Mobile Adhoc Network under the Adaptive TCP Variants Techniques for Maximization of Throughput

Minakshi Halder
M.E. Dept. of ECE
SGSITS, 23 Park Road
Indore, MP, India

L.D Malviya
Assistant prof., dept. of ECE
SGSITS, 23 Park Road
Indore, MP, India

Rekha Jain
Assistant prof., dept. of ECE
SGSITS, 23 Park Road
Indore, MP, India

ABSTRACT
It is an adhoc network which is set up by wireless mobile computers (or nodes) which moves randomly in the places that have no network infrastructure or hard to reach location. Since the nodes communicate with each other to gather network information. They cooperate by forwarding data packets to other nodes in the network. In wireless adhoc networks, cooperation between nodes takes place so that they route each other's packet till it reaches destination. Hence they are exposes to a wide range of security attacks. Also because the vulnerability of routing protocols, the wireless ad-hoc networks have to face several security risks. One of these attacks is the Blackhole Attack against network integrity which absorbs all data packets in the network. Since the data packets do not reach the destination node due to Blackhole attack. As a result data loss will occur. In this paper, we simulated the Black hole attack in various wireless ad-hoc network scenarios: with Blackhole attack and without Blackhole attack and comparison of existing TCP variants: TCP, FullTCP, Reno, Reno/Asym, New Reno, New Reno/Asym, Asym, Sack, Fack and Vegas. The impact of Blackhole attack on the performance of MANET is evaluated on the basis of those two scenarios. The measurements were taken to analyze network performance are Throughput, Packet Delivery Ratio and Total Dropped Packet. The simulation was done by using network simulator (NS-2.34).

Keywords
Mobile ad-hoc network (MANET), TCP variants, routing protocol, network security, Blackhole attack, NS-2.

1. INTRODUCTION
Wireless networks can be configured according to the need of the users at any time anywhere. Adhoc networks are independent network which consist of a collection of mobile nodes that uses wireless transmission for communication. They are self-organized, self-configured, and self-controlled infrastructure less networks [1, 2, 3]. In adhoc network, the devices themselves are the network. These can range from small number of users to large networks where the number of users is in thousands. One of the great features of wireless network is its mobility. This feature gives user the ability to move freely, while being connected to the network. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Thus, a multi-hop scenario occurs, where several intermediate nodes relay the packets sent by the source host, before they reach the destination node [4, 5].
To gather network or environment information, nodes uses some set of rules i.e. routing protocol. Every node required some type of routing protocol to communicate. We used AODV routing protocol which is a reactive type because of its features like supporting unicasting and multicasting, uniform packet size, work as on-demand, routing table needed only required information etc [6, 8].

2. BLACKHOLE ATTACK IN MANET

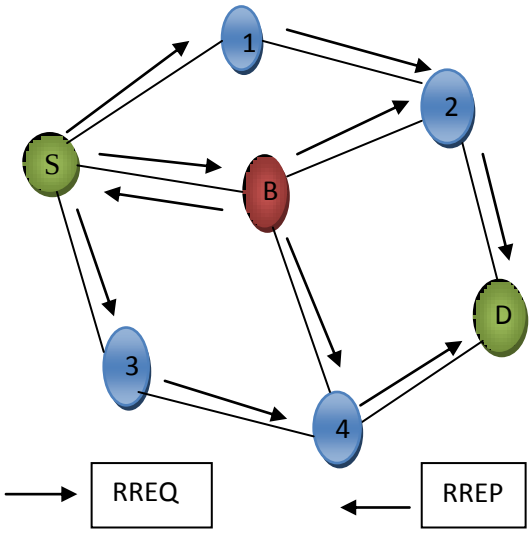


Figure 1: Blackhole attack implementation

Security becomes an important issue in wireless networks since there are no physical limitations. Availability of network services like confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET suffers from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring, and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats [7]. MANETs are vulnerable to various attacks, Blackhole, is one of the possible attack. Blackhole is a type of routing attack where a malicious node advertises itself as having the shortest path to destination. By doing this, the malicious node can deprive the traffic from the source node. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node always have the availability in replying to the route request and thus mislead the data packet and retain it [9, 12]. In protocol based, on flooding, the malicious node's reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and fake route is created. When this route is established, then it's up to the node whether to drop all the packets or forward it to the unknown address [11].

