strong node will elect the next node to which replied to RREQ is forwarding the packets based on reported reference counts. Then again broadcast the find chain message containing the id of the elected node. The main disadvantages of this algorithm are the difference between the regular node and backbone node in the network in terms of power, antenna range which makes it unsuitable for all types of mobile ad hoc network. Also it is not proved that backbone network is optimal in terms of minimality and coverage. Algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong nodes are always trusted node.

In [7] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park proposed two different approaches to solve the blackhole attack. In first proposal the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. The idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route are identified. Once a safe route has identified, these buffered packets will be transmitted. But the main drawback of this algorithm is time delay. In the second proposal every node stores the last sent packet sequence number and last received packet sequence number. When a node receives a RREP from another node it checks the last sent packet sequence number and received packet sequence number, if there is any mismatch then it generates an alarm indicating the existence of a blackhole node. But drawback of this algorithm is if the network is large, mismatch in the sequence numbers does not guarantee the existence of a blackhole node.

In [8] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch used two additional control packets for collecting the neighborhood information for detecting the blackhole node. The formats of these packets are RQNS,RPNS The basic idea of this approach is that the neighbor set difference of one node at different time instance is less than or equal to one, and the probability that the neighbor set difference of two nodes at same time instance is very small. After getting RREP from more than one node the sender sends the RQNS packet. After receiving more than one RPNS packet the sender node compare the received neighbor set, if the difference is larger than some pre defined threshold value then the current network is affected by blackhole attack. But the drawback of this approach is after comparing the neighbor set they use a cryptographic method to identify the actual infected node. This is a costly and less reliable technique in case of ad hoc network.

In [9] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng, and Shun Chao Chang proposed a distributed and cooperative procedure to detect blackhole node. First each node detects the local anomalies, then after finding the local anomalies the sender node calls for a cooperative detective by sending a message to the neighbor of the infected node. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which proceeds by first broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the

node in question is indeed a malicious one. As soon as a confirmed black hole node is identified, the global reaction is activated immediately to establish a proper notification system to send warnings to the whole network. They use a voting scheme to identify the blackhole node. If all the nodes vote for the infected node, then the node is declared as blackhole node. The drawback of this algorithm is it cannot detect the cooperative blackhole attack and the voting scheme is complex one.

In [10], Deng et al. proposed a solution for individual black holes. But they have not considered the cooperative black hole attacks. According to their solution, information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution can not prevent cooperative black hole attacks on MANETs. For example, if the next hop also cooperates with the replied node, the reply for the FREQ will be simply "yes" for both questions. Then the source will trust on next hop and send data through the replied node which is a black hole node.

In [11], Yin et al. proposed a solution to defending against black hole attacks in wireless sensor networks. The scenario that they considered in sensor networks is quite different than MANETs. They consider the static sensor network with manually deployed cluster heads. They did not consider the mobility of nodes. Also they have one sink node and all sensors send all the data to the sink. Each node needs to find out the route only to the sink. Since this scenario is not compatible with MANET, we are not going to discuss it further.

Hesiri Weerasinghe and Huirong Fu [12] simulated the algorithm proposed by [3] with several changes to improve the accuracy of preventing cooperative black hole attacks and to improve the efficiency of the process. They also simulated AODV [17] and the solution proposed by [3] and compared them with [10].

In this scheme proposed solution is applied over the Dynamic Source Routing protocol and the over head of FREQ and FREP is not required as routing will be done based on the trust value of the nodes. The trust values are estimated considering various attributes related to behaviour of the node for a certain time. Each node consists of Association table depending on which the selection of the route is decided. The routing information is discussed in the routing mechanism section.

III. PROPOSED SCHEME

This section presents the improvement of the Association based Route selection to be applied to the DSR protocol in order to enhance its routing security. The purpose of applying the association based route selection to the DSR protocol is to fortify the existing implementation by selecting the best and securest route in the network. In contrast to the current route selection in the DSR which involves selection of the shortest route to the destination node, our proposed protocol choose the most reliable and secure route to the destination based on the trust values of all nodes. For each node in the network, a trust value will be stored that represent the value of the trustiness to each of its neighbor nodes. This trust value will be adjusted based on the experiences [14] [15] [16] [17] that the node has with its neighbor nodes.

