DETECTION OF BLACKHOLE ATTACK BASED ON DSN AND PDR IN MANETS

Abstract

MANETs are more vulnerable to different kinds of network attacks due to its phenomina. A blackhole attack is a kind of routing attack which can destroy all connections and successful transmission of the data in MANETs. This paper proposed a method considering the Blackhole attack problem while implementing the Adhoc On Demand Distance Vector routing. In this, features are extracted and analyzed by simulating the blackhole attack, when a blackhole attack present in the network. Then, we proposed detection method using the Destination sequence number, packet drop ratio and the waiting of a node. To improve the behavioral performance of the network in terms of attack, detection rate and time and to achieve the better throughput this method was proposed. Theresults of this simulation shows that this proposed one is effective and reliable for detecting blackhole attacks.

Keywords: AODV, blackhole, DSN, PDR, RREQ, RREP, Routing table

Authors

Adilakshmi Yannam
Associate Professor
Seshadri Rao Gudlavalleru Engineering College
Gudlavalleru, Andhra Pradesh

Shaik Salma Begum
Assistant Professor
Seshadri Rao Gudlavalleru Engineering College
Gudlavalleru, Andhra Pradesh

Ragavamsi Davuluri,
Assistant Professor
Seshadri Rao Gudlavalleru Engineering College
Gudlavalleru, Andhra Pradesh

Ashok Reddy kandula
Assistant Professor
Seshadri Rao Gudlavalleru Engineering College
Gudlavalleru, Andhra Pradesh

I. INTRODUCTION

From the past we have the significant evolution of wireless networks, resulting in the emergence of several associated technologies, topologies, and applications [1]. One of the technologies that has attracted a lot of attention. The so-called mobile ad hoc networks are popular among researchers (MANETs).

MANETs are self configured wireless networks connected with mobile nodes that may move independently from one place to another place. Each and every node connects to another, relying on node cooperation since there are no centralized nodes to control the network. Because autonomous mobile nodes in MANETs can move independently and employ peer-to-peer wireless communication, the network topology is flexible[1]. Due to these characteristics, MANETs are excellent for non-infrastructure communication systems like those used in emergency situations, but they also make them susceptible to a variety of network attacks, such as channel access misbehaviour, data forwarding threats, and routing protocol attacks [1].Security concerns related to this communication paradigm are becoming more and more important as MANETs spread [5]. Different special aspects, primarily those relating to the design or implementation of such security mechanisms in another assault, must be taken into consideration when dealing with them. The blackhole node accumulates network traffic, making it more likely to produce a wormhole attack or other network assault [2].The goal of this work is to create a blackhole detection technique that reduces detection time and increases detection rate. By choosing the blackhole node and examining the node's properties, we present an efficient blackhole node detection method in this study.

1. **Black hole attack:** Every time a source needs to communicate, generates a route request packet (RREQ packet), increments its sequence number by one, and includes this in the route request packet header before broadcasting the RREQ. To prevent sending the same RREQ several times, this sequence number is used. A fresh request is indicated if the SN is high. The malicious or attacking node listens in on a portion of the communication channel and records the sequence numbers of each RREQ coming from each node[3]. An attacker initiates a blackhole assault by creating a bogus RREP with a sequence number. Attacker Node lacks a distinctive id. By increasing the sequence no., an attacking node creates fake route reply packets.

