A Review of Prevention of Black Hole Attack in MANET

Navjot Kaur[1], Harleen Kaur[1]

[1]Chandigarh Engineering College, Mohali, Punjab, India

***Abstract* -** Black hole attack is a serious security problem to be solved for successful delivery of packets in mobile ad-hoc networks. In this problem, a malicious node uses routing protocol to advertise itself as having the shortest path to the node whose packets it wants to seize. In flooding based protocol, if the malicious node reply reaches the requesting node before the reply from the actual node, a forged route is created. This paper deals with the presentation of Black hole attack in Mobile Ad Hoc Network (MANET). Various prevention techniques have been discussed in the papers that are used to prevent black hole attack. MANETs are susceptible to various attacks, so attacks have to be mitigated in initial setup.

***Keywords* -** Routing, Black Hole attack and Security, DSDV.

I. INTRODUCTION

Wireless network is the network in which various mobile nodes are physically connected with each other to transfer the data from one node to another node. The main advantage of wireless network is that it can connect number of clients or nodes wirelessly in a wide range. The disadvantage is their limited bandwidth, processing capabilities, memory and open medium [1]. Two basic system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is an infrastructure-less network and thus decentralized type of wireless network. On the basis of network connectivity, the topology will change because the nodes are wirelessly connected with each other and forma different network for exchanging the data and also managing the responsibility of the entire network. 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]. Routing protocols can be divided into three types (proactive, reactive and hybrid protocols), depending on the routing topology. Proactive protocols are typically table-driven and routing information will be updated in a routing table. Examples of this type include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP). Reactive or source-initiated on-demand protocols, in contrary they do not periodically update the routing information in any table. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) and Associativity Based Routing (ABR). Hybrid protocols make use of both reactive and proactive protocol approaches. Example of this type includes Temporally Ordered Routing Algorithm (TORA), Zone Routing Protocol (ZRP). Security is a major concern in all forms of communication networks, but infrastructure less networks face the greatest challenge due to their inherent nature. As a result, there exist a mess of attacks that can be performed on an Ad hoc network. [1][4]. But these protocols does not work well so this paper contains the introductory part to swarm optimization algorithms. This manuscript is divided in four sections. Section I provides brief introduction to the paper. Section II comprises a detailed explanation of black hole attack and its types. In Section III various black hole prevention techniques have been discussed and finally the manuscript is concluded in Section IV.

II. BLACK HOLE ATTACK

The black hole attack is one of many possible 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 [3]. There is a one malicious node present in the black hole attack, it collects the complete packet from source, adding or changing in the parameters of routing message and create a fake route to deny the communication between the source and the destination. The fake route will not give all the packets to the destination, it drop the packets. The Black hole attack is of two types.

a) Single Black Hole attack

In Single Black Hole attack, only one node act as a false node that collects the whole packet from source and drops the packet [4]. The single Black hole attack is shown in Fig.1.1. The source node P wants to talk with destination R. Firstly, it sends Route Request (RREQ) to the neighbor node. If it has applicable route to reach destination then it sends the packet through the path. If it does not contain a route then it forwards the RREQ to the neighbor's node until reach destination. The node Q act as a false node that sends Route Reply (RREP) with maximum sequence number before any other node respond, even if any transitional node sends RREP to the source. The Source node P rejects the reply and it assumes that the Q node has direct path to reach destination and it sends the packet from end to end on that path. So, the node

Q collects all the packets coming from founded node which creates black hole problem.

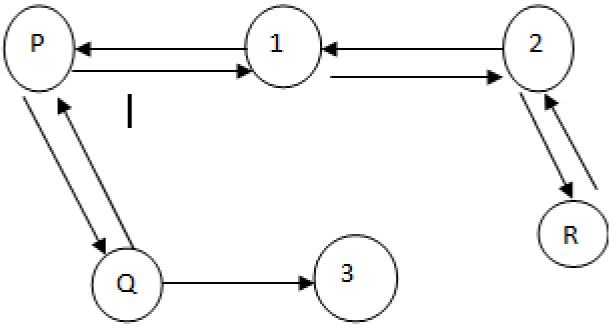

Fig 1.1: Single Black Hole Attack

b) Co-operative Black Hole attack

In Co-operative Black Hole attack, more than one node combined equally and act as Fake nodes is called as supportive Black hole attack [4]. This will reduce the network performance. As shown in Fig.1.2. Whenever node F receives RREQ packets, it claims that it has the shortest route to the destination node and immediately sends a false RREP packet to the source node, even though it might not be having the route to the destination. The F node creates a fake route from source to destination and do not send the packets properly or drop the packets from source to destination, were P is source node and R is the destination node.

