DETECTING AND PREVENTING BLACK HOLE ATTACKS IN MANETS USING CBDS (Cooperative Bait Detection Scheme)

A.Agalya[1] ,C.Nandini[2] , S. Sridevi[3]

PG Scholar[1, 2],Assistant Professor[3]
Department of CSE,Vels University,Pallavaram,Chennai.

Abstract - In MANET, a major necessity to distribute the communication between nodes is that each node should work along with each other [1]. This communication could face many obstacles created by adversary resulting in disconnection [1]. To overcome this problem a new mechanism based on dynamic source routing (DSR) which could be mentioned as cooperative bait detection scheme (CBDS). It merges the favors of both proactive and reactive protection phenomena. This method performs a reverse tracing technique which aids in accomplishing the desire [1]. As a result CBDS perform better than the existing method which includes the DSR and 2ACK protocols with regard to packet delivery ratio and routing overhead.

Index Teams-Black hole attacks, gray hole attack, cooperative bait detection scheme (CBDS), mobile ad hoc network (MANET), malicious node

1. INTRODUCTION

Mobile ad hoc networks (MANETS) play a vital role in networks. In wireless network there may be a serious security issue. The network is decentralized, where discovering the topology and delivery of messages must be executed by the node itself. A MANET is a kind of ad hoc network that can use different location and configure itself in air. The applications for network in MANETs are separate, to large scale, mobile, highly dynamic network.

There is less security in MANET, it is used in military operations and traffic control in networks.In MANET there is no infrastructure, on-demand, dynamic topology. The node is the mobile network, so it is difficult to identify the hacker node. The routing process may disrupt due to the collaboration attacks by malicious node in MANET. The malicious node may cause security problems like gray hole and collaborative black hole attacks. Many research people say about the prevention and detection of MANET. Due to the dynamic topology the mobile nodes will face several attacks. The most frequent attacks are black hole and gray hole attacks.

There are two types of attacks in MANET. They are active attack (black hole) and passive attack (gray hole).

Black hole attack is defined as if a source is going to send a data in the mobile ad hoc network its sends through several nodes to reach the destination. The black hole establishes the information to source that it has the shortest path to the destination. The hacker node will attract all the data packets by using fake route reply (RREP) to make shortest route for the destination. The black hole attack is also known as active attack. The gray hole attack which is called as passive attack at first it acts like good node later it behave as malicious node. This is also called as trust based security solution. It does both forwarding and discarding the packets, the gray hole attack is very tough to find in initial stage.

These attacks can be resolved by dynamic source routing protocol based on cooperative bait detection scheme.

2. EMPIRICAL WORK

- In 2010[2] avoiding black hole attacks in wireless ad hoc network is proposed. The node which is the middle forwarding will act as hacker and leaks the data packet which passes through it, without forwarding them to the following node, this process is called black hole attack. A secure mechanism is found which checks the good forwarding of data packets by the malicious node. The merkle tree is as the secured principle for avoiding the black hole attacks and cooperative black hole attacks.

- In March 2011[3] CBDS in hybrid defense architecture is established. The protocol in present AODV, DSR nearly take account in execution. It doesn't have the similar mechanism in finding and response. A technique to find hacker node introducing cooperative black hole attacks and black/gray hole attacks is called as cooperative bait detection scheme (CBDS). It merges the proactive and reactive architectures, and stochastically works with random adjacent node. By using the address of the neighbor node as the bait destination address and finds the malicious node by reverse tracing program and consequently prevent the attacks.

- In 2010[4] to detect and remove black/gray hole attack in mobile network is published. At first the source node need to make the packet transmission, so it ask the nearest node for Blocked IP (BIP). The nearest node will get the BIP response to the source node from the unknown IP addresses. The reply RREP is send to both BIP and destination continuously. If the source node gets reply from the normal destination, it means there is no black hole in the path. When source node gets reply from the BIP, it says Black hole attacks are present in the path. Finally the source finds the black hole in the route. After finding the black hole attack, source node sends the dummy data to the destination. The nearby node finds the packet drops and it informs the source node. Here the algorithm finds the location of black hole.

- In September 2009 [5] to prevent collaborative pack drop attacks in ad hoc network is introduced. The hash function based mechanism is used for finding packet drops in the network. It holds the knowledge from packet traffic and data forwarding routes. The above method is opposed to the collaborative attacks. To inquire the security of the proposed mechanism and diminish the overhead.

- In 2009[6] REAct is stated. This study reported the difficulty of finding the group of improper nodes which rejects the data packets without forwarding them to destination. To overcome the above problem the method called REAct is introduced. REAct finds malicious node by the number of random audit mechanism on execution drop. A source node and destination can able to find malicious node by using REAct mechanism based on proofs. A Proof is made by using bloom filters and it reduces the communication overhead problem for malicious node detection.

3. COMPARISON OF DSR AND TCP/IP PROTOCOLS

A. TCP PROTOCOL:

Transfer Control Protocol is very popular used commonly in the internet. There are four layers in TCP protocol

Application layer
Host-to-host layer
Internet layer
Network access layer

The network layer is in charge for sending and receiving TCP data packets in the network. The network layer does the work of datalink layer and physical layer which is presented in the OSI model. The internet layer is responsible for packing the data, addressing and routing the packets to the destination. In host-to-host layer the data packets are transported and deliver them to the application layer. The transport layer is used for transporting and sequencing the packets in the network. Finally it recovers the data packets from the source.