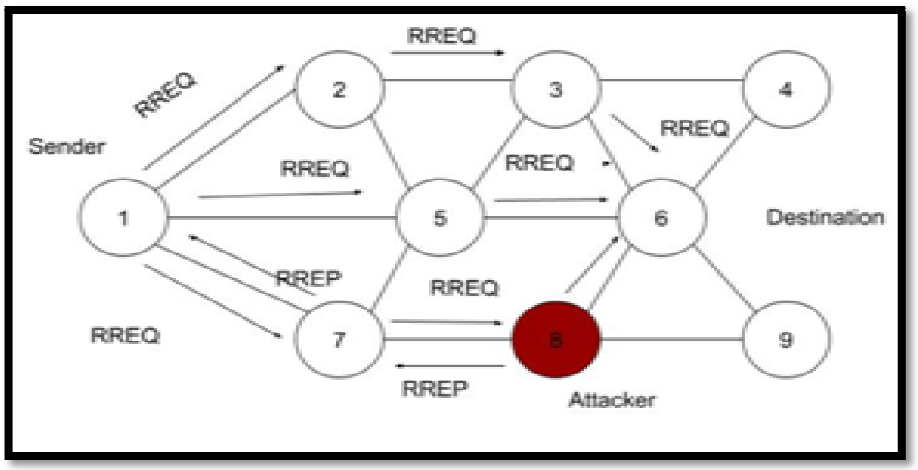

Figure 1: Network with Blackhole attacker

According to above Figure 1. The sender Broadcast RREQ to all other nodes and getting RREP in reverse with sequence number just increment by one of the source machine request. An attacker node 8 carefully observe the sequence number of the RREQ transmitted and send the bogus route reply packet (RREP) with this number than the target node because attacker treats the source node as targeted node . The source node by receiving this fake RREP, see the higher sequence number and believe that it is the original reply with hop count as 1 and decides that there is a direction to the destination with less number of hopes. The node updates its cache by deleting the all routes from the target node and stores the new fake route in the routing table. And source node simply ignore all route reply packets from the other nodes because the sequence number of this node RREP is less than the previous route reply message[4]. Now all the traffics are diverted to the target node through Blackhole node. From that point onwards the blackhole node can control the messages transmission from source to destination.

2. **Proposed methodology:** In MANET the Source node has a RREP with destination sequence number to that direction. The source one processed the incoming RREPs for consideration of route calculation. The attacker produces a RREP to form Blackhole by following that

- Request field is set to RREP
- Hop count sets to 1;
- Source IP address is set as this node of the route and the destination address
- DSN is Increased by at least one;
- Set the source address to a nonexistent address.

Attacker finds the faked RREP[12] message to the source node. When originating node receives the faked RREP message, it will modify its direction to destination node through the non-existent one. Then Black hole of RREP was formed. Then the Blackhole attacker tries to drop the entire communication that is happening between source and target node[6].

Hence the solution proposed here to detect the blackhole node by that the network life time and performance can be improved without any delays[7]. So, the proposed method basically updates the running process of the originating node without altering intermediate and destination nodes by using a modified AODV with DSN and PDR. In this three things were added, a new Routing-Table , Waiting Time and a variable Intruder Node ID to the data structures in the default AODV Protocol[8].

Step by step Procedure for Modified AODV with DSN and PDR

Source node S
Target Node D
Node ID as N_ID

- Step 1: Initiate the network with n of nodes and with timer and add the current time of simulation to waiting time by considering all these parameters.

Direction Request RREQ
Direction Reply RREP

Routing Table RT
Intruder Node IN
Intruder Node ID I_ID
Intruder Table IT
Source frame number SSN
Destination frame Number DSN
Waiting Time WT

- Step 2: Until the time exceeds do the following:
  Store the RREP from all the nodes with DSN and N_ID in RT.

- Step 3: Retrieve the each and every entry from the RT and check the following

  Repeat

  If
  The node DSN is > the SSN // not just increment by one
  Then treat it as malicious node and store in Intruder Table.
  Else
  Process the node and establish the route for communication and continue the packet transmission.

  For the nodes in IT do the following

  If
  (the packet drop ratio at this node > the normal node and the time for RREP > WT)
  then treat it as harmful node and generate alarm to warn other nodes.
  Else
  The node is considered as normal node.
  Until(Malicious node detected)

- Step 4: Then for the reaming nodes in the network continue the following process

  The malicious node detection process is explained in the following flowchat.

