ISSN: 0976-3031

International Journal of Recent Scientific Research

Impact factor: 5.114

ANALYSIS OF EFFECTS OF NODE DENSITY VARIATIONS ON A WSN WITH RESPECT TO BLACKHOLE ATTACK

Nitin Kumar and Shagun Chaudhary

Volume: 6 Issue: 10

THE PUBLICATION OF
INTERNATIONAL JOURNAL OF RECENT SCIENTIFIC RESEARCH
http://www.recentscientific.com
E-mail: recentscientific@gmail.com

ISSN: 0976-3031

Available Online at http://www.recentscientific.com

International Journal of Recent Scientific Research
Vol. 6, Issue, 10, pp. 7003-7005, October, 2015

International Journal of Recent Scientific Research

RESEARCH ARTICLE

ANALYSIS OF EFFECTS OF NODE DENSITY VARIATIONS ON A WSN WITH RESPECT TO BLACKHOLE ATTACK

Nitin Kumar and Shagun Chaudhary

Department of Electronics & Communication Engineering, JIET-SETG, Jodhpur

ARTICLE INFO

Article History:

Received 05thJuly, 2015
Received in revised form 08thAugust, 2015
Accepted 10th September, 2015
Published online 28st October, 2015

Key words:

Performance parameters, End to end delay, Throughput, Overhead, NS-2, Node density, Packet drop

ABSTRACT

Wireless Sensor Networks have found a large number of applications in very short time due to the possibility of diverse applications ranging from everyday use to specialized fields. These networks are playing important role in the dream of ubiquitous or pervasive computing. But due to increasing complexity of tasks to be performed, the network architecture of these networks are also becoming complex at a rapid pace. This complexity is generally in terms of increased number of nodes i.e. node density. The behavior of networks changes with changing node density and therefore the WSN characteristics has to be studied carefully under varying node density.

INTRODUCTION

Wireless sensor networks are playing an important role in large number of application due to their diverse nature. This diversity arises from various physical and virtual topologies, different data acquisition methods, varied physical shapes and sizes and different data communication protocols.

Each network is suited for specific type of work but the overall goal remains the same to provide flexible wireless network with multiple application. The nature and range of a WSN depends on the number of nodes it's made up of. The network and hence the nodes can be static or dynamic. As the number of nodes increases, the behavior of the network changes in terms of certain parameters. Thus it's essential to study and predict the network parameters which define the network performance with varying node density.

Black hole Attack [1][2][3][4][5][10]

Due to their open nature of distribution and operation, Wireless Sensor Networks are susceptible to different types of network attacks. Some attacks are non-invasive while others diminish the network efficiency by restricting or destroying critical network resources [6][7][8][9]. Black hole attack is one such attack that interferes with the normal working of network by increasing packet drop.

A malicious black hole node attracts all the traffic in its proximity and drops the packets.

This results in large number of retransmissions leading to increased network overhead and reduced available bandwidth for actual communication. This effect magnifies with increasing number of nodes affecting all the network performance parameters.

Simulation Model

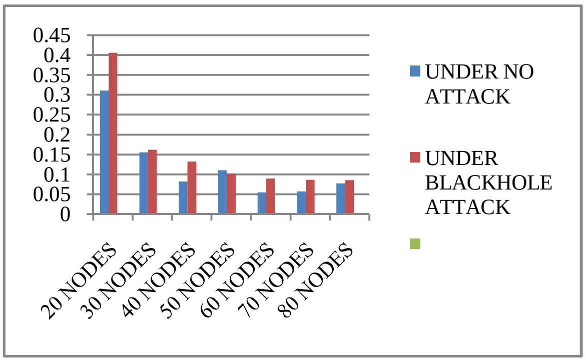
The following simulation model was used for simulating black hole attack on a WSN-

Simulator	NS2 (version 2.35)
Simulation Time	200 (s)
Number of Nodes	80
Simulation Range	1000 m^2
Routing Protocol	AODV
Traffic	CBR
Pause Time	10 m/s
Max Speed	20 m/s
Operating system	Ubuntu-12.04 LTS

Corresponding author:* **Nitin Kumar
Department of Electronics & Communication Engineering, JIET-SETG, Jodhpur

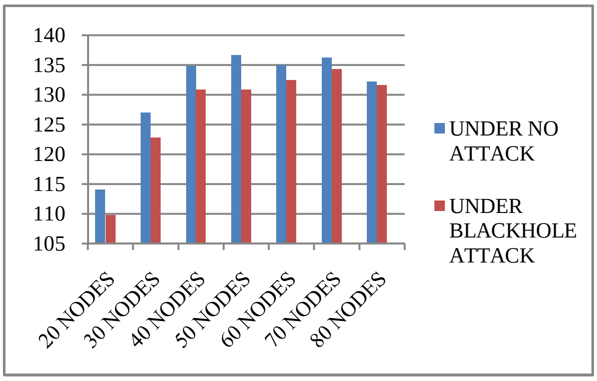
SIMULATION ANALYSIS

Average End to end delay



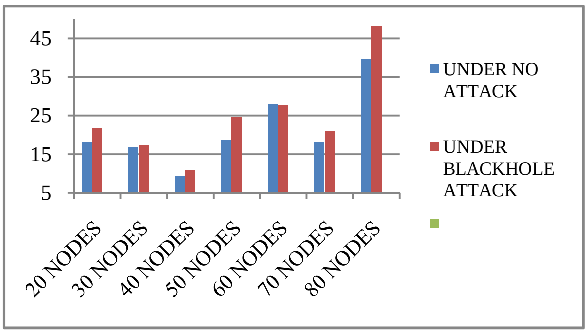
Explanation – Increasing node density leads to increase in available routes and thus the average end to end delay decreases with simultaneous increase in number of nodes. The blackhole attack results in extreme packet drop and congestion and therefore the delay will always be greater for a node under attack compared to the same node undergoing communication without any attack.

