Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.670 – 675

RESEARCH ARTICLE

PERFORMANCE EVALUATION of ENERGY EFFICIENT MODIFIED AODV USING CLUSTERING METHOD in MANET

Mr. Ramanpreet Singh, Mr. Ajay Kumar Dogra

Computer Science Department, Punjab Technical University, Jalandhar, Punjab, India

Computer Science Department, Beant College of engineering & Technology, Gurdaspur, Punjab, India

E-mail: arora_raman2020@yahoo.com

E-mail: dogra2613@yahoo.com

Abstract- Mobile Ad hoc network is a wireless network without having any fixed infrastructure. It consist of mobile nodes which are free in moving in or out in the network. MANET is make sure mutual confirmation of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity. MANET attacks generally include attempting to drop packets, gaining substantiation or procuring authorization by inserting forged packets into data stream. This paper is presenting energy efficient modified AODV routing protocol using Clustering method in Manet. The protocol deals with various parameters as PDR, energy consumption, average end to end delay, & throughput. This protocol will be detect the black hole attack & improve the energy level of Manet.

Keywords- AODV, black hole attack, PDR, Energy consumption, throughput & delay.

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without any fix common infrastructure in place like wireless access point or radio based station. MANET has dynamic topology where devices or nodes in the network can change their position or disappear from the network rapidly. In black hole attack, malicious nodes falsely claim a fresh route to the destination to absorb transmitted data from source to that destination and drop them instead of forwarding. Black hole attack in AODV protocol can be classified into two categories: black hole attack caused by RREP and black hole attack caused by RREQ.

A.Manet Routing Protocols

Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later. Routing in a MANET depends on many other factors including topology, selection of routers and location of request initiator and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. This makes the routing area perhaps the most active research area within the MANET domain. Especially over the last few years, numerous routing protocols and algorithms have been proposed and their performance under various network environments and traffic conditions closely studied and compared. Discussed below are three categories that existing ad hoc network routing protocols fall into three parts:

a.Proactive Routing: Proactive protocols maintain routing tables of known destinations. This routing reduces the amount of control traffic overhead because packets are forwarded immediately. The routing tables must be kept up-to-date due to which memory consumed and nodes periodically send update messages to neigh-bours, even when no traffic is present. The bandwidth gets wasted. Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change which leads to increased control message overheads which can degrade network performance at high loads. Examples of this type include Destination Sequence Distance Vector (DSDV).

*b. Reactive Routing:*Reactive Protocols use a route discovery process to flood the network with route query requests when a packet needs to be routed to the destination using source routing or distance vector routing. Source routing uses data packet headers containing routing information .So nodes don't need routing tables, but this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets. This requires nodes to store active routes information until no longer required or an active route timeout occurs. Reactive routing broadcasts routing requests whenever a packet needs routing. This can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and have typically lower memory usage than proactive. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV).

c.Hybrid Routing: Hybrid protocols combine features from both reactive and proactive routing protocols attempting to exploit the reduced control traffic overhead from proactive systems while reducing the route discovery delays of reactive systems by maintaining some form of routing table. Example of this type includes Zone Routing Protocol (ZRP).

B. Manet attack

MANET is make sure mutual confirmation of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity. MANET attacks generally includes attempting to drop packets, gaining substantiation or procuring authorization by inserting forged packets into data stream.

a.Black hole attack: It refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient.

C. Cluster Head

Cluster head (CH) election is the process to select a node within the cluster as a leader node. Cluster Head maintains the information related to its cluster. This information includes a list of nodes in the cluster and the path to every node. The responsibility of the CH is to communicate with all the nodes of its own cluster. However CH must be able to communicate with the nodes of other clusters as well, which can be directly or through the respective CH or through gateways. Communication is done in three steps. First of all the cluster head receives the data sent by its members, secondly it compresses the data, and finally transmits the data to the base station or other CH. Suitable cluster head can reduce energy utilization and enhances the network lifetime

II. RELATED WORK

AHMAD ZAID [1] This paper presents three modified AODV protocols were studied, namely ids AODV, HDAODV and EAODV, and a new modified protocol is proposed. Using NS-2 network simulator, the performance of these protocols under no-attack and under-attack scenarios were collected and analyzed. Simulations were conducted by varying the pause times in random waypoint mobility model. The performance results are presented using comparative analysis based on different performance matrices such as throughput, Packet Delivery Ratio, End-to-end delay, Network Routing Load and Energy usage. The results show that the three modified AODV protocols give positive effect to network performance in both conditions - under-attack and no-attack environment. EAODV protocol outperforms other modified protocols with highest network performance, but with longer delay and higher energy usage than the other modified protocols.

