International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 15 (2015) pp 35856-35861
© Research India Publications. http://www.ripublication.com

An Efficient Secure Intrusion Detection System for Data Integrity in MANET

N.Sureshkumar

Research Scholar, Karpagam University, Coimbatore

Dr.S.Bhavani

Professor and Head, Department of ECE, Karpagam University, Coimbatore, India

Abstract - Mobile Ad hoc Networks consists of mobile nodes which are organized randomly. These nodes are communicated with each other without any access point. Due to mobility of nodes, the network is totally affected by the several attacks. In MANET, Black hole attacks may cause packet dropping, misrouting the information form source to destination. So the performance of the network is totally degraded. To overcome this issue, we propose the modified proactive secret sharing scheme to ensure the data confidentiality, data integrity and authenticity. In first phase of the proposed algorithm, the detection of black hole attacks is achieved using trust active and recommendation of the nodes. In second phase of the work, modified proactive scheme is used to provide the data authentication and integrity. Here, we detect the misbehaviour using verifiable secret sharing scheme. By simulation results the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, less packet overhead and end to end delay than the existing schemes.

Keywords – MANET, Verifiable secret sharing, modified proactive secret sharing scheme, end to end delay, overhead, misbehavior detection efficiency and delivery ratio.

I. INTRODUCTION

A. Mobile Ad Hoc Networks (MANETs)

The aims of Ad hoc networks and particularly MANET have in recent years not only seen widespread use [1] in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's range from simple wireless home and office networking to sensor networks and similarly constrained tactical network environments. Security aspects play an important role in almost all of these application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks.

B. Intruders

In this type of attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other.

A malicious node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When a source node wants to send data packets to a destination node, if there has no route available in its Routing Table (RT), it will initiate the routing discovery process. For example assume, B to be a malicious node. Using the routing AODV protocol, node B claims that it has the routing to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of RREQ first, everything works well; but the reply from node B could reach the source node first, if node B is nearer to the source node. Moreover, node B does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through node B are simply consumed or lost. Node B could be said to form a black hole in the network, and we call it as the black hole attack.

II. RELATED WORK

Amol A. Bhosle et.al [2] proposed the watchdog mechanism detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provides a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. They also proposed the time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.

Firoz Ahmed et.al [3] introduced an Encrypted Verification Method (EVM) that effectively detects a black hole attack. A detection node that receives an RREP from a suspicious node sends an encrypted verification message directly to destination along the path included in the RREP for verification. The approach not only pins down the black hole nodes, but also reduces control over-head significantly.

In [4], mobile agent based IDS is introduced in order to reduce the overheads. The use of distributed ID consists of multiple mobile agents which assist over a large network and to make communication with each other. This as a whole reduces the network bandwidth usage by moving data analysis computation to the place of the intrusion data & sustains on the heterogeneous platforms.

M. Umaparvathi and Dharmishtan K. Varughese et.al [6] proposes a secure routing protocol, Two Tier secure Adhoc On-Demand Distance Vector (TTSAODV), which is an extension of the well known Adhoc On-Demand Distance Vector (AODV) routing protocol that can be used to protect the route discovery mechanism against black hole attack. This paper evaluates the performance of AODV and TTSAODV protocols under black hole attack. This protocol detects and finds the secure path against single as well as collaborative black hole attacks. This protocol uses symmetric key system and verification messages to discover a safe route.

Disha et.al [7] demonstrated an adaptive method to detecting black and gray hole attacks in ad hoc network based on a cross layer design. A course-based method is adopted in network layer to overhear the next hop's action is proposed. This scheme is not suitable to send extra control packets and saves the system resources of the detecting node. Collision rate reporting system is established in MAC layer to guess dynamic detecting threshold so as to lower the false positive rate. DSR protocol is preferred to test algorithm.

Sushil Kumar et.al [8] analyzed the performance of AODV with and without black hole (malicious node) attack under simulation result analysis. The route discovery process in the AODV is susceptible to black hole attack and efficient security schemes were not deployed to avoid such attacks.

