International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

Variation in Wireless Sensor Network Performance Parameters under Black Hole Attack and It's Mitigation

Mr. Nitin Kumar
Asst. Professor, Dept. of ECE, JIET School of Engg. And Technology for Girls
Jodhpur, Rajasthan, INDIA
nitinkumarece@gmail.com, 9950589895

Abstract— Wireless sensor networks deployed in harsh and unsupervised environments are prone to large number of attacks ranging from physical tampering, performance degradation, passive eavesdropping to complete network failure. These attacks can be individual or cooperative in nature. Also the target of attack can be a discreet node or distributed set of nodes. Denial of service attack (Dos) is the most common attack in a WSN having several variants like hello flood, Sybil and black hole. Black hole is an active attack which severely deteriorates a WSN from inside with the intent of exhausting the available power by forcing multiple retransmissions. In this paper, I am discussing some black hole attack prevention techniques and also using a modified version of Ad-hoc On Demand Distance Vector (AODV) protocol to analyze the effect of black hole attack and later the effect of prevention algorithm.

Keywords— WSN, Modified AODV, black hole attack, Dos, NS-2, end to end delay, RREQ

INTRODUCTION

A wireless sensor network is a collection of large number of wireless mobile nodes. Each of these nodes has a monitoring or sensing unit, a transducer, a microcomputer with limited memory, a transceiver and a power source [5]. They have the ability to communicate with each other without using conventional network infrastructure and generally lack a central administration. The lack of central control and limited computing power with limited battery resource results in vulnerability of high order. Various kinds of attacks can occur on a WSN based on intent of the attacker and the point of attack [8] [9] [13] [14].

CHARACTERISTICS AND METHODOLGY OF BLACKHOLE ATTACK

A Black Hole attack [8] [10] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to attract all the data packets and drop them instead of forwarding [11] [13] [14]. In black hole attack a hostile node uses its modified routing protocol in order to advertise itself for having the shortest path to the destination node [2] [7] [9] [12]. This malicious node advertises its availability of fresh routes irrespective of checking its routing table [1]. Thus the RREP from the malicious node will always reach the sender first as compared to other normal nodes which check there routing table entries for availability of fresh routes before replying to the sender of the RREQ packet.This results in setup of a forged route between the sender and the attacker nodes [1] [2] [3] [6]. After acquiring the data packets it's up to the attacker node whether to drop all the packets or forward it to other unknown address, packet dropping being more prominent choice [3] [4] [15].

PROPOSED SIMULATION MODEL

The following simulation model was used for simulating black hole attack on a WSN and then applying a modified AODV variant to minimize the effect of attack in terms of various network parameters -

Simulator	NS2 (version 2.35)
Simulation Time	200 (s)

Number of Nodes	70
Simulation Range	1000 × 1000 m
Routing Protocol	AODV
Attack Type	Black-hole
Traffic	CBR – 6 Traffic patterns for 20 to 70 nodes
Pause Time	10 (m/s)
Max Speed	20 (m/s)

Attack was progressed by random selection of black hole node which updates the routing table by fake hop count wand with higher number representing fresher route to the destination. Attack detection was performed by comparison of sequence number of RREP packet received in reply of RREQ from the source. Six different traffic scenarios and six different network topologies were made for simulation purpose. 100 simulations for normal WSN working, 100 for black hole attack and its prevention were carried out yielding results which were further carefully analyzed to produce comparative results in terms of network parameters.

