The Approach for the Prevention of Black Hole Attack in MANET using DSR Protocol and Ant Colony Optimization Technique: A Review

Hashneet Kaur*
Hardeep Kaur**

Abstract

Ad Hoc Networks (MANETs) are self-organized network where nodes are free to move in any direction. MANET doesn't need any centralized system. Due to its dynamicity, Black hole attack is a serious security issue to be resolved. It takes place when a malicious node called as black hole enters into the network. Black hole node shows its fake behaviour during the process of route discovery. Today, many prevention techniques have been proposed for MANET. However, in the presence of fake nodes, the networks are subjected to different kinds of attacks.In this problem, a fake node advertises itself of having a shortest path to another node whose packets the fake node want to drop. In this flooding process, if the reply from the actual node reaches later than the fake node reply as requested by the main node .A forging path is created via a fake node. An ideal path is one in which the packet reach to destination with minimum delay and lesser overhead. In this paper we apply Dynamic Source Routing (DSR) protocol in order to prevent black hole attack using Ant Colony Optimization.

Keywords: Black Hole Attack, Dynamic Source Routing, Ant Colony Optimization.

I. Introduction

Wireless network is the network in which nodes are connected via a wireless link having no fixed infrastructure. All nodes are having with same processing power .In MANETs all the nodes are cooperate in distributed manner. The main advantage of wireless network is the number of clients is connected in a wide range. Limited bandwidth, open medium and memory are the main disadvantages of wireless network. The two basic models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An adhoc network is(decentralized) i.e. they have no central control for network operation as well as handling it is a multi-hop routing process and also a light weight terminal with small memory size and low CPU capability. MANETs should be self-configured as well as self built.

Hashneet Kaur*
Student – MTech.
Department of Electronics Technology
Guru Nanak Dev University, Amritsar

Hardeep Kaur**
Department of Electronics Technology
Guru Nanak Dev University, Amritsar

Whenever a node requires sending data from source to destination, it runs an appropriate path finding algorithm.

Hence in addition to acting as hosts, each mobile node does the function of routing and forward messages for other mobile nodes [1]. Most important networking operations include routing and network management [2].There are three types of routing protocols broadly classified as proactive routing protocol, reactive routing protocol, Hybrid routing protocol.

II. Routing Protocols

In order to find out suitable routes between communication nodes routing protocols act as second hand. It is a self-directed collection of mobile users that speak moderately over bandwidth constraint wireless link [3].THE network topology keeps on changing unpredictably over time and place as nodes are free to move. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes [4]. Routing protocols are broadly classified into two categories mainly [proactive, reactive].

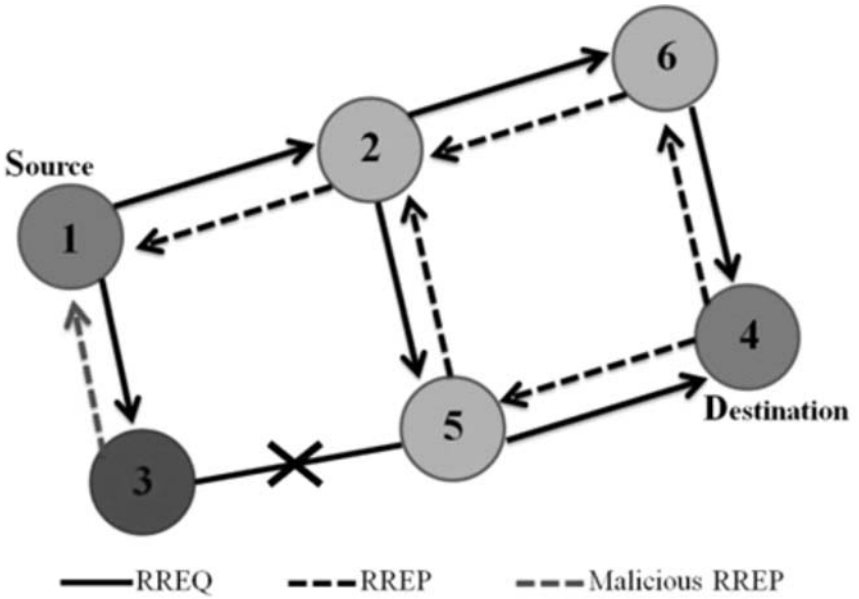

Fig. 1: Node 1 as Black hole

(Source: http://www.spiroprojects.com/webadmin/uploads/z.jpg)

III. Adhoc Routing Protocol

1. Proactive Routing Protocol (mainly table driven):- WRP, DSDV, CGSR.
2. Reactive Routing Protocol (on demand):-DSR, AODV, TORA, ABR.

