ISSN: 0975-766X
CODEN: IJPTFI
Available Online through **Research Article**
www.ijptonline.com

PERFORMANCE ANALYSIS OF MOBILE AD-HOC NETWORKS WITH MALICIOUS NODES IN VARIOUS MOBILITY SCENARIOS

K. Padma Monika[1], M. Sujatha[2]
Student, Dept of ECE, Saveetha School of Engineering, Chennai, India.
Assistant Professor, Dept of ECE, Saveetha School of Engineering, Chennai, India.

Received on: 25.09.2016 *Accepted on: 15.10.2016*

Abstract:

An Ad-hoc system is a gathering of hubs which includes transmission of information without a central hub. Ad-hoc networks are the specially appointed systems which can convey with no settled base. The steering conventional routing for this ad-hoc networks is given by AODV protocol(ad-hoc on-demand distance vector). The fundamental risk included in MANET(mobile ad-hoc networks) is that the impact of black hole attack. Once in a while this assault might likewise emerge because of the varieties in AODV convention. There is an expanding danger of attacks on the Mobile Ad-hoc Networks (MANET). The hubs are helpless against different sorts of attacks because of their portability. Black hole attack is one of the security risk in which the activity is diverted to such a hub, to the point that really does not exist in the system. In this attack a traded off hub promotes itself to have a most brief way to send information to destination. In this paper we simulate executive analysis of MANET with dynamic mobility and blackhole attack.

Keywords: MANET, blackhole, AODV.

I. Introduction

A mobile ad-hoc network could be a self-configuring infrastructure less network of mobile devices connected by wireless links. Ad-hoc is Latin and suggests that for this purpose. Every gadget in associate in passing MANET is liberal to move in any direction, and might so modification its links to different devices usually. Each ought to forward traffic unrelated to its own use, then be a router. The primary challenge in building a MANET is mobilization each device to incessantly maintain the data required to properly route traffic. Such internetworks would possibly operate by themselves or may even be connected to the larger net.

Blackhole attack is a sort of attack in which a router that should hand-off bundles of information rather disposes of them. This typically happens from a router getting to be traded off from various distinctive causes. Because bundles are routinely dropped from a lossy system, the blackhole attack is difficult to identify and avert.

The noxious router can likewise fulfill this attack specifically, e.g. by dropping bundles for a specific system destination, at a specific time, a parcel each n parcels or each t seconds, or an arbitrarily chose part of the bundles. On the off chance that the malignant router endeavours to drop all bundles that come in, the attack can really be found decently fast through basic systems administration devices. Likewise, when different hubs notice that the malignant hub is dropping all movement, they will by and large start to expel that hub from their sending tables and in the long run no activity will stream to the attack. In any case, if the pernicious switch starts dropping bundles on a particular time period or over each n parcels, it is regularly harder to recognize on the grounds that some movement still streams over the network.

The blackhole attack can be as often as possible sent to attack remote ad-hoc systems. Since remote systems have a very different engineering than that of a run of the mill wired system, a host can show that it has the briefest way towards a destination.

By doing this, all movement will be coordinated to the host that has been bargained, and the host can drop parcels at will. Also over portable specially appointed system, hosts are particularly helpless against shared attacks where various hosts will get to be traded off and misdirect alternate hosts on the network.

II. Related Works

Blackhole attack are one in all the kinds of attacks that are conceivable on MANET. The black hole create MANETS helpless as they can journey to increase delicate data from MANET [2].

MANETs frequently expertise the sick effects of security attacks as a results of its parts like open medium, dynamical its topology increasingly, absence of focal perceptive and administration, agreeable calculations and no clear barrier part. These parts have modification the front line circumstance for the MANETs against the security dangers [3].

III. Route Discovery Process in Manet

Amid the Route Discovery process, the source hub sends RREQ parcels to the middle of the road hubs to discover crisp way to the planned destination. Noxious hubs react instantly to the source hub as these hubs don't allude the directing table. The source hub expect that the course disclosure procedure is finished, disregards other RREP messages from different hubs and chooses the way through the vindictive hub to course the information bundles. The hub now drops the got messages as opposed to transferring them as the convention requires. In AODV, the arrangement number is utilized to decide the freshness of directing data contained in the message from the beginning hub. While creating RREP message, a destination hub thinks about its current grouping number, and the arrangement number in the RREQ parcel in addition to one, and after that chooses the bigger one as RREPs grouping number. After accepting various RREP, the source hub chooses the one with most noteworthy grouping number so as to develop a course. Yet, in the incite of blackhole when a source hub telecasts the RREQ message for any destination, the blackhole hub quickly reacts with a RREP message that incorporates the most noteworthy succession number and this message is seen as though it is originating from the destination or from a hub which has a sufficiently new course to the destination.

The source accept that the destination is behind the dark gap and disposes of the other RREP bundles originating from alternate hubs. The source then begins to convey its bundles to the blackhole hub assuming that these parcels will achieve the destination.

