Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

A Common Architecture for Detection and Prevention of Black Hole and Warm Hole Attack in MANET

Namita Yadav, Arvind Upadhyay
Rajiv Gandhi Proudyogiki Vishwavidyalay (RGPV)
Dept: Computer Science
Bhopal(Madhya Pradesh) India

***Abstract*— Mobile ad hoc network is a collection of mobile devices which are communicating in self-organizing manner to support the communication additionally there are not any centralized control available for support the security and performance. Thus a number of contributions are made for providing solution for security and performance issues in network. This presented work is an investigation of the recently made solutions for the security in ad hoc network as well as the performance issues in network. Thus for experimentation and demonstration two more frequently deployable attacks namely Black hole and wormhole attacks are considered for work.**

In order to provide the efficient and secure solution first the efficient routing protocol is obtained which servers efficiently not only for small networks as well as for large networks. Therefore in comparison of DSR routing protocol AODV routing protocol is considered for implementation. Furthermore, the solution is derived using the attack characteristics first for distinguish the Black hole attack their packet drop and for the wormhole detection the RTT threshold is obtained first. These thresholds are used to discover safe route among the source and destination. The given method not only optimize the security in network that also delivery the data efficiently.

The implementation of the proposed modification is performed in network simulator 2 environment and the performance is computed in terms of end to end delay, throughput and packet delivery ratio. The obtained results show the effectiveness of solution for attack conditions communication. Thus the proposed solution is more adoptable and efficient than the traditional security and routing solutions.

***Keywords*— Include at least 5 keywords or phrases**

I. INTRODUCTION

The proposed study addresses the challenges and issues in mobile ad hoc network. Due to weak performance and rapid configuration of network technology that is keep attracted researchers. The given chapter includes the overview of presented work. Mobile ad hoc network is a new generation network technology that is self-defined by their name ad hoc network. The main advantage of such kind of network is their rapid configuration and hurdle free operation. The MANET is adoptable in those areas where the network management and maintenance is complex enough such as remote areas and battle field. Due to their advance technique there are no needs to install a stable infrastructure for organizing the network. Due to mobility and adoptive nature of network various different issues are arises in this network. The main issue of the network is performance and security, most of the time network adopts those nodes that are untrusted. Therefore the performance of network is affected due to the malicious behaviour of newly joined node. Therefore most of the security issues are arises through the routing protocols. Therefore in this study routing protocols and their type of attacks are investigated and explored for finding the solution of routing protocol based attack deployment. Mobile ad hoc network is a group of wirelessly connected network devices. In this network all the nodes having similar functionality and features. All the participating devices are free to move independently in any direction at random speed. In this network not any kind of fixed infrastructure is available for communication. Therefore the nodes those are not in range of the source nodes who wants to send data is transmitted through the multi-hop option. In this kind of message transmission the network simulates the cooperative behaviour, and message is transferred using the intermediate nodes in network. Due to this the proposed study is focused on study of different kinds of attack deployed in the network and their solution development. In this study two main issues is aimed namely black-hole and wormhole attack. Both kinds of attacks are different in characteristics and can harm the network in different manners. In black-hole attack the malicious node attracts traffic and drop most of the data. On the other hand more than two attackers are involved in wormhole attack; both the malicious nodes are connected through the high speed data buses. Most of the time these nodes capture data and tunnel it, so due to this TTL of data are expired and a significant amount of data are lost in network. Therefore required to develop a new approach by which the MANET can be preserved for the serious attack situations.

II. PROPOSED WORK

A. Problem Domain

In the proposed work the main aim is to design such kind of method by which the network becomes free from the black and wormhole attack. The main issues and challenges are given in these sections.

1. During black-hole attack a certain amount of data is lost.

2. Black hole attack attracts traffic by promising to have a shortest path between source and destination.
3. Wormhole attack misguide the traffic during attack conditions
4. There is not a much promising way to detect the accurate location of wormhole link in network.

Therefore a new kind of technique required to find by which the selected route between source and destination that is secure and free from the attackers.