Ping Yi et.al [9] demonstrated an adaptive approach to detecting black and gray hole attacks in MANET based on a cross layer design. In network layer, a path-based method is proposed to overhear the next hop's action. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. This scheme does not send out extra control packets and saves the system resources of the detecting node.

N.Bhalaji et.al [10] presented a trust based routing model to deal with black hole and cooperative black hole 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 analyze the cooperative black hole attack over the proposed scheme to analyze its performance. The next step will consist of analyzing the protocol over Grey hole and cooperative grey hole attacks.

In [11], Mehdi proposed and approach to combat the Cooperative/ Multiple Black hole attack by using negotiation with neighbors who claim to have a route to destination. The percentage of packets received through the proposed method is better than that in AODV in presence of cooperative black hole attack.

In [16], Thamarai selvi presented an ant based novel approach reliability to detect anomalies. The proposed approach is decentralized, active and extensible. In order to provide better performance in the mobile architecture this work ensures security for mobile nodes. Such nodes were declared as malicious node. This work will provide efficient strategy to fight against threats like Black hole attack using the fitness function generated from ACO (Ant Colony Optimization).

The research work is categorized as follows. Overview of MANETs and black hole attacks is described in section 1. The previous work is discussed in section 2 which is related to the wormhole attacks. Section 3 is devoted for the implementation of proposed model. Section 4 describes the performance analysis and the last section concludes the work.

III. IMPLEMENTATION OF PROPOSED ALGORITHM

In the proposed algorithm, malicious nodes are found using trust based authentication model. Secret sharing is proposed to secure the data against network attackers.

A. Intrusion Detection System

Step 1. Source S wants to communicate with node D. It broadcasts the request message RREQ. RREQ includes the level of security it requires and D's id, a sequential number and P_b D [S_{id}] is the Source's id encrypted by Destination's public key and Trust Active. RREQ is like this :{ RREQ, seq_num, P_b D [Si d], D_{id}, T_A}. Where T_A Trust active is the time-dependent trust value. Initially node A have the trust value on node B is at time t_1; but after a certain period, node B may travel to another zone which is out of radio range of node A due to nodes mobility in MANET. At time t_2, node B happens to back in node A's radio range again. The trust value should decay during this time gap. Let ${}_AT_B$ (t_1) be the trust value of node A to node B at time t_1 and ${}_AT_B$ (t_2) be the decayed value of the same at time t_2. Then trust active is defined as follows,

$$ {}_AT_B(t_2) = {}_AT_B(t_1) * e^{-({}_AT_B(n)\Delta t)^{2k}} \quad (1) $$

Step 2. Node A receives RREQ. It looks up its trust list for the trust values of the neighbors. And A will encrypt if own id with proper policy and append in the message. The message which will sent by A is like this:{RREQ, seq_num, P_b D[P_v A[A_{id}], P_bD[Sid], Did , R_B^A } where P_v A is the private key of A. Where R_B^A (Node proposal) is also used to identify the malicious behavior. Evaluating the recommendation is given by R_B^A which is node A's evaluation to node B by collecting recommendations,

$$R_B^A = \frac{\sum_{\upsilon \in \gamma} V \mid A \rightarrow C \mid * V \mid C \rightarrow B \mid}{V \mid A \rightarrow C \mid} \qquad (2)$$

γ is a group of recommenders.

$V \mid A \rightarrow C \mid$ is trust vector of node A to C.

$V \mid C \rightarrow B \mid$ is trust vector of node C to B.

Step 3. D receives RREQ. It uses its private key and the public key of the intermediate nodes to authenticate them. D checks if there are any bad nodes. If they are all trusted, D generates a number for the flow Fid , and broadcasts the following message(suppose A and B are the intermediate nodes): {RREP,Pb B[Fid , Pb A[F_{id} , Pb S[Pv D[F_{id}]]]]};

Step 4. Intermediate node that receives the RREP uses its private key to decrypt the message and gets the flow id. Then it updates its route table with Fid designated to destination D;

Step 5. S receives RREP, uses its private key to decrypt the message and D's public key to identify the destination. Afterwards, it will send message with the flow id Fid.

