INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume3, Issue2)

Available online at www.ijariit.com

Black Hole Attack in Mobile ad Hoc Networks: A Review

Harsimran Kaur
Department of Computer Science,
Punjabi university, Punjab, India

Kamaljeet Mangat
Assistant Professor,
Department of Computer Science,
Punjabi university, Punjab, India

Abstract: Mobile ad hoc networks are widely used networks in the present times. The nodes in such network consist of laptops, mobile phones etc. These devices often have very important information in them. Security of these networks is very vital. These networks are prone to various kinds of attacks such as black hole attack, wormhole attack, DDoS attack etc. Out of many other attacks possible, black hole attack is pretty dangerous as it drops all the packets received by it. This paper presents various studies that have been done by many authors in the past regarding detection and prevention of such attacks.

Keywords: MANETs, Black Hole, Worm Hole, DDoS.

I. INTRODUCTION

MANETs have some special features such as unreliable wireless media or links used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery lifetime and computation power of nodes etc. where these characteristics are essential for the flexibility of MANETs these networks includes specific security concerns that may not be present in wired networks .Mobile ad-hoc networks often suffer from security attacks because of lack of trusted centralized authority, ambiguous nature of attacks inside the network, open medium, dynamic topology, resource limitation and multi-hop routing. Because the communication of MANET uses the open medium, an attacker can easily overhear message that is transmitted in the network. Due to the characteristics of MANETs, for instance, wireless connection and dynamic network and distributed network Mobile Ad Hoc Network are exposed to many security attacks like Wormhole attack, Packet Drop Attack, Black hole attack, Gray hole attack, Flooding attack, jellyfish attack, Sybil attack etc. Though, wireless networks are fully distributed and have the ability to work without the aid of any permanent infrastructure or access points.

MANETs lacks in central controlling entity due to this feature along with undefined and insecure boundaries make its security a very challenging issue. Black hole and gray hole attacks can in fact seriously compromise the performance of a critical infrastructure like a MANET. In MANETs, various kinds of attacks targeting the network layer have been identified and the most common types of attacks it deals with are Denial of Service attacks which compromise black hole attacks in it. These attacks breach the security by performing packet forwarding and routing misbehavior and cause a denial of service in MANETs. Black hole attack is also known as selfish node attack which is a dangerous active attack on the mobile Ad hoc Networks (MANETs), Selfish nodes resist resource to cooperate with each other in its presence. A Black hole node is a malevolent node that can inject itself into the path between the source and destination to fabricate packets from source and absorb network traffic by proclaiming to have shortest optimal path to desired destination node, which is fake shortest path and the packets received by the black hole node are dropped without having it to forward to destination node. Black hole attack attracts all packets by using forged RREP to falsely claiming a fresh and shortest route to the destination and then discards them without forwarding them to the destination. The malicious node may reply with the high sequence number so the sender node would think that the malicious node is a destination node or it has a fresh node to the destination. Mobile ad hoc networks routing protocols are often classified into three categories as Table-driven routing protocols also called as proactive protocols which maintain a continuous view of the network. On-demand protocols are also called reactive protocols which search for a route between source and destination. Hybrid routing protocols combine best features of table driven in case of intra-domain routing and demand routing protocol for inter-domain routing. The characteristics of MANETs make them susceptible to different types of attacks that occur in different layers of the network protocol stack.

This paper presents related work done by the various authors in past regarding detection or prevention of the black hole attack in the network.

II. LITERATURE SURVEY

T. Prasanna Venkatesan, P. Rajakumar, A. Pitchaikkannu et al. [1] In this paper, the authors have briefly explained on existing intrusion detection techniques in the context of MANETs. Since Intrusion prevention alone is not sufficient to achieve security in a network, it is presented a way to manage MANET security, by enhancing the existing secure protocols adding the component of Malicious nodes, not only in determining the route for sending packets, but also avoiding attempts of Denial of Service from Malicious Nodes. The accuracy of IDS can suffer from the high false positive or low false negative rates. If the majority of the mobile nodes are compromised, then the intrusion detection becomes fail. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, which may be addressed in future.

Payal N. Raj and Prashant B. Swedes et al. [2] proposed an approach DPRAODV (Detection, Prevention, and Reactive AODV) to prevent security threats of a black hole by notifying other nodes in the network of the incident. The simulation results in ns2 (ver-2.33) proves that the protocol proposed by the authors not only prevents Black hole attack but on the other hand improves the overall performance of (normal) AODV in presence of black hole attack.

Djamel Djenouri, Nadjib Badache et al. [3] propose a novel monitoring approach that overcomes some watchdog's shortcomings and improves the efficiency in detection. To overcome false detections due to nodes mobility and channel conditions the authors have proposed a Bayesian technique for the judgment, allowing node redemption before judgment. Finally, they have suggested a social-based approach for the detection approval and isolation of guilty nodes. The solution was analyzed and assess its performance by simulation. The results illustrate a large improvement of our monitoring solution in detection vs. the watchdog, and an efficiency through our judgment and isolation techniques as well.

Djamel Djenouri, Nadjib Badache et al. [4] this paper deals with the misbehavior nodes in mobile ad hoc networks (MANETs) that drop packets supposed to be relayed, whose objective may be either saving their resources or launching a DoS attack. It proposed a new solution to monitor, detect, and safely isolate such misbehaving nodes, structured around five modules: (i) The monitor, responsible for controlling the forwarding of packets, (ii) the detector, which is in charge of detecting the misbehaving of monitored nodes, (iii) the isolator, basically responsible for isolating misbehaving nodes detected by the detector, (iv) the investigator, which investigates accusations before testifying when the node has not enough experience with the accused, and (v) finally the witness module that responds to witness requests of the isolator. These modules are based on new approaches, aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead.