B. Solution Domain

The solution for the above described issues in network leads to find a secure and optimum route between source and destination. Therefore, the proposed solution considered two main parameters by which the selected route is ensured for security.

1. During the route discovery process in the AODV routing protocol, first source node send the RREQ message. At this time when RREQ packet is received by the attacker node. First attacker response the source node with a RREP packet. The source router finds a shortest path for destination through the malicious node and all the data is dropped by attacker node. Therefore if a node having a higher packet drop ratio it may be suspected node.
2. Wormhole is a complex kind of attack deployment, in this attack more than one attacker can involve in network and misguide the traffic. In addition of that due to mobility and tunnelling the wormhole attack is not detected. In addition of that the geo positioning based algorithms are failed to approximate the issue in network. Therefore with the packet drop ratio the transmission delay between source and target is desired to compute for secure communication.

This section provides the basic solution for finding the optimum route between source and destination. In the next section the proposed method is concluded using algorithm steps.

C. Algorithm Design

The solution algorithm design is formulated as:

Assumptions

a. Black hole attack attract network traffic and increases the packet drop ratio
b. Wormhole link tunnel the packets from one end and deliver the packet at other end in network.
c. Under attack conditions total time required in deliver a packet from malicious route is greater than to the normal route.

Pseudo code

```
a. Broad cast the RREQ packet to 1 hop nodes.
      • Start timer
b. Wait for RREP message
      • Stop timer
c. Add additional information in routing table
      • Th = Stop time-start time
      • PDR(packet drop)
d. Traverse through source node to destination and compute
      • $A_{th} = \frac{1}{H}\sum_{i=0}^{H} Th_i$
e. If $A_{th} > T_{th}$
      • Path contains wormhole link
      • Remove path entry
f. If $PDR > PDR_{th}$
      • Path contains black hole
      • Remove path entry
g. Else
      • Select route for transmission
```

D. Algorithm description

The given algorithm is an adoptive technique of attack detection and prevention. In this technique first the network performance is tested in terms of packet drop ratio and average time consumption during normal (ideal conditions with any attacker node). Using the obtained performance the threshold values for algorithm is computed. Than after, during route discovery in AODV routing protocol the allowable threshold is checked for individual intermediate to distinguish honest node or malicious node.

III. IMPLEMENTATION

This chapter provides understanding about the implementation of the proposed concept of secure routing against the Blackhole and wormhole attack in mobile ad hoc network. Additionally the chapter includes the simulation scenarios and network environment setup for experimentation.

A. Network Simulation Setup

To prepare the desired simulation model for detection and prevention of Blackhole and wormhole attack the below given network parameters are used as listed in given table 4.1. The table includes the network parameters and the values for the simulation environment.

Simulation properties	Values
Antenna model	Omni Antenna
Dimension	750 X 550
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	43
Routing protocol	AODV
Time of simulation	10.0 Sec.

Table 1. Simulation setup

B. Simulation Scenarios

The given section demonstrate the simulation conditions and experimental environment by which the problem domain and suggested solution's effect is provided.

1. Using simple network: that is an ideal condition of network when not any malicious node is introduced. In these conditions the threshold values are calculated for restricting the malicious node in network.
2. Attack conditions: in this simulation scenario the network is deployed with the attacker nodes namely black hole node and wormhole nodes. In addition of that the performance of the system is evaluated.

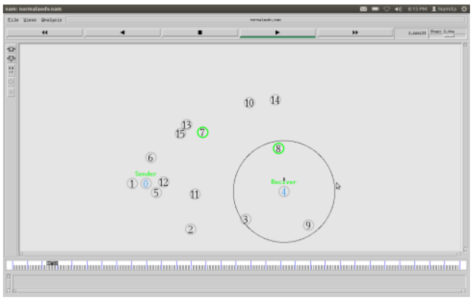

Figure 1 network under attack

3. Solution scenario: in this simulation the proposed method for detection and prevention of the black hole and wormhole attack is simulated and performance of the proposed system is estimated. The simulation screen given in figure 1 demonstrates the solution scenario. In this given simulation sender and receiver nodes are labelled with blue fonts in figure that are presented through 0 and 4 node. And the malicious node is given using the node 7 and 8 the green node represents the wormhole link in network.

