ISSN No. 0976-5697

Volume 8, No. 5, May-June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Black Hole Attack Detection Using Counters for AODV in MANET

Rajni Rani
Department of Computer Science and Engineering
SLIET, Sangrur, Punjab

Gurjinder Kaur
Department of Computer Science and Engineering
SLIET, Sangrur, Punjab

Abstract: A mobile ad hoc network (MANET) is repeatedly self constructing and infrastructure less network, having mobile nodes (MNs) connected to each other wirelessly. One of the most prevalent routing protocols used in MANET is Ad hoc on demand distance vector (AODV). The problem with AODV is its vulnerability to several attacks. The most devastating attack in AODV is black hole attack. In this paper, a strategy for detection of Black Hole (BH) attack is proposed which leads to preservation of energy due to negligible control packet overhead. The performance of proposed strategy is compared with the existing techniques and the results depict that the proposed strategy effectively detect and prevent the BH attack in MANET while preserving the energy.

Keywords: mobile ad hoc network; AODV; black hole; denial of service attack; routing protocol

I. INTRODUCTION

A MANET is comprised of MNs which use radio waves to communicate each other. The MNs are free to move unrestrictedly and form random network topology without any centralized access point. The network is completely dispensed without any fixed infrastructure. MNs can directly transmit the packets to other nodes which are one hop away from them. In other scenario, when MNS are multihop away from each other then they need the help of intermediate node for communication[1, 2]. At that time, routing protocol is required to find out precise choice of route. The routing protocols are generally categorized into three types- proactive, reactive and hybrid. In *proactive routing protocol*, all MNs maintain tables in advance that represent whole network topology. The tables are shared among the neighboring nodes to maintain the current information. *Reactive routing protocol* finds out path when some MN wants to communicate with other MN. A path is established on demand so that there is no regular overhead of routing traffic. *Hybrid* is a combination of both reactive and proactive routing protocol. It takes decision for optimum route to the destination [3].

AODV is a reactive routing protocol that includes two phases- route discovery and route maintenance. In route discovery phase, routes are found out on the basis of two control packets named as route request (RREQ) and route reply (RREP). These control packets use sequence number (seq_no) to actuate the freshness of route. When some MN wants to communicate with other MN for which it has no route in past then it broadcasts a RREQ over the network. The MNs update their route tables according the received RREQ and introduce reverse pointer to the source [2]. A node may unicast a RREP in two cases only. When it is either the destination or has a fresh path to the destination. After getting RREP source MN sends packet to the path given in RREP [2, 4]. At the time of route discovery phase there may be a chance of different type of attacks such as wormhole attack, flooding attack, rushing attack, spoofing attack, packet dropping attack and black hole attack etc. Wormhole attack is caused by a pair of malicious MN that uses high speed private network for transmit the packet toward destination to collect and manipulate network traffic. In flooding attack, a malicious MN flood the network with fake RREQ because of this network throughput is underutilized. The rushing attack is introduced by a contestant who can flood exiguous routing packets against the destination, leading to tribulation with routing. In spoofing attack, a malicious node can try to take over the identification of another node to obtain all packets intended to the authorized node, may give fake routes. Packet dropping attack is caused by a node that can advertise paths through it to promiscuous other nodes and can start diminishing the obtained packets rather than advertising them [5, 6]. The black hole attack is one of denial of service attack which is precarious to AODV because it consumes overall network traffic. In this attack, when malicious MN receives a RREQ then it generates fake RREP without looking in the routing table whether it has a fresh path to destination. Fake RREP contains exponentially high sequence number and minimum number of hop count to destination. Source thinks, Path given in fake RREP is optimum one and sends data packets on given path. After receiving data packets, BH drops all the packets intentionally [1].

BH attack is extremely hard to identify and protect, which causes end to end delay increases and immense decrease in PDR and throughput. Hence the detection of black hole node becomes the current area of research.

Remaining part of the paper is structured as follows. Section II, contains the summary of related work done on the Blackhole attack detection and prevention in AODV. Section III includes the description about the proposed work as well as flow chart and algorithm. Section IV comprises of result analysis against two already existing techniques. At the end conclusion with advantage of proposed work is described in section V.

II. LITERATURE REVIEW

Shield problems in MANETs have regularly been a current subject and much experimentation are available in the literature.

Kshirsagar et al. [1] in this paper solution for black hole attack detection and prevention are given by real time monitoring of nodes. In this method, neighboring MN of suspected MN brings itself in a promiscuous mode and maintains two counters, fcount and rcount. These counters are used for counting the number of forwarded and received packets respectively [2]. The neighboring MN forward the data packets to the originator MN till fcount reach at a threshold value. At that time if rcount is zero then suspected MN declare as black hole MN.