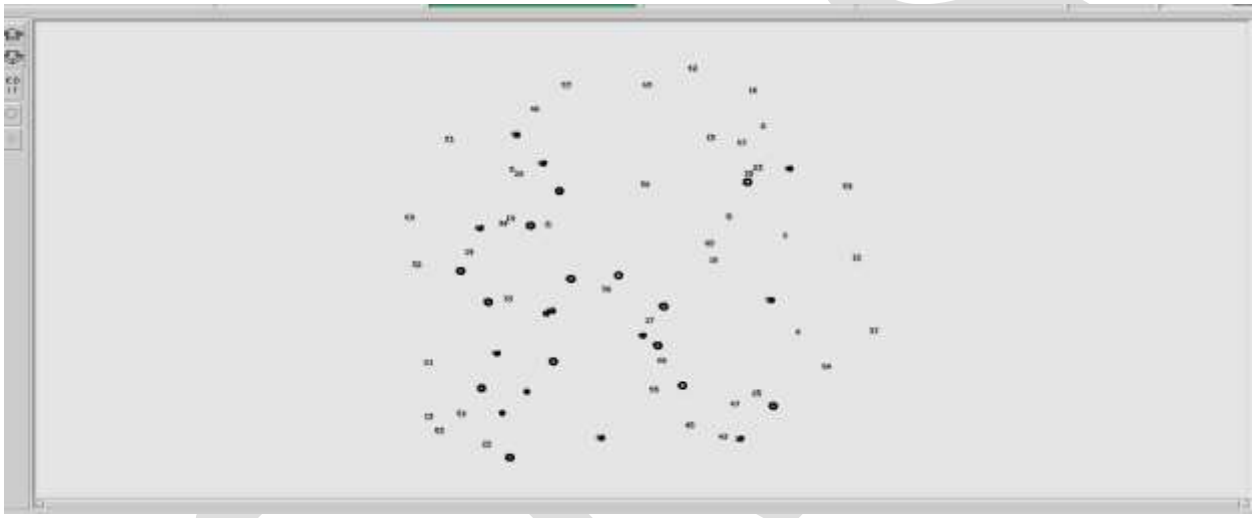

Fig. 1 Topology Scenario for 70 nodes

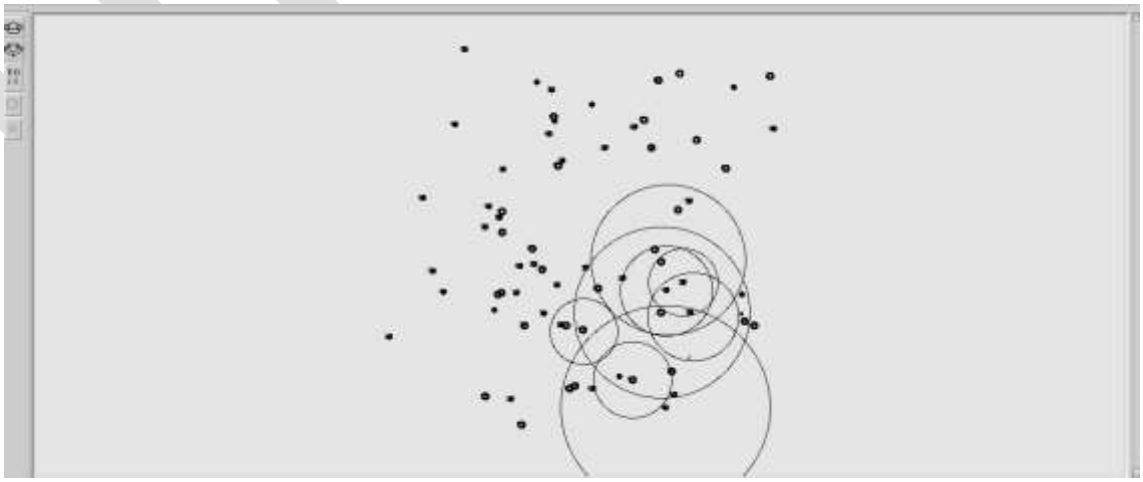

Fig 2 Simulation in progress

RESULTS AND ANALYSIS

The performance of the WSN under Black hole attack and under the effect of modified AODV for attack prevention was analyzed on the basis of five parameters: End to end delay, throughput, packet delivery ratio, system overhead and packet drop ratio.

Average End-to-End Delay

The performance of WSN under normal working with unmodified AODV shows the smallest delays in the network. Under black hole attack the average End-to-End delay rises due to network congestion and route disruption. By using the new modified AODV protocol the performance of the network can be increased by reducing the delay in real time. Although the effect is less visible as the number of nodes increases.

