International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 341-347
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

Mobile Ad Hoc Network

Pandi Selvam Raman
Assistant Professor & Head
PG Department of Computer Science
Ananda College, Devakottai
Tamilnadu, India
pandiselvamraman@gmail.com

Abstract

Mobile ad hoc networks (MANETs) are autonomous system of randomly moving nodes with no central network authority or fixed infrastructure. Due to its unpredictable nature of mobility nodes may join and leave the network at any point of time. Therefore, MANETs highly vulnerable to security attacks. The black hole attack is a kind of Denial of Service (DoS) attack in mobile ad hoc networks. This attack node first needs to invade into the multicast forwarding group and absorbs all the data packets regarding to drops fully or partially. So, that the destination node will not be able to get the data packets fully and this will affect the Packet Delivery Ratio (PDR).Multicast is a communication between a single sender and multiple receivers on a network. Otherwise it transmits a single message to a particular group of recipients. Instead of sending a single message to multiple receivers simultaneously, it is advantages to use multicast in order to save bandwidth and resources. This paper goal is to measure the impact of black hole attack with respect to three scenarios: Black hole near sender, near receiver and near gateway in cluster based multicast routing protocol.

I. Introduction

As a significant growth of wireless communication technology today's peoples are expecting to communicate anywhere and anytime. Mobile Ad hoc Network (MANET) is a type of wireless communication technology where the networks are formed with autonomous nodes without any predefined and fixed infrastructure [1]. In MANET each node acts not only as a host but also a router for relaying messages from one node to other. Therefore, the nodes must maintain the trust and co-operation to manage network functionality [2]. Due to the dynamic topology such that nodes can easily join or leave the network at any time. So that providing security is a major concern because of various types of malicious attacks [3]. One of these attacks is Black Hole attack or Packet Drop attack is a passive and way to perform Denial of Service. The malicious node generates fault reply packet for route request packets and claims that it has the best or shortest path to the destination. By receiving data packets malicious nodes would drop the packets partially or all [4]. Multicast is type of communication between a single sender to multiple receivers on a network. Otherwise it transmits a single message to a particular group of recipients simultaneously in a single transmission. Instead of sending through multiple unicast, the multicast is used to minimize the bandwidth consumption, processing time and communication cost [5]. The Cluster Based Routing Protocol (CBRP) is a reactive or on-demand routing protocol where the nodes are grouped into several disjoint or overlapping clusters and only a few cluster heads maintains the local information in order to save the energy and bandwidth [6]. In this paper, we present a simulation based study of the effects of black hole

attacks on cluster based multicast in MANETs. This paper starts with this brief introduction. Section II describes the cluster based multicast routing protocol and Black hole attack. The improved model Impact of black hole attack on cluster based multicast in Mobile Ad hoc networks is presented in Section III. Section IV discusses the experiments and results. Finally, conclusions and future direction are given in Section V.

II. Related Work

a. Cluster Based Multicast Routing Protocol

Cluster Based Multicast Routing Protocol is hybrid routing protocol and it combines with the merits of both proactive and reactive routing protocol approaches to maintain the stability and scalability in the network [7]. The CBMRP composed with the following two objectives.

i. *Cluster Formation:* Cluster formation is a process of dividing a large network into several disjoint or overlapping clusters i.e. sub-networks. This formation starts with cluster information that is maintained by each node to know their own status such as cluster head, cluster gateway or cluster member by exchanging the information with neighbors.

ii. *Cluster Head Election:* The cluster head election may be done by calculating nodes connectivity, mobility and weight [8]. However, the weight based clustering algorithms are most preferable to have maximum number of possible cluster members under single cluster head. In these algorithms, the each node weight calculated and declared largest weight node as cluster head node. Then the head node sends request to the neighbors and gets immediate reply to form the clusters. The cluster heads only maintains and exchanges the routing information between clusters in order to maintain scalability.

iii. *Routing in CBMRP:* In cluster based multicast routing, the communication can be in two ways [9].