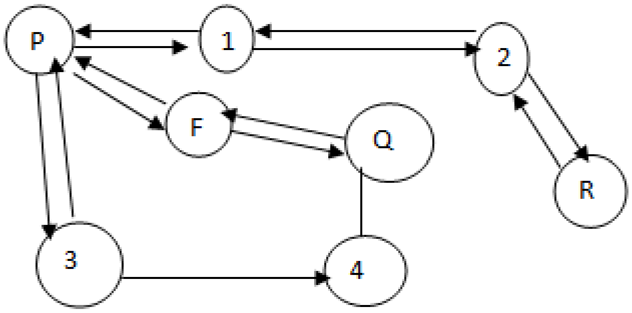

Fig 1.2: Co-operative Black Hole Attack

III. BLACK HOLE PREVENTION TECHNIQUES

a) Artificial Bee Colony

This algorithm is a swarm based algorithm based on the foraging behavior of honey bee colonies. It is a very simple, robust and population based stochastic optimization algorithm [13].It is used in various fields like Bench Marking Optimization, Bioinformatics, Scheduling, Clustering and Mining applications.

b) Ant Colony Optimization

The basic principle of an ant routing algorithm is that ants deposit on the ground a hormone, the pheromone, while they roam looking for food. Ants can also smell pheromone and tend to follow with higher probability those paths characterized by strong pheromone concentrations [14]. It is used in cell placement problems arising in circuit design, the design of communication networks, or bioinformatics problems.

c) Bacterial Foraging Optimization

This technique BFOA (bacterial foraging optimization algorithm) is new comer to the biological techniques. The process, in which a bacterium moves by taking small steps while searching for nutrients, is called chemo taxis and key idea of BFOA is mimicking chemo tactic movement of virtual bacteria in the problem search space, individual bacterium communicate to other by sending signals. It is a global optimization algorithm for various optimization problems. This technique is also inspired by the social foraging behavior like ant colony and particle swarm optimization. It attracts the researchers due to its efficiency in solving real world optimization problems and gives better results than traditional methods of problems solving [15].It is used in radio frequency identification network scheduling, antenna problem, to optimize both amplitude and phase of weights of a linear array of antennas for maximum factor at any desired direction and null in a specific direction.

d) Particle swarm optimization

Particle swarm optimization is a popular multidimensional optimization technique. Ease of implementation high quality of solutions, computational efficiency and speed of convergence are strengths of PSO. PSO has been a popular technique used to solve optimization problems in WSNs due to its simplicity, high quality of solution, fast convergence and insignificant computational burden [9].It is used in mechanical designing, heating system planning problem.

IV. CONCLUSION

Black hole attacks in wireless can be prohibited using different protocols and optimization algorithms so that data can be securely transferred from source to destination. Black hole attack is a huge hazard to the security of mobile ad hoc networks. Various techniques have been discussed and each has its own significance. This paper provides a comprehensive review of the Ant Colony Optimization Technique. It is an iterative process technique. Ant Colony Optimization has been and continues to be a fruitful paradigm for designing effective combinatorial optimization solution algorithms. After more than ten years of studies, both its application effectiveness and its theoretical groundings have been demonstrated, making ACO one of the most successful paradigms in the met heuristic area.

V. 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] 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.

[4] Vennila, G., D. Arivazhagan, N. Manickasankari, "Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm," International Journal of Engineering and Technology (IJET),Vol. no. 6, pp. 0975-4024, Oct. 2014.

[5] Rao, DB Jagannadha, KarnamSreenu, and ParsiKalpana, "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks," International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, pp. 522-529, October 2012.

[6] Crosbie, Mark, Gene Spafford, "Applying genetic programming to intrusion detection," Working Notes for the AAAI Symposium on Genetic Programming. MIT, Cambridge, MA, USA: AAAI, 1995.

[7] Yih-Chun Hu, Perrig, A., Johnson, D.B., "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications, Vol.24, no.2, pp. 370-380, Feb. 2006.

[8] MarianneAzer, Sherif El-Kassas, Magdy El-Soudani Attacks, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole in wireless Ad Hoc Networks,"International Journal of Computer Science and Information Security, Vol. 1, no.1, May 2009.

[9] Saurabh, ShekharTandan, Praneet, "A PDRR based detection technique for black Hole attack in MANET," International Journal of Computer Science and Information Technologies, Vol. 2, pp. 1513-1516, 2011.

[10] Nath, Ira, Dr. RituparnaChaki, " BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, pp. 113-121,August 2012.

[11] Bhosle, Amol, TusharThosar, Snehal Mehatre, "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.

[12] Trupti Patel, Ch.Shyamala Rani, Mrs. Hina Patel, "Performance evaluation of DSR protocol under DoS attack," International Journal of Electronics and Computer Science Engineering, vol1, pp. 9-14, 2012.

[13] DeOca, Marco A. Montes, "A comparison of particle swarm optimization algorithms based on run-length distributions," Ant Colony Optimization and Swarm Intelligence.Springer Berlin Heidelberg, pp. 1-1, 2006.

[14] 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.

[15] Gulia, Preeti, SumitaSihag, "Review and Analysis of the Security Issues in MANET," International Journal of Computer Applications, Vol.75, No.8, pp. 23-26, Aug. 2013.

[16] Kalucha, Richa, Deepak Goyal, "A Review on Artificial Bee Colony in MANET," International Journal of Computer Science and Mobile Computing, Vol. 3, pg. 34-40, July 2014.

She is pursuing his Master's degree from Chandigarh Engineering College, Mohali, Punjab, India. She has completed his B.Tech Degree from SBBSIET, Jalandhar, Punjab, India. Her area of Interest includes Wireless Communication.

She has completed her Master's degree from Punjabi University, Patiala, Punjab, India. Currently, She is assistant professor at Chandigarh Engineering College, Mohali, Punjab, India. Her area of Interest includes Wireless Communication.