Detection and Recovery of Packet Drop under Network Layer Attack in MANET

C. Deepika Shiny*, I. Muthumani
Department of Electronic and Communication Engineering, ACCET, Karaikudi, India

Article Info
Article history:
Received 12 February 2015
Received in revised form
20 February 2015
Accepted 28 February 2015
Available online 6 March 2015

Keywords
Mobile Ad-hoc Network,
Dynamic Source Routing Protocol,
Cooperative Bait Detection Scheme,
Black Hole attack,
Packet Delivery Fraction

Abstract
Mobile Ad-hoc Network is a wireless temporary network setup by mobile nodes. In MANET each node works both as host and also as router. As it is an infrastructure less network the malicious nodes will disturb the Routing process. The malicious activities will give rise to layer attacks. One of the attacks is black hole attack in which the malicious behavior affects the data packets which is sent to the destination, so there occurs a packet drop. The work is to detect the black hole attack which acts in groups which is called as co-operative black hole attack. The (CBDS) scheme is based on the DSR routing mechanism is designed to accomplish the goal. The Simulation result is based on the PDF.

1. Introduction

A Mobile Ad-hoc network is a collection of wireless nodes that can dynamically set up anywhere and anytime without using any pre-existing network structure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at same time therefore the limited wireless transmission range of each node gets extended by multi-hop packet forwarding. Each device in a MANET is free to move independently in any direction, and therefore there will be a change in the links frequently. Each node has its connection with wireless links and routing protocol helps in Routing process. [3]The MANET has many attacks. The attacks are mainly because of misbehavior of the malicious nodes among the Network nodes. The presence and collaboration of malicious nodes in the network may disrupt the routing leading to a malfunctioning of the network operations. The lack of infrastructure leads to attacks like black hole and gray hole. The Black hole problem is one of the main issues in MANET. In this, the malicious node will advertise itself for the shortest path with the help of Routing protocol to reach the destination. In this attack, adversary node drops all the packets passed it. In order to do this, the adversary node attracts the neighbor node with false route reply with less hop count and greater sequence number**.** When the black hole attacks in groups it is said to be co-operative Black hole attack.

2. Related Work

The problem of security has received considerable attention among the most of the researchers. A Co-operative bait detection approach to detect the malicious nodes in the network. Many Solutions have proposed by Researches in detecting single black hole attack in the Network. The detection processes helps in detecting the black hole attack but the routing overhead is increased. [1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen demonstrated the method to detect the malicious nodes in the network by hybrid architecture. [2]. Corson and J. Macker, analyzed the issues in the routing protocol issues.

Corresponding Author,
E-mail address: deepikshiny30@gmail.com

3. Types of Network Layer Attacks

MANETs are vulnerable to different attacks both from inside and outside of the Network.

3.1 Black Hole Attack

Initially in the routing process the data is sent from the source to the destination. [7] The Black hole is when the malicious node will falsely advertise that it has the shortest route to the destination from the source. The black hole attacks can also occur in groups which are known as co-operative black hole attack. In the following diagram the node B acts as the Black hole node and it drops the data packets which it gets from the source node.

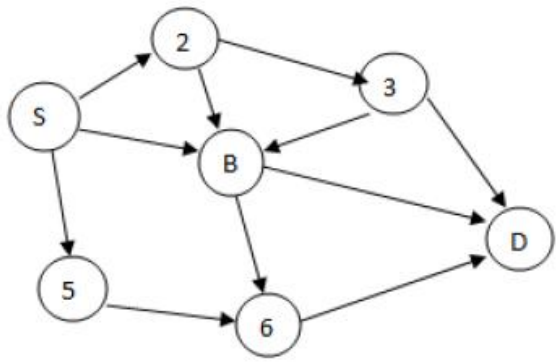

Fig: 1. Black Hole Attack

3.2 Worm hole Attack

In the wormhole attack, [7] the malicious node will suck the data packets from the source node and tunnels it to another node. The tunnel process between the malicious known is the worm hole attack.

3.3 Replay Attack

The Replay attack is normally called as active attack. It records the control signals of the [7] nodes alwa ys. It will not affect the node information; rather it will just send stale packets to make use of bandwidth and Battery power. The Replay attacks mainly deals in disturbing the routing operation.

