Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on Effects of Black Hole Attacks in Mobile Ad hoc Networks

Kamaluddeen Ibrahim Yarima, Aparajita Nailwal, Aliyu Ashiru
Depat of computer Science & Engineering,
Sharda University, Greater Noida,
Uttar Pradesh, India

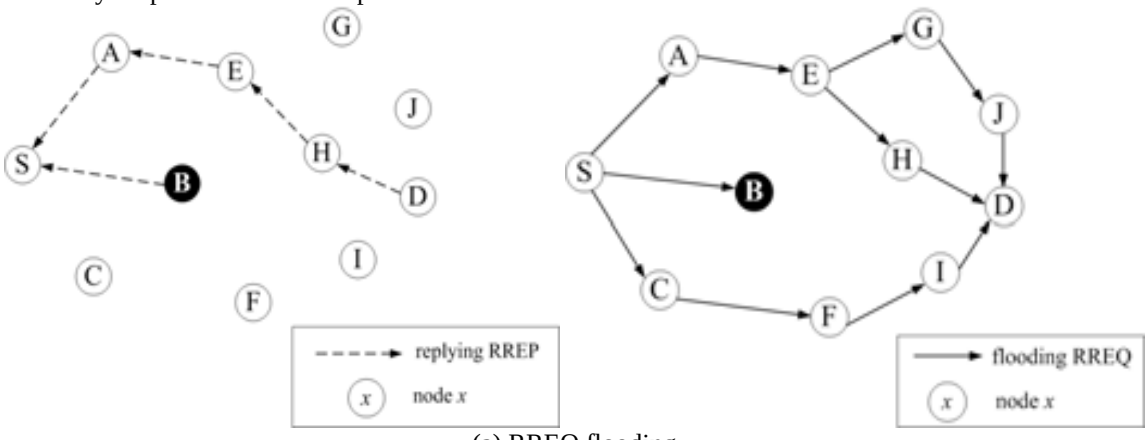
Abstract- Black hole attack this is one of the known security threats/issues in Mobile Ad hoc Networks. The malicious node uses the loophole to carry out their malicious behaviours due to necessity of route discovery process in Mobile Ad hoc Networks Many researches have been conducted using different detection techniques to propose so many types of detection schemes. In this paper, we survey the existing solutions at hand and discuss the state-of-the-art routing methods. We intend to classify these proposals into single black hole attack and collaborative black hole attack and also analyse the categories of these solutions and provide a comparison table.

Keywords: mobile ad hoc networks, routing protocols, single black hole attack, colla- borative black hole attack.

I. INTRODUCTION

The currently available routing protocols for MANETs are mainly categorised into proactive routing protocols and reactive routing protocols. In a proactive routing protocol, every node proactively searches for routes to other nodes, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up-to-date and correct, such as DSDV (Destination Sequence Distance Vector) [1] and OLSR (Optimized Link State Routing Protocol) [2]. In a reactive routing protocol, a route is searched and established only when two nodes intend to transfer data; and therefore, it is also called an on-demand routing protocol, such as AODV (Ad hoc On-Demand Distance Vector) [3] or DSR (Dynamic Source Routing) [4]. A source node generally broadcasts a route request message to the entire network by means of flooding, in order to search for and establish a route to the destination node. The AODV [3] is the most popular routing protocol and has been extensively discussed in research papers; therefore, this study deploys and evaluates the proposed IDSs on AODV-based MANETs.

A black hole attack can be achieved by a single node or by several nodes in collusion. A single-node black hole attack forges the sequence number and hop count of a routing message in order to forcibly acquire the route, and then eavesdrop or drop all data packets that pass. Figure 1 depicts the behavior of a black hole attack, wherein source node S is intended to establish a route to destination node D. In an AODV [3] routing protocol, node S would broadcast a Route Request (RREQ) packet to search for destination node D; the normal intermediate nodes would receive and continuouslybroadcast the RREQ, rather than the black hole node. As shown in Figure 1(a), the black hole node would directly reply through an RREP with an extremely large sequence number and hop count of 1 to source node S. When receiving RREQs from normal nodes, the destination node D would also select a route with a minimal hop count, and then, return a Route Reply (RREP) packet, as shown in Figure 1(b). According to the AODV design, a source node would select the latest (largest sequence number) and shortest route (minimal hop count) to send data packets upon receipt of several RREPs packets. Thus, a route via a black hole node would be selected by node S. The black hole node will then eavesdrop, or directly drop the received data packets.



