International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 05, May 2017
www.ijates.com
ijates
ISSN 2348 - 7550

COLLABORATIVE APPROACH FOR DETECTION & PREVENTION OF BLACK HOLE ATTACKS ON MANET (AODV PROTOCOL)

Parminder Kaur Sandhu[1], Kirandeep Kaur[2], Balraj Singh[3]

[1]*Department of Computer Engineering, Punjab Technical University, Jalandhar, Punjab(India)*

[2]*Shaheed Bhagat Singh State Technical Campus, Ferozpur, Punjab (India)*

ABSTRACT

Many studies have been done on routing in MANETs and many routing protocols are developed. However, these protocols need trustworthy environment to work properly, which are not available frequently. In many situations, environment may not be protected. For example, Some Nodes may be malicious, selfish or influenced by attacker. To address these situations, many schemes have been proposed to secure routing in networks. All types of attacks are detected and prevented to make MANETs safe. In This paper, we implement blackhole attack on AODV protocol. Then mechanism to detect and prevent blackhole attack is introduced.

Keywords – AODV, AODV BL, MANET, MAODV

I. INTRODUCTION

In worlds of communications, wireless technologies are becoming important. It is because of three main reasons: - mobility, good bandwidth and low cost [1]. MANETs are self maintained networks. MANET networks do not have any access point or any fixed infrastructure. In ad-hoc network there is no need of any infrastructure or any centralized administration [2]. In ad-hoc network, each node acts as a host as well as router. Main Problem in ad-hoc networking is delivery of data packets to mobile nodes where topology is not pre-determined. Hence routing is viewed as a challenge due to frequently changing topology [3].

In Proactive routing protocol, with respect to time up-to-date information of network topology of all node is maintained [4]. Routes are built already from each node to every other node before they are required. Each change that may occur in topology is broadcasted throughout network. Routing information about available routes in network is maintained even if these routes are not used currently [5]. Major drawback of these approaches is that bandwidth may be occupied by maintenance of unused path due to frequently changing topology [6]. In Reactive routing protocols, routes are created on demand basis. Route discovery mechanism is invoked to find route from source to destination. Only routes that are used currently are maintained so that network load is controlled and there will be low overhead [7].

II. AODV (AD HOC ON-DEMAND DISTANCE VECTOR)

Ad-hoc on – demand distance vector (AODV) is a reactive protocol. When a nodes want to communicate with other nodes [8]. They broadcast a route request (RREQ) to its neighbor nodes. Neighbor nodes broadcast RREQ

to their intermediate nodes until destination is found [9]. Each RREQ in uniquely identified by its sequence number and by source's ID [10]. Neighbor nodes also keeps track for intermediate nodes from which RREQ comes to establish valid reverse path. Intermediate nodes sends route reply back to intermediate node from which RREQ came [11]. Neighbor nodes setup routing information based on nodes from which they receives Route reply (RREP) packet. These paths are time based and will expire if is not used recently [12].

III. BLACKHOLE ATTACK

In this type of attack, malicious node sends false message to all or route requesting node [13][14]. It claims that it possess shortest path from it to destination node. So Requesting node or all other nodes update their routing table with this information and forward data toward malicious node (attacker node) [15]. Attacker node (malicious node) may drop all incoming packets or information from other nodes [16].

IV. MECHANISM FOR DETECTION & PREVENTION OF BLACKHOLE ATTACK

The mechanism of Detection & prevention of black hole attack on the context of AODV protocol is implemented by considering the working of AODV & behavior of black hole attack which mainly consist of four phases as: (a) Initialization Phase (b) Storage Phase (c) Investigation Phase (d) Resumption Phase