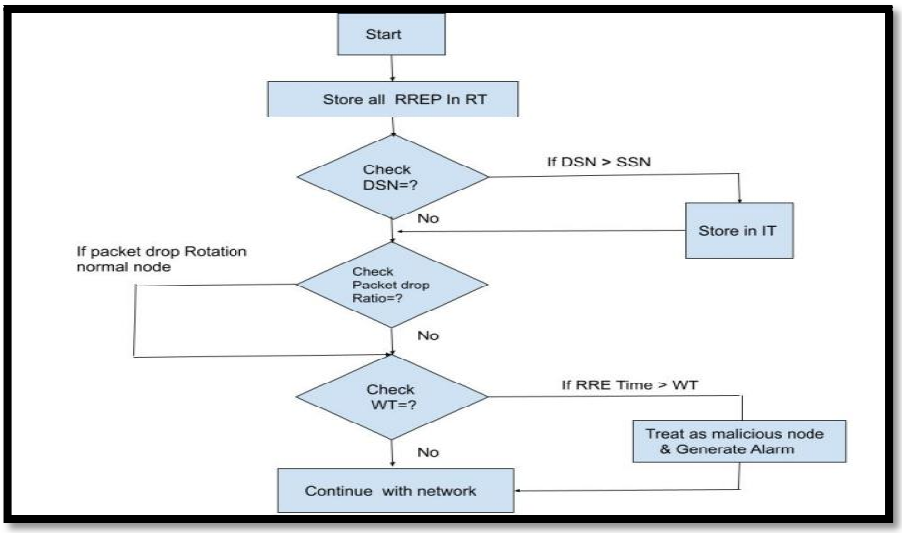

Figure 2: Process of malicious node detection

Surely the node is the malicious node, immediately remove that entry from the RT[9]. This is how malicious node is identified and then check for the packet transmission ratio for selected node. If the packet drop ration at this node is more than the normal node treat it as dangerous node. In final process the selected node receiving time is verified with waiting time, it it exceeds, it can detected as malicious node and blocked. After that alarm is generated and broadcasted to the network to warn all other nodes. The proposed one maintains the identity of the harmful node asId,so that, it can discard any control messages[10].

II. RESULTS

Describes the simulation concepts with all of the network parameters.This simulation study makes use of the NS-2[13] simulator [12]. Three scenarios are examined in this study: Adhoc On Demand Vector, AODV under RREQ flooding assault, suggested method. Example situations, configuration is 10001000 m with a constant number of nodes (CBR) of 15, 30, or 45, and a variable stop period (CBR) of 1 to 10 seconds. The parameters and their corresponding values, which were used to assess the behavioral performance of the network, are shown in Table I.

Parameter	Value
time	149 Sec
area	999 m x 999 m
Antenna(Tower)	Omni
Size of the Packet	511 Byte
Max length of the queue	49
Network Traffic	Constant bit rate
Transport Layer	User Datagram Protocol
Data Speed	9 m/s
Transmission Rate	8 packets / second

Throughput is the ratio of the quantity of source data that a sender sends to receiver to the amount of time it takes for the destination to receive the last one. In packets per second or Frequent topology changes, inconsistent communication, MANETs. A network with high throughput is preferred constrained bandwidth, and restricted bits per second, it is measured. energy are some factors that reduce throughput in Frequent topology changes, inconsistent communication, MANETs. A network with high throughput is preferred constrained bandwidth, and restricted. Using adhoc On Demand Vector, AODV under RREQ flooding attackand the proposed technique, we simulated network. It displays the throughput performance. Under RREQ Flooding attack, network throughput falls as pause time varies where as it is improved in proposed method.