A. Nature of Association & Association estimator technique

In our proposed scheme we classify the Association among the nodes and their neighboring nodes in to three types [18] as below. In an adhoc network the Association between any node x and node y will be determined as Unknown, Known, Companion. These Associations are represented in an Association table which is part of every node in the adhoc network.

The Association status [16] [17] which we discussed in the previous section depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. We propose a very simple equation for the calculation of trust value.

$$T = \tanh (R1+R2+A) \qquad (1)$$

Where

T = Trust value

R1= Ratio of number of packets actually forwarded by a node to the number of packets forwarded by that node.

R2 = Ratio of number of packets received from a node but originated from others to total number of packets received from it.

A = Acknowledgement bit. (0 or 1)

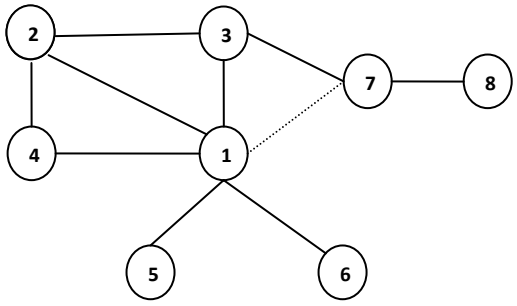

Fig.2.Nodes in Adhoc network

TABLE I: ASSOCIATION TABLE FOR NODE 1 IN FIG. 2

Neighbors	Nature of Association
2	C
3	C
4	K
5	C
7	UK

The threshold trust level for an unknown node to become a known to its neighbor is represented by T_K and the threshold trust level for a known node to become a

Companion of its neighbor is denoted by Tc. The Associations are represented as

$$A \text{ (node x} \rightarrow \text{node y)} = C \text{ when } T \geq 0.6$$

$$A \text{ (node x} \rightarrow \text{node y)} = K \text{ when } 0.3 \leq T < 0.6$$

$$A \text{ (node x} \rightarrow \text{node y)} = UK \text{ when } 0 < T \geq 0.3$$

Also, the Association between nodes is asymmetric, (i.e.,) R (node x → node y) is an Association evaluated by node x based on trust levels calculated for its neighbor node y. R (node y → node x) is the Association from the Association table of node y. This is evaluated based on the trust levels assigned for its neighbor. Asymmetric Associations suggest that the direction of data Flow may be more in one direction. In other words, node x may not have trust on node y the same way as node y has trust on node x or vice versa. The Threshold parameters are design parameters. Simulation is to be carried out with suitable values or all the parameters and the threshold thrust levels so as to obtain optimum performance. There is a trade off between offering good security in adhoc networks and overall throughput of the network. Hence, choosing an optimal value is crucial for the good functioning of the network.

B.Routing Mechanism

```
Notations:
SN: Source Node IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
Reliable Node: The node through which the SN has routed data
 SN broadcasts RREQ
 SN receivesRREP
 IF (RREP is from Companion node)
{
 Route data packets (Secure Route)
 }
 ELSE
{
 IF (RREP is from Known node)
 Route data packets (Secure Route)
}
 ELSE
RREP is from Unknown node
Insecure Route
 Node may be a black hole node
} While (IN is NOT a reliable node)
}
```

When any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighboring nodes. The ROUTE REPLY obtained from its neighbor is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a Companion, then that path is chosen for message transfer. If its one-hop neighbor node is a known, and if the one hop neighbor of the second best path is a companion choose C. Similarly an optimal path is chosen based on the degree of Association existing between the neighbor nodes. The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions. In the proposed scheme the route is not selected on the basis of first arrival of RREP and waits till it gets the RREP from all neighboring nodes and decides the path to be routed based on the nature of Association between them. Thus the black hole nodes will be identified as unknown in both the hops and were not given preference in the route selection.

IV. SIMULATION SET UP

The simulation is implemented In Network Simulator 2 [19], a simulator for mobile adhoc networks. The simulation parameters are provided in Table 3. We implement the random waypoint movement model for the simulation, in which a node starts at a random position, waits for the pause time, and then moves to another random position with a velocity chosen between 0 m/s to the maximum simulation speed. A packet size of 512 bytes and a transmission rate of 4 packets/s, congestion of the network are not likely to occur.