Figure 1 shows how Blackhole attack implementation arises, here node "S" wants to send data packets to node "D" and initiate the route discovery process. So if node "B" is a malicious node then it will claim that it has active route to the destination as soon as it receives RREQ (route request) packets. It will then send the response to node "S" before any other node. In this way node "S" will think that this is the active route and thus route discovery is complete. Node "S" will ignore all other replies from other nodes and start seeding data packets to node "B" in dilemma that these packets where going to destination "D". In this way all the data packet will be consumed or lost [15].

2.1 What is sensor network?

Wireless sensor network is like mobile adhoc network except it has an especial phenomenon i.e. sensors which has capability to sense. A wireless sensor network (WSN) consists of a set of automated devices called sensor nodes. A sensor node is a computational device that has memory, battery, processor, a short-range wireless transceiver and a sensing device (for monitoring temperature, pressure, acoustics etc.). These nodes are distributed across an area and communicate among themselves, forming an adhoc network. Sensor networks contain special nodes that process and store the information collected by the network; they are called sink nodes. Communication between two nodes is preferred in multiple hops if they are not within each other's transmission range.

Wireless sensor networks can collect data from the environment where they are embedded. The data are often first processed by the sensor nodes and then sent over non-secure channels to the sink node for further processing. WSN technology enables monitoring of vast and remote geographical region, in such a way that abnormal events can be quickly detected. Some of the applications envisioned for sensor networks are environmental monitoring, infrastructure management, public safety, medical, home and office security, transportation, forest fire detection, under water observations and battle field surveillance. Given their criticality, these applications are likely to be attacked. The cost of sensor nodes varies from hundreds of dollars to a few cents, depending upon their size, cost and complexity. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, network lifetime, memory, computational speed and transmission range.

2.2 TCP and its variants

2.2.1 TCP

TCP is a connection oriented, reliable and conforming transport protocol [10]. Here prior to transmitting data, a connection establishment phase must be completed. That is known as 3-way handshake. During transfer, TCP employs both flow control and congestion control. Flow control between source to destination and congestion control in the rate of data at enter into the network.

2.2.2 FullTCP (two-way TCP agent)

It is different from (and incompatible with) the other TCP agents in the following ways [16]:

1. Connections may be established and town down (SYN/FIN packets are exchanged).
2. Bidirectional data transfer is supported.
3. Sequence numbers are in bytes rather than packets.
4. It sends data earlier than the typical TCP sends to receiver.

2.2.3 TCP Reno

Reno retains slow starts and the coarse grain retransmit timer. It has some intelligence which detects packet loss earlier. Reno requires that to receive immediate acknowledgement whenever a segment is received [14]. Probability of packet loss is high so RENO uses algorithm called fast retransmits. Whenever it receives three duplicate ack (acknowledge) it shows the sign that the segment is lost then retransmit the segment without timeout.

2.2.4 TCP New Reno

New RENO is a slight modification over TCP-RENO. It is able to detect multiple packet losses and thus is more efficient that RENO. New-Reno also enters into fast-retransmit when it receives multiple duplicate packets, however it differs from RENO in that it doesn't exit fast-recovery until all the data which was out standing at the time it entered fast recovery is acknowledged. In fast recovery it notes maximum segment which is outstanding.

2.2.5 TCP Sack

TCP with Selective Acknowledgments (SACK) is an extension of TCP Reno and it works around the problems face by TCP RENO and TCP New-Reno, namely detection of multiple lost packets, and retransmission of more than one lost packet per RTT. SACK TCP enquires that segments not be acknowledged cumulatively but should be acknowledged selectively [17]. It also retains slow starts and fast recovery. When modified algorithm is not able to detect packet loss it falls in coarse grain timeout.

2.2.6 TCP FACK

The development in TCP SACK with Forward Acknowledgement is identified as TCP FACK. The utilization of TCP FACK is almost identical to SACK but it establishes a little enhancement evaluated to it. It uses SACK option to better estimate the amount of data in transit. TCP FACK introduces a better way to halve the window when congestion is detected [18]. When CWND (congestion window) immediately halved, sender stops transmitting for a while then resumes when enough data left the network. So one RTT (round trip time) is avoided when window gradually decreases.

