A QOS Parameter Analysis using TCP Variants under Abnormal Behavior of AODV for MANET Environment

Bimal Patel, Parth Shah

Abstract*: Mobile Ad-hoc networks dynamically form temporary network in infrastructure less manner with decentralized environment, scalable approach and communicate with neighbors through reactive and proactive routing protocol. Due to frequent topology changes, fluctuating link capacity and limited resources there is significant packet loss which may directly degrade QoS parameter. In this article denial of service attack like blackhole and grayhole behavior is considered as security threat and analyzed with reactive routing protocol AODV.Due to reliable nature and congestion control behavior of TCP variants like New Reno which continues under fast recovery until window gets deflated and Vegas which is based on queuing delay based mechanism is considered. QoS parameter can be improved under abnormal behavior using TCP variants is analyze with the help of NS-2 in mobile Adhoc environment.

Index Terms*: Mobile Adhoc Networks, AODV, Denial of Service, TCP Variants, QoS.

I. INTRODUCTION

Mobile Ad Hoc network can be established at any time and at any place without any planning or infrastructure when mobile node with wireless communication support come into radio range of other nodes. Nodes performs responsibility of host as well as router and forwards data to/from other nodes. Decentralized environment, scalability, flexibility and low cost makes MANET popular for many applications like battle-field, disaster management and social community networks [01]. However fluctuating link capacity, dynamic network topology and limited resources makes it highly challenging to perform efficient operations and routing [02], [03]. AODV (Adhoc On Demand Distance Vector) reactive routing protocol helps to achieve dual role. Wireless Adhoc networks due to its flexibility are usually susceptible to different security threats which may cause degradation to various QoS parameters.

In Section 2 reactive routing protocol is explained and security attacks like Blackhole attack and Grayhole attack is explained in Section 3 and Section 4. To analyze QoS parameter performance TCP New Reno packet loss probability based mechanism and TCP Vegas queuing delay based approach is considered in Section 5 and Section 6. Throughput analysis is considered using NS in Section 7 with conclusion and future enhancement in Section 8.

II. AD-HOC ON DEMAND DISTANCE VECTOR (AODV)

Reactive routing protocol which discovers routes only when it is required. It discovers routes using route discovery process.Fig.1 (a) shows how RREQ broadcast message is used while discovery and RREP unicast message is used for reply. AODV repairs link breakages and thus provides loop free routes with the help of RERR message which is shown in Fig. 1(b) and Fig. 1(c). AODV doesn't include or add any packet overhead if route is already available [04].

When any node sends a RREQ message, the intermediate node either sends Reply message if it is having a valid route or forward the request message to the destination node. The role of broadcast identifier and Source id is to detect if the node has achieved the copy of Request message or not.

It may happen that source node gets more than one reply message about the valid node, in that case, source node decides choosing the message with the most prior hop count. Each node stores the previous node number and broadcast identifier before sending the message to another node. To maintain the information of message received and send, AODV uses timer that detects about the timing of sent message and received message to and from a particular node. The link failure situation is handled by observing and sequentially determining ACK and BEACON message packet [05], [06].

III. BLACKHOLE ATTACK AND CLASSIFICATION

Denial of service attack where normal node behave in selfish manner by falsely claiming route available to destination and drop all packets intentionally. It achieves this by advertising itself having fresh and shortest route to destination before actual genuine node reply thus retaining data packet control for dropping purpose. To successfully carry out this process attacker/intruder must generate RREP destination sequence greater than destination node always. In Fig. 2 single node (node 3) acting as blackhole attack falsely claiming path available to destination node4 and eventually drops all packets and causing degradation to quality of service parameters. If more than one node act as blackhole in cooperative manner it will devastating effect to whole network [7]-[11].

Revised Manuscript Received on May 28, 2019.

Bimal Patel, Department of Information Technology,CHARUSAT,Changa,India.

Dr. Parth Shah, Department of Information Technology,CHARUASAT,Changa,India.

