International Journal of Future Generation Communication and Networking
Vol.10, No.5 (2017), pp.49-58
http://dx.doi.org/10.14257/ijfgcn.2017.10.5.05

Analysis of TCP traffic under Blackhole Attack in MANETs

Nikita Malik[1], Prakash Rao Ragiri[1] and Rashmi Chaudhary[1]

[1]*Department of Computer Science, Ambedkar Institute of Advanced Communication Technologies and Research, GGSIPU*
New Delhi, India-110031
{nikitamalik92,prakashraoragiri,rashmii0525}@gmail.com

Abstract

Mobile Ad hoc Network (Manet) is a collection of self-configuring nodes which move around and communicate with each other without the use of wires or any existing infrastructure. Such a dynamic topology, lack of a central network management point and limited resources serve as challenges to the network opening up possibilities for launching several attacks in order to exploit the vulnerabilities. In this paper, blackhole attack (the network layer attack), has been simulated in the mobile ad hoc network over AODV routing protocol, and the effect of the reliable transport layer protocol TCP has been analyzed over such a network. A variant of the same, TCP Vegas has also been analyzed for the effects of the attack on such a network. Performance has been measured using metrics of average throughput, normalized routing load and end to end delay and conclusions have been drawn based on that.

Keywords*: Manet, AODV, TCP, Blackhole attack, ns2*

1. Introduction

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each node must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is to equip each device to continuously maintain the information required to properly route the traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain single or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. A mobile ad-hoc network (MANET) is an ad-hoc network but an ad-hoc network is not necessarily a MANET.

Transmission Control Protocol (TCP) is a reliable, connection-oriented end-to-end delivery protocol which operates at the transport layer of the network model. Traditionally designed for wired networks, TCP is used in wireless ad hoc networks as well. Apart from losses due to attacks at various layers of the network model, losses may occur in MANETs due to frequent link failure or channel errors because of mobile behavior of nodes in ad-hoc natured network. TCP may however interpret these as effects of congestion which leads to inappropriate reductions of the congestion window, and numerous delays and losses, which result in unnecessary throughput degradation for traditional TCP applications. This introduced variants such as TCP Vegas to be applied as transport layer protocols in wireless ad hoc networks.

1.1 Classification of Attacks in Manets

Attacks on networks can be classified as either internal or external or as passive or active. An internal attack refers to the attacker being involved as a part of the network,

ISSN: 2233-7857 IJFGCN

gaining access and participating in network activities to create trouble. An external attacker however, is not involved as a part of the network but tries to gain access to it in order to perform the attack. A passive attack mainly involves breaching the confidentiality of the network by means of eavesdropping, monitoring the network traffic and extracting productive information from that. An active attack, on the other hand includes activities that harm the functioning of the network. These are malicious activities such as deleting messages, injecting erroneous messages, impersonating a node *etc.* Attacks can also be categorized according to the layer of the Internet model that they target.

The active attacks, based on their occurrence on the network layer of the Internet model, can be categorized as shown in Table 1.

Table 1. Network Layer Attacks in Manets

Attacks	Characteristic Feature
Worm Hole Attack	Colluding nodes prevent data transfer to destined node by tunneling packets among themselves
Black Hole Attack Byzantine Attack Sybil Attack	Malicious node sends fake route reply to source and swallows all the packets
Sleep deprivation	Malicious node creates routing loops or forwarding of packets on non-optimal path and selective dropping
Routing Cache Poisoning	Attacker acts at several different identities/nodes in order to forge the result of voting in threshold security mechanisms
Packet Replication	Attacker broadcasts route request packets to notify nodes continuously and consume their limited resources
Rushing Attack	Attacker node broadcasts spoofed messages to a route through itself so that overhearing nodes add this route to their route caches
State Pollution Attack	Malicious node replicates stale packets and forwards them to other nodes in order to create confusion and use up their resources
Modification	Selfish node floods packets to all nodes in the network at a faster rate than any other node
Fabrication/ Masquerading	Malicious node provides incorrect response regarding requested parameters, obstructing entry of new nodes in the network