Chavda et al. [2] had proposed a solution in which the source continuously accepts the RREP packets and calls the process name as Compare_RREP, which actually compare the destination sequence number of two route replies and select the route reply with higher destination sequence number, if the difference between them is not significantly high. RREP contains exceptionally high destination sequence number, is suspected to be malicious.

Khandelwal et al. [4] presented a work where source MN store all the RREP in newly created RREP table and compares destination sequence no. from a newly created table with source sequence number. If the destination sequence number is found much higher as compare to source sequence number then the entry is discarded from the table.

Singh et al. [5] proposed a technique, if RREP generated by intermediate MN then the MN preceding suspected MN brought itself into promiscuous mode and sends the hello message to destination through suspected MN [6]. If hello message is forwarded by intermediate MN then declare as normal MN otherwise sends an alarm message about the malicious MN.

Kaur et al. [8] projected a work for detecting and isolating the black hole MN. In this approach, source MN floods the Fake RREQ which contains the internet protocol address of the destination that does not exist in network. MN who gives the reply is considered to be black hole MN. Source sends the RREQ packet and after getting the RREP does not select the path that is from malicious MN.

Kalia et al. [9] proposed a method on the basis of fake RREQ. The source sends the fake RREQ, included source internet protocol address at the place of destination. A Source has the most recent sequence number for itself. In case, if the reply came then it can be from malicious MN only. The source MN has detected the malicious MN and notifies other MNs.

Sa et al. [10] defined a solution for detecting the single and collaborating black hole attack. The sender MN broadcasts a fake RREQ and after getting the reply, it includes those MNs in black hole list and find out the average of all the DSN from recently get replies .That average value is used as a threshold value.

Patel et al. [11] had proposed a method where all the RREPs are stored in new table till initialization time get expire. After that average for all destination Sequence number, have stored in newly created table is computed. The result is considered as a threshold value. If some stored RREP has greater sequence number than threshold, mark as Blackhole MN.

Abdelhaq et al. [12] presented a solution for black hole attack security. The previous MN to the intermediate MN buffers the RREP packet and sends the FRREQ to the next MN by using new route. After getting FRREP, if there is a route to the intermediate and destination MN then buffered RREP sends toward source otherwise RREP is discarded.

Chavan et al. [13] performed a work against black hole attack. If RREP is generated by intermediate MN then it sends a verify packet to destination. The content of verify packet is stored in a table by destination. After getting the reply from intermediate MN, sender MN sends the check verification packet to the destination. When the check verification is received, destination matches the source id of both the packets. If match is found, sender MN receives the final reply. In case of black hole MN, final reply does not reach at source.

III. PROPOSED WORK

In this paper, symbolic attempts have put on designing security mechanism against black hole attack. An adequate method is proposed on the basis of energy to detect black hole. In this proposed work two counters REP_COUNT and REC_COUNT are used to detect the black hole MN in MANET. As per the property of black hole, it sends reply to each request that it receives. Hence the accepted REEQs and generated route replies are equal in amount. In this work, two counters are maintained at each MN to store these two values. Initially any random source sends fake RREQ which contains source address in place of destination address. The purpose of fake RREQ is to distinguish between normal MN and malicious MN because primarily REP_COUNT and REC_COUNT have zero values. When any MN receives the RREQ then REC_COUNT is incremented by one and when any MN sends the RREP then REP_COUNT is incremented. When any MN sends RREP it also sends the value of these two counters. After receiving the RREP, source MN checks the value of these two counters, if these values are equal then it discards the RREP otherwise sends the packet to the path gives in RREP.

***Algorithm for proposed technique*:**

1. Maintain the two counters at each MN, initially their value is set to zero.
2. FRREQ packet is randomly sent by any source MN.
3. REC_COUNT is incremented if MN receives a RREQ while REP_COUNT is incremented if MN gives a reply.
4. The MN sends RREP as well as value of counters.
5. After getting the RREP, source MN checks the value of these two counters. If these values are equal discards the RREP otherwise sends the data packets on that path.