Throughput



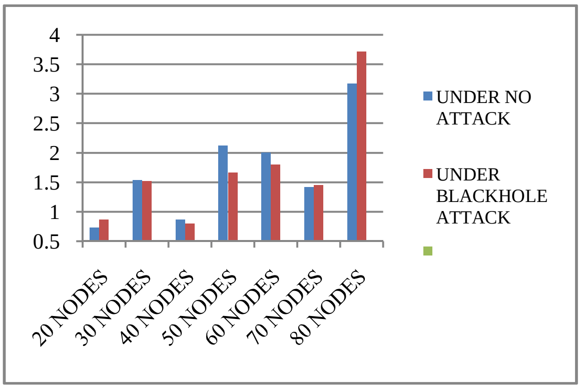
Explanation – The throughput of a WSN depends on various parameters like packet drop, delay, congestion, packet delivery ratio and number of retransmissions. All these factors are affected by blackhole attack and thus average throughput is lower compared to the no attack condition for the same number of nodes. The throughput remains almost constant since increase in number of nodes provides increased number of paths available.

Average Packet drop



Explanation – The average packet drop is directly related to network congestion packet data collisions under no attack condition. In case of black hole attack the data packets are routed to the malicious node and then dropped. This results in large number of retransmissions which further increases packet data collisions. With increase in node density, the network becomes more congested and therefore more packet drop occurs. Numbers of nodes are sufficiently high, packet drop is reduced to some extent due to increased available paths.

Overhead



Explanation – With increase in node density, packet drop increases resulting in increased retransmissions. This leads to excessive number of control data bits in the network further increasing congestion and packet drop. Under blackhole attack this condition worsens and therefore the overhead is more in case of network attack.

CONCLUSION

The behavior of a wireless sensor network is drastically affected by the number of nodes present in the network. We have studied, simulated and analyzed some of the most common network parameters and their variation with respect to increase in node density. The network performance is analyzed under attack and no attack conditions to provide a prospective of parameter variations for the above mentioned two conditions.

References

1. Yash Pal Singh, Dr. P.K Singh and Jay Prakash “A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs” *Journal Of Information, Knowledge And Research In Computer Engineering*.
2. Nidhi Chhajed and Mayank Sharma “Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN’s): A Review” *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue* 11, November 2014.
3. Ms. Twincle G. Vyas and Mr. Dhaval J. Rana “Survey on Black Hole Detection and Prevention in MANET” *International Journal of Advanced Research in*

Computer Science and Software Engineering, Volume 4, Issue 11, November 2014.

4. Ms.B.R.Baviskar and Mr.V.N.Patil "Black Hole Attacks Mitigation And Prevention In Wireless Sensor Network" *International Journal of Innovative Research in Advanced Engineering (IJIRAE), ISSN: 2349-2163 Volume 1 Issue* 4 (May 2014).
5. Jaspreet Kaur and Tavleen Kaur "A Comparative Study of Techniques Used in Detection and Prevention of Black Hole Attack in wireless Sensor Networks" *International Journal for Research in Applied Science and Engineering Technology* (IJRASET).
6. Shio Kumar Singh, M P Singh and D K Singh "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks" *International Journal of Computer Trends and Technology - May to June Issue* 2011.
7. J.Steffi Agino Priyanka, S.Tephillah and A.M.Balamurugan "Attacks and Countermeasures In WSN" IPASJ *International Journal of Electronics & Communication (IIJEC). A Publisher for Research Motivatin. Volume* 2, Issue 1, January 2014.
8. Dr. G. Padmavathi and Mrs. D. Shanmugapriy "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) *International Journal of Computer Science and Information Security*, Vol. 4, No. 1 & 2, 2009.
9. S. Kannan, T. Maragatham, S. Karthik and V.P. Arunachalam "A study of Attacks, Attack detection and Prevention Methods in Proactive and Reactive Routing Protocols" International Business Management 5 (3): 178-183, 2011. ISSN: 1993-5250. *Med well Journals*, 2011.
10. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong "Security in wireless sensor networks: Issues and Challenges" ISBN: 89-5519-129-4, ICACT, Feb 20-22, 2006.

****

How to cite this article:

Nitin Kumar and Shagun Chaudhary.2015, Analysis of Effects of Node Density Variations on A Wsn With Respect To Blackhole Attack. *Int J Recent Sci Res.* 6(10), pp. 7003-7005.

International Journal of Recent Scientific Research

ISSN 0976-3031

9 770976 303009