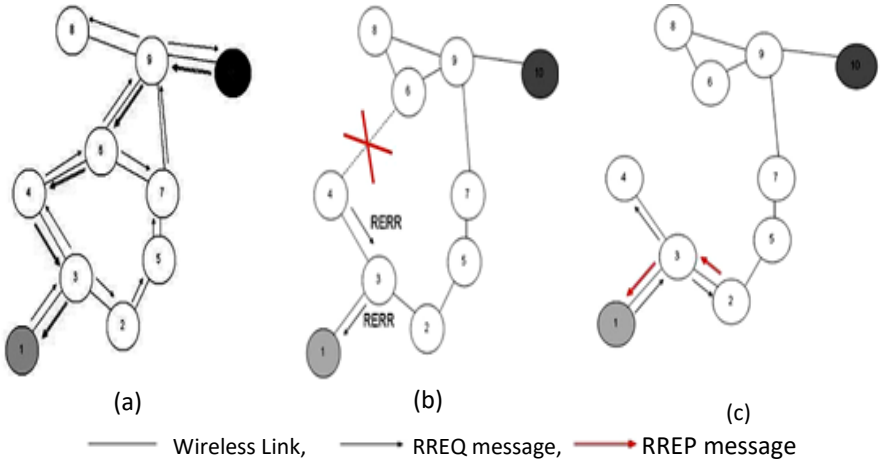

Fig. 1. Route Discovery Process

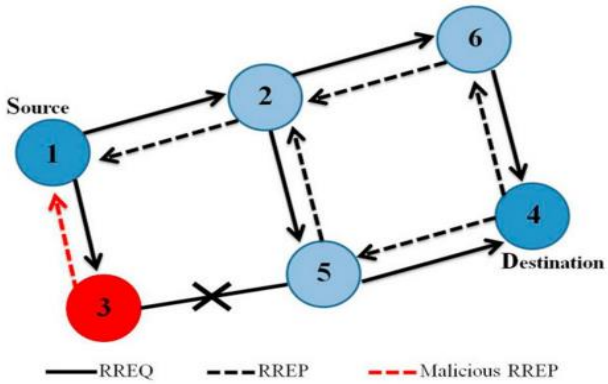

Fig. 2. Single Node Blackhole attack

IV. GRAY HOLE ATTACK

Grayhole attack works in two steps. In first step, selfish node acting as gray hole exploits AODV protocols and act as if it has valid direction to destination node with intention to intercept packets despite of having invalid path. In second step it may drop packets coming from source destined towards certain specific node(s) in the network. A gray hole may show its malicious behavior in different ways at different situation [12]. In another type it may show selfish/malicious behavior for some time by dropping packets and then act normally or as honest node as if nothing has hap-pen. This attack is more difficult to catch than other denial of service attack like black hole where in, it drops received packets for certain amount of time continuously. Due to selfish behavior it may degrade network performance and eventually QoS parameters is affected [13], [14].

V. TCP NEW RENO

TCP variants generally follows four phases as shown in Fig. 3 given below which are Slow Start, Congestion Avoidance, Fast Retransmit and Fast recovery with the help of addictive increase and multiplicative decrease mechanism on congestion window size(cwnd)[15],[16].

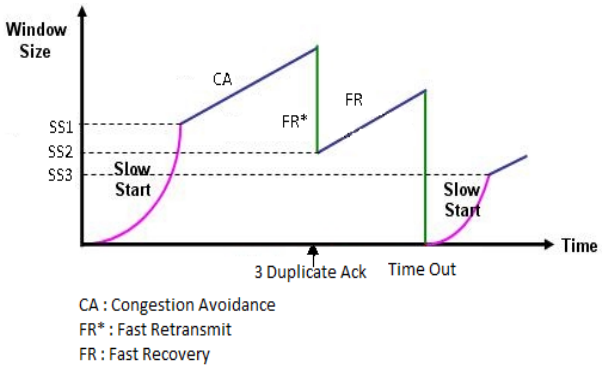

Fig. 3. TCP Congestion Controls techniques

New Reno works on packet loss probability based mechanism. Reno exit fast recovery when multiple packets are dropped but New Reno continues fast recovery mode for outstanding packets despite of partial acknowledgement is received [17]. After all outstanding packets are acknowledged it exit fast recovery reduces window size and then follow linear increase mechanism [18], [19].