VI. RESULT ANALYSIS

The given chapter provides the results analysis from the different experimentation performed with the network simulation. The reported results are one of the most optimum result that are obtained.

A. Packet delivery ratio

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

The amount of packet is delivered during a communication session is defined as packet delivery ratio.

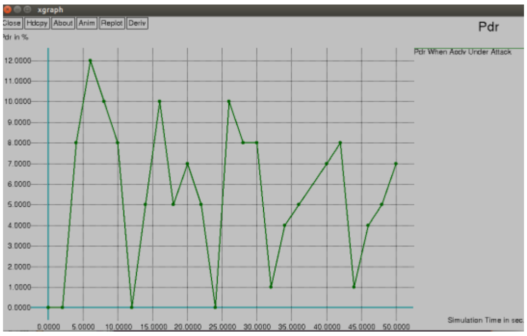

Figure 2 AODV PDR under attack

The figure 2 shows the experimentation results of AODV routing protocol under the attack conditions. In this diagram the X axis shows the simulation time and Y axis shows the amount of packets delivered at the destination in terms of percentage. According to the observation during the attack in network too few amount of data is riches at the destination therefore the packet delivery ratio is varies between 0-12%. On the other hand the proposed secure routing protocol is simulated using figure 2. In this diagram the packet delivery ratio is also simulated in terms of percentage which is varies between 69-99%. Therefore the results show the effectiveness of the proposed secure routing protocol against the Blackhole and wormhole attack. According to the observation of proposed routing protocol's performance both attacks are neutralized or not much effective during the secure route discovery and packets securely delivered to the destination end.

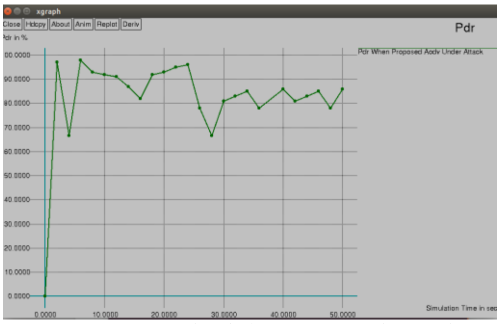

Figure 3 proposed technique's PDR under attack

Finally the comparative performance under attack conditions are simulated using figure 3, where the performance difference of both namely traditional and proposed AODV routing can be shown clearly.

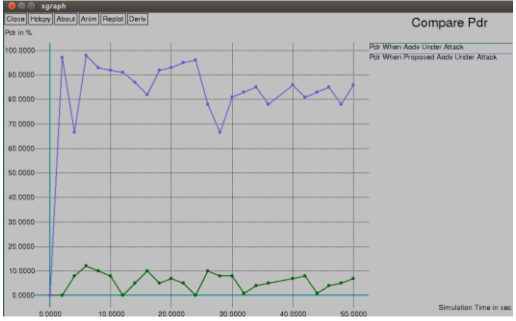

Figure 4 Comparative PDR under attack

B. End to end delay

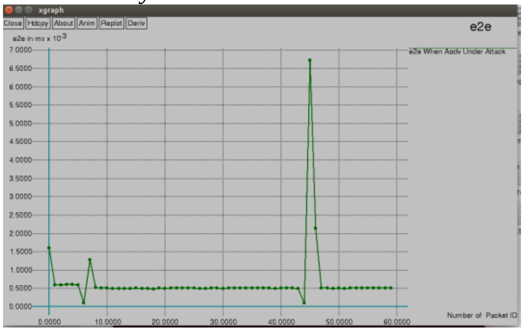

Figure 5 AODV e2e delay under attack

End to end day on network refers to the time taken for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2e\ delay = receiving\ time - sending\ time$$