4.1. Methodology

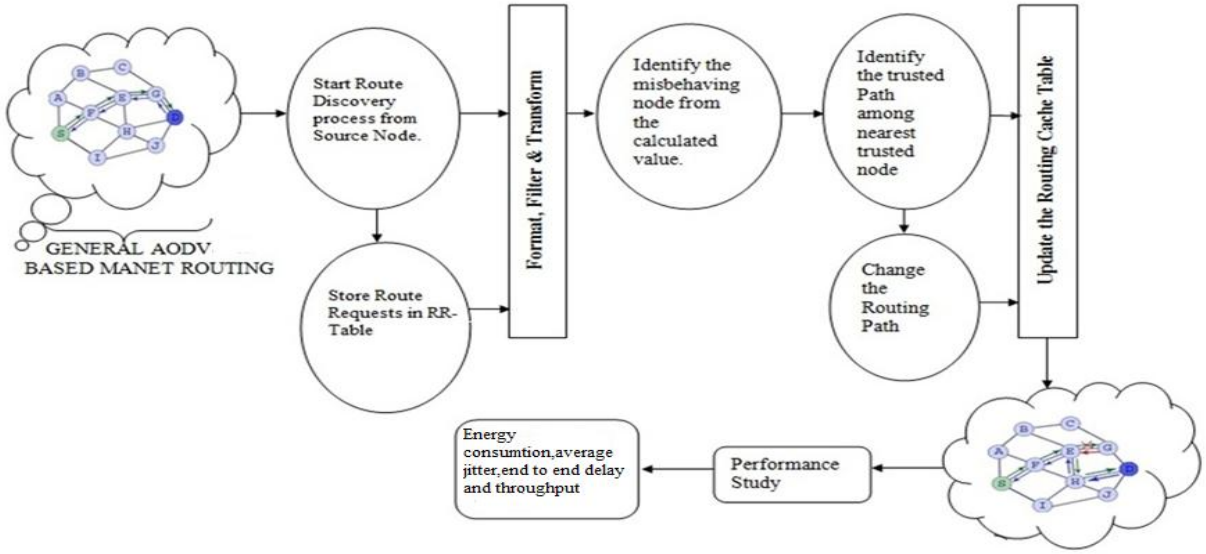


Fig. 1. Flowchart

4.2. PROPOSED WORK

Step 1: Initialization phase

Generate discovery process from the source node by generating (new hash value). Assigned current time and time required to receive reply.

Step 2: Storage phase

Store all the route replies from neighboring nodes then check the speed of the nodes and compute the threshold which decide whether to put the node into blacklist or not.

Step 3: Investigation Phase

Repeat the step 1 and 2 until reach the destination in effective way. Once the node identified as a black hole, the route node update table by adding black hole node address.

//Initialize blacklisted neighbors

AodvBlacklistNode*current=BlacklistTable->head

AodvBlacklistNode*previous=NULL

Step 4: Resumption Phase.

Continue default process of AODV**.**

V. RESULT AND DISCUSSIONS

Case 1: Simulating Reactive routing protocol (AODV) with variations in nodes and analyzing the performance of AODV in the light of Energy Consumption while Communication, Throughput, average jitter and end to end delay in MANET.

Case 2: Implement the black hole attack under AODV and analyze the performance of AODV named as AODV BL (AODV Black hole).

Case 3: Detect and mitigate the black hole attack using algorithm and evaluate the performance of routing protocol (AODV) and named MAODV (Modified Ad-Hoc on Demand distance Vector).

VI. SIMULATION RESULT AND ANALYSIS

The overall goal of this simulation study is to evaluate and analyze the performance of AODV routing protocol under black hole attack. The simulation have been performed using Qualnet version 6.1, software that provides scalable simulations of Wireless Networks. The simulation model over different networks in which network varies from 10 to 40 nodes over a terrain of 1500m*1500m area. The sender and receiver are same in each model among network members are placed at same place initially but as the simulation start ,the node starts moving and the location of source and destination node changes and also of other nodes which are in the network.

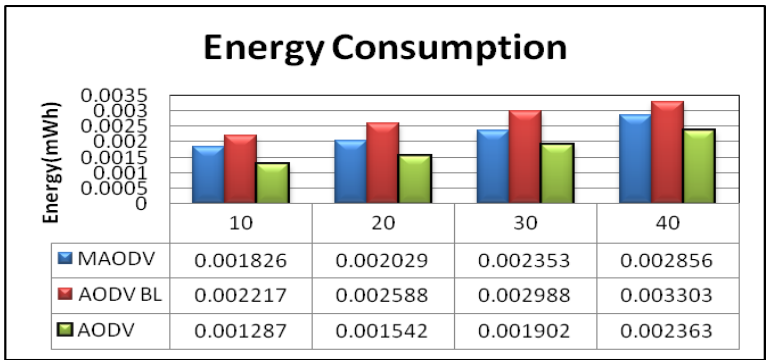
All simulation results will be shown in this section. All simulations result has been executed on Qualnet. Energy consumption, Average jitter, end to end delay and throughput are performance metrics that have been used. The following results show Energy consumption, Average jitter, end to end delay and throughput of AODV, AODV blackhole and MAODV.