4. Co-Operative Black Hole Attack

The Black hole is when the malicious node falsely advertises that it has the shortest route to the destination from the source. The black hole attack can also occur in groups which are known as co-operative black hole attack. In the diagram the co-operative black hole attack is given, in which the B is the Black hole node. [14]The Black hole node will extract the data packets from the source by falsely advertising that it has the shortest route to the destination. The a , b, c nodes are the co-operating nodes of the Black hole node, this is how they occur in groups . Many approaches are given to detect and eliminate the single black hole data drop. To deal with the multiple black hole attack, the above mentioned CBDS scheme is used.

5. Routing Protocol

Dynamic source routing protocol is the demand driven protocol that is based on source routing that is the sender is aware of the complete hop-by-hop route to the destination. The source routing allows packet routing to be loop-free, avoids the need for up-to-date routing informat ion in the intermediate nodes through which packets are forwarded. These routes are stored in route cache. This protocol contains two phases: Route Discovery and Route Maintenance.

6. CBDS (Co-Operative Bait Detection Scheme.

The cooperative bait detection scheme (CBDS) is designed here, in which the detection and prevention of malicious nodes creates black hole attacks in MANETs. [1]The source node will randomly selects an adjacent node with which to cooperate, and the address of that node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are there by detected and prevented from participating in the routing operation, with the help of reverse tracing technique. Whenever there is a drop in the number of packets delivered, an notificat ion is sent in the form of alarm to the destination node back to the source node to start the detection mechanism again. The CBDS scheme has the advantage of both the proactive and reactive detection in the init ial step. The CBDS is purely based on the DSR Routing protocol . So that, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. The detection is based on the Reverse tracing technique, which when a node is found to be malicious then the remaining nodes are alerted not to communicate with that particular node.

5.1 Initial Bait step

The initial Bait step is to entice the malicious node to give the RREP by giving the RREQ. [1]The source node selects the adjacent node, within one hop neighborhood and co-operates by taking the address of the destination. When the node moves randomly then the node next to it will change in its properties.

5.2 Initial Reverse step

The Reverse Tracing step is to detect the behavior of the malicious node. If the malicious node receives the RREQ, it will reply with false RREP. The malicious node will reply for every RREQ. So to overcome this the CBDS is used.

The CBDS has the ability to detect the more than one malicious node simultaneously. The CBDS is capable of identifying whether the malicious nodes would drop the packets or not.

Steps of CBDS process

1. Initially the Source node will selects the bait address of the neighbor node to bait the malicious node.
2. Source node sends Bait RREQ
3. If any other node replies RREP except the normal node which leads to the destination.
4. Then the Reverse tracing program is started and node sends test packets.
5. The source node will detect the malicious node and list it on the Black hole list and send the alarm, so that the malicious behavior can be detected

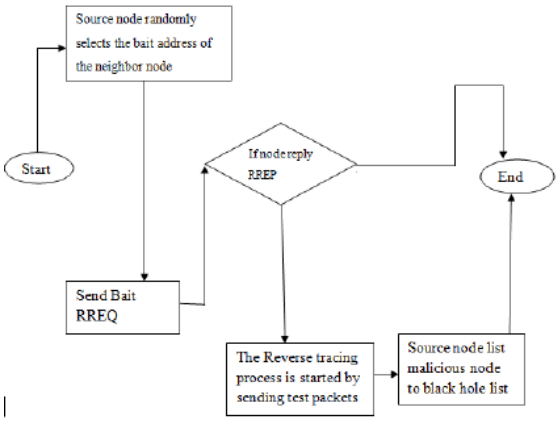

Fig: 3. Flowchart of CBDS Process

7. Program Coding

```
puts hacker_is_14
#$ns_ at 28.01 "[$node_(13) set ragent_] hacker"
$ns_ at 0 "[$node_(14) set ragent_] meli"
set annotate_ 1
if {1} {
set nam_write [new Agent/NAM_]
$nam_write namattach $namtrace
foreach nd [array names node_] {
[$node_($nd) set ragent_] nam_write $nam_write
}
$ns_ at 3 "$nam_write anot_ \"0 stoped the communication
\""
}
```

8. Simulation Parameters

The process is carried out using the network simulator Ns-2 and the language used is the TCL (Tool Command Language).