2.2.7 TCP Vegas

Vegas are a modification of Reno [13.17]. TCP Vegas is different from TCP Reno in the way that:

1. A new retransmission mechanism is used.
2. An improved congestion avoidance mechanism that controls buffer occupies.
3. A modified slow start mechanism.

It include a modified retransmission strategy that is based on fire-gained measurements of the RTT (means defined by system clock) as well as new mechanism for congestion detection during slow start and congestion avoidance.

In TCP Reno coarse grain timer estimate RTT and variance, which results in poor estimates. TCP Vegas extends TCP Reno's retransmission mechanism.

3. SIMULATION SETUP AND RESULT DISCUSSION

Various performance metrics are used for evaluation of AODV protocols. Performance metrics that includes Throughput, Packet Delivery Ratio, and Total Dropped

Packets. These matrices are important to analyze the performance of the network.

3.1 Performance Metrics

The performance metrics chosen for the evaluation of Blackhole attack under mobile adhoc network.

3.1.1 Throughput

It is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second. In MANETs throughput is affected by changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter of the network.

3.1.2 Packet delivery ratio

The ratio of the number of delivered data packet to the destination i.e. number of packets received to the number of packets send.

Packet delivery ratio = $\frac{\sum \text{number of packet receive}}{\sum \text{number of packet send}}$

The greater value of packet delivery ratio means the better performance of the routing protocol.

3.1.3 Total Dropped packet

A packet drops for any reason, it may be due to link breakage (failure) or queue of node is full.

3.2 Simulation setup

Simulation has been performed using NS-2 network simulator version 2.34. The numbers of nodes are 30 and node mobility is varying from 30m/s to 120km/hr. The traffic type is File Transfer Protocol (FTP), with varying topology and position of nodes. The wireless nodes are randomly allocated in a 1000x1000 square meter. The node transmission range is 200 meter. Ten different types of TCP variants were used to evaluate the performance of MANET. These are TCP, FullTCP, TCP Reno, TCP Reno/Asym, TCP New Reno, TCP New Reno/Asym, TCP Asym, TCP Sack, TCP Fack and TCP Vegas.

3.3 Simulation Results

Simulation has two scenarios. In the first one every node is working in cooperation with each other to keep the network in communication i.e. a normal adhoc network. The second simulation has one Blackhole node that carries out the Blackhole Attack. This study compares the result of these two simulations scenarios to understand the network and node behaviors.

3.4 Utilization of speed

In this paper, we have taken the speed range from 30m/s to 120km/hr means from speed of two wheeler (motor bike) to speed of a car or truck that run over highway. From this we can analyze that how MANET performs when speed of mobile varies from low to very high [19, 20].

Scenario one: Behavior of AODV routing protocol in MANET when Blackhole attack is not performed.

Table 1. Performance of TCP Variants for Scenario I

	TCP	FullTCP	TCP Reno	TCP Reno/Asym	TCP New Reno	TCP New Reno/Asym	TCP Asym	TCP Sack	TCP Fack	TCP Vegas
Throughput	542.46	260	537.29	547.59	553.87	547.59	547.59	542.35	545.83	287.07
Packet delivery ratio	98.2127	97.9167	97.6411	98.0789	98.3307	97.7712	98.3281	98.2051	98.2844	99.1259
Total dropped packets	105	40	142	149	110	129	108	120	110	69

Table 1 shows the maximum values of Throughput, Packet Delivery Ratio and minimum values of Total Dropped Packets for all the TCP variants.

Scenario two: Behavior of AODV routing protocol in MANET when Blackhole attack is performed.