Table I. Simulation Parameters

Parameters	Values
Routing Protocol	AODV
Terrain Size	1500*1500
Mobility Model	Random Waypoint Model

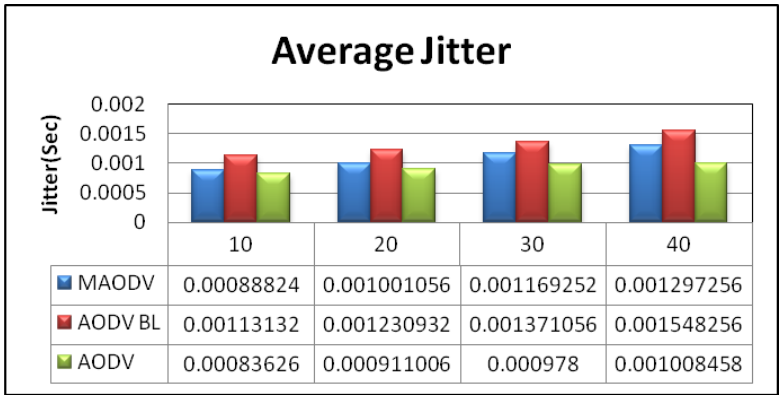
No. of Source	10,20,30,40
No. of Black hole	1,2,3,4
Simulation Duration	30 sec
Data Traffic Rate	CBR

6.1. Energy Consumption



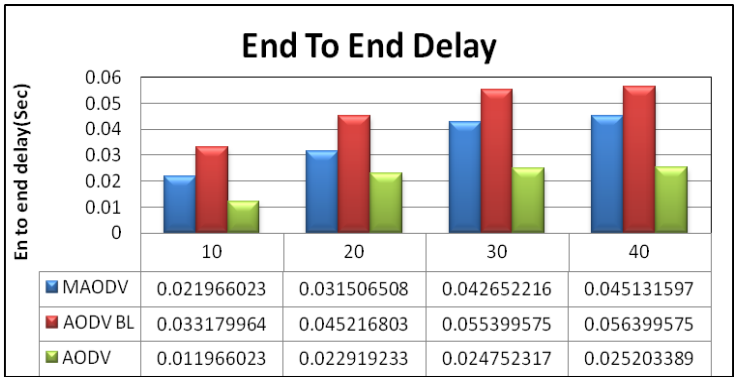
	10	20	30	40
MAODV	0.001826	0.002029	0.002353	0.002856
AODV BL	0.002217	0.002588	0.002988	0.003303
AODV	0.001287	0.001542	0.001902	0.002363

6.2. Average Jitter



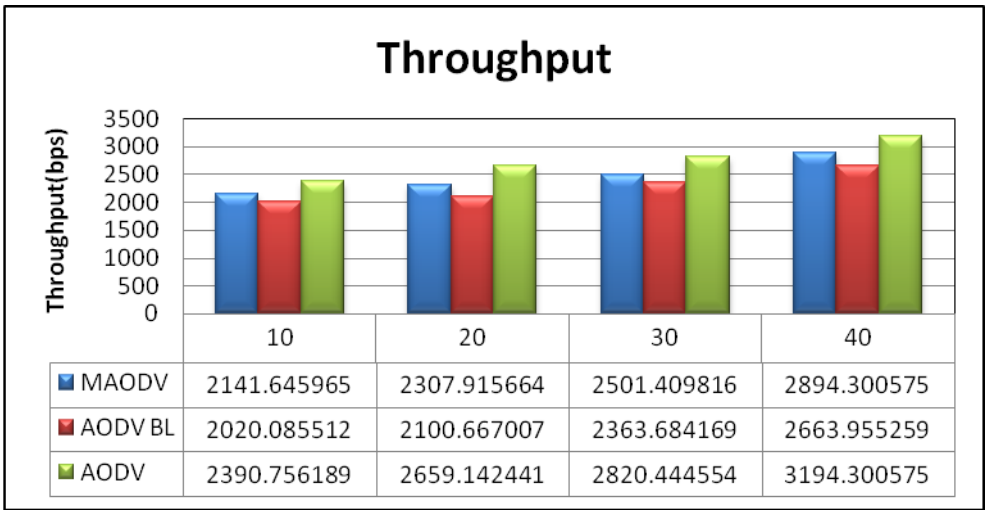
	10	20	30	40
MAODV	0.00088824	0.001001056	0.001169252	0.001297256
AODV BL	0.00113132	0.001230932	0.001371056	0.001548256
AODV	0.00083626	0.000911006	0.000978	0.001008458