TABLE III: Simulation parameter

Parameter	**Value**
Examined Protocol	DSR
Application traffic	CBR
Transmission range	250 m
Packet size	512 bytes
Transmission rate	4 packets/sec
Pause time	10 s
Maximum speed	20 m/s
Simulation time	900 s
Number of nodes	50
Area	1000 m * 1000 m
Propagation Model	Free space
Maximum Malicious nodes	10/4
Movement Model	Random waypoint
Types of attack	Blackhole and cooperative blackhole attack

V. RESULTS AND DISCUSSIONS

For the performance analysis of the Association based DSR protocol the throughput is compared with the standard DSR in presence of the malicious nodes. The other parameters [20] to be considered are packet delivery ratio and Latency

Performance Metrics: In our simulations we use several performance metrics to compare the proposed DSR protocol with the existing one. The following metrics were considered for the comparison were

Packet Delivery Ratio: it is the ratio of the number of packets received and the number of packets sent.

Throughput: This gives the fraction of the channel capacity used for data transmission.

Average Latency: Gives the mean time (in seconds) taken by the packets to reach their respective destinations

Fig. 3a&3b depicts the performance results for the DSR protocol in the presence of malicious nodes. The results indicate that the throughput of the protocol rapidly drops with the increase in the number of malicious nodes. The throughput drops in DSR rapidly when the number of malicious nodes increases.

Fig. 4a&4b. Shows the percentage of packet delivery ratio under the threat of increasing malicious nodes. Here too the proposed protocol performs better than the conventional one.

The simulation results in Fig 5a&5b. Illustrates that the average latency which is slightly higher than the conventional one due to the trust based routing.

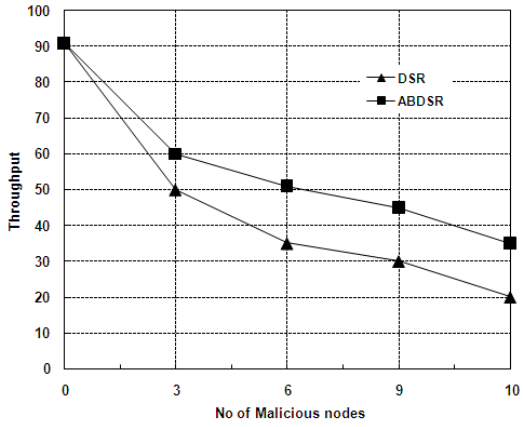

Fig. 3a.Comparison of Throughput (Blackhole)

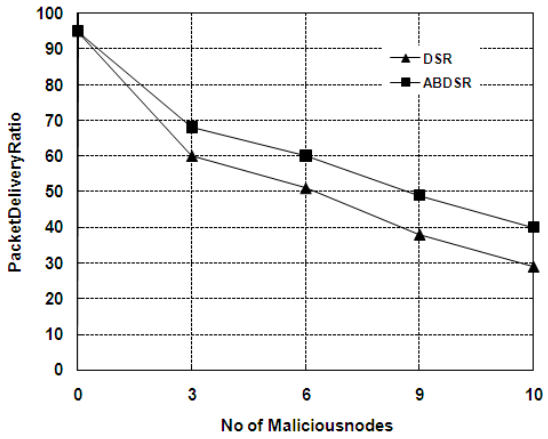

Fig.4a.Comparison of Packet delivery Ratio (Blackhole)

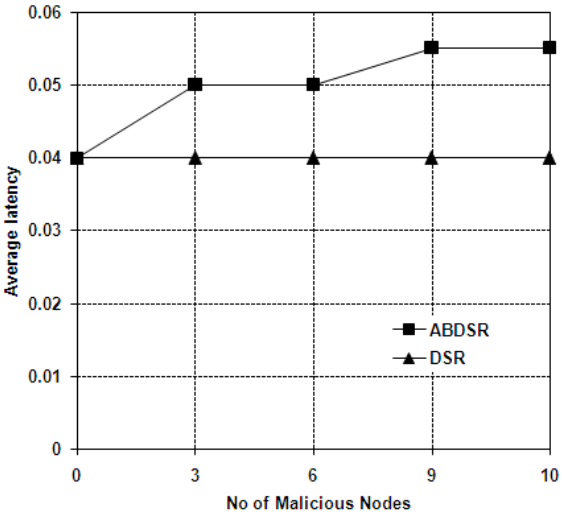

Fig.5a.Comparison of Average latency (Blackhole)