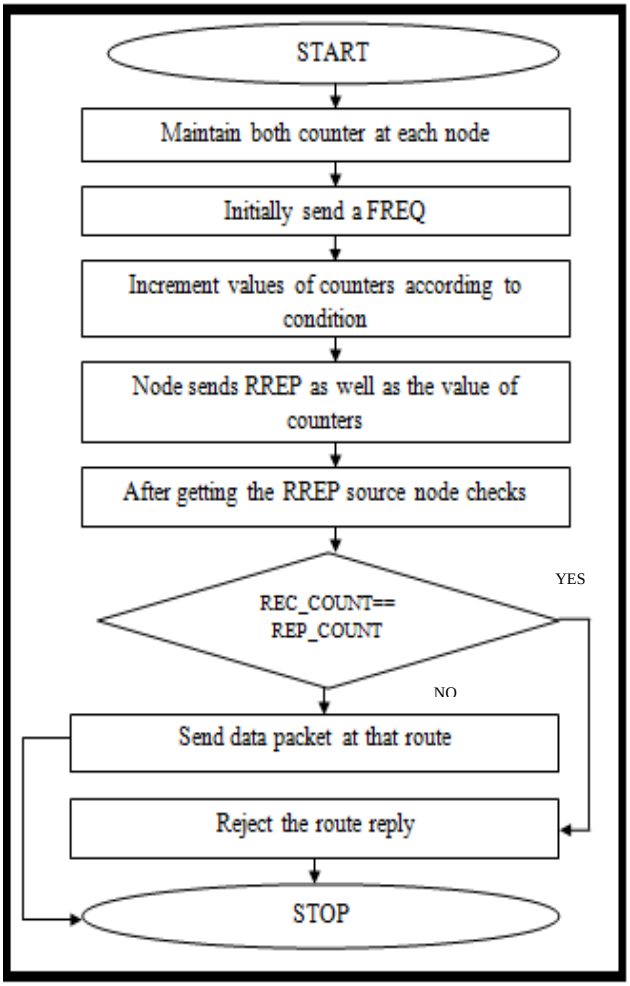

Fig 1: Flow Chart for proposed technique

IV. RESULT AND DISCUSSION

The model is simulated in MATLAB .The network have initially 50 MNs that are distributed randomly, 10% of these MNs are considered as black hole MNs arbitrarily. Model computes the results by varying no. of MNs. These nodes are distributed in an area of 50*50 meter square.

In order to evaluate the performance of the proposed work, the performance parameters throughput, resource overhead and end to end delay are considered.

PERFORMANCE PARAMETER:

AVERAGE END-to-END delay: it is the time taken for a data packet to be transmitted over a network from source to target.

$$E = \frac{\sum_{i=1}^{n} xi}{\sum_{i=1}^{n} e1 - s1} \qquad (1)$$

ROUTING OVERHEAD: it refers to the number of routing packets forwarded per data packet. The performance is improved when routing overhead is low.

$$RO = \sum_{i=1}^{n} Ri \qquad (2)$$

THROUGHPUT: It is expressed as total number of packets received (X) at the destination in the network divided by the difference of stop (t2) and start time (t1) of the simulation time [14].

$$T = \frac{\sum_{i=1}^{n} Xi}{t2 - t1} \qquad (3)$$

These parameters are computed in order to check the performance of the network. An analysis of Resource Overhead, Throughput and End to end delay has been shown in fig. 2, fig. 3 and fig 4 to analyze the performance of proposed work against control packet based technique proposed by Kalia [9] and fake RREQ based technique proposed by Jaspinder Kaur [8] when the percentage of Blackhole node is constant and number of nodes are varied from 50 to 100 and 150.

An analysis of fig. 2, fig. 3 and fig. 4 show that the performance of the proposed work is better as compared to control packet based technique and fake RREQ based technique in the case of Routing Overhead, Throughput and End to end delay.