6.3. End to End delay



	10	20	30	40
MAODV	0.021966023	0.031506508	0.042652216	0.045131597
AODV BL	0.033179964	0.045216803	0.055399575	0.056399575
AODV	0.011966023	0.022919233	0.024752317	0.025203389

6.4. Throughput



VII. CONCLUSION

After the Research work, we evaluate the effect of black hole attack under the performance of AODV protocol. The performance metrics are energy consumption, average jitter, end to end delay and throughput. The simulation result shows that when there is black hole node in network then it can be affected and degrade its performance. Use an algorithm for detection and prevention of black hole. It is also observed that when attacker is near the source the impact is severe than it is farther. Similarly as the number of black hole increases, it degrades the performances.

REFERENCES

[1] P.R.Jasmine jeni, A.Vimala Juliet, R.Parthasarathy and A.Messiah Bose, "Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET" *International Conference on Smart Structures & Systems*, ISBN: 978-1-4673-6240-5/32©2013 IEEE. .

[2] Mona N.Alslaim, Haifaa A.Alaqel and Soba S.Zaghloul, "A Comparative Study of MANET Routing Protocols" ISBN: 978-1-4799-3166-8©2014 IEEE.

[3] Latif Ullah Khan, Faheem Khan and Naeem Khan, "Effect of Network Density on the Performance of MANET Routing Protocols" *International Conference on Circuits, Power and Computing Technologies*, ISBN: 978-1-4673-4922-2/13©2013 IEEE.

[4] *Mr.B.Karthikeyan,Mrs. N.Kanimozhi and Dr.S.Hari Ganesh,* "Analysis of Reactive AODV Routing Protocol for MANET" ISBN:978-1-4799-2877-4/14© 2014 IEEE.

[5] Gagandeep and Aashima, "Study on Sinkhole Attacks in Wireless Adhoc Networks" *IJCSE*, ISSN:0975-3397, 2012.

[6] Gagandeep, Aashima and Pawan kumar, "Analysis of Different Security Attacks in MANETs on Protocols Stack. A-Review " *IJEAT*, ISSN:2249-8958, 2012

[7] Pragya Gupta and Sudha Gupta, "Performance Evaluation of Mobility Models on MANET Routing Protocols" *International Conference on Advanced Computing & Communication Technologies"* ISBN:9780-0-7695-4941-5/13©2013 IEEE.

[8] Ajinkya. D.Kadam and Prof. Sharad.S.Wagh, "Evaluating MANET Routing Protocols Under Multimedia Traffic " *ICCCNT-2013*, IEEE-31661.

[9] Mazhar H malik, Qasim Always, Mohsin Jamil and Dhyani, "Performance Analysis of Proactive and Reactive Protocols in Mobile Ad-Hoc Networking:A Simulation based Analysis" *ICREATE* ,ISBN:978-1-4799-5132-1/14©2014 IEEE.

[10] Changling Liu.Jorg Kaiser, "A Survey of Mobile Ad Hoc Routing Protocols".

[11] Shabana Habib, Somaila Saleem and Khawaja Muhammad Saqib, "Review on MANET Routing Protocols and Challenges" *Student Conference on Research and Development,* ISBN:978-1-4799-2656-5/13 ©2013 IEEE.

[12] Beigh Bilal Maqbool and Prof.M.A.Peer, "Classification on Current Routing Protocols for Ad Hoc Networks-A Review" *International Journal of Computer Application,* ISSN:0975-8887, 2010.

[13] Neeraj Arora and Dr. N.C.Barwar, "Evaluation of AODV, OLSR and ZRP Routing Protocols under Black hole attack" *IJAIEM,* ISSN:2319-4847, 2014.

[14] Alfy Augustine and Manju James, "Black hole Detection using watchdog" *International journal of Current Engineering And Technology.*2015, ISSN: 2277-4106, P-ISSN 2347-5161.

[15] Amin Mohebi and Simon Scott, "*A survey on Detecting Black hole methods in Mobile Ad Hoc Network."International Journal of Innovative Ideas.*" ISSN:2232-1942.@2013.

[16] Rutvij H.Jhaveri and Sankita J.Patel, "*DoS Attacks on Mobile Ad-hoc network." Second International conference on Advanced Computing & Communication Technology.* 2012.2(2), p535-540.