Satyendra Tiwari, Anurag Jain and Gajendra Singh Chowhan et al. [5] proposed a modified ack-based scheme for decision ambiguity for a requested node on the basis of finite state machine. The finite state machine is an automaton of the theory of computation here the authors have used deterministic finite automata for the decision making of the node and improved node authentication and minimize packet dropping in ad hoc network.

K. Selvavinayaki, DR. E. Karthikeyan et al. [6] To reduce the effect of black hole attack, a New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to detect the black hole nodes and to ensure the data confidentiality, data integrity and authenticity has been proposed. In the first phase of the proposed algorithm, the detection of black hole attack is achieved using trust active and recommendation of the nodes. In the second phase of the work, Enhanced Proactive secret sharing scheme is used to provide the data authentication and integrity. The simulation results show the proposed algorithm achieves the better packet delivery ratio, misbehavior detection efficiency, fewer packets overhead and low end to end delay than the existing schemes.

Akshat Jain, Shekher Singh Sengar & Vikas Goel et al. [7] This paper proposed a method to detect colluding black hole nodes in Ad hoc On-Demand Distance Vector (AODV) routing protocol. A Light Weight Packet (LWP) routing mechanism is devised. LWP is digitally signed up by the sender. Also, the concept of the authentic table for neighbors is used to detect whether the neighbor is authentic or not. The further work can be done to evaluate the simulation result of proposed algorithm and compare it with existing solutions for optimality.

Bobby Sharma Kakoty et al. [8] In this work it is observed that presence of Blackhole node in MANETs, drastically changes the network performance in terms of higher loss in packets as well as generating lower throughput. It is very difficult to apply traditional attack prevention schemes such as cryptographic technique or general authentication technique due to dynamically changing topology with decentralized node distribution.

Hicham Zougagh, Ahmed Toumanari, Rachid Latif, Y. Noureddine. Inbounder et al. [9] This paper proposed a cooperative black hole attack against MANETs exploiting vulnerabilities of OLSR. In this attack, two attacking nodes cooperate in order to disrupt the topology discovery and prevent routes to a target node from being established in the network.

Abderrahmane Baadache, Ali Belmehdi et al. [10] In this paper, after having specified the black hole attack, a secure mechanism, which consists of checking the good forwarding of packets by an intermediate node, was proposed. The proposed solution avoids

the black hole and the cooperative black hole attacks. Evaluation metrics were considered in simulation to show the effectiveness of the suggested solution.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto et al. [11] This research paper proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently. The simulation results show the effectiveness of our scheme compared with conventional scheme.

Jian-Ming Chang et. al [12] proposed a bait detection scheme to detect black hole attacks in MANETs. In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes that nodes should cooperate with each other. In the presence of malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious node launching gray hole or collaborative black hole attacks is a challenge. This paper has attempted to resolve this issue by designing dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious code attacks, the CBDS outperforms the DSR, 2ACK, and best-effortful-tolerant routing (BFTR) protocols (chosen as benchmarks)in terms of packet delivery ratio and routing overhead (chosen performance metrics).

REFERENCES

[1] T. Prasanna Venkatesan, P. Rajakumar, A. Pitchaikkannu, "An Effective Intrusion Detection System for MANETs" International Journal of Computer Applications® (IJCA) (0975 – 8887) International Conference on Advances in Computer Engineering & Applications (ICACEA-2014) at IMSEC, GZB.

[2] Payal N. Raj and Prashant B. Swades, "DPRAODV: A Dynamic Learning System Against Black Hole Attack in AODV Based MANET" IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[3] Djamel Djenouri, Nadjib Badache, "Struggling Against Selfishness and Black Hole Attacks in MANETs", wireless communication Mobile computing. (WCMC) 8 (6) (2008)689-704.

[4] Djamel Djenouri, Nadjib Badache, "On eliminating packet droppers in MANET: A modular solution" Ad Hoc Networks 7 (2009) 1243–1258, Available online at www.sciencedirect.com.

[5] Satyendra Tiwari, Anurag Jain and Gajendra Singh Chowhan, "Migrating Packet Dropping in Ad hoc Network Based on Modified ACK based Scheme Using FSA" International Journal on Emerging Technologies **2**(2): 102-105(2011).

[6] K.Selvavinayaki, Dr. E. Karthikeyan, "A secured data transmission method using enhanced proactive secret sharing scheme to prevent black hole attacks in MANETS" Journal of Theoretical and Applied Information Technology 30th September 2014. Vol. 67 No.3.

[7]Akshat Jain, Shekhar Singh Sengar & Vikas Goel, "Colluding Black Holes Detection in MANET" International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 1, January- 2013 ISSN: 2278-0181.

[8] Bobby Sharma Kakoty, **"**Simulation and Analysis of Black Hole Attack in MANETs for Performance Evaluation**"** International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 1 January 2013.

[9] Hicham Zougagh, Ahmed Toumanari, Rachid Latif, Y. Noureddine. Idboufker, "Discovering a Secure Path in MANET by Avoiding Black Hole Attack" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 8, 2014.

[10] Abderrahmane Baadache, Ali Belmehdi, **"**Avoiding Blackhole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks**"** (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[11] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto**, "**Detecting Black Hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method**"** International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[12] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks byMalicious Nodes in MANETs: A Cooperative BaitDetection Approach", IEEE SYSTEMS JOURNAL, VOL. 9, NO. 1, MARCH 2015.

