International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 02 - Issue 07 || July 2016 || PP. 07-11

A SURVEY OF BAIT DETECTION SCHEMES IN MANET

Ashwini S. Barote[1], Dr. P. M. Jawandhiya[2]
1(Department of Computer Science and Engineering, Amravati University, Buldana-Maharashtra-India)
2(Department of Computer Science and Engineering, Amravati University, Buldana-Maharashtra-India)

ABSTRACT: This paper focus on study of MANET and bait detection schemes in MANET. In mobile ad-hoc networks (MANETs) the main problem is security as well as formation of communication range among nodes. A primary requirement for establishment of communication range among nodes is, nodes should cooperate with each other. Avoiding or sensing malicious nodes initiating attacks is the main challenge. In this paper we focus a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures. In this paper, we survey innovated techniques to detect selfish nodes for MANETs.
KEYWORDS: MANET, CBDS, DSR, BFTR, RREP,RREQ .

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring communications less network of mobile devices connected by wireless links, each device is free to move independently in any direction, and hence will change its link with other devices frequently. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network [8]. Moreover, ad hoc networks can also perform multi-hop wireless networks. In this way, ad-hoc networks have a dynamic topology such that nodes are mobile in nature, so that they can easily join or leave the network at any time.The mobile ad hoc network is shown in following figure 1.

Fig. 1 The mobile ad-hoc network.

1.1Application of MANET

Some Applications areas of MANET are as follows

1.1.1 Military battlefield

MANET is to maintain an information network between the soldiers, vehicles, and military information head quarter.

1.1.2 Collaborative work

For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

1.1.3 Personal area network and bluetooth

A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

1.1.4 Commercial Sector

Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

2. TYPES OF ATTACK IN MANET

The primary goal of Mobile ad hoc network is each device to continuously maintain the information required to properly route traffic. These networks are highly susceptible to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks).

2.1 Black hole: A black hole means that the malicious node exploits the routing protocol to claim that it has the shortest path to the destination node, it does not forward packets to its neighbors instead it drops the packets. The main issue is that the PDR decreases. There are two types of blackhole attacks-

a. Single blackhole attack**:** In single blackhole attack only one malicious node attack on the root.

b. Collaborative Black hole: Collaborative blackhole attack means malicious nodes act in a group.

2.2 Gray hole: A Gray hole attack is tougher to detect because nodes can drop packets partially due to its malicious nature or due to overload, congestion and selfish nature of the nodes which are involved in the routing process.

3. CBDS
(A COOPERATIVE BAIT DETECTION SCHEME TO PREVENT MALICIOUS NODE FOR MANET BASED ON HYBRID DEFENSE ARCHITECTURE)

This paper proposed a malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes causing black or gray hole attacks and cooperative attacks. It merges the proactive and reactive defense structure, and the source node randomly establishing cooperation with the adjacent node. Using the address of the adjacent node as the destination bait address, it baits malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again, which can achieve the capability of maintenance and immediately reactive response.

With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results the rapid development of the technology. Due to MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to use in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention. The common routing protocols in current such as DSR AODV and so on almost take account in performance. They don't have the related mechanism about detection and response. Aiming at the possible attacks by malicious nodes, based on the DSR protocol, this paper presented a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS).

3.1 Dynamic source routing in ad hoc wireless networks

DSR routing protocol is an on demand destination routing protocol where an accumulated node of the routes, including those destination routes known by the node, are stored. Here, the data entered to the route accumulation revealing new information about the current routes, are updated. Two main phases of this protocol are discovery and maintenance of the route. Once the source node wants to transmit a packet to the destination node, it scans its route hoard to determine whether it needs a route to destination or not. If there exists an appropriate route to destination, it uses the given route in packet transmission. On the other hand, if there not such a route, it initiates the route discovery process through packet distribution. When RREQ process is sent, the node waits for RREP and once the RREPs come from the nodes, it responses to the first arrived RREP. The node sends packets with this RREP, this route to its route cache and then starts to send data packets using the route included in the packet which in turn leads to ignoring other REEPs. Such a process leads to ignoring the security or insecurity of the route.

4. TECHNIQUES FOR MALICIOUS NODE DETECTION

4.1 Neighborhood-based and routing recovery scheme

The detection scheme used neighborhood-based method to detect the black hole attack. It present a routing recovery protocol to build the true path to the destination. A method is designed to deal with the black hole attack based on the neighbor set information, which consists of two parts: detection and response.

