KAAV INTERNATIONAL JOURNAL OF SCIENCE, ENGINEERING & TECHNOLOGY
A REFEREED BLIND PEER REVIEW QUARTERLY JOURNAL
KIJSET/OCT-DEC (2017)/VOL-4/ISS-4/A2 PAGE NO.8-13
ISSN: 2348-5477 IMPACT FACTOR (2017) – 6.9101
WWW.KAAVPUBLICATIONS.ORG

PERFORMANCE EVALUATION OF ENERGY EFFICIENT MODIFIED AODV USING CLUSTERING METHOD IN MANET

[1]SARTHAK GUPTA
[1]Department of Computer Science & Engineering, Bhagwant Institute Of Technology,Muzaffarnagar

[2]SACHIN CHAUDHARY
[2]Asst. Prof., Department of Computer Science & Engineering Bhagwant Institute Of Technology,Muzaffarnagar

[3]Dr. PUSHPNEEL VERMA
[3]Asso. Prof, Department of Computer Science & Engineering Bhagwant Institute Of Technology,Muzaffarnagar

ABSTRACT
Mobile Ad hoc network is a wireless network without having any settled framework. It comprises of versatile hubs which are free in moving in or out in the system. MANET is ensured common affirmation of member hubs, classification and respectability of traded information, accessibility of the system assets, get to control to the correspondence medium and the secrecy. MANET assaults for the most part incorporate endeavoring to drop bundles, picking up substantiation or acquiring approval by embeddings manufactured parcels into information stream. This paper is displaying vitality effective adjusted AODV directing convention utilizing Clustering technique in MANET. The convention manages different parameters as PDR, vitality utilization, normal end to end delay, and throughput. This convention will be recognize the dark gap assault and enhance the vitality level of MANET.

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

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 gadgets or hubs in the system can change their position or vanish from the system quickly. In dark opening assault, malignant hubs dishonestly guarantee a crisp course to the goal to retain transmitted information from source to that goal and drop them as opposed to sending. Dark opening assault in AODV convention can be arranged into two classifications: dark gap assault caused by RREP and dark gap assault caused by RREQ.

A. MANET Routing Protocols

Routing protocols between any combine of hubs inside a specially appointed system can be troublesome in light of the fact that the hubs can move arbitrarily and can likewise join or leave the system. This implies an ideal course at a specific time may not work seconds after the fact. Directing

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org

in a MANET relies upon numerous different variables including topology, choice of switches and area of demand initiator and particular hidden qualities that could fill in as a heuristic in finding the way rapidly and effectively. This makes the steering zone maybe the most dynamic research zone inside the MANET area. Particularly finished the most recent couple of years, various directing conventions and calculations have been proposed and their execution under different system situations and activity conditions firmly contemplated and looked at. Examined underneath are three classes that current specially appointed system directing conventions fall into three sections:

a) **Proactive Routing:** Proactive protocols maintain routing tables of known destinations. This routing lessens the measure of control activity overhead since parcels are sent promptly. The routing tables must be stayed up with the latest because of which memory devoured and hubs intermittently send refresh messages to neigh-bours, notwithstanding when no movement is available. The data transfer capacity gets squandered. Proactive steering is unacceptable for exceedingly powerful systems in light of the fact that directing tables must be refreshed with every topology change which prompts expanded control message overheads which can corrupt system execution at high loads. Examples of this compose incorporate Destination Sequence Distance Vector (DSDV).

b) **Reactive Routing:** Reactive Protocols utilize a course revelation procedure to surge the system with course inquiry demands when a bundle should be directed to the goal utilizing source steering or separation vector steering. Source directing utilizations information parcel headers containing steering data .So hubs don't require directing tables, yet this has high system overhead. Separation vector steering utilizes next jump and goal delivers to course bundles. This expects hubs to store dynamic courses data until the point when never again required or a dynamic course timeout happens. Receptive steering communicates directing solicitations at whatever point a bundle needs directing. This can cause delays in bundle transmission as courses are computed, however includes next to no control movement overhead and have commonly bring down memory utilization than proactive. Case of this write incorporates 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 ensure shared confirmation of members hubs, privacy and uprightness of traded information, accessibility of the system assets, get to control to the correspondence medium and the secrecy. A MANET attack for the most part incorporates endeavoring to drop bundles, picking up substantiation or getting approval by embeddings fashioned parcels into information 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

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org

RELATED WORK

HMAD ZAID [1] This paper presents three changed AODV conventions were considered, in particular ids AODV, HDAODV and EAODV, and another adjusted convention is proposed. Utilizing NS-2 arrange test system, the execution of these conventions under no-assault and under-assault situations were gathered and broke down. Recreations were led by shifting the delay times in irregular waypoint portability display. The execution comes about are displayed utilizing similar investigation in light of various execution frameworks, for example, throughput, Packet Delivery Ratio, End-to-end delay, Network Routing Load and Energy utilization. The outcomes demonstrate that the three changed AODV conventions give beneficial outcome to arrange execution in the two conditions - under-assault and no-assault condition. EAODV convention beats other adjusted conventions with most elevated system execution, however with longer postponement and higher vitality use than the other changed conventions.