VI. TCP VEGAS

TCP Vegas is queuing delay based variant which sets window size based on flow of data rates. As shown in Fig. 4 it depends on low and high threshold values (α and β). Based on difference between expected and actual it updates congestion window size (cwnd) [19], [20].

It updates window size based on following equations:

"diff. (Estimated backlog in queue) = (cwnd/Minimum Round trip time)-(cwnd/Actual round trip time)"

Using estimated backlog value window size is adjusted as follows:

$$\text{cwnd} + 1 \text{ if diff} < \alpha$$
$$\text{cwnd} - 1 \text{ if diff} > \beta$$
$$\text{cwnd} = \text{cwnd otherwise}$$

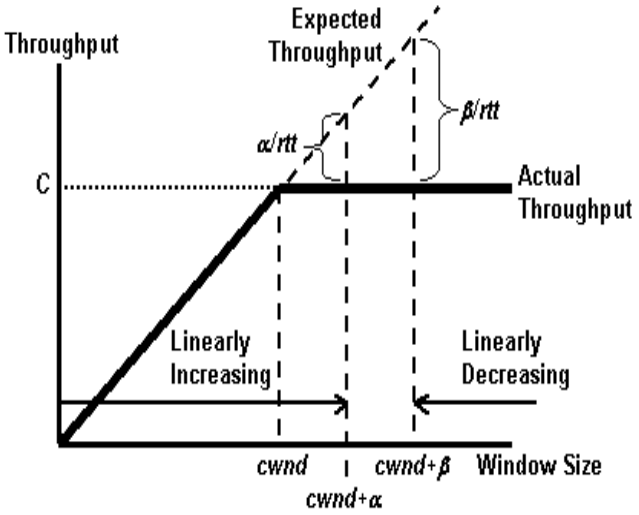

Fig. 2. TCP Vegas Congestion Avoidance

Table 1 shows the comparison of selected approach based on four technique of congestion control [21], [22].

Table 1. Comparison of Proposed Variants

Algorithm/TCP Variants	New Reno	Vegas
Slow Start	Yes	EV
Congestion Avoidance	Yes	EV
Fast Retransmit	Yes	Yes
Fast Recovery	EV	Yes
Retransmission	N	NM
Congestion Control	N	NM

N- Normal, E V-Enhanced Version, N M- New Mechanism

VII. Simulation Environment and Results

In order to analyze abnormal behavior adaptive TCP variants is consider i.e. Vegas and New Reno to improve QoS parameter. Since due to TCP traffic there is not much degradation of PDF and increase in NRL so only throughput parameter is considered under the abnormal behavior of Grayhole and Blackhole attack using NS2[23],[24]. The simulation is based on tcp traffic which is generated dynamically using cbrgen and setdest parameters.

- Traffic generated using cbrgen.tcl

ns cbrgen.tcl -type tcp -nn (10,30,50) -seed 0.0 -mc (8,15,35) -rate 4.0 > tcpfiles

- Node movement using setdest parameters

. /setdest -n (10,30,50) -p 2.0 -s 10.0 -M 40.0 -t (200) -x 500 -y 500 > nodefiles.

Case-1 (Grayhole attack with 1 grayhole nodes)

There is not much degradation in case of grayhole/blackhole attack so variable blackhole attack and grayhole attack with one grayhole attack is considered. The common simulation parameter is shown in Table 2.

Table 2. Simulation Parameters

Parameters	Values
No of nodes	10,30,50
Simulation Time	200
Packet Size	512
Environment Size	500*500
Routing Protocol	AODV,blackholeAODV,grayhole AODV,TCPVariants
Traffic type	tcp

Result analysis and comparison

The result comparison of one grayhole node is shown in Table 3

Table 3: Comparison of QoS parameters under fixed grayhole node

Avg. Throughput 1 Gray hole node (200 simulation time)				
No of Nodes	**AODV**	**Gray hole**	**New Reno**	**Vegas**
10(1)	401.67	355.84	362.58	377.69
30(1)	423.67	408	417.42	419.55
50(1)	390.14	377.63	382.60	388.21

By using tcp variants there is 3% to 7% improvement in case of throughput for fixed grayhole attack. The graph generated for throughput is shown in Fig. 5 and Fig. 6 using Xgraph facility. Red line in Fig. 5 indicate normal throughput for AODV while throughput gets degraded when denial of service gray hole attack is applied. TCP variants in form of New Reno and Vegas shown in yellow and green shows some improvement.