Therefore, the malignant hub will draw in every one of the bundles from the source and as opposed to sending those parcels to the destination it will essentially dispose of those. In this manner the parcels pulled in by the blackhole hub won't achieve the destination.

IV. Proposed Methodology

- MANETs are simulated with varying number of nodes (15, 25, 50).
- The performance of simulated networks is analysed.
- MANETs with blackhole nodes are simulated.
- Number of blackhole nodes in each network is varied so as to analyse the performance of MANET in various blackhole densities.
- The speeds of the mobile nodes are varied and the performance for each case is analysed.
- A comparative study of MANETs in varying mobility scenarios in the presence and absence of blackhole nodes is carried out.

V. Results & Discussion

This section presents the performance analysis of MANETS with multiple speed with varying blackhole densities and network sizes. The performance summary of MANETs with mobile nodes having various speeds are done and the simulated results are represented graphically. The number of nodes versus throughput percent is represented in the Figure1.

The X-axis denotes the number of blackhole nodes in the given network and Y-axis represents the performance of the network in percentage throughput. It is observed that when in the absence of blackhole node and one blackhole present, the throughput is same. This implies that lesser the blackhole, poorer is its impact on the network performance. However, as the number of blackhole node increase, the diminishment the throughput percent can be observed.

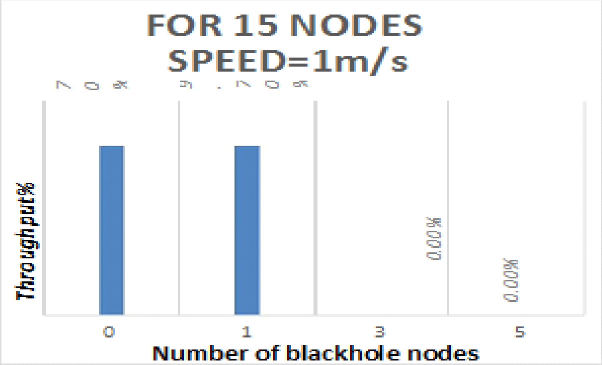

Figure1

This effect is proved in the figures of 2 and 3.

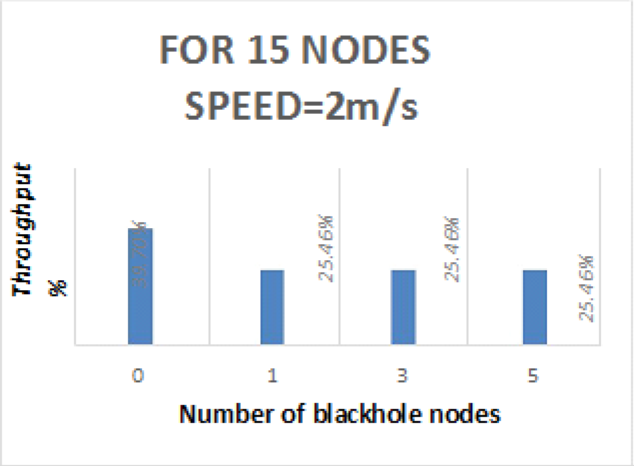

Figure2

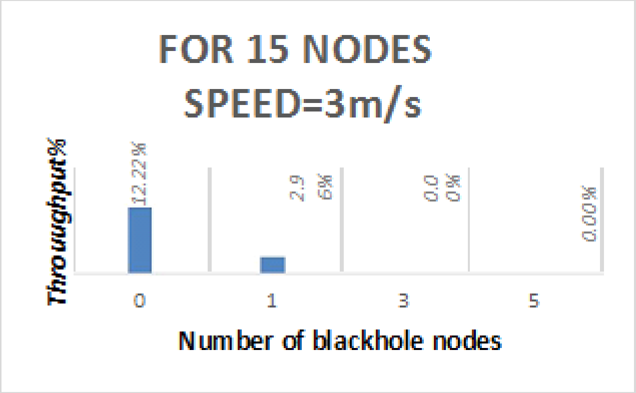

Figure3

Average of throughputs for 15 nodes:

The average of throughputs of 15 nodes taken at three varying speeds is plotted with speed on x-axis and average of throughput on y-axis. The plot is given in Figure4. It can be noted from figure4 that when the nodes move faster in a 15 node network, the throughput is greatly reduced. This is because MANETs depend on multihop for successful communication. As the nodes are moving faster, less nodes take path in communication, which impacts the performance of the network.

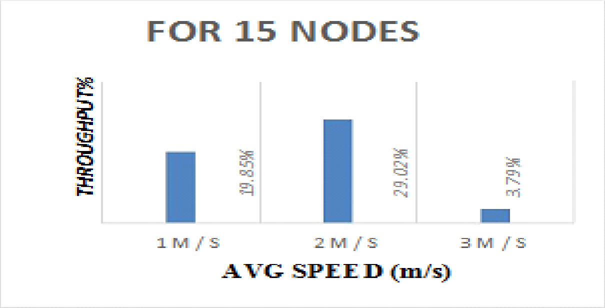

Figure4

For 25 nodes:

The degradation in the network performance in forms of throughput , for 25 nodes is shown in figures5,6 and 7. In all the plots, it can be seen that the successful transmissions are decreased, as the number of blakhole nodes increases.