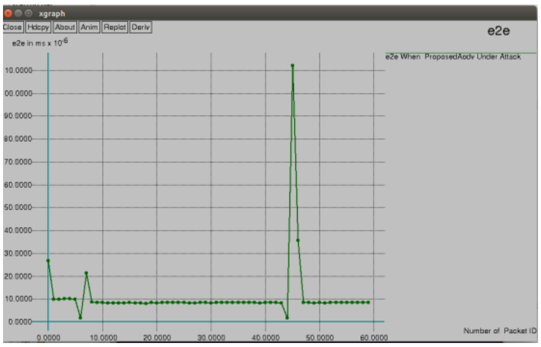

Figure 6 Proposed algorithm e2e delay under attack

The performance of the AODV routing under attack conditions in terms of end to end delay is given using figure 4 in addition of that the performance of the proposed routing protocol is given using figure 5. Additionally the comparative end to end delay of both the routing protocols is simulated using figure 6. In all the simulation results the X axis shows the simulation time and the Y axis shows the corresponding end to end delay in terms of milliseconds. According to the obtained comparative outcomes end to end delay of the proposed technique is less than the traditional routing protocol under the attack conditions. During attack conditions the end to end delay of network higher because the packets are misrouted or attempting to deliver in unavailable host in network thus the no packets are reached at the destination end therefore the end to end delay of network is unexpectedly increases and decreases.

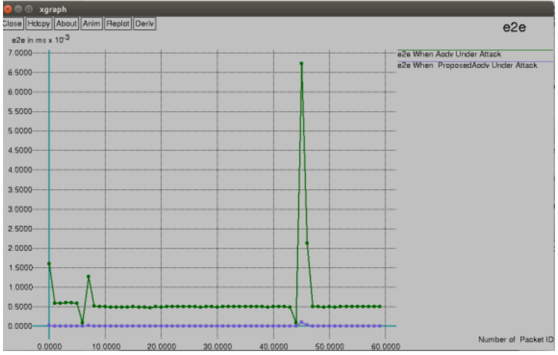

Figure 7 comparative e2e delay

C. Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

Received data = ($bytes/$time)* 8/1000000

througput_in_mbps = bytes_recv_per_unit_of_time* 8/1000000

The throughput of the network in terms of KBPS is estimated for the network in both the conditions during simple AODV protocol implementation and after implementation of the proposed secure routing protocol. The simulation results during simple AODV routing protocol implementation is given using figure 5.7 in this diagram the bandwidth consumption

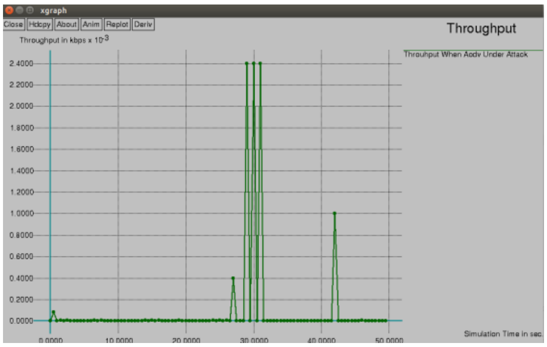

Figure 8 AODV throughputs under attack

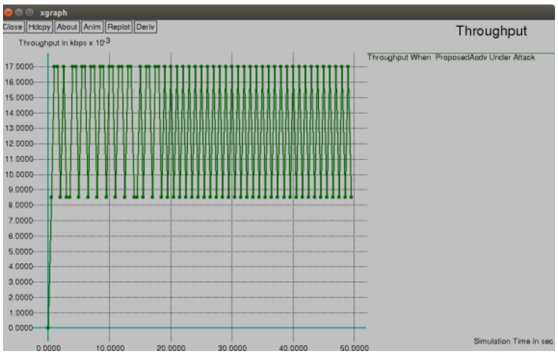

Figure 9 proposed algorithm throughput under attack

Of network tends to zero because fewer amount of data are delivered at client end and on the other hand the throughput of the network as given in figure 7 are increases therefore the number of successfully delivered packets are increases. Thus the performance of the network under the attack during the proposed routing protocol is efficient than the traditional routing protocol.