FIDEL THACHIL [4] presents a trust based collaborative approach to mitigate black hole nodes in AODV protocol for MANET. In this approach every node monitors neighbouring nodes and calculates trust value on its neighbouring nodes dynamically. If the trust value of a monitored node goes below a predefined threshold, then the monitoring node assume it as malicious and avoids that node from the route path. The experiments reveal that the proposed scheme secures the AODV routing protocol for MANET by mitigating and avoiding black hole nodes.

GAURAV [5] presents the idea behind clustering is to group the network nodes into a number of overlapping clusters. In the clusters of MANET The resource constraints leads to a big problem as decrease in performance and the network partitioning leads to poor data accessibility due to false and selfish node. This proposal find false node inside clusters of MANET with the help of modified false node detection algorithm and try to remove them and also compare the result according to throughput and delay.

U.RAMYA [17]:The authors have considered three factors like node mobility, malicious behavior and unauthenticated node, in order to minimize the energy consumption of the node. By limiting these factors, the node consumes less energy. For that, the author have developed the Energy Based Routing Algorithm (EBRA) which is integrated into the Dynamic Source Routing (DSR) protocol to ensure the minimum energy consumption rate.

JASPAL [9] The author has analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. The author has analyzed the Black hole attack with respect to different performance parameters such as end-to-end delay, overhead and packet delivery ratio. The Simulation results show that IAODV performs better than AODV.

M. KHALILI [13] The author investigate the effect of this attack on ad hoc networks. Furthermore, It use hash chain to prevent this type of attack in a network that uses AODV as a routing protocol and results of applying this method has been investigated. Simulation results using OPNET simulator indicates that packet delivery ratio, in the presence of malicious nodes, reduces remarkably and proposed approach can prevent the effect of black hole attacks.

III. ENERGY EFFICIENT MODIFIED AODV USING CLUSTERING METHOD

Our literature search indicates that EAODV have the potential of becoming a preferred protocol to mitigate Black Hole problem, the mitigation method used in EAODV protocol also uses multiple RREP from a different path to alleviate the effect of black hole by allowing multiple routing update processes. The main strategy is, by assuming the actual destination node at any point of time will send the RREP, all previous route entry including from malicious nodes will be overwritten by latest incoming RREP. The updating process will continue until RREP from the actual destination node is received. EAODV protocol is implemented by modifying the AODV routing update mechanism involving two processes to mitigate the black hole attack; namely, 1) changing the routing update logic expression and 2) adding detection and isolation process. We could foresee at least one limitation; i.e. EAODV adds two processes in the mitigation methods that cause extra delay and energy usage. The new proposed algorithm using clustering will perform route discovery process & detect the black hole attack to recover the energy consumption in Manet.

A.Algorithm:
Black Hole Detection at Cluster Head (CH) level to prepare Black_hole_list

1.) CH sends data to its members and waits for reply from its members.
2.) After small intervals, members send reply data packets to their CH; except black hole nodes.
3.) CH checks the nodes which have not send data.
4.) Add these nodes to the black_hole_list

Black hole detection at Cluster head monitor (CHM) level to prepare blackhole_list

1.) CHM sends packet to their respective cluster heads and wait for reply.
2.) After regular intervals, CH sends blackhole_list; except the clusters which are black hole.
3.) CHM checks the CHs which have not send any list.
4.) Add these CHs to blackhole_list and elect any node in that cluster as CH.

This algorithm evaluated the performance of network in two environments: no-attack & under attack. Black hole attack was used as attack model with 5,10 or more malicious attack. AODV is taken as basic protocol for implementing new proposed Energy efficient modified Routing Protocol using Clustering in simulation process. Simulation scenario uses the following parameters which shows the proposed method is better than previous one.