1.2 TCP Congestion Control

TCP is widely used in Internet today. TCP in Manets establishes links dynamically between mobile nodes through its handshake mechanism and provides more reliable packet delivery than UDP by starting a timer whenever a segment is sent, in order to ensure timely delivery of acknowledgements. Packet loss in network demands reaction from TCP to take action against congestion. Intertwined algorithms of slow start, congestion avoidance, fast retransmit and fast recovery are used by TCP to control the congestion window size according to round trip time (RTT) [8]. TCP Vegas introduces a

variant of TCP's congestion control mechanism wherein it proactively detects congestion before congestion occurs. By using packet delay (round trip time) as a primary feedback signal, it estimates the beginning of congestion. For the received acknowledgement, as shown in equations (1), (2), (3), the difference in expected and actual sending rate is calculated and based on two thresholds values α and β, the congestion window size is linearly varied. In case of multiple repetitive acknowledgements, the congestion window (cwnd) is reduced in size to adjust to the anticipated congested scenario. The TCP Vegas congestion window mechanism is represented through a flow chart in Figure 2, which can be compared to the conventional TCP congestion mechanism as shown in Figure 1.

$$\text{Expected} = \text{Window size}/\text{Base RTT} \quad (1)$$

$$\text{Actual} = \text{Window size}/\text{Current RTT} \quad (2)$$

$$\text{Difference} = \text{Expected} - \text{Actual} \quad (3)$$

TCP Vegas has been proved to successfully perform better in networks affected by congestion.