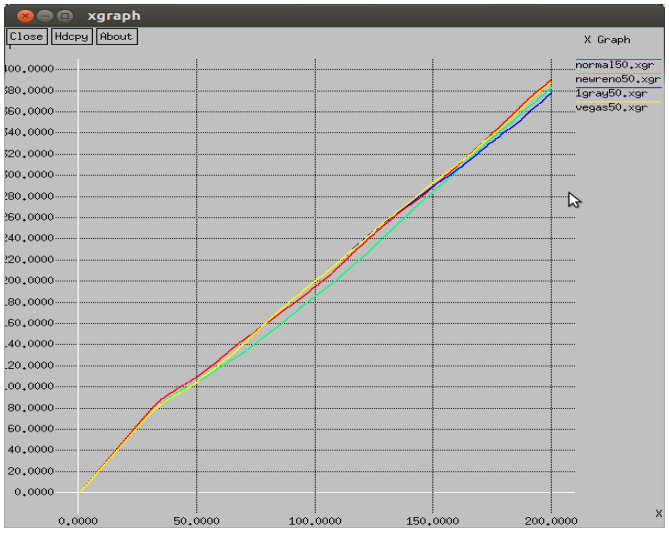

Fig. 5. Throughput for fixed grayhole nodes (50nodes, 1gray)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

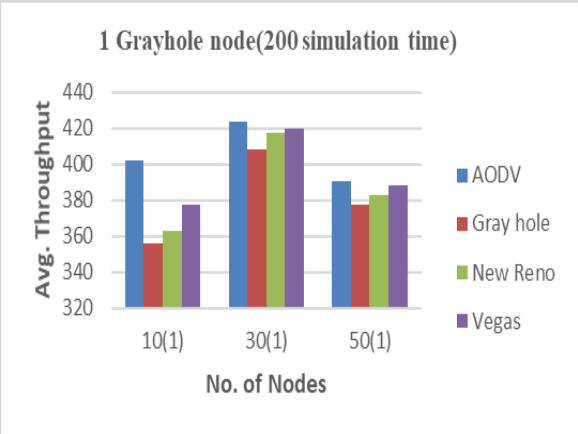

Fig. 6. Avg. Throughput for fixed Grayhole nodes (50nodes, 1gray)

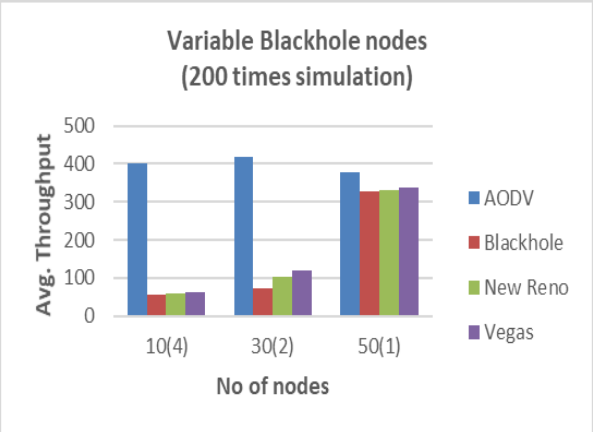

Fig. 8. Avg.Throughput for variable blackhole nodes

Case-2 (Variable Black Hole nodes)

The result comparison of variable blackhole nodes and its enhancement in form of throughput using tcp variants is shown in Table 4.