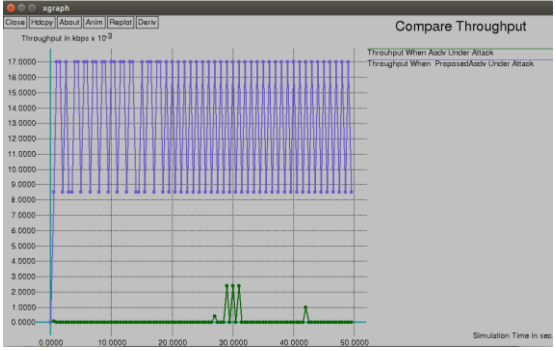

Figure 10 comparative throughputs under attack

Additionally the comparative performance in terms of throughput is given using figure 8 in this diagram the proposed routing protocol consumes more bandwidth as compared to the traditional routing protocol in attack conditions thus the proposed routing protocol is not affected during Blac khole and wormhole attack.

V. CONCLUSION AND FUTURE WORK

The mobile ad hoc network is one of most popular wireless network technology which promises to provide solution for next generation mobile computing and communication. The key advantages of this network are mobility and adoptability of network. Due to mobility the nodes can leave or join the network any time and also for frequent communication can use the multi-hop options. In this communication manner limitation of limited radio range is overcome and nodes pass the information one from other. But the dark side of this advantage is that a malicious node can also join the network and harm the privacy and performance of network.

During the survey there are various kinds of attack deployment techniques are found but Blackhole and wormhole are two key area of interest among researchers. But a limited number of solutions are found for detection and preventions for both. Therefore in this presented work a new kind of solution is introduced which provide solution for both of them using a single algorithm. Thus the proposed algorithm combines two different methods of malicious node detection techniques first is taken from the Blackhole behaviour as the packet drop threshold and second is motivated from the RTT calculations. Both the techniques are implemented with help of the traditional routing algorithm namely AODV routing protocol. The modification in this routing protocol is performed in such manner during the route discovery the protocol only considers the safe or secure route as compared to the shortest route.

The advantage of this it not only secures the data during communication sessions that also provide efficient communication. The implementation of the proposed prototype is performed using the network simulator 2 environment and the performance of the system is also demonstrated under attack conditions. The comparative outcomes of the traditional routing protocol and proposed modified AODV routing protocol is summarized using table 2.

S. No.	Parameters	Traditional AODV	Modified AODV
1	End to end delay	High	Low
2	Throughput	Low	High
3	Packet delivery ratio	Low	High

Table 2 performance summary

According to the obtained performance of the traditional and proposed AODV routing protocol the proposed technique delivers high performance results even in attack conditions. Thus the proposed solution is more adoptable as compared to the traditional AODV routing.

A. Future work

The proposed routing protocol is more adoptable due to their security and the performance under attack conditions. Additionally that is a rule based technique which computes the thresholds of attack characteristics and implement using the route discovery options. Therefore the proposed technique is only feasible for link-layer attacks thus in near future the proposed technique can be optimized for other layers attack detection and prevention.

REFERENCES

[1] Yongguang Zhang, Wenke Lee, Yi-An Huang, “Intrusion Detection Techniques for Mobile Wireless Networks”, Mobile Networks and Applications 2003, p.p. 1-16

[2] Ms. Ankita M.Shendurkar, Prof. Nitin R.Chopde, “A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET”, International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 8 - Mar 2014

[3] Priyanka Patil, M. A. Rizvi, “Improved and Energy Efficient Olsr Protocol Using Spanning Tree in Manet”, IOSR Journal of Comp Engg (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 4, Ver. II (Jul-Aug. 2014), PP 38-42

[4] Martin K Parmar, Harikrishna B Jethva, “Survey on Mobile ADHOC Network and Security Attacks on Network Layer”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013

[5] S. A. Ade & P. A. Tijare, “Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks”, Inter. Jour. of Information Technology and Knowledge Management, July-Dec 2010, Vol 2, No. 2, pp. 545-548

[6] Vinay Sridhara, Nagendra Subramanya, “Evaluating Different Techniques to Improve TCP Performance over Wireless Ad Hoc Networks”, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.80.8842