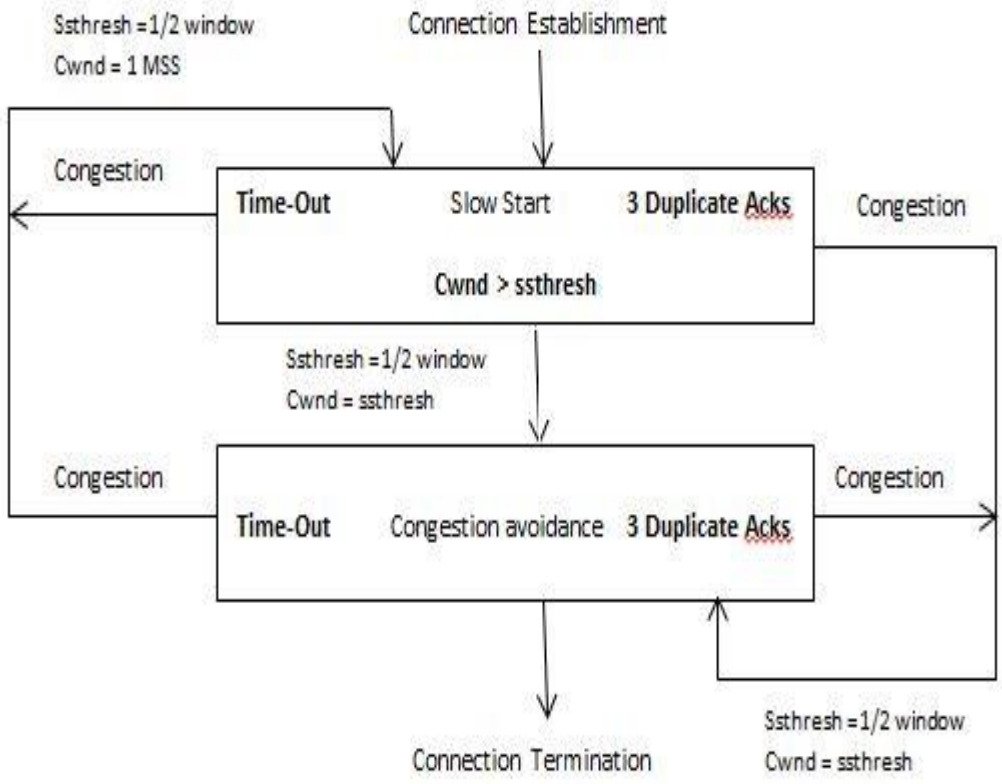

Figure 1. Conventional TCP Congestion Mechanism

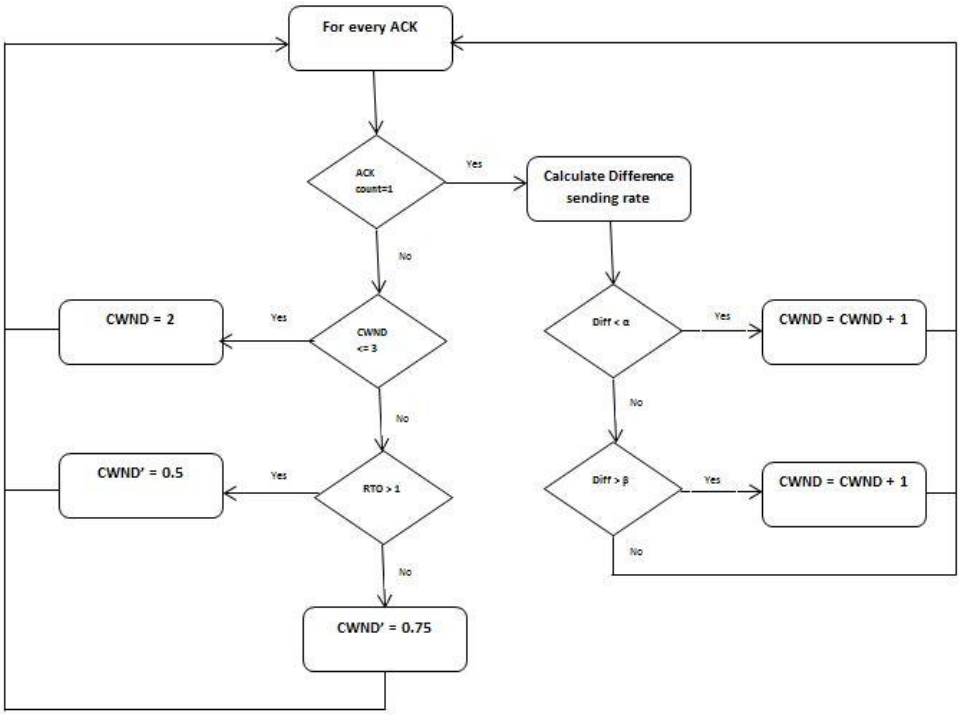

Figure 2. TCP Vegas Congestion Scheme

1.3 TCP in Ad Hoc Wireless Networks

TCP faces degradation in wireless ad hoc networks due to various reasons:

- Misinterpretation of Packet Loss- The loss of packets in network due to factors such as high bit error rate in wireless channel, collisions due to hidden terminals, location dependent contentions or inherent fading properties of the wireless channel may be wrongly attributed to congestion and congestion control algorithm is applied.
- Frequent Path Breaks- Changing topology leading to frequent changes in connectivity cause routes to be broken and established time and again, which is time consuming.
- Effect of Path Length- The possibility of a path break increases with increase in path length, leading to degradation of throughput.
- Asymmetric Link Behavior- Successful delivery of a packet but failure to receive acknowledgement may lead to a link becoming unidirectional, which can lead to invoking of congestion control and multiple retransmissions.
- Multipath Routing- Existence of multiple routes between two nodes can result in out of order packets and generate a set of acknowledgements which causes additional power consumption and invocation of congestion control.

2. Theoretical Background

2.1 Related Work

A range of attacks possible on Manets and Blackhole attack in particular are investigated in detail in [7] and [10]. The blackhole attack process and its prevention and detection methods to provide a secure network are discussed too.

TCP traffic load in Manets and its performance as compared to UDP and other TCP variants is analyzed to determine how the transport layer protocol affects various performance metrics when implemented on different routing protocols [2], [5], [13].

[1], [3], [4], [6], [9], [11] demonstrate implementations of malicious nodes in AODV routing protocol in wireless mobile ad hoc environments and analyze the effects on network performance through various metrics.

2.2 Overview of AODV Protocol

Depending on the process of route discovery in Manets, routing protocols may be classified as proactive (table-driven), reactive (on-demand) or hybrid. In proactive routing protocols, each node maintains a routing table for routes to every other node, which is periodically updated. Contrasting to this, the ad hoc routing protocols take a lazier approach and create routes only when needed. The hybrid approach combines the features of both these routing protocols.