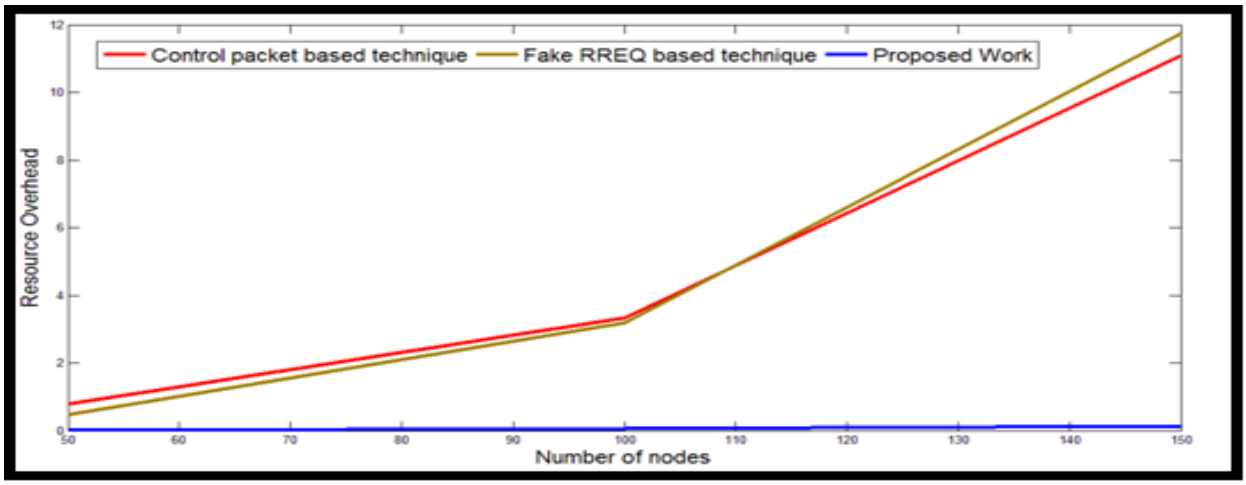

Fig. 2: Resource overhead value for different number of nodes at 10 percent Blackhole