Step 6. Cluster Head maintains the Trust threshold value based on trust active and node proposal to detect the attacks.

Step 7. If any nodes below the Trust threshold value that node is encountered by an attacks.

B. Secret Sharing Scheme

Step1: Let ($S_{1,}$ S_2, ………..S_n) be an (t,n) sharing of the secret key S of the service with the node k having S_k.

When S_k, is defined from a finite a finite field D = Z_r and g is a primitive element in F.

Step 2: Node K (K $\in$ {1,2,3,….n}) which randomly generates S_k's sub shares like (S_{i1}, S_{i2}, ….. S_{in}) for (n,t) sharing.

Step3: All subshares S_{kp} (p $\in$ {1,2,3,….n}) is distributed to node p through the secure link.

Step4: When node j gets the sub shares {S_{1k}, S_{2k}, ….. S_{nk}}. It computes a new share from these sub shares and its old share with an equation.

$$S_p^{'} = S_p + \sum_{k=1}^{n} S_{k,p} \qquad (3)$$

C. Digital Signature Verification

Step 1: Share holder node M sends PSS_start flag to all share holder nodes.

Step 2: All Share holder nodes send the PSS_start_ack flag to the share holder node M.

Step3: Initiated the sharing procedure.

Step 4: Node send the refresh_flag to all share holder nodes . All nodes refresh its share to send shares to other share holder nodes with digital signature and encrypted public key of destination nodes.

Step5: Verify the digital signature trust active using trust mechanism.

Step6: Send end flag to all share holder nodes. After receiving this end flag, send_ack flag again and send refresh_end flag to all share holder nodes.

Step 7: In detection phase, we use the concept of Virtual Sharing scheme procedure to detect any misbehaviour.

Each node verify his own share by using,

$$g^{su} = \Pi_{j=0}^{k} = A_j^{\alpha^{j}{}_u} \qquad (4)$$

If the share holder node does not broadcast the above information, misbehaviour will be broadcasted to all the share nodes.

Step 8: The secret key is reconstructed. If S_k holds shares (m_1, n_1) and S_p hold shares (m_2, n_2) , share holder node reconstructs If $m_1 = m_2$, then the secret is n_1, otherwise the secret is n_2.

IV. PERFORMANCE ANALYSIS

Network Simulator (NS2) is used to simulate our proposed algorithm. Network Simulator-3 (NS2) is used in this work for simulation.NS2 is one of the best simulation tools available for Wireless sensor Networks, Ad hoc Networks and DTN. We can easily implement the designed protocols either by using the otcl coding or by writing the C++ Program. In either way, the tool helps to prove our theory analytically.

In our simulation, 200 mobile nodes move in a 1600 meter x 1600 meter square region for 60 seconds simulation time. All nodes have the same transmission range of 250 meters. Our simulation settings and parameters are summarized in table 1.

Table 1. Simulation Settings and parameters

No. of Nodes	200
Area Size	1600 X 1600
Mac	802.11
Radio Range	250m
Simulation Time	60 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Transmitter Amplifier	150 pJ/bit/m^2
Package rate	5 pkt/s
Protocol	DSR

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

End-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Packet Delivery Ratio: It is the ratio of packet received to packet sent successfully. This metric indicates both the loss ratio of the routing protocol and the effort required to receive data. In the ideal scenario the ratio should be equal to 1. If the ratio falls significantly below the ideal ratio, then it could be an indication of some faults in the protocol design. However, if the ratio is higher than the ideal ratio, then it is an indication that the sink receives a data packet more than once. It is not desirable because reception of duplicate packets consumes the network's valuable resources. The relative number of duplicates received by the sink is also important because based on that number the sink, can possibly take an appropriate action to reduce the redundancy.