Ad hoc on-demand distance vector routing (AODV) is a reactive routing protocol. It is capable of both unicast and multicast routing. When a node wants to establish a connection with other node(s), it does so by broadcasting a request for connection. When a node has data to send, it checks its routing table for a path to the destination node, and on finding an inactivated route or no route, starts with the route discovery process where it broadcasts a RREQ packet to all its neighbors, as represented in Figure3. These nodes then check whether the packet is destined for them, and if not, check their respective tables for an entry of the route for the destination and record the broadcast id and previous node from which the request came, in order to avoid receiving duplicate requests. The neighbors then further broadcast the RREQ to their neighbors recurrently until it reaches the actual destination or the node which has a link to the destination. The destination node generates a RREP packet, which is unicasted along the reverse RREQ path, which is why symmetric links are assumed in AODV. The intermediate nodes, on receiving and forwarding the RREP, keep the broadcast identifier and previous node from which the reply came and update their routing tables. Based on a timer, the nodes, which are not receiving the reply, drop the request packet information. On receiving multiple RREP, the source establishes the route considering the RREP with the hop count value as minimum, and the destination sequence number highest, implying recent channel information. RERR is generated and forwarded to the source whenever a link in the route is broken, making the destination unreachable. The source then again begins with the route discovery process, which is followed by route establishment and route maintenance procedures.

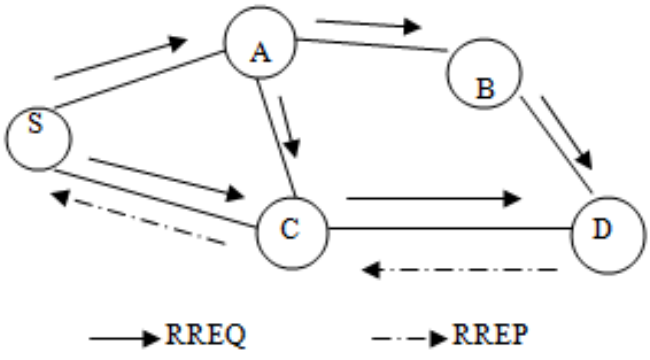

Figure 3. Route Discovery in AODV

2.3 Overview of Blackhole Attack

Blackhole attack is a kind of denial of service (DoS) attack that targets the network layer of the OSI network model. There are two properties of this attack- the malicious

node exploits ad hoc routing protocol such as AODV to advertise itself as having a valid route to the destination node, even though the route is spurious; and the intercepted packets are consumed by the blackhole node.

When the source broadcasts a RREQ packet during route discovery process, the malicious node immediately sends a positive reply RREP packet falsely claiming a path to the destination and advertising the highest destination sequence value and lowest hop count. The source node assumes this to be the shortest valid path to the destination and sends packets along this route. The malicious node acts like a 'blackhole', absorbing all the packets without forwarding them to the intended destination. Figure 4 shows a six node network under blackhole attack [12].

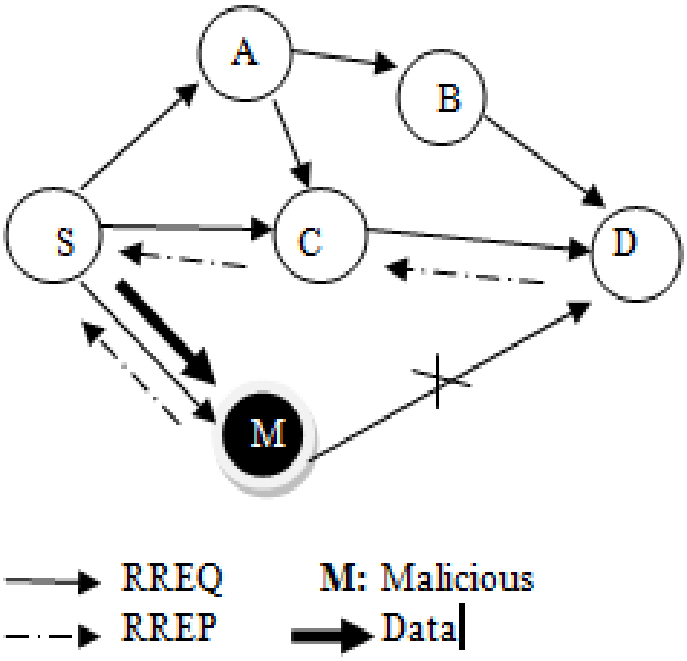

Figure 4. Blackhole Attack in AODV

Algorithm:

Let Bi denote a malicious black hole node
and SN1…SNn be the nodes in the network
Each SNi broadcasts messages and receives messages
Begin route discovery process
SNi broadcasts a RREQ message to neighbors
For every SNi to SNn
If Bi receives RREQ message
Bi responds to SNi with high dest_seq value
SNi chooses Bi as part of route and sends the data packet
Bi drops the data packet
End

3. Simulation

Network simulator version 2.35, a discrete event simulator for wireless network system, has been used to carry out the simulation and evaluate various scenarios. The simulation network consists of mobile nodes varying from 50 to 100, placed randomly

within a 1000m x 1000m area and simulated for 100 seconds. Each node has a transmission range of 250m and moves at a maximum speed of 2 m/s. Data packet size is 512 bytes each and the channel capacity is 2 Mbps over TCP protocol. For analysis of the performance under the presence of malicious node, 20 blackhole nodes have been introduced in the modified AODV protocol called BlackholeAODV, which is tested with TCP and TCP Vegas traffic.

The mobility model chosen for the network is the random way-point model wherein a mobile node begins by choosing a random destination in the simulation area and then travels towards the newly chosen destination with a random speed less than 2m/s. On arrival, the mobile nodes start the process again. Table 2 lists the values of the common parameters used in the simulation environment.

Table 2. Simulation Parameters

Parameter	Value
Routing Protocols	AODV, BlackholeAODV
No. of nodes in network	50,60,70,80,90,100
No. of malicious nodes	20
Size of packet	512 bytes
Simulation time	100 s
Simulation area	1000*1000 m
Max. speed of nodes	2 m/s
Platform	Ubuntu 14.01
MAC	802.11
Channel	Wireless
Propagation	Two ray Ground
Data rate	2 mbps
Traffic connection	TCP, TCP Vegas
Mobility model	Random way point

4. Results Analysis

The metrics used for measuring the performance are:

- Throughput- defined as the average rate of successful packet delivery per unit time over a communication channel. It is calculated as the number of packets received at the receiver node upon the time taken for transmission.
- End to End Delay- defined as the time a packet takes to travel from the source node to the destination node. It is calculated as the average to the end to end delays taken over all the received packets.
- Normalized Routing Load- defined as the ratio of total number of routing packets received to the total number of data packets received.

Figure 5 compares the average throughput in kbps that is achieved when TCP traffic runs in an AODV based network with varying number of nodes, and when blackhole nodes are introduced in the network. The effect of malicious nodes is evident as the throughput value falls significantly. Applying TCP Vegas instead of TCP in case of BlackholeAODV shows that there is very slight difference in the achieved throughput and that TCP Vegas does not outperform traditional TCP in presence of malicious nodes in the network.

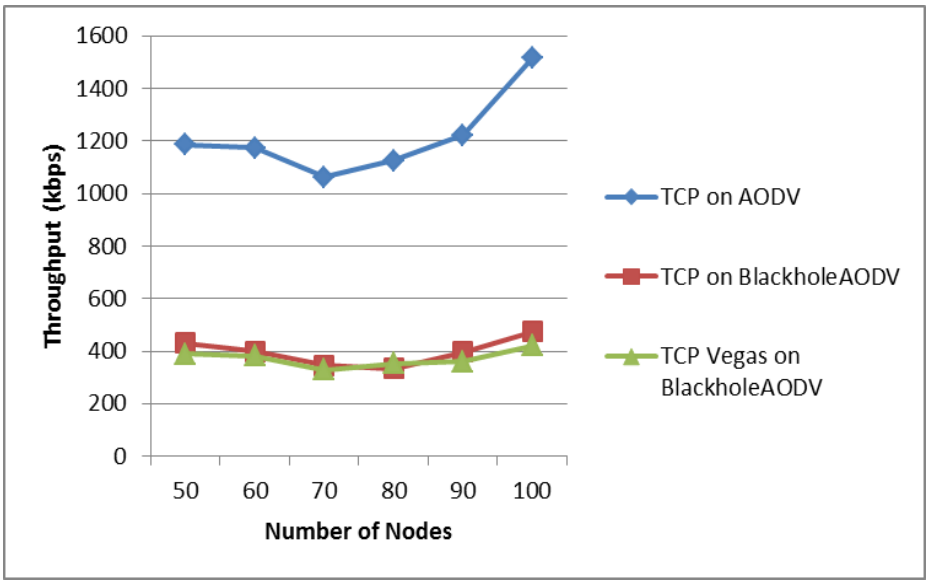

Figure 5. Graph Plot of Throughput Value in Kbps versus Number of Nodes in the Network Under TCP Traffic on AODV, TCP on Blackholeaodv and TCP Vegas on Blackholeaodv

Figure 6 shows how the presence of malicious nodes increases the flow of routing packets in the network as compared to normal AODV. BlackholeAODV observes higher normalized routing load over TCP Vegas than TCP since attempts to improve packet losses in networks with malicious nodes cause a high number of packets to be control packets in the total data packets transmitted.