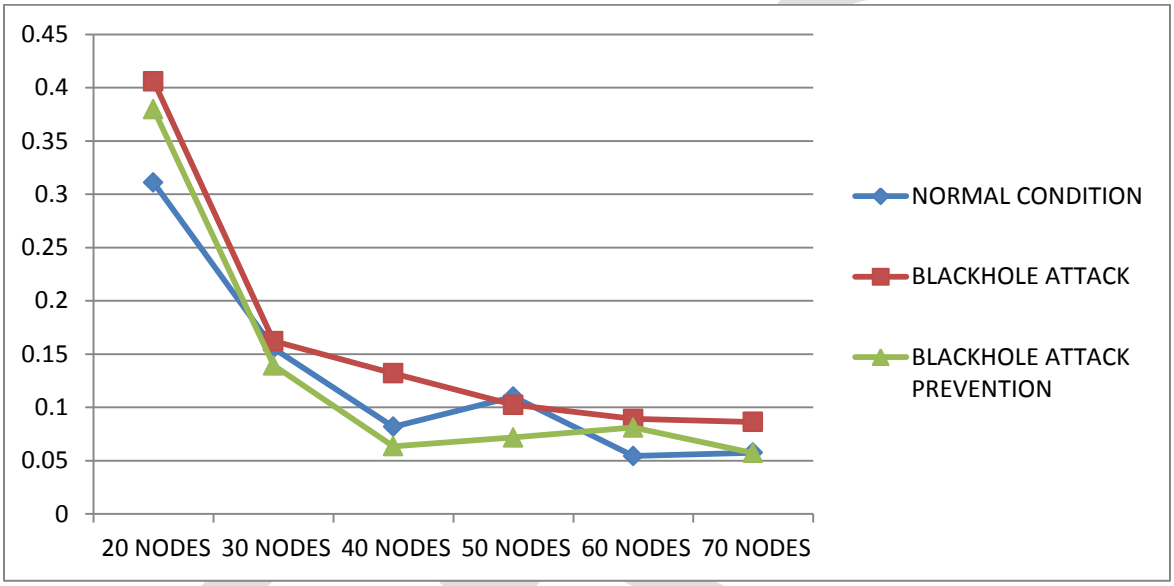

Fig. 3 Average end to end delay analysis

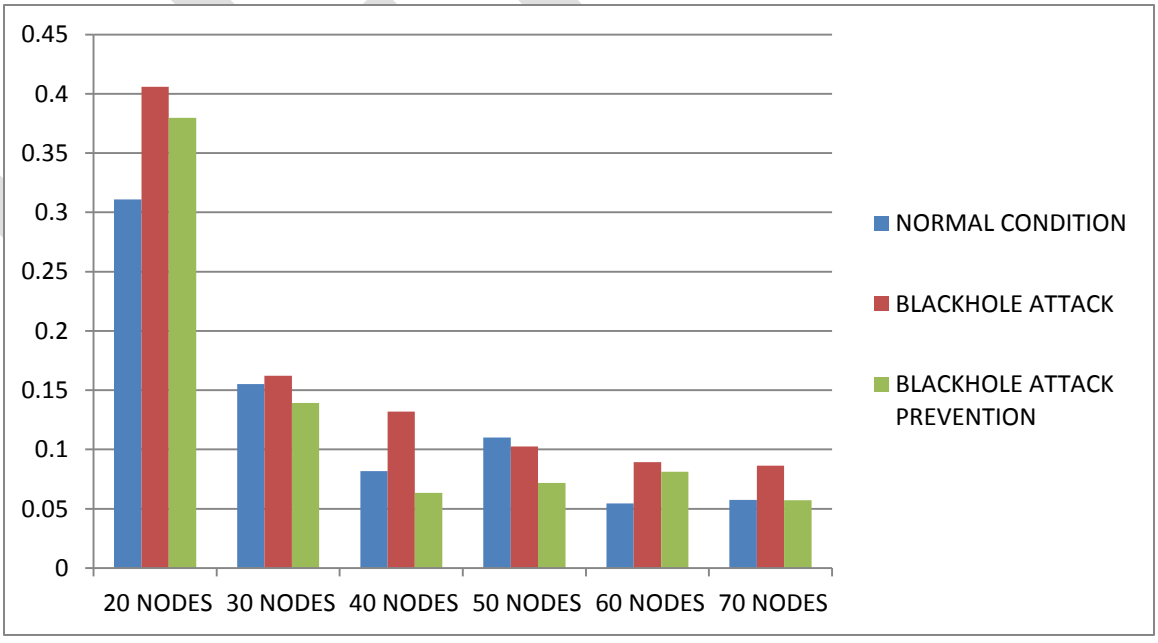

Fig. 4 Average end to end delay analysis

Throughput

The throughput of a normal WSN with unmodified AODV is maximum as shown in the figure below. With introduction of black hole attack the throughput is reduced as compared to previous condition. To improve the network efficiency the modified AODV protocol is used which results in increase in throughput on every node as is clear from the figure below.