Limitation:

- In MANETs, frequent wireless network errors and mobility leads to packet losses as well as congestion
- Due to link failure 80% of packet loss will occur.
- Most of the packet losses in ad hoc are because of path failure.

To overcome the above limitation we are going for the technique called **DSR** (dynamic source routing technique).

B. DSR PROTOCOL:

Dynamic routing protocol is defined as if the source node wants to send the data to the destination, it doesn't know the path for source node S to the destination node D [1]. The source sends the route request (RREQ) to the entire node which is in the network [1]. The source will get route response (RREP) from each and every node in the network with the source address, destination address and unique route request id (RREQ).
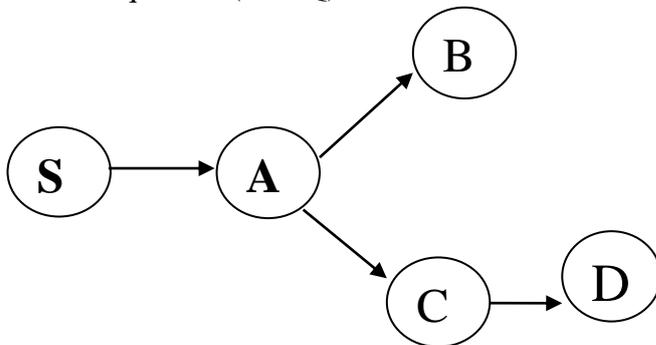
In the above diagram S is the source A, B, C, are the nodes in the network and D is the destination. Source sends the RREQ to all nodes and gets RREP from the destination. The node S does not sure to find which node in the network has the path information [1] to the node D or the hacker node reply fake RREP. From above content the source node S will send data packets through the malicious path chosen by the hacker node [1]. Which is called as black hole attack, to overcome this CBDS algorithm is proposed.

4. COMPARISON OF 2ACK SCHEME WITH CBDS ALGORITHM

A. 2ACK SCHEME:

The 2ACK scheme is used to reduce the hacker's effect in malicious node [7]. The general theme of 2ACK algorithm is, if the source node S sends the packets to its neighbor hop successfully, the destination node D of neighbor choose to send a unique two-hop acknowledgement is called 2ACK to specify that the packets received successfully [7]. The 2ACK transmission is used for only a few data packet transmission. The certain node behavior id identified after watching its activity for a few hours [7].

The 2ACK scheme is to find the adversary node which is suppose to forward the data packets from the source node but it oppose to do so when the data packets arrived [7]. The 2ACK will monitor and transmits only when the routing performance is very low and it has very well authentication to check the packets are genuine [7]. The main drawback is, 2ACK scheme is a proactive method to find the malicious nodes.

B. CBDS ALGORITHM:

Initially the detection mechanism is of two types, they are proactive and reactive.

Proactive: proactive mechanism is to find and prevent the network from the malicious node in initial stage [1].

Reactive: reactive mechanism is to detect that node which will be active only after the destination node finds a packet drop in the packet delivery ratio [1].

Cooperative Bait Detection Scheme is used for preventing and detecting the black hole/gray hole attacks [1]. A black hole attack is defined as if the source node wants to send the data packets to the destination, it losses the data packets before forwarding to the destination [1]. The gray hole is nothing but, initially the node act as the good node, after few minutes it changed into malicious node [1]. By using the CBDS algorithm, at first the source node will select the neighbor node with the cooperation of that node [1]. The address of the selected node is known as bait destination address to trap the malicious node to send a request reply message [1]. By using tracing technique the adversary node is detected and prevented [1]. If any packet drop occurs in the packet delivery ratio, an alarm is send to the source node by the destination node to activate the detection mechanism [1]. The CBDS scheme combines the proactive scheme to find the malicious node in the initial stage and reactive mechanism to find the adversary node later in the network.

5. BASIC IDEA OF THE SYSTEM

Initially the source S choose the cooperative bait address of the one hop neighbor node Nr to detect the malicious node and [1] sends the RREQ to all the nodes in the ad hoc network [1]. If there is no reply from any of the in the network means there is no malicious node in the network. Suppose the source node gets RREP from any node in the network, it triggers the reverse tracing program and sends test packets, recheck message to detect the malicious node in the MANET [1]. The source node lists the malicious node in the black hole attack and sends the alarm packet.

In another case source node sends RREQ to the nodes in MANET [1], if it gets the reply RREP from the original destination address then the system does not contain any adversary it is free from malicious node [1]. Suppose the reply RREP is not from the true destination address, then it exceeds the new hop limit.

6. CONCLUSION

Finally the new technique cooperative bait detection scheme is used in this paper to overcome the gray hole and black hole attacks. The CBDS algorithm is merges to types of detection mechanism namely proactive and reactive.

7. FUTURE WORK

 Basically in normal ad hoc network route selection will be select by source node only, in case any hacker can be enter the network in hidden way,. It is too difficult to find. So in this proposed system destination node will take a charge of finding hacker even it be a hidden hacker.

After finding the route, source node will send a originating message to their neighbor nodes. Neighbor nodes will check the activities of its neighbor node. If there is any misbehavior activities found the node will send the hacker details to destination node.

Finally destination node will check the particular node is in available on selected path, if it is true it will trigger source node for finding different route, otherwise it will select the same path for data forwarding.

REFERENCE

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" in proc IEEE journal, 2014, pp. 1–11.

[2] 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.

[3] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks,"in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[4] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[5] W. Wang, B. Bhargava, and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[6] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, 2009, pp. 103–110.

[7] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," in Proc. IEEE Tran., in Mobile Computing MAY 2007.