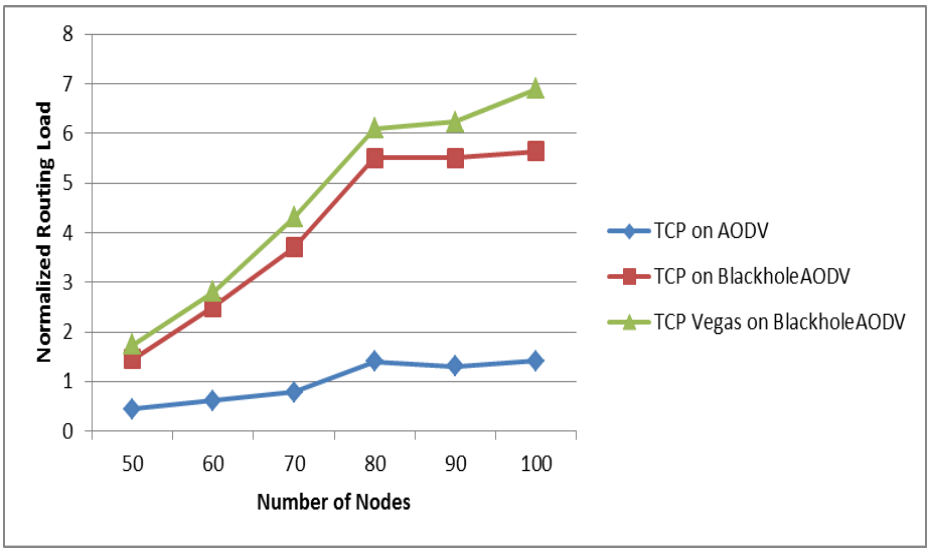

Figure 6. Graph Plot of Normalized Routing Load Value versus Number of Nodes in the Network Under TCP Traffic on AODV, TCP on Blackholeaodv and TCP Vegas on Blackholeaodv

Figure 7 represents end to end delay values as observed in AODV and BlackholeAODV under TCP and TCP Vegas. The time delays for TCP packets to be transmitted are higher in presence of malicious nodes because of introduced losses and need for alternate route discovery. TCP Vegas further introduces delays due to invoking of congestion controls.

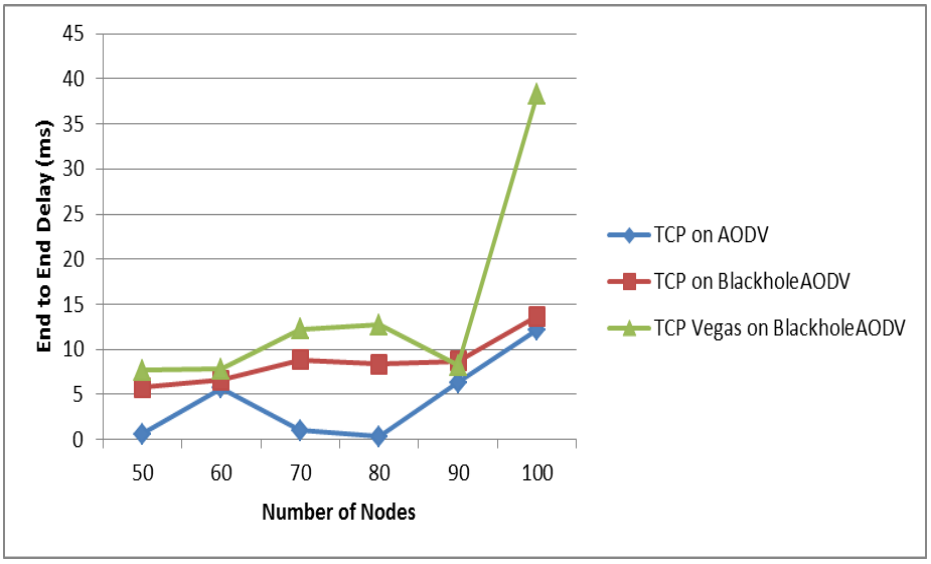

Figure 7. Graph Plot of End to End Delay Value in Ms versus Number of Nodes in the Network Under TCP Traffic on AODV, TCP on Blackholeaodv and TCP Vegas on Blackholeaodv