- Intra-cluster (Communication of nodes within the same cluster): Source and destination are in same cluster and the cluster head maintains the topology.
- Inter-cluster (Communication among clusters): Source and destination are in different cluster. The cluster head of the source node sends the request packet through the corresponding gateway nodes.

b. Black hole Attack

Black hole Attack or Packet Drop Attack is a type of DoS attack. The primary aim of this attack is to reducing the quantity of data packets and hence to effect the performance of the network [10]. The black nodes invade into the multicast group and introducing itself as having the shortest path to the destination in order to intercept the data packets. The malicious nodes are immediately sends fake reply to the source node without knowing anything about the route towards destination. Therefore it drops all or small amount of packets instead of forwarding them

to the immediate neighbor or to the destination node. The result is obtaining low delivery ratio. Black hole attacks are two kinds [11] [12]. There are

i. *Single Black Hole Attack:* Single Black Hole attack uses only single node acts as malicious node in the network.

ii. *Cooperative Black Hole Attack:* Collaborative Black Hole Attack uses multiple nodes in a group act as malicious node to drop all the data packets.

III. Improved Model (Impact of Black hole on Cluster Based Multicast)

a. Black hole attack formation

An attacker misbehaves by dropping routing packets instead of relaying them to reach destinations. In cluster based multicast, an attacker may possible misbehave by means of replying false message near sender, near receiver and near gateway as shown in Fig.1. Therefore, simulation is conducted to know how the black hole nodes are affecting the network performance in these three scenarios.

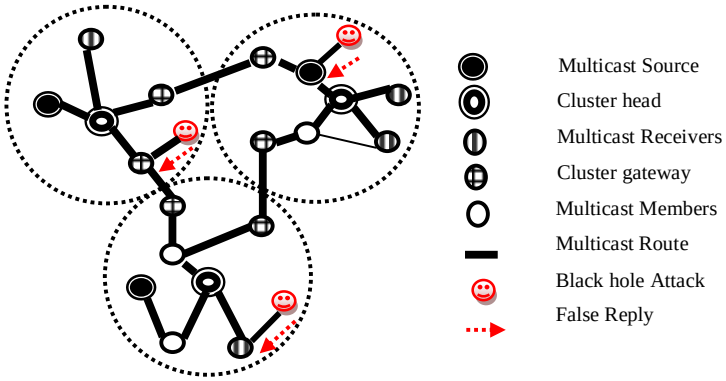

Fig.1 Cluster Based Multicast with Black hole nodes

b. Black hole attack impacts in different positions

Network performance analyzed by considering different positions of malicious (black hole) node i.e. an attacker may invade near sender or receiver or gateway node. When the attacker near sender it tap all the packets and drops out maximum amount of data. The remaining packets only forward to corresponding receiver or to the near member that are the in the routing path. Therefore, the receiver never get full packet and the result is most harmful.

Black hole attack placed near receiver, the attacker can tap the packets when the data packet reaches the receiver. Since most of the cluster member node utmost forwarded maximum number of data packets towards receivers. Therefore there is possible to get greater amount of packets by the receiver and the result is least harmful.

The attacker placed near the gateway (between clusters), it taps and drops the packets when the source and receivers are in different clusters. Therefore there is a chance to drop maximum packets due to forward them to adjacent cluster and the result is somewhat harmful.

IV. Experimental Results

a. Metrics

We run a number of simulations under Linux, using the network simulator NS2 version ns-allinone-2.26. The metrics used to evaluate the PDR (Ratio of the number of packets delivered to the receivers and number of packet to be received by the receivers) with black hole attack node and without black hole attack node applied to three scenarios. The simulation environment is composed with 50 randomly placed nodes in 500 x 500 m area and simulation period is 1000s. Mobility model is random waypoint with node mobility.

b. Results and Discussion

To prove the impacts the proposed approach that the results are conducted with three multicast cluster. Each multicast cluster contains one multicast source and receiver node. The Fig.2 shows both cases, with black hole near the source and without the black hole in the network. The observation is that the PDR is radically decreases when there is attacker in the network. Since the attacker is near sender it drops bulky before forwarding to the cluster member node. Therefore the receiver could not able to receive all packets.