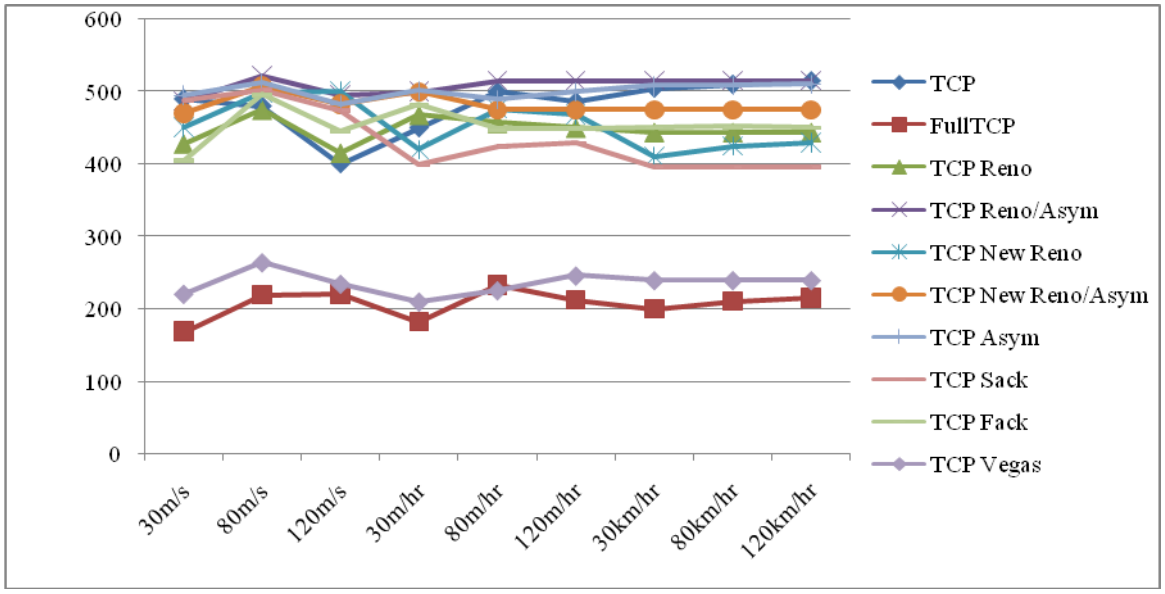


Figure 2: Throughput of TCP variants in Blackhole attack

Figure 2 illustrate the impact of mobility on throughput. It depicts that the AODV heavily suffers from Blackhole attack. The throughput of AODV protocol slightly decreases when the mobility speed increases since high mobility speed causes higher link breakdown probability, and in turn the protocol introduces more route discovery processes.