5. Conclusion

The paper firstly discusses Manets and how TCP works in case of such ad hoc wireless networks. It investigates in detail the working of AODV routing protocol and Blackhole attack and through related works understands the effect of malicious node behavior on AODV based mobile ad hoc networks. A BlackholeAODV protocol has been simulated for analyzing the effects through a set of parameters. Results indicate the performance of TCP and TCP Vegas under AODV and BlackholeAODV in terms of average throughput, end to end delay and normalized routing load. With increase in number of nodes, the throughput value achieved falls significantly for TCP, and further for TCP Vegas in blackhole AODV. The normalized routing load and end to end delay however increase considerably with blackhole attack on TCP. TCP Vegas also fails to improve performance when network is under blackhole attack as the end to end delay and normalized routing load are higher.

References

[1] Bala, Anu, Munish Bansal, and Jagpreet Singh. "Performance analysis of MANET under blackhole attack." Networks and Communications, 2009. NETCOM'09. First International Conference on. IEEE, 2009.

[2] Gopinath, T., AS Rathan Kumar, and Rinki Sharma. "Performance evaluation of TCP and UDP over wireless ad-hoc networks with varying traffic loads." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013.Jeni, PR Jasmine, "Performance analysis of DOA and AODV routing protocols with black hole attack in MANET." Smart Structures and Systems (ICSSS), 2013 IEEE International Conference on. IEEE, 2013.

[3] Khin, Ei Ei, and Thandar Phyu. "Impact of black hole attack on AODV routing protocol." International Journal of Information Technology, Modeling and Computing (IJITMC) Vol 2 (2014).

[4] Kim, Dongkyun, "Analysis of the interaction between TCP variants and routing protocols in MANETs." 2005 International Conference on Parallel Processing Workshops (ICPPW'05). IEEE, 2005.

[5] Kumar, Sushil, Deepak Singh Rana, and Sushil Chandra Dimri. "Analysis and Implementation of AODV Routing Protocol against Black Hole Attack in MANET." International Journal of Computer Applications 124.1 (2015).

[6] Mandala, Satria, "A review of blackhole attack in mobile adhoc network." Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2013 3rd International Conference on. IEEE, 2013.

[7] Meher, Pratap K., and P. J. Kulkarni. "Analysis and Comparison of Performance of TCP-Vegas in MANET." Communication Systems and Network Technologies (CSNT), 2011 International Conference on. IEEE, 2011.
[8] Parmar, Martin K., and Harikrishna B. Jethva. "Analyse impact of malicious behaviour of AODV under performance parameters." Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on. IEEE, 2014.
[9] Puray, Minoti, and Priyanka Palod. "Black-Hole Attack in MANET: A Study." International Journal of Advanced Research in Computer Engineering and Technology 5.3 (2016)
[10] Raja, L., and Dr S. Santhosh Baboo. "Analysis of Blackhole attacks on AODV Routing Protocol in MANET." (2012): 1522-1526.
[11] G.S. Tomar, "Modified Routing Algorithm for AODV in Constrained Conditions", IEEE International Conference AMS 2008, pp-6, May 2008.
[12] Rao, PV Venkateswara, and S. Pallam Setty. "Investigating the Impact of Black Hole Attack on AODV Routing Protocol in MANETS under Responsive and Non-Responsive Traffic." International Journal of Computer Applications 120.22 (2015)
[13] Zaman, Anum, and Sameer Qazi. "On the impact of Transport Layer mechanisms on routing protocols in MANETS", 2013 IEEE Malaysia International Conference on Communications (MICC), 2013.
[14] G.S. Tomar, Manish Dixit & Shekhar Verma, "AODV Routing Protocol With Selective Flooding", IEEE SOCPAR 2009, pp 682-686, 2009.