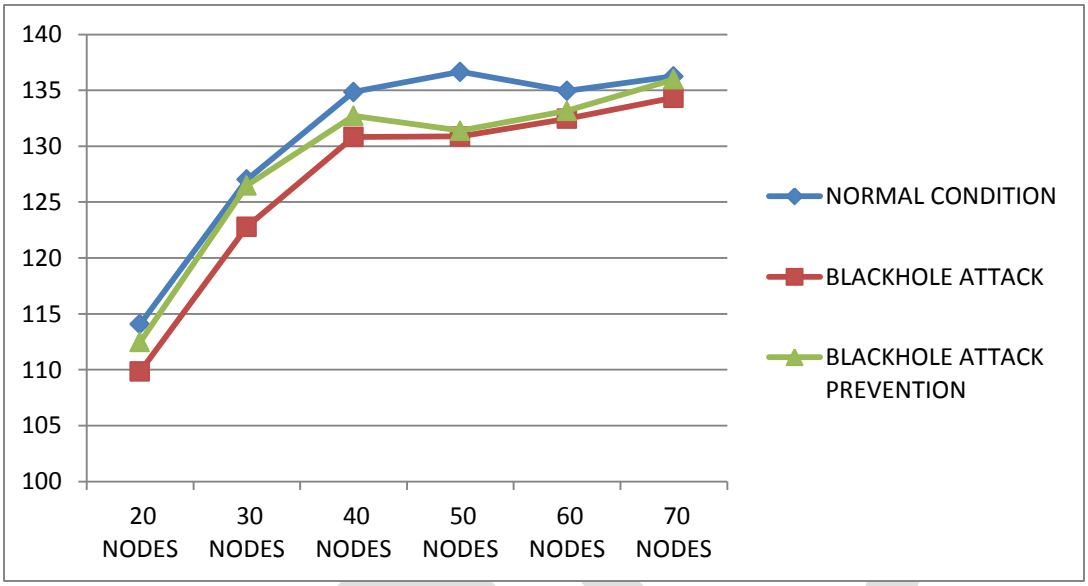

Fig. 5 Throughput analysis

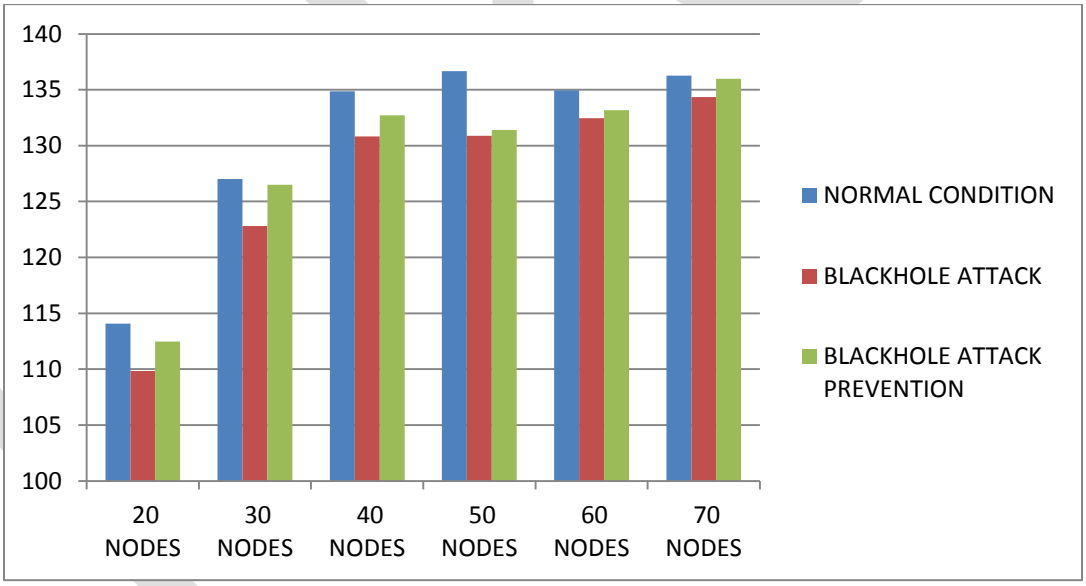

Fig. 6 Throughput analysis

Packet delivery ratio

Maximum number of packets is delivered in case of normal working of WSN with unmodified AODV. As black hole attack is introduced, the packet delivery ratio decreases due to more package loss. The modified AODV increase the net packet delivery efficiency.