Table 4. Comparison of throughput under variable blackhole nodes

Avg. Throughput Variable Black hole nodes(200 simulation time)				
No of Nodes	**AODV**	**Blackhole**	**New Reno**	**Vegas**
10(4)	401.67	55.15	58.055	60.85
30(2)	417.32	71.17	103.79	117.88
50(1)	377.63	328.80	329.912	337.98

In case of variable blackhole attack there is 3% to 5% improvement in throughput using adaptive tcp variants. The graph generated for throughput is shown in Fig. 7 and Fig. 8 using Xgraph facility.

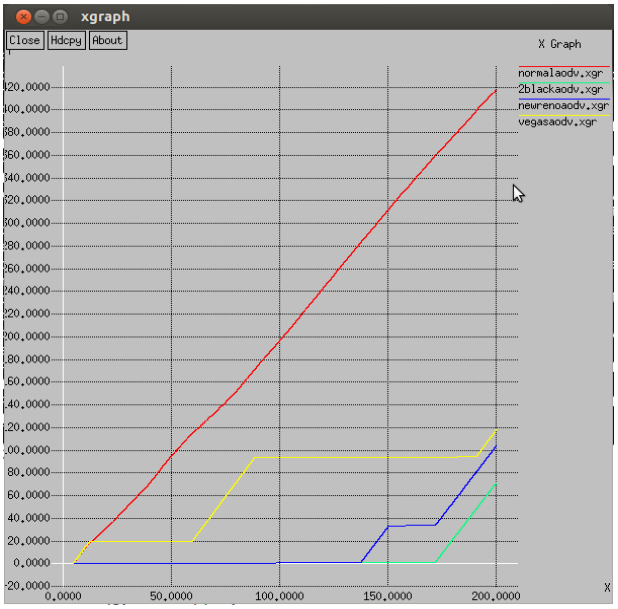

Fig. 7. Throughput for variable blackhole nodes (30nodes, 2black)

VIII. 8 CONCLUSION AND FUTURE ENHANCEMENT

Due to flexibility and decentralized environment securing MANET is one of the major concern. In this study, the performance of AODV under different abnormal behavior is tested i.e. under black hole attack and grayhole attack. By applying adaptive TCP Variants like New Reno and Vegas there is roughly 3% to 7% improvement of throughput under abnormal behavior of AODV.

As a future work other denial of service attacks like wormhole attack can be considered on AODV and performance can be analyzed with the help of other adaptive TCP variants like Tahoe, SACK and Westwood.

REFERENCES

1. Zhou H. A survey on routing protocols in MANETs. Department of Computer Science and Engineering, Michigan State University, East Lansing, MI. 2003 Mar 28:48824-1027.
2. L. Chen and W. Heinzelman, "A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks", IEEE Network, vol. 21, no. 6, pp. 30-38, 2007. Available: 10.1109/mnet.2007.4395108.
3. B. Patel, P. Shah, H. Jethva and N. Chavda, "Issues and Imperatives of Adhoc Networks", *International Journal of Computer Applications*, vol. 62, no. 13, pp. 16-21, 2013. Available: 10.5120/10139-4945.
4. E. Belding-Royer and C. Perkins, "Evolution and future directions of the ad hoc on-demand distance-vector routing protocol", *Ad Hoc Networks*, vol. 1, no. 1, pp. 125-150, 2003.
5. N. Bobade, "Performance Evaluation of AODV and DSR On-Demand Routing Protocols With Varying MANET Size", *International Journal of Wireless & Mobile Networks*, vol. 4, no. 1, pp. 183-196, 2012. Available: 10.5121/ijwmn.2012.4113.
6. S. Taneja and A. Kush, "A survey of routing protocols in mobile ad hoc networks", *International Journal of innovation, Management and technology*, vol. 1, no. 3, p. 279, 2010. [Accessed 14 May 2019].
7. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85-91, 2007. Available: 10.1109/mwc.2007.4396947.
8. D. Mishra, Y. Jain and S. Agrawal, "Behavior analysis of malicious node in the different routing algorithms in mobile ad hoc network (MANET)", *InAdvances in Computing, Control, & Telecommunication Technologies, 2009. ACT'09. International Conference on*, 2009, pp. 621-623.
9. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. 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. 338-46, 2007.