Throughput: It is defined as the number of packets received successfully.

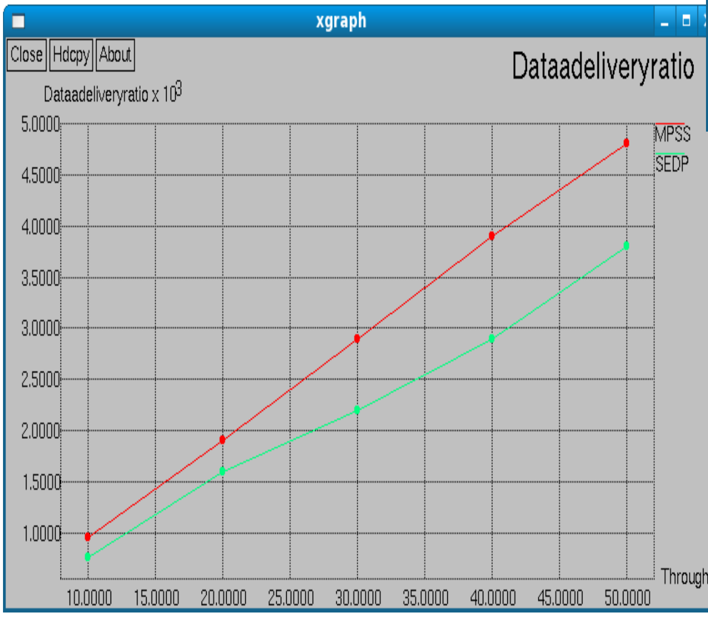

Figure1.Throughput Vs Data delivery ratio

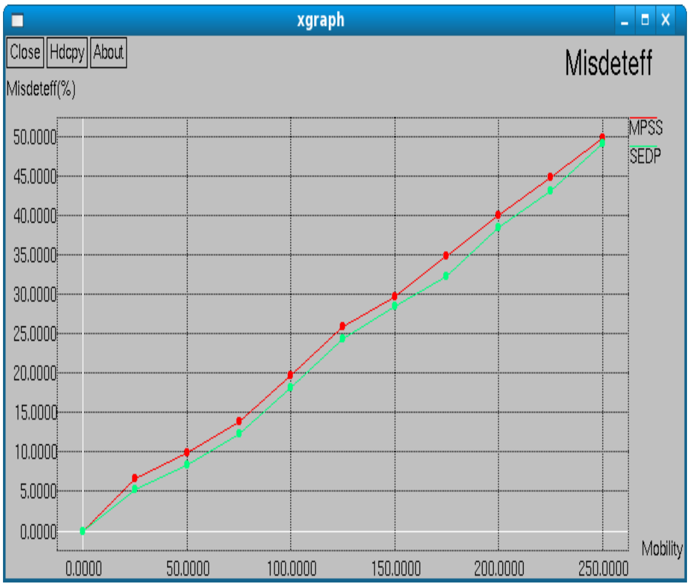

Figure 2.Mobility Vs Misbehavior Detection Efficiency

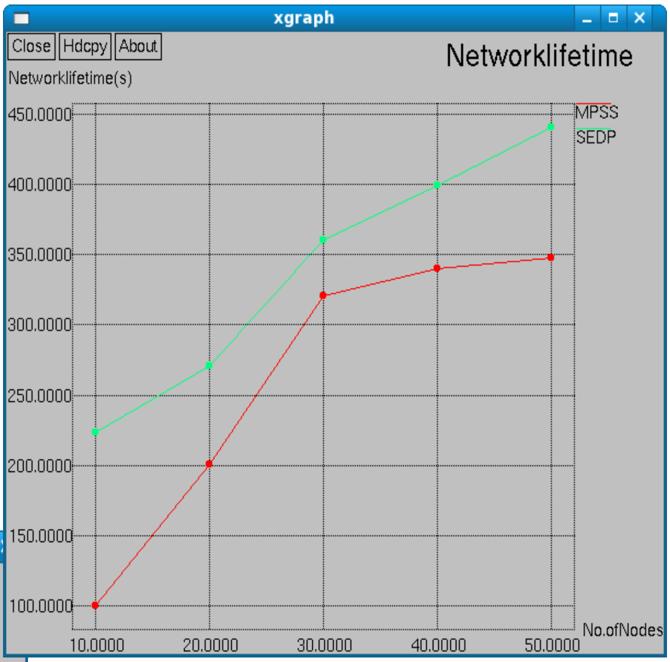

Figure3.No.of nodes Vs Network Lifetime

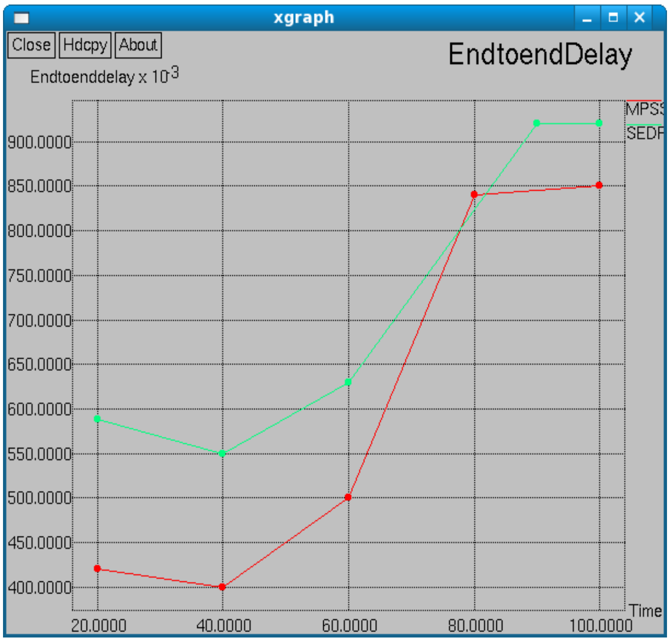

Figure 4.Time Vs End to end delay

Figure 1 shows the results of packet delivery ratio for varying the throughout from 10 to 50. From the results, we can see that MPSS scheme has higher delivery ratio than the SEDP because of security scheme.