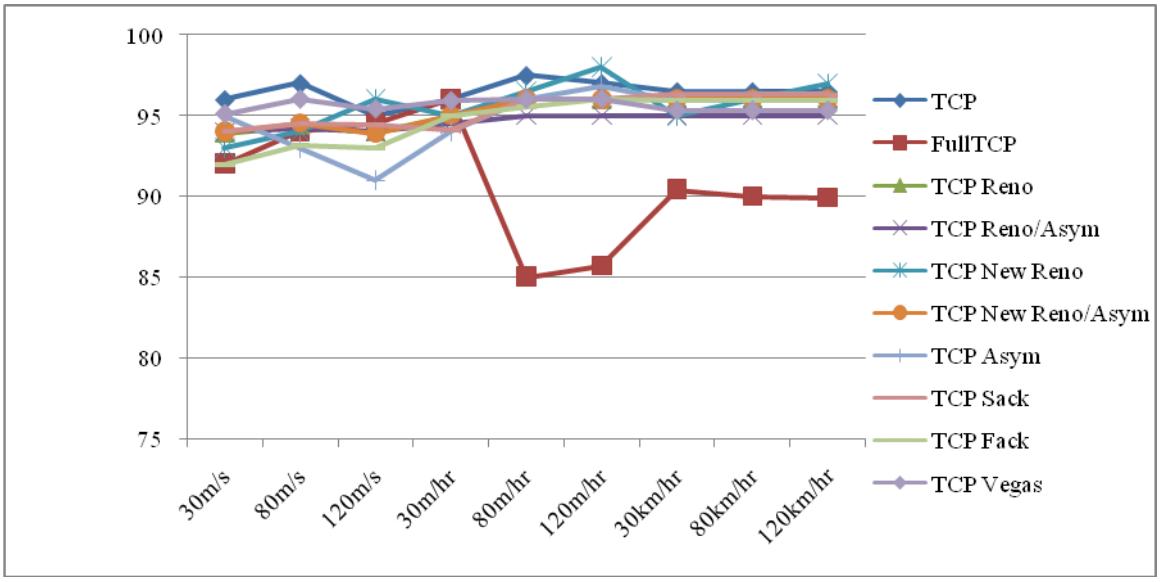
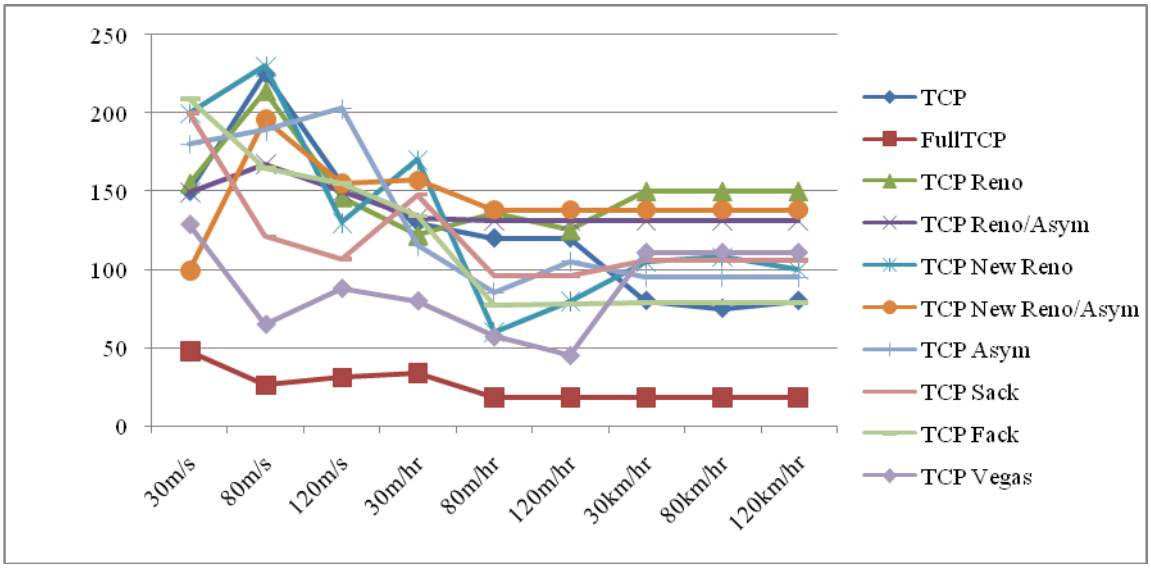


Figure 3: Packet delivery ratio of TCP variants in Blackhole attack

Figure 3 illustrates the impact of the mobility speed of nodes on packet delivery ratio. In all the protocols, with the mobility speed of nodes link breakage occurs. Suppose if packet is transmitted then link breakage happen the packet is not delivered at receiver. Thus it shows big impact on packet delivery ratio. Hence the performance degrades.

Figure 4 illustrates the impact of the mobility speed of nodes on total dropped packets. As the node mobility increases more and more link breakages occur. Hence packet will not deliver to destination. Thus the number of drop packets increases. Because packet drops for any reason.



Node mobility (m/s)

Figure 4: Total dropped packets of TCP variants in Blackhole attack

Table 2. Shows values of matrices in low speed (30m/s) and high speed (120km/hr)

	30m/s	**120km/hr**
Throughput	524.43	542.46
Packet delivery ratio	98.2	98.5
Total dropped packets	75	50

From table 2, the TCP variant which shows maximum throughput is Original TCP, Vegas showing maximum value of packet delivery ratio, FullTCP shows lowest value of total dropped packets among the all ten variants in both speed at 30m/s and also at 120km/hr.

4. CONCLUSION

This study, analyzed the effect of the Blackhole in an AODV routing protocol based network. For this purpose, blackholeAODV protocol was implemented that behaves as Blackhole in NS-2.34. Simulated five matrices where each one has 30 nodes that use AODV protocol and also simulated the same matrices after introducing one Black hole node into the network.

Based on above discussions, we can suggest the adaptive TCP variant technique for the maximization of throughput and packet delivery ratio and for minimization of total dropped packets.

In the scenario one, the TCP variant which shows maximum value of throughput in both the speed is TCP. Hence the performance of TCP is excellent than all selected TCP variant at each speed level and maximum value of packet delivery ratio in both the speed is TCP Vegas. Its performance over the speeds level taken in whole network is larger than all selected TCP variant and for minimization of total dropped packets in both the speed is given by FullTCP. It gives minimum packet drops for speed ranges from 30m/s to 120km/hr.