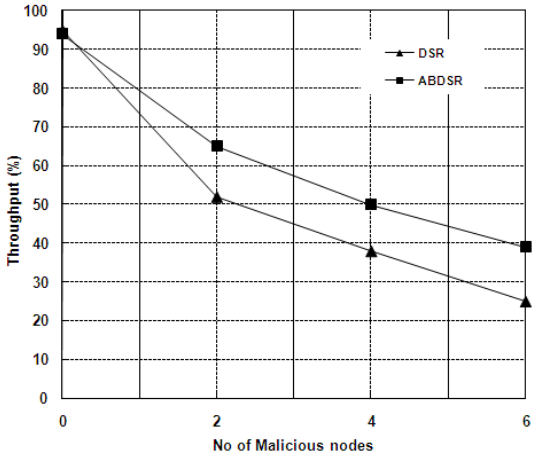

Fig.3b..Comparison of Throughput (cooperative Blackhole)

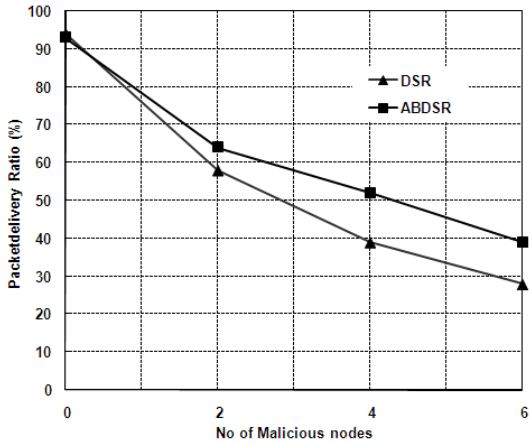

Fig.4b.Comparison of Packet delivery Ratio (cooperative Blackhole)

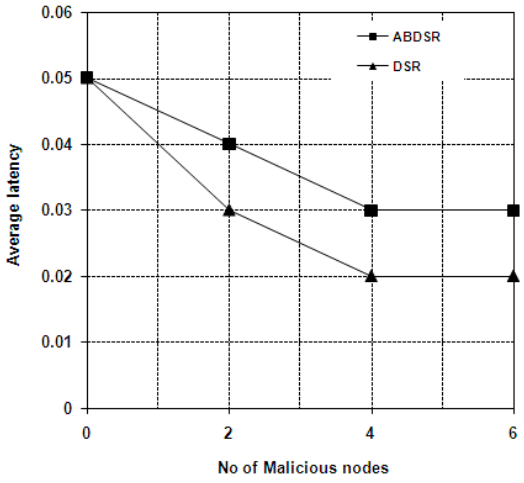

Fig.5b.Comparison of Average latency (cooperative Blackhole)

V. CONCLUSION

In this paper we have presented a trust based routing model to deal with blackhole and cooperative blackhole attacks that are caused by malicious nodes. We believe that fellowship model is a requirement for the formation and efficient operation of ad hoc networks. The paper represents the first step of our research to analyse the cooperative black hole attack over the proposed scheme to analyse its performance. The next step will consist of analyzing the protocol over Grey hole and cooperative grey hole attacks.

REFERENCE

[1] P. Papadimitratos, and Z.J. Haas, "Securing the Internet Routing Infrastructure," *IEEE Communications*, vol. 10, no. 40, October 2002, pp. 60-68. Digital Object Identifier 10.1109/MCOM.2002.1039858

[2] Bracha Hod, "Cooperative and Reliable Packet- Forwarding On top of AODV", *www.cs.huji.ac.il/~dolev/pubs/reliable-aodv.pdf, 2005*

[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard,"Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks", www.cs.ndsu.nodak.edu/~nygard/research/BlackHoleMANET.pdf 2003

[4] Payal N. Raj, Prashant B. Swadas "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet" IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009

[5]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007

[6] Piyush Agrawal and R. K. Ghosh "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks "Proceedings of the 2nd international conference on Ubiquitous information management and communication, Suwon, Korea, ISBN: 978-1-59593-993-7, Pages: 310-314, 2008.