Table 1.Various Parameters of Implementation

Parameter	**Value**
Channel Type	Wireless
Propagation	TwoRayGround
Simulation Time	50 sec
Initial Energy	5000 Joules
Tx Power	250 mW
Rx Power	200 mW
Number of nodes	100
Number of cluster heads	10
Number of Mobile check points	10
Application traffic	CBR
Transmission Range	250
Maximum Speed	10 m/sec
Area	1500*1500
Movement model	Random waypoint
Number of malicious nodes	5, 10, 15, 20

The simulation work for the new technique is done in NS-2. The simulation result shows that the new method is more efficient than the existing method. Table 1 shows the parameters used in simulation. In this simulation, first we set NS-2 parameters like simulation area, time, energy level, no. of cluster heads, no. of mobile check points, number of malicious nodes.

IV. SIMULATION RESULT

The result of comparison between EAODV and Proposed routing protocol is shown in Figures.

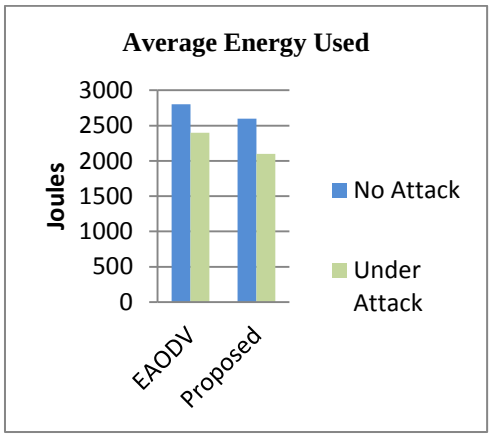

Fig.1.Energy Consumption level

Fig 1.shows the result of energy consumption by protocol. EAODV protocol consumes more energy than new method. So there is less chances of packet loss which leads to more transmission activities.

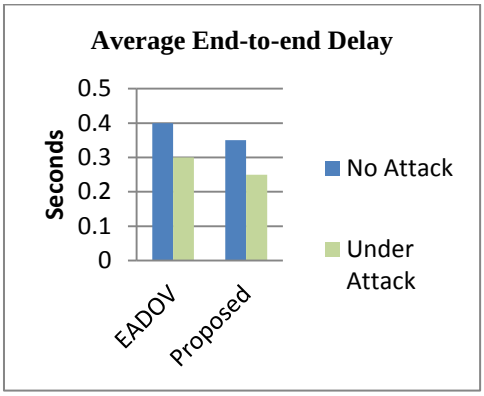

Fig.2. Average end to end delay

Fig.2. shows the average end-to-end delay during the network under attack condition, The average delay for EAODV is 0.30 second. & the proposed method has the lowest delay that is 0.25.

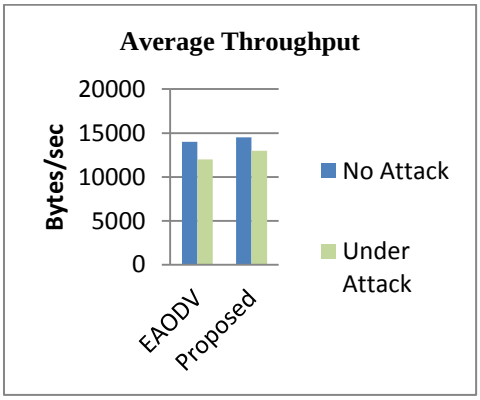

Fig.3. Average throughput

Fig.3 shows the proposed method successfully increases the transmitted data packets so that the throughput level is 13.0 kbytes/sec that is better than EAODV.

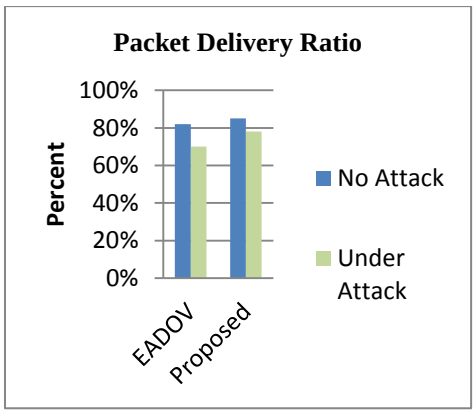

Fig.4.Packet Delivery ratio

Fig.4 shows the proposed method is effective than EAODV protocol. The PDR performance is 78% as compared to EAODV. So this level increases the no. of packets is receiving by destination.