Figure 2 shows the results of detection efficiency for varying the mobility from 0 to 250. From the results, we can see that MPSS scheme has higher detection efficiency than the SEDP scheme..

Figure 3 shows the results of network lifetime for varying the number of nodes from 10 to 50. From the results, we can see that MPSS scheme has network lifetime than the SEDP.

Figure 4 shows the results of time Vs End to end delay. From the results, we can see that delay of MPSS is lower than the SEDP while varying the nodes form 10 to 50.

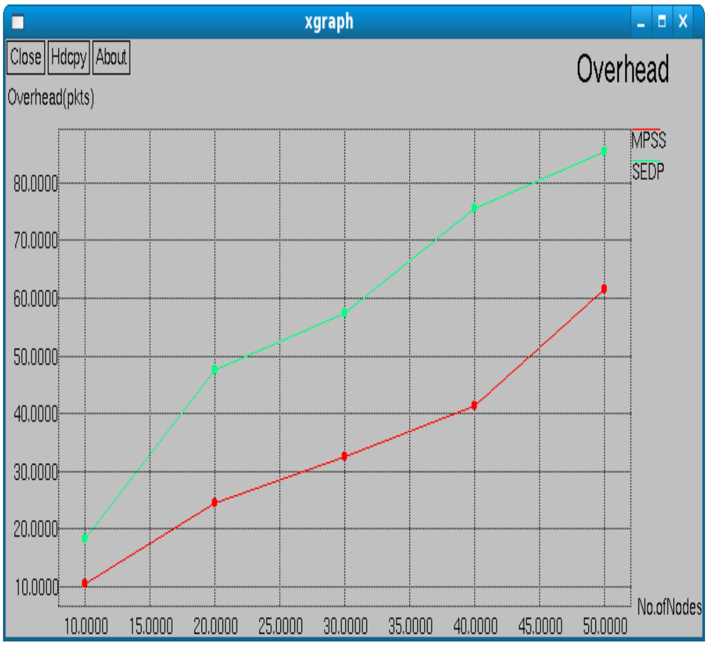

Figure 5.No. of nodes Vs Overhead

Fig. 5, presents the comparison of overhead and throughput. It is clearly shown that the overhead of MPSS has low overhead than the SEDP.