(a) RREQ flooding

Figure 1 Diagram of a black hole attack

Black hole attacks have serious impact on routing algorithms, which uses sequence numbers to determine whether a message is fresh, and selects the shortest route of minimum hops, such as AODV [3] or DSR [4]. Some of related researches can be found in [5, 6, 7]. In this paper, IDS nodes are deployed in MANETs to identify and isolate black hole nodes. An IDS node observes every node's number of broadcasted RREQs, and the number of forwarding RREQs in AODV, in order to judge if any malicious nodes are within its transmission range. Once a black hole node is identified, the IDS node will send a block message through the MANET to isolate the malicious node. The remainder of this paper is organized as follows. Section 2 describes the AODV routing protocol; Section 3 presents the implementation of IDS nodes; Section 4 discusses the experimental data and analysis of ns2; and conclusions are given in Section 5.

II. ROUTING PROTOCOLS IN MANETS

Routing is the process of information exchange from one host to the other host in a network [4]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialised router itself [3].
DifferentStrategies:
Routing protocol for ad-hoc network can be categorized in three strategies.
A) Pro-activerouting protocol. B) Re-activerouting protocol. C) Hybrid protocols

A. Proactive (table-driven) Routing Protocol

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbor's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol [5] and Optimized link state routing (OLSR) protocol [6].

B. Reactive (on-demand) Routing Protocol

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compareto the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: - Ad hoc on-demand distance vector (AODV) [7] and Dynamic source routing (DSR) [8] protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [9] and Temporally-ordered routing algorithm (TORA) [10].

III. ROUTING IN MANETS WITH AND WITHOUT BLACK HOLE

Generally routing in MANET is done either by table driven routing protocol or ad hoc on demand distance vector routing protocol. In case of table driven process, each and every node in MANETs maintains some up-to-date information about the network. Every node has the information about latest network topology, any changes happened to the network is generally propagated to the network, accordingly node updates their routing table .But this kind of protocol creates several problems to the network in terms of bandwidth overhead, wastage of battery power of the nodes, entry of unnecessary redundant route etc. Due to these difficulties, ad hoc on demand distance vector (AODV) routing protocol is preferred. In this protocol, routing tables are dynamically created when needed. So, whenever source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When destination sends a RREP packet to source throughshortest path, the source sends data through this path. Though it looks very simple, but this kind of protocol suffers from several vulnerabilities of attack. If the path cannot be established then RERR messages is generated. AODV protocol is very much acquainted with dynamic network condition, low processing and memory overleaf, less bandwidth wastage with small control messages. Due to these kinds of reasons AODV becomes one of the most popular protocols in MANETs. Whenever a RREQ packet is generated by the source, every node that receives the RREQ packet will check whether this packet is meant for them or not. If so, immediately they will generate RREP message, otherwise every node tries to forward the packet to their neighbor to reach destination, if their routing table doesn't contain valid entry to destination. If the routing table contains valid entry to destination then next step is to check the destination sequence number. Usually destination sequence number is maintained by every node. Its value depends on network traffic and participation of node in packet forwarding. If the destination sequence number is same for more than one RREP then it goes for the specific path where number of hops to reach destination is lesser. Thus higher the se-

quence number implies the fresh route to destination. In case if the source receives multiple RREP then it decides the path where sequence number is higher

IV. BALACK HOLE ATTACK IN MANET

Attacks on MANETs can be divided into two categories, passive and active attacks. An active attack alters the operation of networks by modifying and interrupting data. A passive attack does not disturb the operation of networks.
In black hole attack, black hole node acts like black hole in the universe. In this attack black hole node absorbs all the Here we assume that if nodes are in their vicinity, they can traffic towards itself and doesn't forward to other nodes. Whenever, source node wants to send packet to the destination important issue. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node. Two types of black hole attack can be described in order to distinguish the kind of black hole Attack

A) Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

B) External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.
External black hole attack can be summarized in following points

a.) Malicious node detects the active route and notes the destination address.
b.) Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
c.) Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
d.) The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
e.) The new information received in the route reply will allow the source node to update its routing table.
f.) New route selected by source node for selecting data.
g.) The malicious node will drop now all the data to which it belong in the route

V. RELATED WORK

A number of researches are being carried for enhancing the security in Manet. Since there is no particular line of defense, security for manet is still a major concern for man. Some of the researches for the detection of black hole attack are given. W. Kozma, and L.Lazos,"REAct: resource-efficient for node misbehaviour in ad hoc networks based on random audits," [3] Based on Audit Procedure. When destination node detects a heavy packet drop, it triggers the source node to initiate the audit procedure. Source node chooses an audit node and it generates behavioral proof. Similarly source node prepares it behavioural proof .On the basis of comparison of results malicious nodes are detected. Drawback was that it is a reactive approach .Only if there is a drop in packet delivery ratio, the mechanism is triggered. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," [4] Introduced the concept of route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack in AODV. The intermediate node along with RREPs sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node checks in its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. It was dependent on the intermediate nodes reply. Also it was able to detect only single black hole.W. Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," [5] Introduced the approach of hash based function in REAct system. Enabled the data traffic and forward path detail available in behavioral proof. Upon drop in the packet delivery ratio initiates the blackhole detection. Based on the reactive detection.