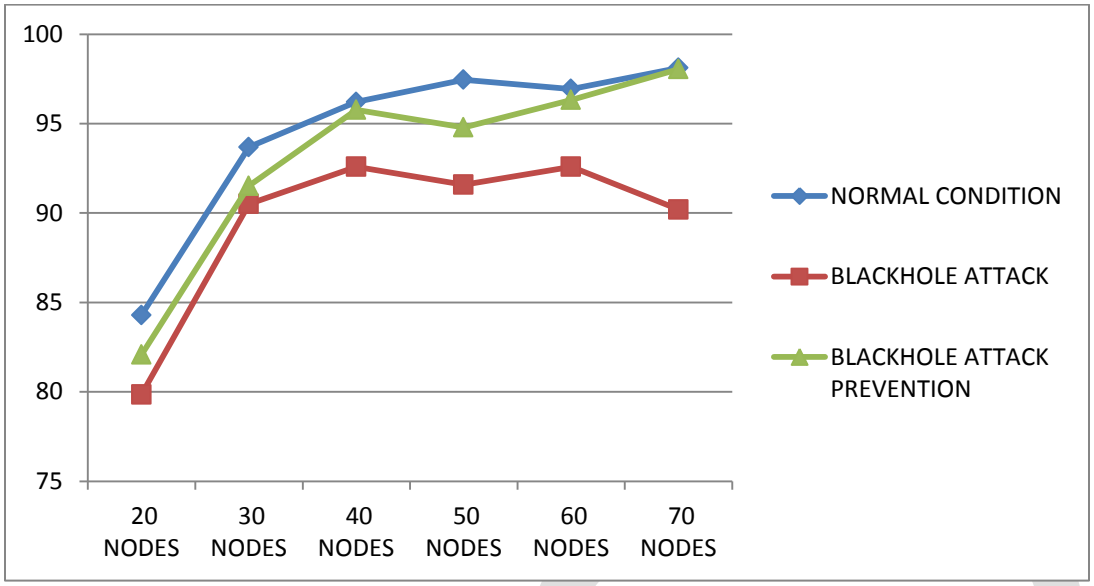

Fig. 7 packet delivery ratio analysis

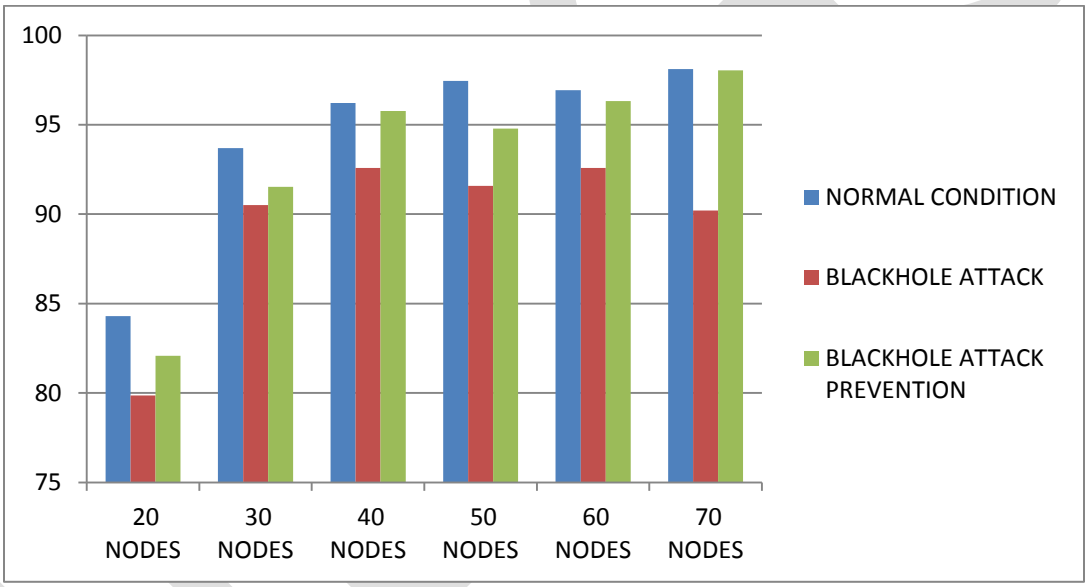

Fig. 8 packet delivery ratio analysis

Packet drop ratio

The unmodified AODV results in lowest number of drops in the system as shown in the simulation result below. Introduction of black hole attack in the system results in more packet drop by rerouting the traffic through the malicious nodes. The modified AODV protocol compares the routing tables on sender and malicious and isolates the route to the malicious nodes resulting in fewer packet drops.