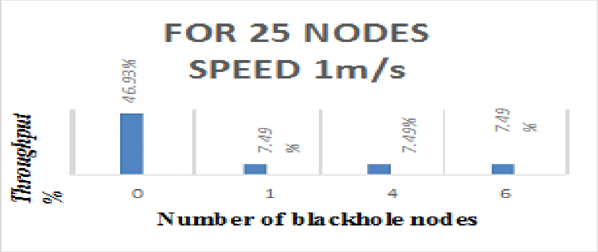

Figure 5

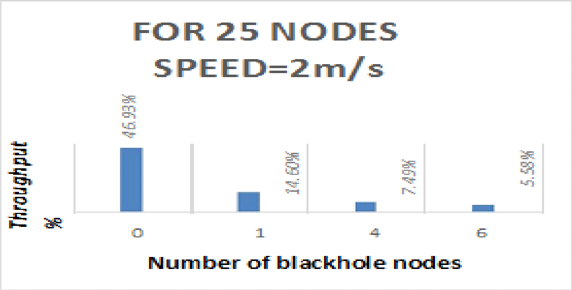

Figure6

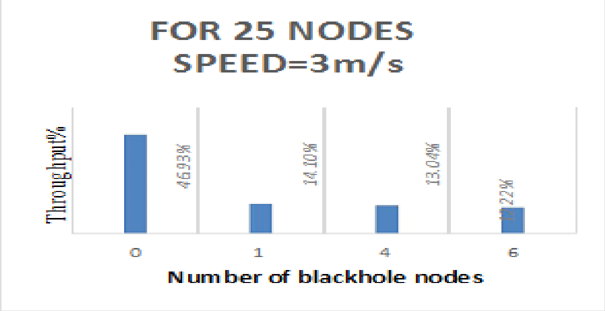

Figure7

Average of throughputs for 25 nodes

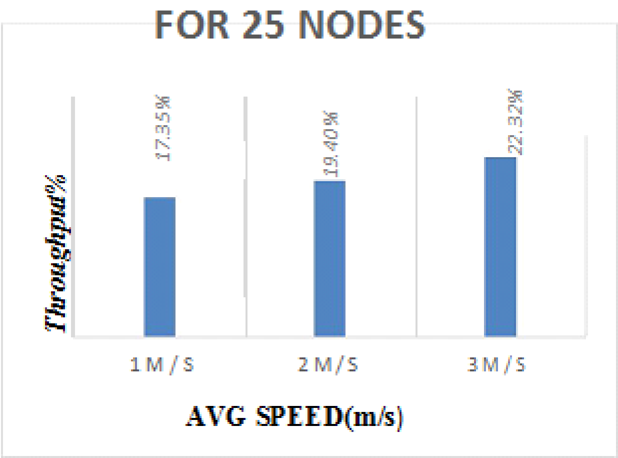

Figure8

From Figure8, it has been analysed that even when the speed increases, the throughput is more. This is because when there is more number of nodes the communication will not be affected though the speed is increased.

VI. Conclusion and Futurework

In this paper, we examined a particular sorts of assault, known as blackhole attack, made on MANET. The simulation carried out using 15 and 25 nodes MANETS show that the performance of the network is affected by the presence of blackhole nodes. This is more so when the number of blackhole nodes increases. This paper also monitored the effect of node mobility on the network performance. The simulation results for three different speeds of mobile nodes prove that, when the network size is smaller, the node mobility has greater impact. When the network size grows, the effect of node mobility is not pronounced much. In future, larger networks with varying blackhole node densities and traffic intensities will be simulated and the performance comparison will be carried out.

VII. References

1. V.S.Chaudhari, Professor P.N.Matte, Professor V.P.Bhope, “Simulation and Performance Analysis of Mobile Ad-hoc Network Routing Protocol”, International Journal of Advanced Research in Computer Engineering and Technology IJARCET Volume 4 Issue 4, April 2015.
2. Marpu Devadasi, K. Vinay Kumar, “Protoceting Mobile Ad-hoc Networks from Blackhole Attacks”, Mobile Computing IJCSMC, Vol. 3, Issue. 12, December 2014.
3. IrshadUllah and Shahzad, “Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.
4. Irshad Ullah,, Shoaib Ur Rehman , “Analysis of Black Hole Attack on MANETs Using Different MANET

Routing Protocols" , Thesis no: MEE 10:62 June, 2010.

5. Roy B., Banik S., Dey P., Sanyal S and Chaki N, "Ant Colony Based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services", JETCIS, Vol. No 3, Issue No. 1, January 2012.
6. P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
7. K.Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology Sweden, 22nd March 2007.
8. VydekiDharmar, Ayisha Razeena Parveen,M.A., Bhuvaneswaran.R.S. "Blackhole reduction in Ad-hoc networks using neural networks", Journal of innovation in computer science and engineering, Vol.2(1), pp 29-33, 2012.