V. CONCLUSIONS & FUTURE WORK

In this work, a new Black Hole Detection technique is proposed that detects black holes using a vice cluster head. A comparative analysis has been done on the performance of this new technique with the performance of an existing EADOV protocol. The results obtained after extensive simulation shows that the new Technique performs better than EAODV. It records better Packet Delivery Ratio, Average end-to-end Delay, Network Throughput and Average Energy Used.

In case of low network density, this technique causes some excessive overhead, proving it unsuitable for such networks. In future, this work can be extended by devising a better technique system that reduces the overhead of selecting cluster head and vice cluster head, further reducing the average end-to-end delay and increasing overall network throughput.

ACKNOWLEDGEMENT

Thanks to my Guide, friends and family member who always support, help and guide me during my dissertation.

REFERENCES

[1**]** Ahmad Zaid, Abd. Jalil Kamarularifin, Ab Manan Jamalul-lail, "*Performance Evaluation on Modified AODV Protocols"* IEEE , December 11 - 13, 2012.

[2] Ali Norouzi and A. Halim Zaim, *Energy Consumption Analysis of Routing Protocols in Mobile Ad Hoc Networks.*

[3] Anagha R. Raich1 , Prof. Amarsinh Vidhate, "*Best Path Finding using Location aware AODV for MANET* **",** IJACR, 11 September-2013.

[4] Fidel Thachil, K C Shet, " *A trust based approach for AODV protocol to mitigate black hole attack in MANET***"** International Conference, 2012 IEEE.

[5] Gaurav, Naresh Sharma**, "***An Approach: False Node Detection Algorithm in Cluster Based MANET"* IJARCSSE, February 2014.

[6] H. A. Esmaili, M. R. Khalili Shoja, "*Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator*, *WCSITJ*, 2011.

[7] Harmandeep Singh1, Manpreeet Singh2**, "***Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs",* IJATCSE, May - June 2013.

[8] Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin , "*Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash*" 2013 IEEE.

[9] Irshad Ullah* and Shahzad Anwar**, "***Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols*", IJCS, May 2013

[10] Jaspal Kumar, M. Kulkarni, Daya Gupta, "*Effect of Black Hole Attack on MANET Routing Protocols*", JCNIS, 2013.

[11] Madhusudhananagakumar KS, G. Aghila, "*A Survey on Black Hole Attacks on AODV Protocol in MANET***",** IJCA Volume 34, November 2011.

[12] Meenakshi Patel, Sanjay Sharma, "*Detection of Malicious Attack in MANET A Behavioral Approach***",** 3rd IEEE (IACC), 2013.

[13] Mehdi Medadian, M.H. Yektaie, "*Combat with Black Hole Attack in AODV routing protocol in MANET***",** 2009 IEEE.

[14] M. Khalili shoja, H. Taheri, and S. Vakilinia," *Preventing Black Hole Attack in AODV through Use of Hash Chain.*

[15**]** Ms. Bhumi Jani1, Prof. Hitesh Patel2, "*Mitigation of Blackhole for AODV (Ad hoc On Demand Distance Vector)*", IJCSMP Issue. 5, May 2013.

[16] P. R. Jasmine Jeni, A. V imala Juliet , "*Performance Analysis of DOA and AODV Routing Protocols with Black Hole Attack in MANET*", JCSSS-20 13, March 28 - 29, 2013.

[17] Sapna Gambhir, Saurabh Sharma, "*Prime Product Number based Malicious Node Detection Scheme for MANETs", 3rd* IEEE (IACC), 2013.

[18] U.Ramya1, M.Arockiya Stalin Mary2 & R.Kayalvizhi3, *"Reducing Energy Consumption in MANET under Different Scenarios",* (IJAIST), August 2012,

[19] Zaid Ahmad, Kamarularifin Abd. Jalil, Jamalul-lail Ab Manan "*Black hole Effect Mitigation Method in AODV Routing Protocol",* (IAS)2011 IEEE.