10. F. Tseng, L. Chou and H. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", *Human-centric Computing and Information Sciences*, vol. 1, no. 1, p. 4, 2011. Available: 10.1186/2192-1962-1-4.
11. B. Patel,V. Rathod,H. Jethva,N. Chavda,"Performance Comparison of normal and abnormal AODV under random traffic and node movement".
12. J. Sen, M. Chandra, S. Harihara, H. Reddy and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks", in *InInformation, Communications & Signal Processing, 2007 6th International Conference on*, 2007, pp. 1-5.
13. R. Jhaveri, S. Patel and D. Jinwala, "DoS attacks in mobile ad hoc networks: A survey", *InAdvanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, 2012, pp. 535-541.
14. U. Usha and B. Bose, "Comparing the impact of black hole and gray hole attacks in mobile adhoc networks", *Journal of Computer Science.*, vol. 8, no. 11, p. 1788, 2012.
15. H. Paul, A. Kumar Saha, P. Pratim Deb and P. Sarathi Bhattacharjee, "Comparative Analysis of Different TCP Variants in Mobile Ad-Hoc Network", *International Journal of Computer Applications*, vol. 52, no. 13, pp. 19-22, 2012. Available: 10.5120/8262-1802.
16. M. Islam Khan, "A Survey Of Tcp Reno, New Reno And Sack Over Mobile Ad-Hoc Network", *International Journal of Distributed and Parallel systems*, vol. 3, no. 1, pp. 49-63, 2012. Available: 10.5121/ijdps.2012.3104.
17. L. Grieco and S. Mascolo, "Performance evaluation and comparison of Westwood+, New Reno, and Vegas TCP congestion control", *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, p. 25, 2004. Available: 10.1145/997150.997155.
18. A. Gurtov, T. Henderson,S. Floyd,Y. Nishida,"The NewReno Modification to TCP's Fast Recovery Algorithm". RFC 6582, October; 2015 Oct.
19. B. Sardar and D. Saha, "A survey of tcp enhancements for last-hop wireless networks", *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 20-34, 2006. Available: 10.1109/comst.2006.253273.
20. L. Brakmo, S. O'Malley and L. Peterson, "TCP Vegas", *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 4, pp. 24-35, 1994. Available: 10.1145/190809.190317.
21. A. Al Hanbali, E. Altman and P. Nain, "A survey of TCP over ad hoc networks", *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3, pp. 22-36, 2005. Available: 10.1109/comst.2005.1610548.
22. S. Biradar, S. Sarkar and C. Puttamadappa, "A Comparison of the TCP Variants Performance over different Routing Protocols on Mobile Ad Hoc Networks", *International Journal on Computer Science and Engineering*, pp. 340-344, 2010.
23. E. Altman and T. Jiménez, "NS Simulator for Beginners", *Synthesis Lectures on Communication Networks*, vol. 5, no. 1, pp. 1-184, 2012. Available: 10.2200/s00397ed1v01y201112cnt010.
24. The Network Simulator-ns-2, http://www.isi.edu / nsnam/ns/index.html

AUTHORS PROFILE

Bimal Patel received B.E. in Information Technology from Charotar Institute of Technology Changa, Gujarat University, India, in 2000. He received M.Tech in Information Technology from prestigious L.D. College of Engineering, Ahmedabad, Gujarat Technological University in 2013 with gold medal. He has guided more than 3 students at master level and published more than 7 papers in Journal and International Conferences. His research interest include MANET, Wireless Sensor Networks and Internet of Things. Currently a Ph.D. student at Charotar University of Science and Technology, Changa, India.

Dr. Parth Shah has obtained Ph.D. in the area of Security in Cloud Computing from CHARUSAT, Changa, Gujarat. He has more than 14 years of teaching experience. Currently, he is working as Associate Professor at Department of Information & Technology, CHARUSAT, Changa, Gujarat. His research interest includes High-Performance Computer Architecture and Information Security. He has guided more than 30 ME/M Tech dissertation. He has published more than 40 papers in Journal and conference proceedings. Currently, he is head of IT department in CSPIT, CHARUSAT. He has received grants of 134900.00 from GUJCOST, MHRD, and CSI.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication