*International Journal of Engineering & Technology*, 7 (3.29) (2018) 470-473

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# Finding an accuracy on legitimacy & reputation value based malicious node detection & removal scheme on cluster in MANETs

**D. Sameera [1] *, V. C. Gayathri [2]**

*[1] Research Scholar, SSSUTMS, M.PAssistant Professor, ITBVRIT, Narsapur, TS, India*
*[2] Assistant Professor, IT, BVRIT, Narsapur, TS, India*
**Corresponding author E-mail: sameerach24@gmail.com*

**Abstract**

While Nodes forms networks dynamically & they doesn't have any central control infrastructure in mobile ad hoc networks thus routing becomes a significant issue. As packet forwarding is done by nodes itself there is increased possibility of packet dropping or DOS (denial of service) .so, the security in wireless networks became a challenging issue in MANET. For getting secure delivery of data we require efficient routing scheme, here is the proposal "Finding an Accuracy on Legitimacy & Reputation value Based Malicious Node Detection & Removal Scheme on Cluster in MANETs" for detecting and removal of malicious nodes in a cluster. In this paper for a structured MANET, Network has number of clusters with number of nodes, each cluster has a cluster Head(CH), as packet forwarding done by nodes they need a node ID (including CH needs node ID) which is a prime number. Here to identify and use secure route between a source and a destination, every node need to maintain legitimacy value table(LVT) and reputation level table(RLT) in the network. The cluster head node Deny or Entail the malicious nodes from the identified route and select the most optimized route to a determined destination based on legitimacy value LV & reputation value RV.
As proposed in existing system the reputation values calculation is not producing good accuracy and if we use the same calculation the efficiency will affect. So, we proposed the alternative solution for this and we identified new attack and here we are providing solution for this attack by finding accurate reputation value of Malicious Node (MN) by comparing in Reputation Level Table (RLT).

***Keywords***: *Use about five key words or phrases in alphabetical order, Separated by Semicolon.*

## 1. Introduction

Mobile Ad hoc networks (MANET) are infrastructure less networks with wireless nodes. Due to short range connectivity, each node depends on other nodes for forwarding the packets, which leads to a multi Hop communication due to its dynamic topology [2]. As there won't be any central control of network operations, the control will be given to list of nodes. So, nodes need to be cooperative with each other and each node should exchange the data as needed to implement routing and security.
MANET has security threats, as it is wireless. In designing a network MANET faces many security challenges. Ad hoc network functionality is established through node cooperation. So, the MANET faces attacks like Black, Grey [1] [5] & worm hole attacks [1].
Black hole attack: In this, the attacker sends wrong route to destination through itself. It drops the packet when the actual data packets arrive.
Grey Hole attack: this attack works same as black hole, the differences here is dropping of selective packets of some kind.
Worm whole attack: By this the control over the network can be taken by the attacker, as the attacker makes special short circuit to forward all
Packets.

## 2. Related work

Malicious node detection in MANET is very tectonic and problematic from many years & many researchers are deliberate about this problem.
Saurabh Sarma ET. al. [1], proposed CRCMD&R introduced, in cluster every node having separate ID (Node ID) and for each cluster there will be one cluster head, to know about the secure data transfer.
Saurabh Gupta et.al [4] proposed an approach for black hole attack (BAAP) i.e. AOMDV. In this, for finding optimized path he introduced a table i.e. Legitimacy, it is maintained by each node. An optimized path and legitimacy ratio calculations are based on path and sent count fields.
Rutvij H. Jhaveri ET. al. [5] proposed an approach i.e. on demand secure routing protocol for finding gray and black hole attacks. With this approach, we can find malicious nodes and forward the malicious node information to whole network.
Subrat kar ET. al. [6] narrate a protocol WHOP. To nurture cooperation among nodes it uses hound packets. Based on node ID only complete route selection criteria will done and at the time of path setup each node should expose its ID.
Adrian Perrig ET. al. [7] Like RAP protocol, he proposed AODV. For authentication purpose, it uses highly systematic digital signa-

ture-based cryptography. To find out Legitimate neighbour, he designed an uncomplicated delay time based three step authentication neighbour detection protocol. RAP also can find utilize path for empower successful routing and deliver the packets.

## 3. Proposed scheme

In this section presents our malicious node detection scheme, now a days finding malicious node is main issue of network to send packets from source to destination throughout the path, because attacks are increasing day by day. To form the Optimized path this scheme uses AODV (Ad hoc On-Demand Distance Vector). To store information about all the nodes, the cluster head need to maintain three tables, i.e. Neighbour table, legitimacy value table and reputation level table [1][3]. In this scheme, in a group of feasible intermediate nodes, the selected intermediate node whose replied information is correct or prime product term is fully divisible or reputation value of that node does not cross the threshold value (level 0 &level 1) that is optimal node. In proposed, some differences are identified by considering AODV and CRCMD&R, improved calculations for throughput.

1) RREQ Packet:

It's a route request packet from source to destination. In this Packet structure consists of hop count, request ID & CH node ID, with IP addresses of Source and destination as well as Sequence no. of source and destination [1].

| Types | J | R | D | G | U | Reserved | Hop Count |
|---|---|---|---|---|---|---|---|
| Cluster Head Node ID of the originator | | | | | | RREQ ID | |
| Originator IP Address | | | | | | | |
| Originator Seq Number | | | | | | | |
| Destination IP Address | | | | | | | |
| Destination Seq Number | | | | | | | |

**Fig. 1:** RREQ Packet in Proposed.

2) RREP packet

It is a route reply packets from Destination to Source. Node ID of next node of D i.e., $N_{RREP, Prime}$ Product number, $N_{RREP}$'s CH node ID [6], hop count, IP address of Source & Destination, sequence number of D are the fields of the RREP packet [1].

| Types | R | A | Reserved | Prefix Size | Hop Count |
|---|---|---|---|---|---|
| Source IP Address | | | | | |
| Destination IP Address | | | | | |
| Destination Seq Number | | | | | |
| $N_{RREP}$ Next Node | | | | Life time | |
| Node ID | Prime Product Number | | | Cluster Head Node ID of $N_{RREP}$ | |

**Fig. 2:** RREP packet in Proposed

3) Neighbour Table:

This is used to know CH node ID of every Node in network [1].