DSR (Dynamic Source Routing): DSR is an on-demand routing protocol having Route Discovery and Route Maintenance it's two parts. In DSR, when a node wants to send a packet from the source who does not have a path to reach the destination in its route cache memory, the source node will initiates a Route Discovery in order to find out a route between source and destination and that node is known as the source target, and the destination where the packet is to reach is known as the Destination target. In the route discovery process the source node will generate a route request with unique id and broad caste that packet to all the nearby nodes. Here each node will receive the Route Request and check whether it has recently seen the route request or not. If the node already seen that request it will discards. Otherwise, it will check in its route cache memory whether it has a route to the destination or not. When the Request reaches the destination, the destination node will sends a Route reply back to the source node, and giving a copy of the list of route record from the route Request. The source node will update the new route in its Route Cache memory after having a reply from the destination node.

But when the topology is changing or the link between source and destination is broken. It leads to the failure in the communication between the source node and the destination node and thus route maintenance mechanism is involved in this. In order to transfer the packet, it will find out another relevant path toward the destination and if it fails to find out the path, it will again attempt the new route discovery in order to find out the new path towards the destination.

IV. Black Hole Attack

Black Hole Attack is one of the serious attacks in mobile ad-hoc network. In Black Hole attack, a single or multiple nodes starts dropping the message packets before it reached to the final destination [5]. In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the packets. The

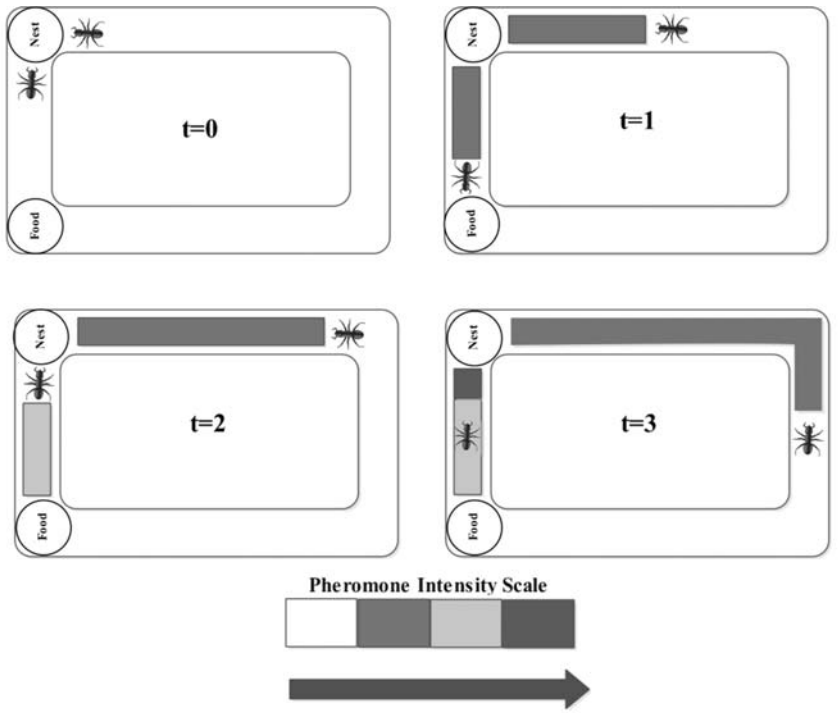

Fig. 2: The shortest path mechanism used by ants. The different colors indicate Increasing levels of pheromone intensity. The scenario is depicted in successive time steps (Source: Baluja& Davies, 1998)

black hole attack is broadly classified into two types(i)single black hole attack in which a single fake node will drop the packets And (ii)gray black hole attack in which more than one node act as a fake node and drop the packet. Black hole attack mainly involved two properties. It will advertise itself to the source node as having a valid route through it toward the destination. Even though the route is fake. The fake node will DROP the obstruct packet.