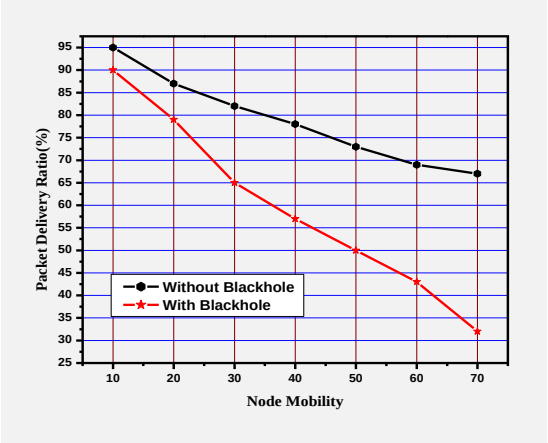

Fig.2 Black Hole Attack near Sender

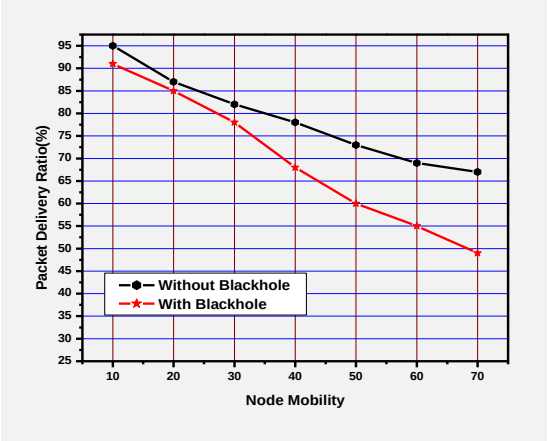

Fig.3 Black Hole Attack near Receiver

Fig.3 describes how the black hole attack affect the network performance while a attacker invade near any one of the receiver. The result is utmost all the packets reached safely and hence PDR goes on increasing because of promoting the packets by the members to the receiver.

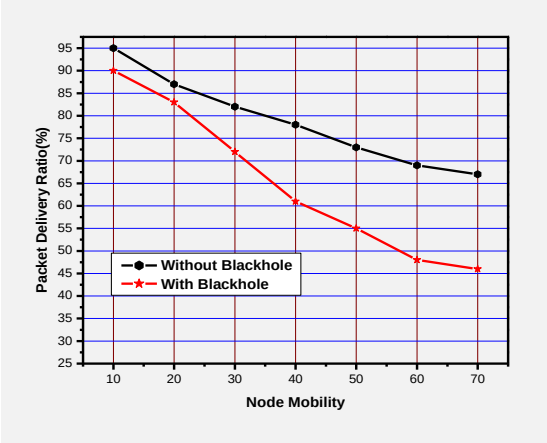

Fig.4 Black Hole Attack near Gateway

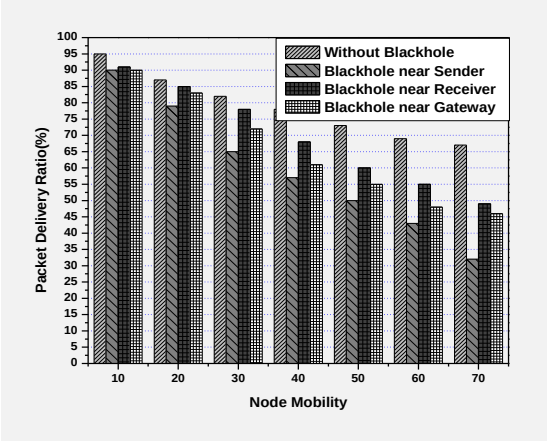

Fig.5 Comparison among the three scenarios

Fig.4 illustrates what happens while the black hole agitates near the gateway. The outcome is partial amount of packet only forwarded safely to the receivers that are in nearby clusters. Therefore the acceptable amount of PDR is the outcome in this situation. The Fig.5 compares these three scenarios performance in terms of PDR while increasing the node mobility.