[7] Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04,April 2-3,2004,Huntsville,AL,USA.

[8]Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch "Detecting Black-hole Attack in Mobile Ad Hoc Network". 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495

[9]Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magazines, vol. 40, no. 10, October 2002*.

[11] Jian Yin, Sanjay Madria, "A Hierarchical Secure Routing Protocol against Black Hole", *IEEE SUTC 2006 Taiwan, 5-7 June 2006.*

[12]Hesiri Weerasinghe and Huirong Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" *International Journal of Software Engineering and Its Applications* ,pp 39-54,Vol. 2, No. 3, July 2008

[13] C.E.Perkins and E.M.Royer "Ad hoc on demand distance vector routing", *Proceedings of IEEE Workshop on Mobile computing systems and Applications 1999*, pp. 90-100, February 1999.

[14] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: Towards Routing Security, Fairness and robustness in Mobile ad hoc networks. *In proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network–based processing,* Pages 403 – 410. Canary Islands, Spain. January 2002. IEEE Computer Society.

[15] Sergio Marti.T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in Mobile ad hoc networks. *In Proceedings of MOBICOM 2000.* Pages 255-265, 2000.

[16]N.Bhalaji, A.Shanmugam "Association between nodes to Combat Blackhole attack in DSR based MANET" in *Proceedings of Sixth IEEE-IFIP International conference on WOCN, April 28-30, 2009, Cairo,* ISBN: 978-1-4244-4704-6, DOI: 10.1109/WOCN.2009.5010579

[17]N.Bhalaji, Dr.A.Shanmugam "Reliable Routing against selective packet drop attack in DSR based MANET" in *Journal of Software*, Vol. 4, No. 6, August 2009. pp 536-543

[18] Richard Dawkins. *The selfish Gene.* Oxford University press, 1980 edition, 1976.

[19] Kevin Fall, Kannan Varadhan: *The ns manual, http://www.isi.edu/nsnam/ns/ doc/index.html*

[20] J. Broch, D. Johnson, D. Maltz, Y. Hu, J.Jetcheva, "A Performance Comparison of Multihop Wireless Ad Hoc Networking Protocols", *Proceedings of 4th ACM/IEEE International Conference on Mobile Computing and Networking*, 1998

N. Bhalaji received his Bachelor of Engineering degree in Computer Science Engineering (Periyar University, India) in 2002, Master of Engineering Degree in Computer Science Engineering in 2007 (Anna University Chennai, India) and Pursuing his Ph.D. on Improved DSR Protocol For Mobile Adhoc Networks. (Anna university of technology Coimbatore) since April 2008.

He has coordinated 2 national level symposium and one national level conference His publication includes 5 international journals, 9 international conferences and 2 National conferences. He is a member of WASET, IAENG, IACSIT, and ACEEE, IACSE.

Dr. A.Shanmugam received the B.E, degree in Electronics and Communication Engineering from PSG College of Technology., Coimbatore, Madras University, India in the year 1972 and the M.E, degree in Applied Electronics from College of Engineering, Guindy, Chennai, Madras University, India in the year 1978 and received the Ph.D. in Computer Networks from PSG College of Technology., Coimbatore, Bharathiyar University, India in the year 1994.From 1972 to 1976, he served as a Testing Engineer at Test and Development Center, Chennai, India. From 1978 to 1979, he served as a Lecturer in the Department of Electrical Engineering, Annamalai University, India. From 1979 to 2004, he served different level as a Lecturer, Asst.Professor, Professor and Head in the Department of Electronics and Communication Engineering of PSG College of Technology, Coimbatore, India. Since April 2004,he assumed charge as the Principal, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India. He works in field of Optical Networks, broad band computer networks and wireless networks, Signal processing specializing particularly in inverse problems, sparse representations, and over-complete transforms. Dr.A.Shanmugam received "Best Project Guide Award" five times from Tamil Nadu state Government. He is also the recipient of "Best Outstanding Fellow Corporate Member Award" by Institution of Engineers (IE),India -2004 and "Jewel of India" Award by International Institute of Education and Management, New Delhi–2004 and "Bharatiya Vidya Bhavan National Award for Best Engineering College Principal 2005" by Indian Society for Technical Education (ISTE). "Education Excellence Award" by All India Business& Community Foundation, New Delhi**.**