[7] M. S. karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, “Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols”, proceedings of the inter multi conf. of engineering and computer scientists, Vol II, march 2010

[8] Vikas Solomon Abel, “Survey of Attacks on Mobile Ad hoc Wireless Networks”, (IJCSE) ISSN : 0975-3397 Vol. 3 No. 2 Feb 2011

[9] Animesh Patcha and Amitabh Mishra, “Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks”, 0-7803-7829-6/03/$17.00 0 2003 IEEE

[10] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, licensee Springer. 2011, http://link.springer.com/article/10.1186/2192-1962-1-4/fulltext.html

[11] Shree Om and Mohammad Talib, “Wireless Ad-hoc Network under Black-hole Attack”, 2011 ISSN 2225-658X.

[12] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil, “Black Hole Attack Injection in Ad hoc Networks”.

[13] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng et al. Human-centric Computing and Information Sciences 2011.

[14] Abder Rahmane Baadache, Ali Belmehdi, “Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks”, ISSN 1947-5500 (IJCSIS) Vol. 7, No. 1, 2010.

[15] Varsha Patidar, Rakesh Verma, “Black Hole Attack and its Counter Measures in AODV Routing Protocol”, ISSN 2250-3005 Sep. 2012

[16] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”.

[17] Nishant Sitapara, Sandeep B. Vanjale, “Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks, ICETE-201O" on Emerging trends in engineering on 21st Feb 2010.

[18] Kamatchi. V, Rajeswari Mukesh,Rajakumar, “Black Hole Attack Prevention Using random Dispersive Routing For mobile ad hoc Networks”, (Ijans) Vol. 2, No. 4, October 2012.

[19] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, Abbas Jamalipour, “A survey of routing attacks in mobile ad hoc networks”, 1536-1284/07/$20.00 © 2007 ieee.

[20] Baltej Kaur Saluja, A.K.Gupta, “Detection and Prevention of Wormhole Attack in Spontaneous Wireless Network”, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December 2014

[21]Vrutik Shah and Dr.Nilesh Modi, “Responsive Parameter based an AntiWorm Approach to Prevent Wormhole Attack in Ad hoc Networks”, ACEEE Int. J. on Network Security , Vol. 5, No. 1, January 2014

[22] Shiva Shamaei and Ali Movaghar, “A Two-Phase Wormhole Attack Detection Scheme in MANETs”, July 2014, Volume 6, Number 2 (pp. 183–191)

[23] Mr. B. Satheesh kumar, Ms. R. Kalaivani, “Privacy Protection Against Wormhole Attacks In MANET”, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January-2014, pg. 56-62

[24] Akansha Agrawal, Prof. Amit Saxena, “Wormhole Detection and Prevention Scheme using Beacon Node Mechanism with Neighbor Node Discovery”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6620-6625

[25] Subhashis Banerjee and Koushik Majumder, “Wormhole Attack Mitigation In MANET: A Cluster Based Avoidance Technique”, International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014

[26] Gaurav Garg, Sakshi Kaushal and Akashdeep Sharma, “Behavioural Study of Reactive Protocols with Wormhole Attack in Mobile ADHOC Networks”, Journal Of Emerging Technologies In Web Intelligence, Vol. 6, No. 4, November 2014

[27] R. Rajamohamed and V. Rajamani, “A Secure Hashed Variable Bit Rate Source Routing Protocol and Mitigation of Wormhole Attack for Manets”, Middle-East Journal of Scientific Research 22 (1): 91-98, 2014 ISSN 1990-9233 © IDOSI Publications, 2014

[28] Ali Hassan, Syed Ahsan, Saleh Alshomrani, Adel Alshamrani, “Packet Travel Time based Mechanism for Detection and Mitigation against Wormhole Attack in AODV for MANETs”, Life Science Journal 2014;11(10s)

[29] Neha Sahu, Deepak Singh Tomar, Neelam Pathak, “A Modified Aodv Protocol to Detect and Prevent The Wormhole: A Hybrid Approach”, IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.2, February 2015