FIDEL THACHIL [4] presents a trust based cooperative way to deal with alleviate dark opening hubs in AODV convention for MANET. In this approach each hub screens neighboring hubs and figures trust an incentive on its neighboring hubs powerfully. On the off chance that the trust estimation of a checked hub goes underneath a predefined limit, at that point the observing hub accept it as pernicious and stays away from that hub from the course way. The trials uncover that the proposed conspire secures the AODV directing convention for MANET by moderating and maintaining a strategic distance from dark gap hubs.

GAURAV [5] presents the thought behind bunching is to amass the system hubs into various covering groups. In the bunches of MANET The asset requirements prompts a major issue as abatement in execution and the system apportioning prompts poor information openness because of false and narrow minded hub. This proposition find false hub inside groups of MANET with the assistance of changed false hub discovery calculation and endeavor to evacuate them and furthermore contrast the outcome concurring with throughput and postponement.

JASPAL [9] the creator has broke down the impacts of Black gap assault on portable specially appointed directing conventions. Chiefly two conventions AODV and Improved AODV have been considered. The creator has dissected the Black opening assault regarding distinctive execution parameters, for example, end-to-end postponement, overhead and bundle conveyance proportion. The Simulation comes about demonstrate that IAODV performs superior to AODV.

III. ENERGY EFFICIENT MODIFIED AODV USING CLUSTERING METHOD

Our writing look shows that EAODV have the capability of turning into a favored convention to relieve Black Hole issue, the moderation technique utilized as a part of EAODV convention likewise utilizes numerous RREP from an alternate way to reduce the impact of dark gap by permitting various directing refresh forms. The fundamental system is, by expecting the real goal hub anytime of time will send the RREP, all past course section including from malevolent hubs will be overwritten by most recent approaching RREP. The refreshing procedure will proceed until the point when RREP from the genuine goal hub is gotten. EAODV convention is actualized by altering the AODV steering refresh component including two procedures to moderate the dark gap assault; to be specific, 1) changing the directing refresh rationale articulation and 2) including identification and disengagement process. We could anticipate no less than one restriction; i.e. EAODV includes two procedures in the relief strategies that reason additional deferral and vitality utilization. The new proposed calculation utilizing bunching will perform course revelation process and distinguish the dark gap assault to recuperate the vitality utilization 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

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org

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 essential convention for actualizing new proposed Energy productive adjusted Routing Protocol utilizing Clustering in recreation process. Recreation situation utilizes the accompanying parameters which demonstrate the proposed strategy is superior to past 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 demonstrates that the new technique is more productive than the current strategy. Table 1 demonstrates the parameters utilized as a part of 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, and number of malicious nodes.

IV. SIMULATION RESULT

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

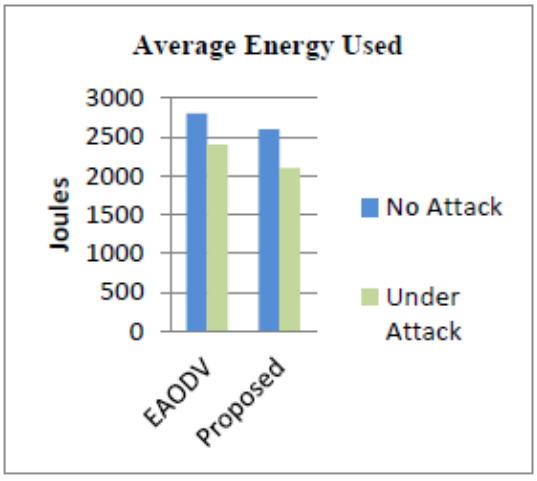

Fig.1.Energy Consumption level

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.

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org

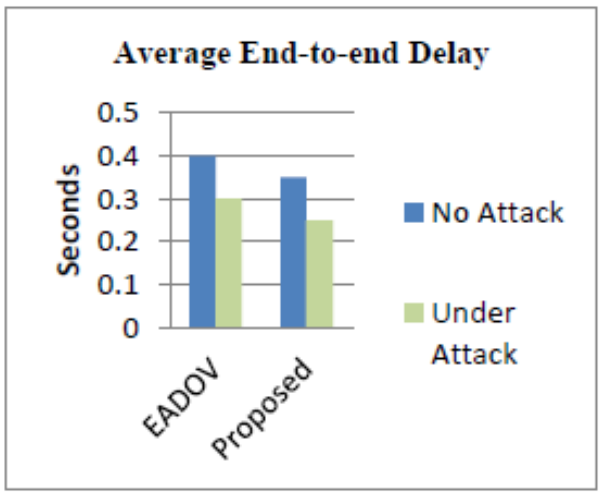

Fig.2. Average end to end delay

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.