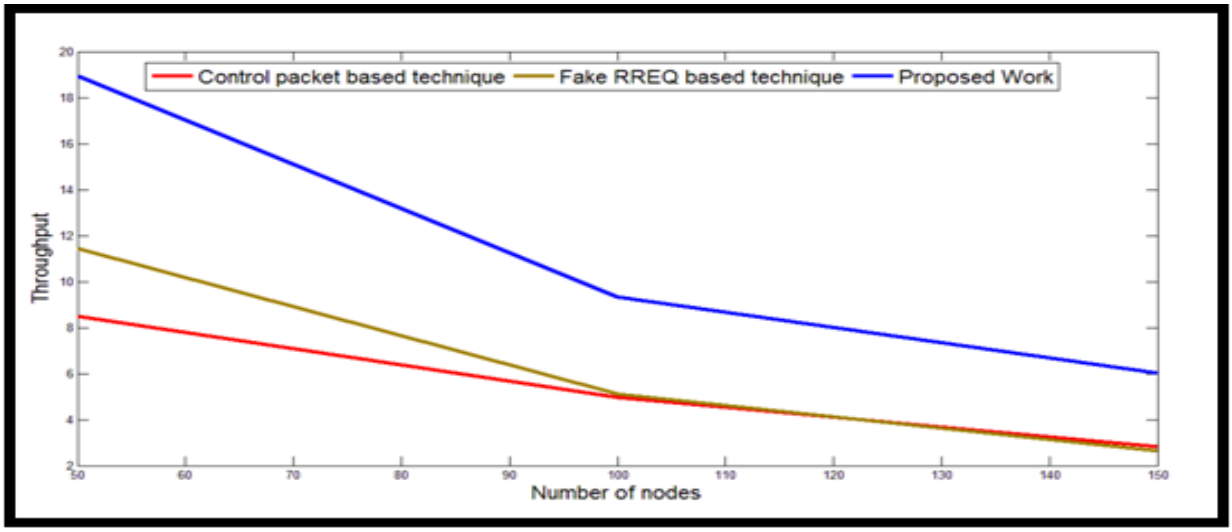

Fig. 3: Throughput value for different number of nodes at 10 percent Blackhole

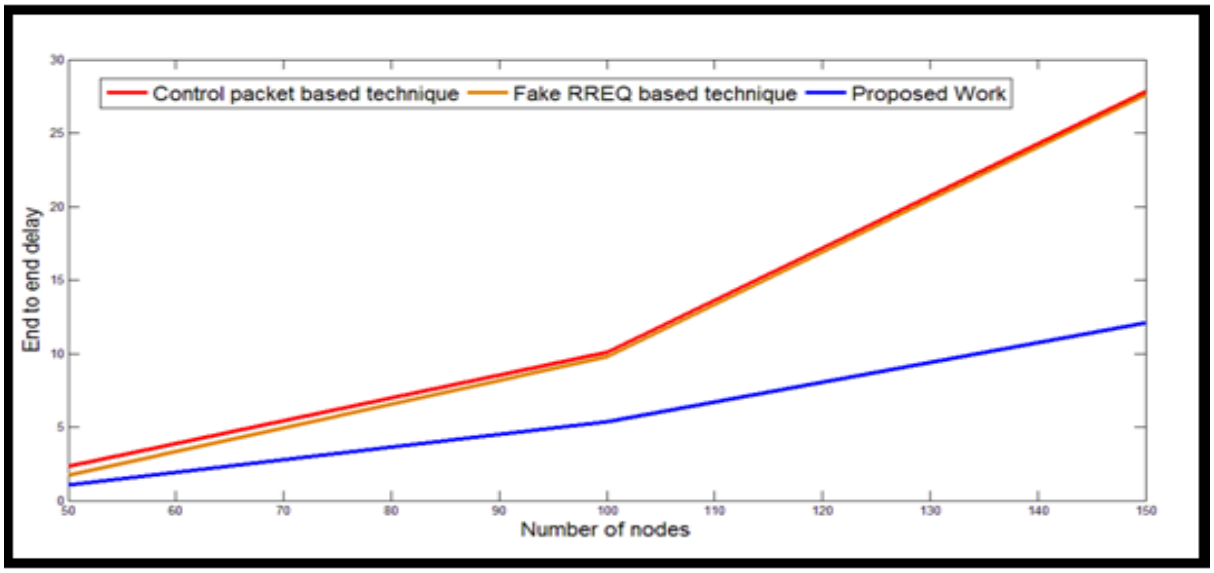

Fig. 4: End to end delay for different number of nodes at 10 percent Blackhole

A plot of the Resource Overhead regarding number of nodes from 50 to 150 (with an interval of 50) is shown in Fig. 2 which gives the variation in the value of PDR with respect to number of nodes. The number of nodes in the network may vary according to the environment; the results have been taken by considering a plot of throughput against number of nodes which has been shown in Fig. 3. This Figure shows the deviation in the value of throughput regarding the amount of nodes. Fig. 4 has shown that the network performance with respect to PLR is changed when the number of nodes is varied.

V. CONCLUSION

Black hole attack detection is important because black hole reduces the throughput, increases the end to end delay which results in degradation of overall network performance. In this paper, a new approach for detecting black hole MN is proposed on the basis of two counter values. As concluded from results proposed solution gives better result as compared to the two already existing techniques. The routing overhead is reduced as the battery consumption is less which is the main problem in Ad hoc on demand routing .The considerable fall in End to End delay and rise in throughput are observed through the proposed approach. This work can also be applicable to other routing protocols for detecting Black hole attack.

VI. REFERENCES

[1] D. Kshirsagar and A. Patil, “Blackhole attack detection and prevention by real time monitoring,” In *Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference on IEEE*, pp. 1-5, 2013.

[2] K. S. Chavda and A. V. Nimavat, "Removal of black hole attack in AODV routing protocol of MANET," In *Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference on IEEE*, pp. 1-5, 2013 .

[3] D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa, and R. H. Jhaveri. "A survey of reactive routing protocols in MANET," In *Information Communication and Embedded Systems (ICICES), 2014 International Conference on IEEE*, pp. 1-6 , 2014.

[4] V. Khandelwal and D. Goyal, "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume* 2, pp. 1555-1559, 2013.

[5] P. K. Singh and G. Sharma, "An Efficient Prevention of black hole problem in AODV routing protocol in MANET," In *11th*

International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, pp. 902-906, 2012.

[6] S. Ahmed, M. Elsabrouty, and A. Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)," In *Computational Science and Engineering (CSE), 16th International Conference on IEEE, pp. 346-352,2013.*

[7] A. Bhattacharyya, A. Banerjee, D. Bose, H. N. Saha and D. Bhattacharya, "Different types of attacks in Mobile ADHOC Network," *arXiv preprint arXiv:1111.4090*, 2011.

[8] J. Kaur, and and B. Singh, "Detect and Isolate Black hole attack in MANET using AODV Protocol," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, 2014.

[9] N. Kalia, and H. Sharma. " Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," International Journal on Computer Science and Engineering (IJCSE), Vol. 8, pp. 0975-3397, 2016.

[10] K. S. Arathy, and and C. N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET," *Procedia Technology* 25, pp. 264-271, 2016.

[11] S. C. Satapathy, A. Joshi, N. Modi, and N. Pathak, Proceedings of International Conference on ICT for Sustainable Development: ICT4SD, Springer, Vol. 2 , 2015.

[12] S. S. Abdelhaq, R. Alsaqour, and M. Tanaka, "A local intrusion detection routing security over MANET network," Electrical Engineering And Informatics(ICEEI), 2011 *Fourth International Conference on*, IEEE, pp. 1-5, 2016.

[13] A. A. Chavan, D. S. Kurule, and and P. U. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack," *Procedia Computer Science* 79, pp. 835-844, 2016.

[14] S. Gurung, and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks, Springer Science+Business Media New York, pp. 1-15,2016.*

[15] S. Kopekar, and A. Kumar, "A Study of Ad-Hoc Wireless Networks: Various Issues in Architectures and Protocols," *International Journal of Computer Applications, Volume 122*, pp. 0975-8887, 2015