V. Conclusion and Future Direction

The objective of this paper is to demonstrate the abnormal behavior of black hole attack in the cluster based multicast routing protocol. For this suggestion we used NS2 to observe the crash of malicious node with respect to three positions. The simulation shows that the black hole near sender is very dangerous attack position and incurs the lowest PDR. Black hole near receiver is the least harmful attack position and incurs highest PDR than other two situations. At last case,

attacker near gateway also offers higher PDR than the near sender but lower than the near receiver. In this paper, the attacker impacts are measured when there is only one sender and multiple receivers in the cluster based communication network. As future work, the impact may be proved in the group communication i.e. in the multi-source multicast routing protocol. Furthermore we assumed only one attacker node (Single Black Hole) for future it can be extended with two or more attacker (Cooperative Black Hole) in the network.

References

[1] Magnus Frodigh, Per Johansson and Peter Larsson, *"Wireless Ad Hoc Networking - The Art of Networking without a Network," Ericsson Review*, pp.248-262, 2000.

[2] Ram Ramanathan and Jason Redi, *"A Brief Overview of Ad hoc Networks:Challenges and Directions,"* IEEE Computer Magazine, pp.20-22, 2002.

[3] L. Zhou and Z. J. Haas. "*Securing ad hoc networks,"* IEEE Network Magazine, pp.24–30, 1999.

[4] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, *"Ariadne: A secure on-demand routing protocol for ad hoc networks,"* ACM International Conference on Mobile Computing and Networking (MobiCom '02), *September 2002.*

[5] Changling Liu and Jorg Kaiser, *"A Survey of Mobile Ad hoc Network Routing Protocols,"* Univ. of Ulm, Tech. Rep.Series, 2005.

[6] Krishna Gorantala, *"Routing Protocols in Mobile Ad hoc Networks,"* Master Thesis in Computing Science, Umea University, Sweden, 2006.

[7] Tim Daniel Hollerung *"The Cluster Based Routing Protocol,"* Mobile Ad-hoc Networks based on Wireless LAN, pp.1-12, 2003.

[8] Ratish Agarwal and Mahesh Motwani, *"Survey of Clustering Algorithms for MANET,"* International Journal on Computer Science and Engineering, vol.1 (2), pp.98-104, 2009.

[9] Mingliang Jiang, Jinyang Li and Y. C. Tay, *"Cluster based Routing Protocol (CBRP),"* Internet Draft, draft-ietf-manet-cbrp-spec-01.txt.

[10] Palanisamy, P. Annadurai, S.Vijayalakshmi, "*Impact of Black Hole Attack on Multicast in Ad hoc Network (IBAMA),"* IEEE, 2010.

[11] Latha Tamilselvan, Dr. V Sankaranarayanan, "*Prevention of Co-operative Black Hole Attack in MANET,"* Journal of Networks, vol. 3, no. 5, pp 13 – 20, 2008.

[12] Miss Bhandare A.S. and Dr. Mrs. Patil S.B. *"Securing MANET against Co-operative Black Hole attack and its Performance Analysis-A case Study,"* International Conference on Computing Communication Control and Automation,IEEE, 2015.

AUTHOR PROFILE

Pandi Selvam Raman working as Assistant Professor & Head of PG Department of Computer Science, Ananda College, Devakottai, Tamilnadu. He has received M.Sc., M.Phil., and Ph.D. Degrees from Alagappa University in 2007,2008 and 2015 respectively. He has published over 12 International Journals (including IEEE & ACM) and presented papers in 20 International/National conferences in various areas. His research interest includes mobile computing, ad hoc wireless networks & security and computer algorithms.