1. **PDF (Delivery Ratio)**

The Packet Delivery Fraction is the ratio of packets delivered to the packets sends out by the source node. When the PDF is high then the network is considered to be Good and its performance is better.

2. **Simulation Results**

The Simulation with the proposed scheme (CBDS) has been carried out by the ns -2 network simulator. Init ially the design of the Network topology was done with the certain number of nodes. The topology includes source node, destination node and also the hacker node in it.

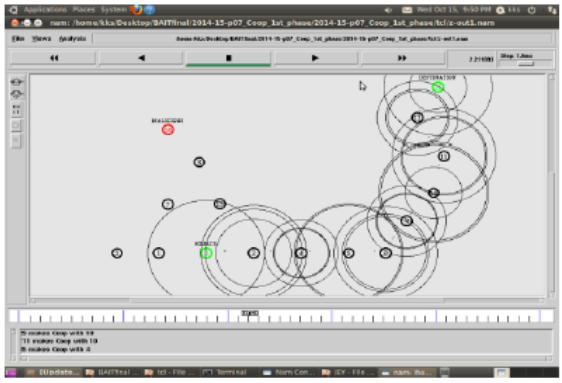

Fig: 4. The CBDS process to find the correct destination from the Source

The Routing process normally aims in detecting the correct destination. The above proposed CBDS scheme has the property of detecting the black hole attack among the nodes whichcreates the black hole attack and to recover the packet drop.

Fig: 5. Comparison of PDF with the malicious node and without the malicious (after the CBDS process)

The Simulation Results revealed that in the presence of the malicious nodes the Packet Delivery Fraction (PDF) is low when compared when without the malicious nodes. Here in the diagram the presence of malicious node and the corresponding PDF will be 5% which is low. The CBDS helps in detecting the malicious nodes which creates the black hole attack in the network. After the inclusion of the CBDS approach there will be a increase in the PDF. The packet Delivery Fraction after the CBDS is 90%. Thus the scenario is created with nodes and the presence of the malicious node is detected and the Packet Delivery Fraction was determined. The PDF in the presence of malicious node and the recovery process by the CBDS scheme was noted. And the PDF is higher when the CBDS scheme is used. In the presence of malicious node the PDF is found to be 5%, after the detection and rerouting the PDF is 90%. So, the CBDS scheme is advantageous.

9. Conclusion and Future Work

Thus the CBDS is best way in the detection of the malicious nodes which creates co-operative black hole attack that is whenmalicious nodes acts in groupsand to recover the packet drop which is the advantage of CBDS and the PDF is high. The further work is to protect network from the replay attack which is also a type of Network layer attack and to detect that and rerouting process and also to investigate the feasibility of adjusting the CBDS approach to address other types of collaborative attacks on MANETs and to investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

Acknowledgement

I whole heartedly thank Prof. I. MUTHUMANI, Head of the Department for the Guidance and the support throughout my Project.

References

[1] P. C. T sou, J.-M. Chang, H.-C. Chao, J.-L. Chen, CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture, in Proc. 2nd Intl. Conf. Wireless Communication. VITAE, Chennai, India

[2] S. Corson, J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, 1999.

[3] C. Chang, Y. Wang, H. Chao, An efficient Mesh - based core multicast routing protocol on MANET s, J. Internet Technol., 8(2), 2007, 229–239

[4] D. Johnson, D. Maltz, Dynamic source routing in ad hoc wireless networks, Mobile Comput., 1996, 153–181

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, E. Caballero, T BONE: A mobile-backbone protocol for ad hoc wireless networks, in Proc. IEEE Aerosp. Conf., 6, 2002, 2727–2740.

[6] A. Baadache, A. Belmehdi, Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks, Intl. J. Comput. Sci. Inf. Security, 7(1), 2010

[7] Gandadeep, Aashima, P. kumar, analysis of Different security attacks in MANET ’s on Protocol stack A-Review, International journal of Engg. And Advanced T ech.1(5), 2012