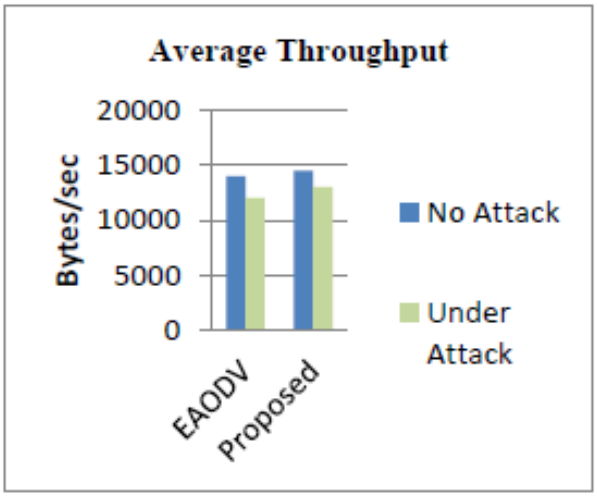

Fig.3. Average throughput

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.

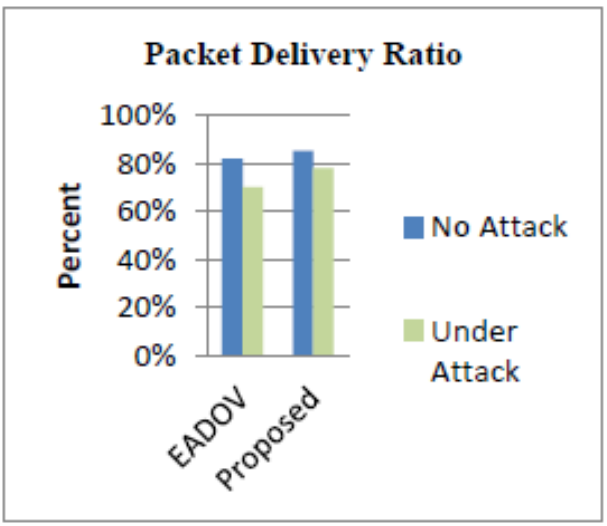

Fig.4.Packet Delivery ratio

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.

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org

CONCLUSIONS

In this work, another Black Hole Detection procedure is suggested that distinguishes dark openings utilizing a bad habit bunch head. A relative examination has been done on the execution of this new system with the execution of a current EADOV convention. The outcomes got after broad reproduction demonstrates that the new Technique performs superior to EAODV. It records better Packet Delivery Ratio, Average end-to-end Delay, Network Throughput and Average Energy Used. If there should be an occurrence of low system thickness, this method causes some extreme overhead, demonstrating it inadmissible for such systems. In future, this work can be reached out by concocting a superior method framework that lessens the overhead of choosing group head and bad habit bunch head, additionally decreasing the normal end-to-end postpone and expanding general system throughput.

REFERENCES

- Ahmad Zaid, Abd. Jalil Kamarularifin, Ab Manan Jamalul-lail, "Performance Evaluation on Modified AODV Protocols" IEEE , December 11 - 13, 2012.
- Ali Norouzi and A. Halim Zaim, Energy Consumption Analysis of Routing Protocols in Mobile Ad Hoc Networks.
- Anagha R. Raich1 , Prof. Amarsinh Vidhate, "Best Path Finding using Location aware AODV for MANET ", IJACR, 11 September-2013.
- Fidel Thachil, K C Shet, " A trust based approach for AODV protocol to mitigate black hole attack in MANET" International Conference, 2012 IEEE.
- Gaurav, Naresh Sharma, "An Approach: False Node Detection Algorithm in Cluster Based MANET" IJARCSSE, February 2014.
- H. A. Esmaili, M. R. Khalili Shoja, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator, WCSITJ, 2011.
- Harmandeep Singh1, Manpreeet Singh2, "Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs", IJATCSE, May - June 2013.
- Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin , "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash" 2013 IEEE.
- Irshad Ullah* and Shahzad Anwar, "Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols", IJCS, May 2013
- Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", JCNIS, 2013.
- Madhusudhananagakumar KS, G. Aghila, "A Survey on Black Hole Attacks on AODV Protocol in MANET", IJCA Volume 34, November 2011.
- Meenakshi Patel, Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach", 3rd IEEE (IACC), 2013.
- Mehdi Medadian, M.H. Yektaie, "Combat with Black Hole Attack in AODV routing protocol in MANET", 2009 IEEE.
- M. Khalili shoja, H. Taheri, and S. Vakilinia," Preventing Black Hole Attack in AODV through Use of Hash Chain.
- Ms. Bhumi Jani1, Prof. Hitesh Patel2, "Mitigation of Blackhole for AODV (Ad hoc On Demand Distance Vector)", IJCSMP Issue. 5, May 2013.
- 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.
- Sapna Gambhir, Saurabh Sharma, "Prime Product Number based Malicious Node Detection Scheme for MANETs", 3rd IEEE (IACC), 2013.
- U.Ramya1, M.Arockiya Stalin Mary2 & R.Kayalvizhi3, "Reducing Energy Consumption in MANET under Different Scenarios", (IJAIST), August 2012,
- Zaid Ahmad, Kamarularifin Abd. Jalil, Jamalul-lail Ab Manan "Black hole Effect Mitigation Method in AODV Routing Protocol", (IAS)2011 IEEE.

Copyright © 2017 Published by kaav publications. All rights reserved www.kaavpublications.org