CORRELATION OF VARIOUS SOLUTIONS TO BLACK HOLE ATTACK

The table below shows the comparisons between various solutions
to black hole attack.

Technique proposed	Technique	Type of Black hole Attack	Merits	Demerits	Routing Protocol
Payal N. Raj1 And Prashat B Swadas2, 2008	Compares The RREP Sequence numbers with threshold value using dynamic learning method	Single And multiple black hole	Increases PDR With Minimum Increase in Average end-to-end delay	Higher Routing overhead and can't detect cooperative black holes	AODV
Y.Zhang And W.Lee,200 0	Introduces the CREQ and CREP to avoid black hole	Single Black hole	Low cost	Time delay and false positives	AODV
Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Nov. 2007	A New detection method based on dynamically updated training data.	Single Black hole	Detection rate And false positive rate improve	Network delay	AODV
Ming-Yang Su; Kun- Lin Chiang; Wei-Cheng Liao, Sept. 2010	An Anti- Black Hole Mechanism (ABM) using IDS	Multiple black holes	High detection rate	Time delay	AODV

VI. CONCLUSION AND FUTURE WORK

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem. In this paper, we first summaryised the pros and cons with popular routing protocol in wireless mobile ad hoc networks. Then, the state-of- the-art routing methods of existing solutions is categorised and discussed. The pro- posals are presented in a chronological order and divided into single black hole and collaborative black hole attack.

According to this work, we observe that both of proactive routing and reactive rout- ing have specialised skills. The proactive detection method has the better packet deliv- ery ratio and correct detection probability, but suffered from the higher routing overhead due to the periodically broadcast packets. The reactive detection method eliminates the routing overhead problem from the event-driven way, but suffered from some packet loss in the beginning of routing procedure. Therefore, we recommend that a hybrid detection method which combined the advantages of proactive routing with reactive routing is the tendency to future research direction. However, we also discover that the attacker's misbehavior action is the key factor. The attackers are able to avoid the detection mechanism, no matter what kinds of routing detection used. Accordingly, some key encryption methods or hash-based methods are exploited to solve this problem. The black hole problem is still an active research area. This paper will benefit more researchers to realize the current status rapidly.

ACKNOWLEDGEMENT

Our thanks to the faculties of Department of Computer Science, Sharda University who have contributed towards development of this paper survey. The constant guidance and encouragement received from Ms. Aparajita Mathpal, Fatima Kamal Dambatta and Prof. Ishan Ranjan, Head of department CSE Sharda University.

REFERENCES

[1] S. R. Murthy and B .S .Manoj,‖ Ad Hoc Wireless Networks‖, Pearson Education, 2008.

[2] Y. Xiao, X. Shen, and D.-Z. Du,‖ A Survey on Intrusion Detection in Mobile Ad Networks‖, pp. 170 – 196 °c 2006 Springer.

[3] Amit Shrivastava, Aravinth Raj Shanmogavel, Avinash Mistry , Nitin Chander ,Prashanth Patlolla, Vivek Yadlapalli ―Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols‖.

[4] Humayun Bakht, ―Computing Unplugged, Wireless infrastructure, Some Applications of MANET‖, issue200410/00001395001.html, April-2003.

[5] Perkins CE, Bhagwat P (1994),‖Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers‖, Paper presented at the ACM SIGCOMM'94 Conference, London, United Kingdom, August 31- September 2, 1994.

[7] Perkins CE, Royer EM (1999),‖Ad-hoc On-Demand Distance Vector Routing‖, Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25-26 February 1999.

[8] Johnson DB, Maltz DA (1996),‖Dynamic Source Routing in Ad Hoc Wireless Networks‖, In: Imielinski T, Korth H (eds) Mobile Computing, Vol 353. Kluwer Academic Publishers, pp. 153–181.

[9] Haas ZJ, Pearlman MR, Samar P (2002),‖ The zone routing protocol (ZRP) for ad hoc networks‖, IETF Internet Draft.

[10] Park V, Corson S (1998),‖ Temporally-Ordered Routing Algorithm (TORA)‖, Version 1 Functional Specification. Internet Draft, Internet Engineering Task Force MANET Working Group.