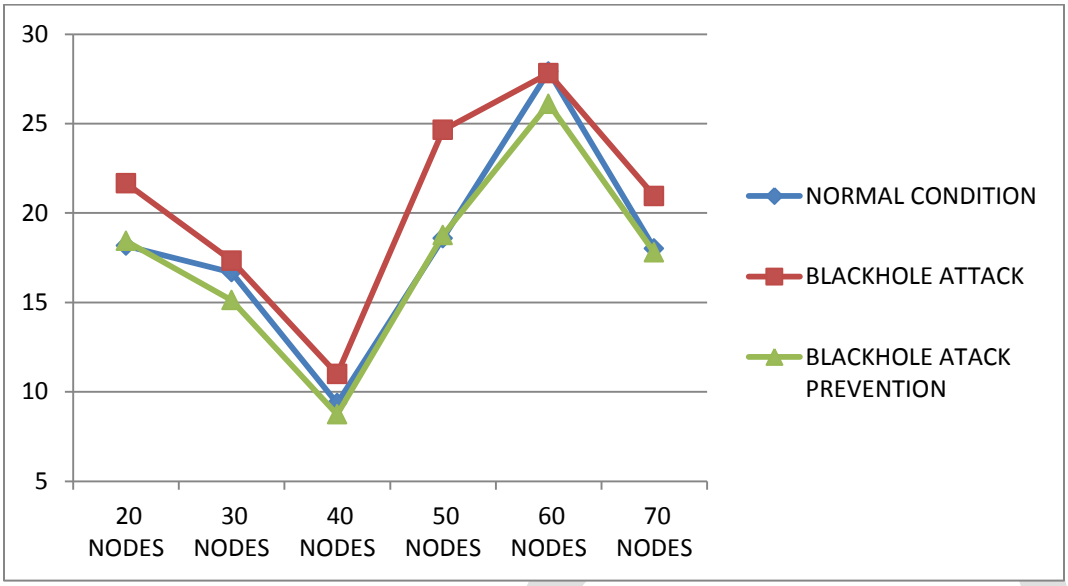

Fig. 9 Packet drop analysis

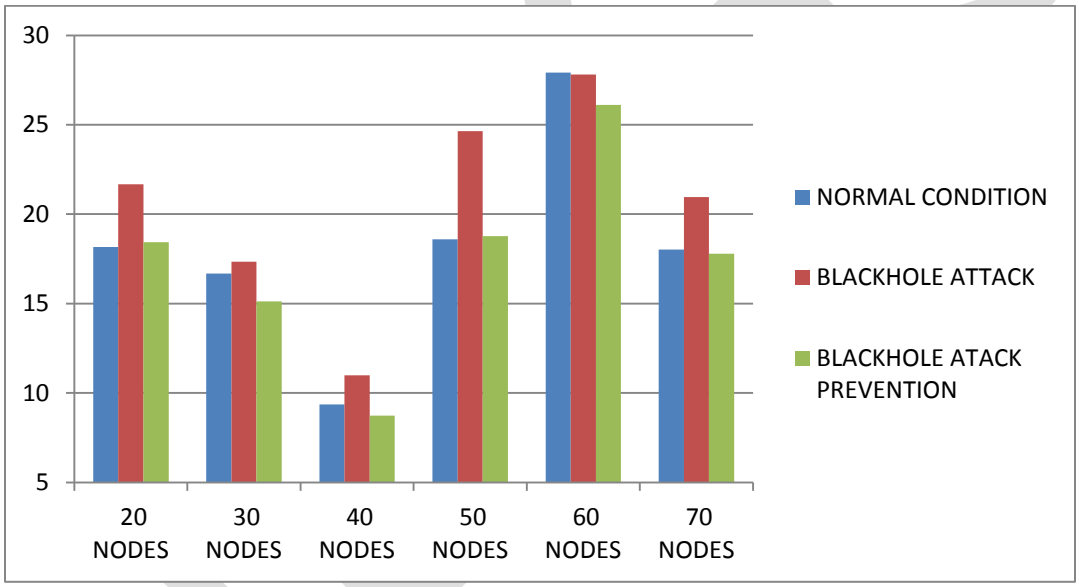

Fig. 10 Packet drop analysis

CONCLUSION AND FUTURE SCOPE

Black hole attack results in system degradation by resulting in higher delay times, higher packet drop ratio, low throughput and low packet delivery ratio. The prevention method analyzed in this paper shows promise in terms of increase in performance and minimizing the adverse affects of black hole attack. The technique used by is based on comparison on RREP sequence number of packet received by the sender from its neighbors broadcasting the availability of fresher or shorter routes. One limitation of this method is that it can only detect and prevent single black hole attack in a network and lacks the ability to detect cooperative black hole attacks caused by a group of malicious nodes. In future applications the intrusion prevention and recovery can be made more efficient by applying a distributed approach which can tackle more than one malicious node simultaneously.

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] Kimia Moradi and Majid Rahiminasab "Investigation of attack types in Ad Hoc networks and simulation of wormhole avoidance routing protocol" Scholars Research Library. European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):207-215.

[7] Ganesh R. Pathak, Suhas H. Patil and Jyoti S. Tryambake "Efficient and Trust Based Black Hole Attack Detection and Prevention in WSN" International Journal of Computer Science and Business Informatics.

[8] 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.

[9] 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.

[10] 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.

[11] Md. Safiqul Islam and Syed Ashiqur Rahman "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches" International Journal of Advanced Science and Technology, Vol. 36, November, 2011.

[12] 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. Medwell Journals, 2011.

[13] Wassim Znaidi and Marine Minier "An Ontology for Attacks in Wireless Sensor Networks" Jean-Philippe Babau.

[14] Mohammad Saiful Islam Mamun, Ernest A.F.M. Sultanul Kabir "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010. Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Network", WCECS 2008, ISBN: 978-988-98671-0-2