In scenario two, TCP Reno/Asym gives maximum value of throughput in all speed ranges specified than all other TCP variant and TCP provides maximum packet delivery ratio in all speed and FullTCP gives minimum packet drops for all speed ranges.

5. REFERENCES

[1] Dokurer, S.; Ert, Y.M.; Acar, C.E. SoutheastCon, *Performance analysis of ad-hoc networks under black hole attacks*". Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.

[2] Payal N. Raj and Prashant B. Swadas,"*DPRAODV: A dynamic learning system against black hole attack in AODV based Manet*", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009.

[3] Sheenu Sharma, Roopam Gupta," *Simulation Study of Blackhole Attack in the Mobile Ad-Hoc Networks***"** Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250.

[4] Madhusudhananagakumar KS , G. Aghila, "*A Survey on Black Hole Attacks on AODV Protocol in MANET*" , International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011.

[5] Monika Roopak , Dr. Bvr Reddy ,"*Performance Analysis of Aodv Protocol under Black Hole Attack*" International Journal of Scientific & Engineering Research Volume 2, Issue 8,August-2011 1 ISSN 2229-5518.

[6] Elizabeth M. Royer and Chai-Keong Toh, "*A Review of Current routing Protocols for Ad Hoc Mobile Wireless Networks*," IEEE Personal Communications, pp 46-55, April 1999.

[7] H. Deng, W. Li, and D. Agrawal, "*Routing Security in Wireless Ad Hoc Networks*", IEEE Comm. Magazine, vol. 40, no. 10, 2002, pp. 70 75.

[8] S. Lu, L. Li, K.Y. Lam, L. Jia, "*SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack*," International Conference on Computational Intelligence and Security, 2009.

[9] A.Vani, D.Sreenivasa Rao, "*Providing of Secure Routing against Attacks in MANETs*",International Journal of Computer Applications (0975 – 8887) Volume 24– No.8, June 2011.

[10] S. R. Biradar 1, Subir Kumar Sarkar*2* , Puttamadappa C," *A Comparison of the TCP Variants Performance over different Routing Protocols on Mobile Ad Hoc Networks*" (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 340-344.

[11] Vikas Solomon Abel," *Survey of Attacks on Mobile AdhocWireless Networks***"** International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 2 Feb 2011.

[12] 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.

[13] Lawrence S. Brakmo and Larry L. Peterson, "*TCP Vegas: End to end congestion avoidance on a global Internet*," IEEE Journal on Selected Areas in Communications, vol.13, pp.1465-1480, October 1995.

[14] Jitendra Padhye , Victor Firoiu , Donald F. Towsley , James F. Kurose, "*Modeling TCP Reno performance: a simple model and its empirical validation*," IEEE/ACM Transactions on Networking (TON), v.8 n.2, p.133-145, April 2000.

[15] Rajib Das,Dr. Bipul Syam Purkayastha, Dr. Prodipto Das "*Security Measures for Black Hole Attack in MANET: An Approach* " International Journal of Engineering Science and Technology (IJEST), ISSN : 0975-5462 Vol. 3 No. 4 Apr 2011.

[16] R. Britto Pradeep, N. Dhinakaran, P. Anitha Christy Angelin,"*Comparison of Drop Rates in Different TCP Variants against Various Routing Protocols***"** *International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.*

[17] B. S. Yew, B. L. Ong, and R. B. Ahmad*," Performance Evaluation of TCP Vegas versus Different TCP Variants in Homogeneous and Heterogeneous Networks by Using Network Simulator 2*" International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 03, 2011.

[18] Md. Shohidul Islam, M.A Kashem, W.H Sadid, M. A Rahman, M.N Islam, S. Anam," *TCP Variants and Network Parameters: A Comprehensive Performance Analysis*" Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.

[19] R. Manoharan and E. Ilavarasan,"*Impact of Mobility on the Performance of Multicast Routing Protocol in MANET*" International Journal of Wireless & Mobile Networks (IJWMN), Vol.2,No.2,May 2010.

[20] 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 Vol. 2, No. 3, July, 2008, USA.