1. The detection procedure includes two major steps:
   - Collect neighbor set information.
   - Determine whether there exists a black hole attack.
2. In Response procedure

In response procedure source node sends a Modify-Route-Entry (MRE) control packet to the destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.
Advantages: This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network.
Disadvantages: It become useless when the attacker agrees to forge the fake replay packets.

4.2 Time-based threshold detection scheme

This techniquebased on an enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named Collect Route Reply Table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.
Advantages: The simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead.
Disadvantages: The end-to-end delay might be raised visibly when the malicious node is away from the source node.

4.3 Random two-hop ack

This solution deals with all kinds of packet droppers, including as well selfish as malicious nodes launching a black hole attack. It also deals with any Byzantine attack involving packet dropping in any of its steps. This solution detects the attacker when it drops packets. The simulation results show that the random two-hop ACK is as efficient as the ordinary two-hop ACK in high true and low false detection, while hugely reducing the overhead. It might be failed if there are multiple malicious nodes.

4.4 Detection, prevention and reactive AODV (DPRAODV) scheme

In DPRAODV an additional check is done to find whether the RREP_seq_no value is higher than the threshold value as compared to normal AODV. If the RREP_seq_no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again.
Advantage: The simulation result shows that the packet delivery ratio is improved as compared to AODV.
Disadvantage: The routing overhead and end-to-end delay is little bit increased. And it fails with cooperative black hole attacks.

4.5 Redundant route method and unique sequence number scheme

Redundant Routetechnique is to find at least two routes from the source to the destination node. Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP packets and after identifying a safe route it transmit the buffered packets. It represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not.

Advantages: Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV. Second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.
Disadvantages: These both techniques fail to detect cooperative black hole attacks.

4. CONCLUSION

In an attempt to find a lasting solution to the security challenges in MANETs, various researchers have proposed different solutions for various security issues in MANETs. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for MANETs is still a major concern. My approach is based on using cooperative bait detection scheme to detect and prevent malicious nodes attack in MANETs. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs with there defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads. The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Therefore, we suggest having a hybrid detection technique which combines the advantages of both reactive and proactive routing for future research direction.

REFERENCES

[1]. Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.
[2]. Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol. 3, ISSN 2151-9617, January 2011.
[3]. Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen, "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture", IEEE, 2011
[4]. P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
[5]. A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.
[6]. Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
[7]. Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACMSE'42), Huntsville, Alabama, 2-3 April 2004.
[8]. Tamilselvan L, Sankaranarayanan V, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 2730 August 2007.
[9]. Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.
[10]. Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.
[11]. Himani Yadav, Rkesh Kumar, "A Review on Black Hole Attack in MANETs", International Journal of Engineering Research and Applications (IJERA) Vol.2 Issue 3, pp.1126-1131 Mayy-Jun 2012.
[12]. Shahram Behzad, Shahram Jamali, Morteza Analoui, "A Survey over Black Hole Attack Detection in Mobile Ad Hoc Network", International Journal of Computer Science and Network Solutions, Vol 2.No.5 May.2014
[13]. Nidhi Gupta, Sanjoy Das, Khushal Singh, "A Comprehensive Survey and Comparative Analysis of Black Hole Attack in mobile ad-hoc network", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.8, no.1, 2014.
[14]. Chandni Garg, Preeti Sharma, Prashant Rewagade ,"A Literature Survey of Black Hole Attack on AODV Routing Protocol", International Journal of Advancement in Electrical and Computer Engineering (IJAECE) Vol 1, Issue 6, pp.152.157 Sep 2012.

Authors:

Miss. Ashwini S. Barote Student of Second year M.E. (Computer Science and Engineering) Pankaj Laddhad Institute of Technology and Management Studies, Buldana Sant Gadge Baba Amravati University. Has earned degree of B.E (Computer Science and Engineering) from Sant Gadge Baba Amravati University in 2014.

Dr. P. M. Jawandhiya, Principal, (Computer Science and Engineering) Pankaj Laddhad Institute of Technology and Management Studies, Buldana Sant Gadge Baba Amravati University. Has earned degree of B.E (Computer Engineering), M.E. (Computer Sci. & Engg.), Ph.D. in Engg. & Tech. (Computer Sci. & Engg.), M.B.A. (Human Resource & Management)