Black hole attack is also known as sleep deprivation attack and it can be generated internally as well as externally.

In internal black hole attack the fake node is within the network itself and drops the packet.

In external black hole attack the node is outside the network and through external process it will drop the packets.

V. Black Hole Preventative Technique Ant Colony Optimization

ACO a famous swarm intelligence approach, has taken the inspiration from real ants who are wandering around their nests to forage for search of food [6]. The basic idea of the ant colony optimization meta-heuristic is taken from the food searching behavior of real ants. This behavior of the ants can be used to find the shortest path in networks. Between the nest and the food source .For finding the shortest path, a volatile chemical solution known as pheromone is secreted by ant .It takes place when an ant is returning back to the nest after finding food and leave the trail of pheromone. Ants can also smell pheromone and tend to follow with higher probability those paths characterized by strong pheromone concentrations [7].The ants are known as the small control packet with unique identity which is used to find the path toward their destination. Because of its robustness, and adaptive nature, ACO can find its applications in routing, assignment & scheduling [8].It is also widely used in bio-informatics and communication networks.

VI. Conclusion

BLACK hole attack is the major issue in mobile adhoc network. Many different researchers proposed various techniques for the prevention of black hole attack. In

this paper reactive routing algorithm i.e DSR is used which will eliminates the routing overhead problem because of its on demand process. along with ant colony optimization. The optimization technique used is iterative in nature. Many different techniques have been proposed in ad-hoc network that determines the path and transmission of data which leads to the loss in packet. More than 15 years of its studies both the productiveness and conceptual background have been revealed, thus making ACO an effective technique for transfer of data with less packet loss as well as lower overhead problem.

References

1. JiwenCai, Ping Yi, Jialin Chen, Zhiyang Wang, Ning Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), pp.775-780 20-23 April 2010.
2. Yibeltal Fantahun Alem, Zhao Cheng Xuan, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," 2nd International Conference on Future Computer and Communication (ICFCC), Vol. no.3, pp.672-676, 21-24 May 2010.
3. Shendre, Ashwini, and P. S. Mohod. "Using SG-PKM Improve security mechanism for Supporting Routing Services on WANET." International Journal of Computer Science & Information Technologies 5.4 (2014).
4. ShailyGoyal," A review on routing protocols based on zone mechanism for wanet",International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 2, Issue 11, November 2013.
5. Bhosle, Amol A., Tushar P. Thosar, and SnehalMehatre, "Black-hole and wormhole attack in routing protocol AODV in MANET, " International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol. 2, no.1, pp. 45-54, Feb. 2012.
6. M. Dorigo and C. Blum, "Ant colony optimization theory: a survey," Theor. Comput. Sci., vol. 344, no. 2-3, pp. 243–278, 2005.
7. Sowmya, K.S., T.Rakesh, Deepthi P. Hudedagaddi, "Detection and Prevention of Black Hole Attack in MANET Using ACO," International Journal of Computer Science and Network Security, Vol. 12, pp. 21-24, May 2012
8. G. D. Caro, F. Ducatelle, and L. Maria Gambardella 2005. AntHocNet: an Ant-Based Hybrid Routing Algorithm for Mobile Ad Hoc Networks. 2005.
9. Sharma et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(12), December - 2013, pp. 512-515
10. Akshay Horane, Amutha Jeyakumar, Sagar Patkar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 2, March -April 2013, pp.1191-1195
11. M. Dorigo and T. Stützle. The Ant Colony Optimization.
12. Vaibhav Godbole, Defence S & T Technical Bulletin, Science & Research Technology Institute for Defence (STRIDE), Vol. 5, No. 2, November 2012, pp. 114-134, ISSN:1985-6571.
13. Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, International Journal of Modeling and Optimization, Vol. 2, No.1, February 2012.
14. Rupinder Kaur and Parminder Singh, The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014.