V. CONCLUSION

Wireless Ad hoc Networks consist of wireless nodes without any centralized infrastructure. Here node may be affected by several attacks. It may cause the packet dropping, misrouting the information to another destination. In our proposed work, we focus on detection of the black hole attacks. This attack degrades the performance of the mobile ad hoc networks. So that, we propose the modified proactive secret sharing scheme to detect the black hole attacks. In first phase, the black hole attacks are detected and isolated. In second phase, the authentication of data packets and data integrity is provided using our proposed proactive scheme. By using the extensive simulation results, the proposed scheme achieves better results than the existing schemes.

REFERENCES

[1] Muhammad Arshad Ali and Yasir Sarwar, “ Security Issues regarding MANET (Mobile Ad Hoc Networks): Challenges and Solutions”, thesis, 2011, pp.1-65.

[2]Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012, pp.45-54.

[3]Firoz Ahmed, Seok Hoon Yoon and Hoon Oh, " An Efficient Black Hole Detection Method using an Encrypted Verification Message in Mobile Ad Hoc Networks", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012, pp.179-184.

[4]Debdutta Barman Roy and 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.

[5]Govind Sharmaq and Manish Gupta, " Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012, pp.297-303.

[6]M. Umaparvathi and Dharmishtan K. Varughese, "Two Tier Secure AODV against Black Hole Attack in MANETs", European Journal of Scientific Research, ISSN 1450-216X, Vol.72, No.3, 2012, pp. 369-382.

[7]Disha G. Kariya, Atul B. Kathole & Sapna R. Heda, "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January 2012, pp.37-41.

[8]Sushil Kumar Chamoli, Santosh Kumar and Deepak Singh Rana, " Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", International Journal of Computer Technology & Applications, Vol 3 (4), 2012, pp.1395-1399.

[9]Ping Yi, Ting Zhu, Ning Liu, Yue Wu and Jianhua Li, "Cross-layer Detection for Black Hole Attack in Wireless Network", Journal of Computational Information Systems, Vol. 8, No.10, 2012, pp. 4101- 4109.

[10]N. Bhalaji and A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, ISSN 1450-216X, Vol.50, No.1, 2011, pp.6-15.

[11]Usha and Bose, "Understanding Black Hole Attack in Manet", European Journal of Scientific Research ISSN 1450-216X, Vol.83, No.3, 2012, pp.383-396.

[12]Mehdi Medadian and Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research, ISSN 1450-216X, Vol.69, No.1, 2012, pp.91-101.

[13]Soufiene Djahel, Farid Na¨It-Abdesselam, Zonghua Zhang And Ashfaq Khokhar, "Defending Against Packet Dropping Attack In Vehicular Ad Hoc Networks", Security and Communication Networks, 2008, Pp.245-258.

[14]Rajiv Ranjan, Naresh Trivedi and Anoop Srivastava, "Mitigating of Black Hole Attack in Manets", VSRD International Journal of CS & IT, Vol. 1 (2), 2011, pp.53-57.

[15] Himani Yadav and Rakesh Kumar, " Identification and Removal of Black Hole Attack for Secure Communication in MANETs", International Journal of Computer Science and Telecommunications, Volume 3, Issue 9, September 2012, pp.60-67.

[16]Thamil selvi C.P, " A Novel method to Detect Black Hole attack in MANET using Efficient ACO Strategy for SEAD Protocol", International Journal of Computer Applications (0975 – 8887) Volume 45– No.17, May 2012, pp.1-4.