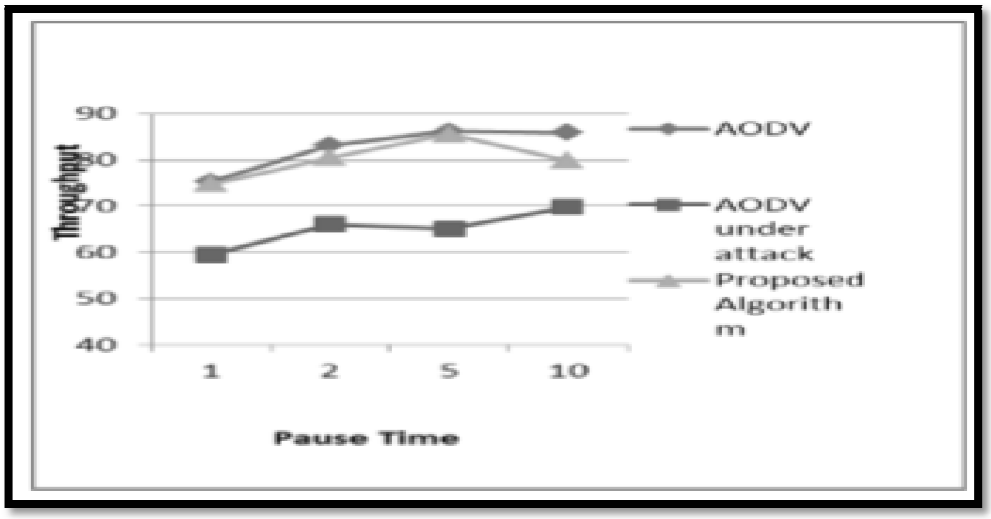

Figure 3: Throughput vs stop Time

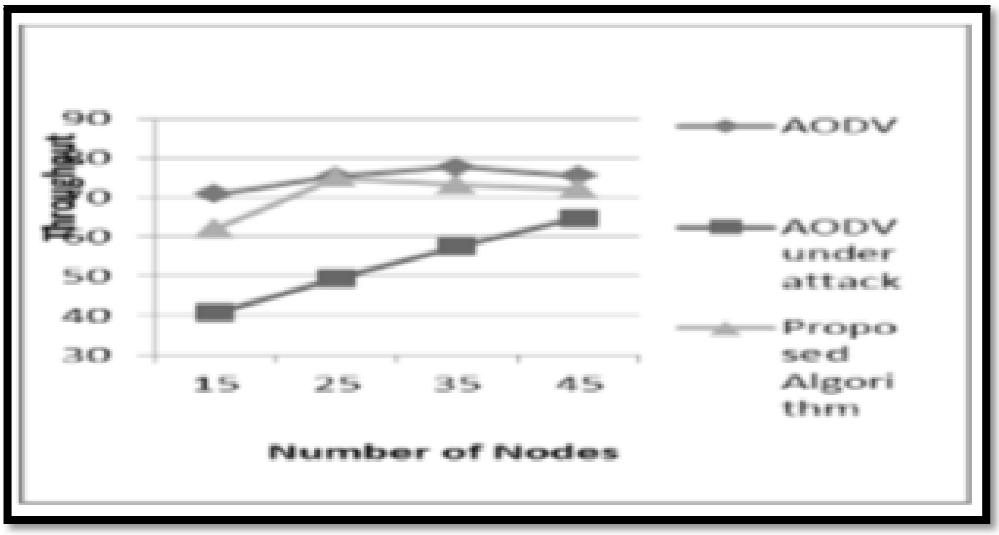

Figure 4: Throughput vs Number of Nodes

The network's throughput declines under the RREQ flooding assault but increases with our suggested mechanism, according to the simulation findings of the source network using normal AODV, Adhoc ODV under the flooding attack and the proposed method.

III. CONCLUSION

From comparisons, we believe the proposed methodology is potable and efficient and very low congestion in implementation . The proposed algorithm was simulated for the modified Adhoc ODV algorithm by considering the Destination sequence number and packet drop ratio at the node considered from the routing table [13] .

REFERRENCES

[1] M. Abdelshafy and P. J. B. King. Analysis of security attacks on aodv routing. In 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pages 1–6, London, UK, 2013.
[2] M. Arya and Y. K. Jain. Grayhole attack and prevention in mobile adhoc network. International Journal of Computer Applications, 27(10):21– 26, August 2011.
[3] Bandyopadhyay, S. Vuppala, and P. Choudhury. A simulation analysis of flooding attack in MANET using ns-3. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on, pages 1–5, 2011.
[4] Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. B¨ ol¨oni, and D. Turgut. Routing protocols in ad hoc networks: a survey. Computer Networks, 55(13):3032–3080, September 2011.
[5] P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications, 9(12):11–15, November 2010.
[6] Y. Guo and S. Perreau. Detect DDoS flooding attacks in mobile ad hoc networks. Int. J. Secur. Netw., 5(4):259–269, Dec. 2010
[7] Mehdi Medadian, Khossro Fardad, “Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol”, European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1, pp.91-101, 2012.
[8] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana, “Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks”, International .J. Computer Technology & Applications, Vol 3 (4), 1395-1399, july -august 2012.
[9] Dr. S. Tamilarasan, “Securing AODV Routing Protocol from Black Hole Attack”, International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]
[10] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, “Detection and Prevention from Black Hole attack in AODV protocol for MANET”, International Journal of Computer Applications (0975 – 8887) Volume 50 – No.5, July 2012.
[11] Ipsa De, Debdutta Barman Roy, “Comparative study of Attacks on AODVbase Mobile Ad Hoc Networks”, International Journal on Computer Science and Engineering ISSN: 0975-3397 Vol. 3 No. 1 Jan 2011.
[12] Watchara Saetang and Sakuna Charoenpanyasak, “CAODV Free Blackhole Attack in Ad Hoc Networks”, International Conference on Computer Networks and Communication Systemsvol.35 2012. [13] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, “Detection and Prevention from Black Hole attack in AODV

