Revamped Malicious Node Detection and Removal Scheme in MANET using Auxiliary Cluster Head

Niveditha P S, Sreeleja N, Unnithan, Prasad R Menon

Abstract: ***The Mobile ad hoc networks are widely accepted due to its wide range of applications in various fields of life. Amidst these advantages MANETs faces a lot of security issues due to its mobile nature and lack of efficient security mechanisms. Proposed EMDR (Esteem based Malicious node Detection and Removal) scheme provides a secure routing method for the efficient transfer of data in the network. This protocol helps to overcome the malicious node attacks effectively. It utilizes the validity value table, esteem level table and neighbor table maintained by every mobile node in the communication network to find and use a secure route between the initiating node and the final node. Depending upon the values obtained in the validity value table and esteem level table, the cluster head node identify the malicious nodes present in the path and find the most reliable route to the destination node. In addition to this security mechanism, here every mobile node has more than one cluster head. This standby cluster head is termed as auxiliary cluster head (ACH). When the main cluster head fails during data transmission, then the source node seeks the help of the auxiliary cluster head immediately. Thus it eliminates the condition of network failure.***

*Index Terms****:Auxiliary Cluster Head, Malicious Node, Network Failure Reduction.***

I. INTRODUCTION

Mobile Ad hoc Network abbreviated as MANET is a dynamic communication system consisting of moving nodes that can communicate with every other node present in the network [1,3]. In a MANET every node will be willing to transfer data to other member nodes at any particular instant of time. The nodes in a network will have specific communication range. Nodes within this range can communicate directly without relying on any others. MANETs don't rely on any fixed infrastructure to exchange information between the nodes [4-7].

These special features of MANETs made it more attractive and acceptable. It has wide range of applications [8] in military or police exercises, disaster relief operations, mine site operations, urgent business meetings etc. Even though it is widely accepted it has some disadvantages too. The routing protocols used in MANETs doesn't have any particular security mechanism to overcome the attacks from the attacker nodes.

Revised Manuscript Received on May 28, 2019.

Niveditha P S, Department of Electronics and Communication Engineering, NSS College of engineering, Palakkad, Kerala, India.
Sreeleja N Unnithan, Department of Electronics and Communication Engineering, NSS College of engineering, Palakkad, Kerala, India.
Prasad R Menon, Department of Electronics and Communication Engineering, NSS College of engineering, Palakkad, Kerala, India

The continuously changing topology of the MANET makes the network unstable [12-17]. High cooperation between the devices is essential to carry out a smooth communication between the nodes. The open media nature of the MANETs result in the easy attack of the selfish nodes

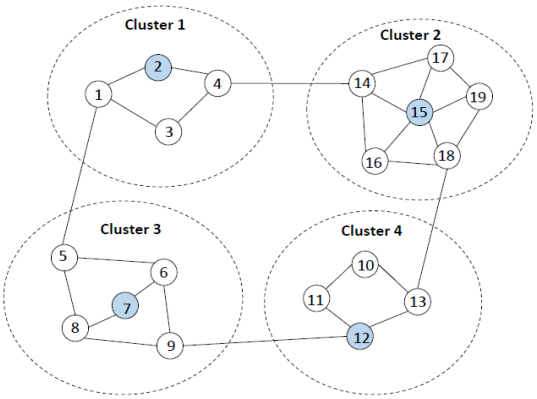

Fig. 1. General diagram of a MANET

1.1 Malicious node attacks

The common protocols in MANETs are vulnerable to the attack of malicious participants, since there are no specific security mechanisms present in it. The malicious participants drop or corrupt the data packets during the transmission between the various nodes present in the communication network. These malicious participants are generally termed as malicious nodes. Different types of malicious node attacks are prevailing. It includes black hole attack, worm hole attack and gray hole attack [14-17].

Figure1 shows the packet drop due to the malicious node attack. In the given scenario node one is the source node and node nine is the destination node. The node marked as m in red color acts as the malicious node. The scenario represented in the figure is a black hole attack, in which the attacker node sends false information to the source node and will create unreliable path to the destination node. All the data packets arriving the selfish node are dropped as shown in the figure. The green boxes represent the data packets. It is very difficult to tackle this attack since the attacker node is capable of mimicking the normal node behaviour. The malicious node will not pass the data packets to the next node. Hence it results in a network failure. In this situation the cluster head will have select another path to reach the destination. A new route without the presence of the selfish nodes will have to be found. This process will

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

consume additional energy and time. Thus it reduces the efficiency of the network.

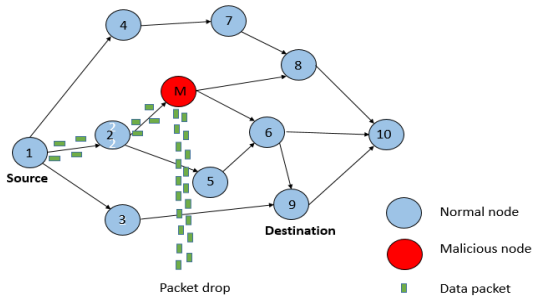

Fig. 2. Data loss due to malicious node attack

The EMDR (Esteem based Malicious nodeDetection and Removal) scheme eliminates the attack from the selfish nodes by using the esteem value. It effectively identifies the selfish nodes and will remove it from the communication network. This will generate additional energy utilization. The RMNDRS (Revamped Malicious Node Detection and Removal Scheme) method incorporates auxiliary cluster head in the EMDR scheme and eliminates the issue of network failure [18].

In this paper we propose a revamped selfish node identification and removal scheme which effectively eliminates the external attacks. In the next section we discuss the related works that were conducted in this field to eliminate the selfish node attack and improve the network security. In the later section abrief idea of Esteem based Malicious node Detection and Removal scheme, which is used to identify and remove the attacker nodes using the esteem value and conformity value is given. In the fourth section we discuss the revamped EMDR method which improves the energy utilization of the member nodes and increases the network lifetime. The last section gives the conclusion of proposed work.

II. RELATED WORKS

Detection and elimination of the selfish nodes has been a topic of burning importance for a long period of time. The most relevant points that emerged during the studies that are carried out by different researchers in different part of the world in this field of mobile adhoc network communication security are the following. Esteem level table maintained by each member node in the network can be used to identify the unreliable nodes present in the communication path by estimating the validity of the node [1]. The member nodes present in the MANET are in a random motion. It is very tiring to estimate their current location. Maintaining an auxiliary cluster head helps to resolve the problem of path failure [3]. Gray hole and black hole are mostly due to the incorrect routing data provided by the member nodes [4]. Check points maintained by the cluster head helps to reduce its work burden and increase the network stability [10]. Dividing the entire communication network into small groups increase the fault tolerance capability of the network [13]. Assigning a unique identity for each node present in a network can help to avoid the intrusion of the attacker nodes. The selfish attacker nodes will be unaware of the identity maintained by the member nodes present in the network. It will help to easily identify the selfish nodes [18].

III. EMDR Based Method

The EMDR (Esteem based Malicious node Detection and Removal) based method is an on demand routing protocol, which is similar to the AODV protocol. It is used to overcome the effect of the malicious participants during the data transmission between source node and the destination node. This method makes use of the AODV protocol to create the path. In EMDR based scheme, each cluster head node maintains the Neighbor Table, Esteem Level Table and Conformity Value Table. These tables are maintained in order to keep data about the nodes present in the communication network. During the route discovery in EMDR scheme, an intermediate node will not transfer the data packets through a node which is malicious. That is, the node which gives a wrong routing information or esteem value greater than 1. The neighbor table of the all the member nodes keeps the list of its nearby members and corresponding cluster heads.

3.1 Conformity value

It is the value calculated to find the number of successful transmission paths. It is the ratio of the success count to the total count. The conformity value is tabulated to generate the conformity value table. The conformity value table consists of four different fields in it. It includes the node ID, success count, total count and the conformity value. The ratio of success count to total count is evaluated to estimate the conformity value. This conformity value is further used to estimate the esteem value. The conformity value of each node is individually calculated.

3.2 Esteem level.

Esteem level table gives the idea regarding a node, that is a reliable node or not. Esteem level table consists of the node ID and the corresponding esteem values. Based on these esteem value, the cluster determines which are the trustworthy nodes and which are not. The decision is taken based on the comparison of the esteem values with a predefined threshold value. The threshold value is selected depending on the results of many repeated experiments. The initial esteem value of every member node is set to the value 0.7. If the esteem value obtained for aparticular node is smaller as compared to the threshold value, then the node is assumed to be a selfish node, which is not trustworthy. If the esteem value is greater as compared the threshold value, then the node is considered as trustworthy and that particular node is included in the path. If the cluster head finds that a particular node is not trustworthy then it declares the node to be malicious and to remove it from the neighbor table of all the nodes. Thus the selfish node attacks can be eliminated.

The esteem value is calculated using the formulae given below

Esteem value = (TDP-PN)/PN + CV (1)

The esteem value is calculated by transmitting some dummy packets by the initiating node to the intermediate node and it calculates the esteem value. In the equation, TDP represents the total number of dummy data packs transmitted by the initiating node to the intermediate node and PN represents the number of dummy data packets transmitted by the intermediate node to the next node. If the intermediate node is a selfish node, then it will silently drop or degenerate some or many of the information bearing packets reaching the particular node. This will create a difference in the value of PN. CV represents the conformity value. The conformity value is also used to find the esteem value.

RMNDRS Based Method

Revamped malicious node detection and removal scheme(RMNDRS) is an improved version of the EMDR scheme. Here in addition to the security RMNDRS provides high level of stability to the network. The stability is achieved by introducing an additional cluster head called auxiliary cluster head to every node present in the communication network. The auxiliary cluster head acts as a stand by cluster head. When the main cluster head fails the auxiliary cluster takes off the duty and will prevent the network failure. The auxiliary cluster head is selected depending on the highest remaining energy of the member nodes.

If the source node wants to communicate with any other cluster member via the cluster head, it can send the data initially to the corresponding cluster head. This is monitored by the auxiliary cluster head. Initially each of the member nodes chooses highest energy node as its cluster head and the second highest energy node acts as the auxiliary cluster head. When the main cluster head fails during the information exchange, rather than re-electing the cluster head, the nodes continue to send the data through the auxiliary cluster head. The auxiliary cluster head thus helps to minimize the energy utilization by effectively avoiding the cluster head election when the main cluster head fails.

IV. RESULTS AND DISCUSSION

The RMNDRS is implemented using the NS2 simulator tool. The simulation is carried out using 30 mobile nodes in the specified area of 960 meter by 960 meter. The simulation is executed for 200 seconds. The packet size is taken to be 512 bytes and each node has 250meter coverage. All nodes are assumed be mobile with random mobility.

1) Malicious node detection.

A node is evaluated to be malicious if the esteem value obtained is less than the assumed threshold value. Here the threshold value is assumed to be 0.7. It is calculated by carrying out a number of repeated experiments and an appropriate value is calculated. During the simulation the node 13 is set as malicious node. Then the esteem value is calculated and found that its value is below the threshold value and that node is marked as the selfish or attacker node. Figure below shows the variation of the esteem value for each node. Only the esteem value of the malicious node that is node number 13 goes below the threshold value. All the other nodes have esteem value above the threshold value indicating they are trustworthy nodes.

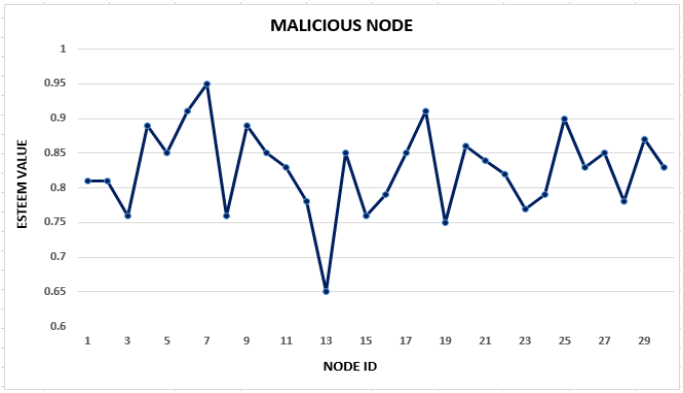

Fig.3. Variation of the esteem value with behaviour of the nodes.

2) Delay

Delay of the packet transmission is calculated by making use ofthe hop count between the initial node and final node, routing time taken and the maximum time required to reach the final node. Figure below shows that the proposed protocol achieves a lower delay as compared to the existing protocols. The presence of auxiliary cluster head helps to reduce the pause time during the data transmission and thus attains less delay.

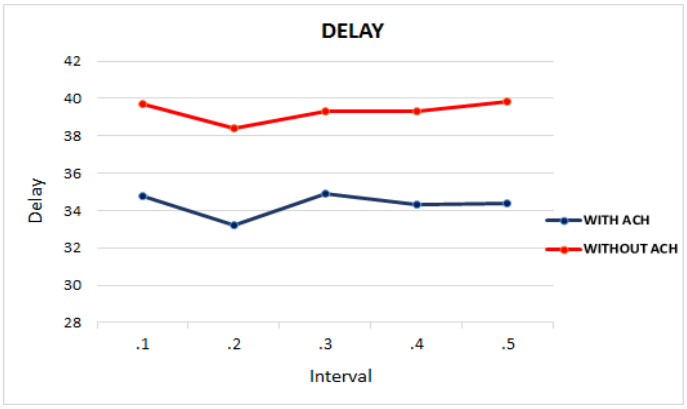

Fig.4. Variation of delay with packet interval

3) Packet delivery ratio

Packet delivery ratio is defined as the percentage of messages or information packets got by the destination node and sent by the initial node.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

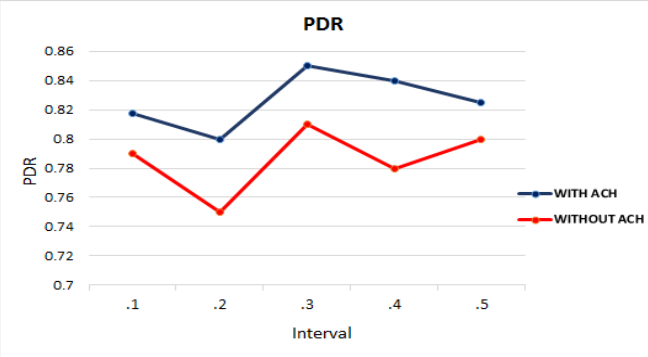

Fig.5. PDR based on packet interval

Best routing ensures the transfer to the destination with minimum packet loss. The PDR obtained for the normal EMDR based method is compared with that including auxiliary cluster head. Figure above shows that the presence of auxiliary cluster head improves the packet delivery ratio by a considerable amount. The number of data packets that reached the destination accurately was found to be increased by more than two percentage of the initial value that obtained without using the auxiliary cluster head. Auxiliary cluster heads eliminate the issue of packet loss due the network failure.

4) Throughput

Throughput is characterized as the measure of information moved effectively starting with one location then onto the next in a given time.It is typically measured in bits per second. It is also known as the rate of fruitful message conveyance. Throughput of a given network increases when the connectivity between the initial node and the final node is high. With the approach of an auxiliary cluster head, it helps to maintain a sustainable link between the nodes without any failure. Thus, the throughput of the network with auxiliary cluster head appears to be increased.

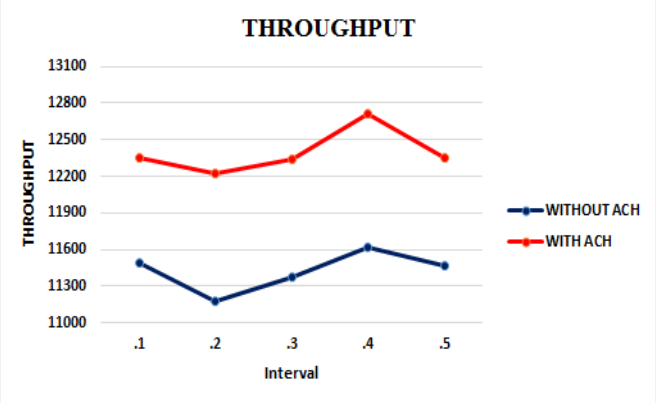

Fig.6. Throughput based on packet interval

Figure above shows the comparison of the values of throughput obtained for networks with and without auxiliary cluster head. It is very clear from the graph that the throughput has improved tremendously by incorporating an additional auxiliary cluster head in the communication network. The auxiliary cluster head eliminates the chances of network failure thereby improves the throughput of the communication network.

V. CONCLUSION

MANETs faces a lot of security issues due to its mobile nature. Hence an efficient routing protocol is inevitable. This work proposes a safe and efficient routing mechanism for protecting the member nodes of the network from the attacker and which eliminates the chances of network failures. RMNDRS (Revamped Malicious Node Detection and Removal Scheme) based method depends on the conformity value and esteem level to identify the selfish nodes. Validity value table, esteem level table and neighbor table maintained by each node in the communication network directs the initiating node to find and use a safe route between the initial node and final node. Esteem level of a particular node is calculated from the conformity value maintained by each member node in the communication network.The proposed protocol makes use of an auxiliary cluster head to avoid the issues of network failures. After the clustering procedure, the member nodes in each cluster elects two cluster heads instead of the normal single cluster head. They are elected based on the highest residual energy available. The auxiliary cluster heads act as a stand by cluster head. If the main cluster head fails during data transmission, then the auxiliary cluster head immediately takes the duty,thus it minimizes the additional retransmissions during the data transfer.

REFERENCES

1. Saurabh Sharma and Dr. Sapna GambhirCRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs, 11th International Conference on Intelligent Systems and Control (ISCO) 2017.
2. Sushant Patial, Jawahar Thakur, Check pointing and Rollback Recovery Algorithms for Fault Tolerance in MANETs: A Review, Int. J. Advanced Networking and Applications 6(3) (2014).
3. Saira Banu S., DhanasekranR., A New Residual Energy Based Multipath Routing Approach for Wireless Sensor Networks, European Journal of Scientific Research 95(2) (2013), 168- 179.
4. Rutvij H. Ihaveri, Sankita J. Patel and Devesh C. linwala, A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad hoc Networks, in Proc. ACCT '12, 2012, p. 556-560.
5. Saurabh Gupta, Subrat Kar, S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet, in Proc. JJT'll, 2011, p. 226-231.
6. Saurabh Gupta, Subrat Kar, S Dharmaraja, BAAP: Black hole Attack Avoidance Protocol for Wireless Network, in Proc. ICCCT'j j, 2011, p.468-473.
7. G. S. Mamatha and Dr. S. C. Sharma Analyzing the MANET Variaitons, Challenges, Capacity and Protocol Issues,International Journal 0/ Computer Science & Engineering Survey (fJCSES) , voU,no.1 , August 2010.
8. G. S. Mamatha and Dr. S. C. Sharma Analyzing the MANET Variaitons, Challenges, Capacity and Protocol Issuesinternational Journal Computer Science & Engineering Survey (IJCSES) , vol.no.1 pp. 14-21 , August 2010.

9. Z. G. M. Zhou and Cao, Cluster-based inter-domain routing (CIDR) protocol for MANETs, IEEE/IFIP WONS, pp. 19–26, 2009.
10. M. H. X. Siwei, Liu. Dejun, An on-demand source based clustering multicast routing protocol in Ad Hoc network, pp. 408–412, 2009.
11. S. Misra, and I. Woungang, Guide to Wireless Ad Hoc Networks. Springer, 2008.
12. RadhaPoovendran and LoukasLazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks,A CM Journal on Wireless Networks (WINET), vol. 13, pp. 27 - 59, March 2007.
13. C. Liu and J. Kaiser, A survey of mobile ad hoc network routing protocols, University of Magdeburg, vol. 13, no. 5, pp. 33–82, 2005.
14. Issa Khalil, Saurabh Gagchi, Ness B. Shroff, LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multi hop Wireless Networks,in Proc. DSN'05, 2005, p. 612-621.
15. M.A.Shurman, S.-M. Yoo, and S. Park, Black hole attack in mobile adhoc networks,in Proc. ACMSE '04, 2004, p. 96-97.
16. T. Cormen, C. Leiserson, R. Rivest, and C. Stein, Introduction to Algorithms. PHI, 2004-2005.
17. I. Chlamtac, M. Conti, and J. Liu, Mobile Ad Hoc Networking: imperatives and challenges, Ad Hoc Networks, vol. 1, no. 1, pp. 13–64, 2003.
18. Yih ChunHu, Adrian Perrig, David B. Johnson, Rushing Attacks and Defense in Wireless Ad hoc Network Routing Protocols,in Proc. WiSe '03, 2003, p. 30-40.
19. Y. Ko and N. Vaidya, Location-Aided Routing (LAR)in mobile ad hoc networks, Wireless Networks, vol. 6, no. 4, pp. 307–321, 2000.
20. M. Steenstrup, Cluster-based networks, in Ad Hoc Networking Ed., chapter 4, pp. 75–138, Addison-Wesley, Reading, Mass, USA, 2000.

AUTHORS PROFILE

Author-1 Photo

Niveditha P S is a M. Tech Student in Department of Electronics and Communication Engineering, NSS College of engineering, Palakkad, Kerala, India.

Author-1 Photo

Sreeleja N Unnithan is a M.Tech student in Department of Electronics and ommunication Engineering, NSS College of engineering, Palakkad, Kerala, India.

Author-1 Photo

Prasad R Menon is working as Assistant Professor in Department of Electronics and Communication Engineering, NSS College of engineering, Palakkad, Kerala, India