**Table 1:** Neighbour Table

| Node ID | Cluster Head Node ID |
|---|---|

4) Legitimacy Table:

Legitimacy Table maintained by CH to know the successful transmission on paths Legitimacy value = Success count / Total count [1-4].

**Table 3.1:** Legitimacy Value Table

| Node ID | Success Count | Total Count |
|---|---|---|

**Table 3.2:** LV Table

| NODE ID | Legitimacy Value |
|---|---|

5) Reputation Level Table:

CH node calculates RV replied node NRREP & next node of $N_{RREP}$ (If both nodes are in same cluster) when it enters promiscuous mode to check prompt forwarding of packets. Reputation Level Value will depend on Reputation Level Table [1-3].

**Table 3:** Reputation Level Table

| Level | Node Status | Reputation Value |
|---|---|---|
| 1 | Distrust | 0, t |
| 2 | Suspect | t,0.7 |
| 3 | Less trust | 0.7,0.9 |
| 4 | Trust | 0.9,1 |

Reputation Level value should be between 0 & 1. If a node is a malicious node, its RV will be 0, or else If a node trust worthy node its RV will be 1. For certainty levels of nodes will refer to RLT. In RLT, 't' stands for threshold value which is initially set to 0.7. based on t value will decide whether the node is malicious or trustworthy.

If RV is < t the node will be In Level 1 & treated as malicious. If the RV is in between t & 0.7 will be treated as suspect node i.e., Level 2 & if the RV is in between0.7 & 0.9 will have treated as less trust i.e. Level 3 & finally if RV in between 0.9 & 1 will consider as trust worthy node in Level 4.

i) Source node (S) broadcast RREQ message into network during secure discovery of route. Intermediate node(I)will responds with RREP message. This message will be included with fields such as i) Cluster Head ID,

ii) product of prime numbers from Destination(D) to Source in the form of Prime Product Number(PPN). After receiving RREP from Intermediate Node (I), the CH of Source(CHs)will divide PPN with number of Node ID's in neighbour table to see whether replied node($N_{RREP}$) reliable or not.

In our Proposed network, Source S is 5 and destination D is 31 as shown in Figure 3 Network topology. When CH of source node & CH of $N_{RREP}$ is not same [1]. The PPN should be divisible then only the node will be partially declared as reliable. Now PPN is calculated as follows: PPN = (31*37*7*2*47*11)/7 = 12617.Now the PPN value is fully divisible, so the source node partially declares the intermediate node as reliable node for source node. As it is reliable node S sends N number of dummy packets towards the intermediate node ($N_{RREP}$) node 47.

As the CHs and CHI is same i.e. node 11, the CHs enters promiscuous mode and counts the reputation value of Intermediate node and next node of it, if in the same region.

Reputation value $\frac{(\frac{TDP_S - PSN_{RREP}}{TDP_S})+K(LV)}{K}$

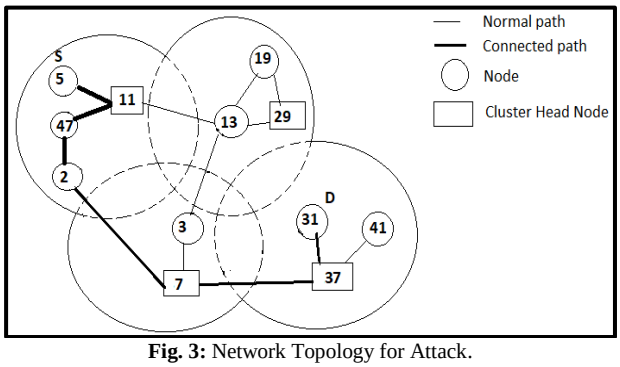


**Fig. 3:** Network Topology for Attack.

TDPS is a total number of dummy packets sent by source to $N_{RREP}$ for forwarding the packets, PS is a total number of packets sent to the next node of $N_{RREP}$ by $N_{RREP}$. LV is the legitimacy value of a node calculated by source node, K is the reputation value weight, which should be > [2].

As CHS i.e., 11 and CH of Intermediate (47) or NRREP is same, source sends 120 dummy packets to $N_{RREP}$. Now, the CH of source node (CHS) enters promiscuous mode & counts the reputation

value (RV) of $N_{RREP}$ and next node of it i.e., Node 2 ($N_{RREP}$). Node 47 receives 120 packets and sends 30 packets to its next node 2, which is in the same region, and suppose Legitimacy value of 47 is 0.2, k is 3(supposed).

$$\text{Reputation value} = \frac{(\frac{(120-30)}{30}+3(0.2)}{3} = \frac{3.6}{3} = 1.2$$

Will compare Reputation Value with Reputation Level Table, As Reputation value is larger than 1, the intermediate node 2(I) is total trust [1].

The next node of replied node NRREP (NNN) is node 2 received 30 packets from $N_{RREP}$ & sends 10 packets to its next node. The legitimacy value of node 2 is 0.4 & K is [3] (supposed). The Reputation value of node 2 is calculated as,

$$\text{Reputation Value} = \frac{\frac{30-10}{10}+3(0.4)}{3} = 1.06$$

Now the Reputation value of node 29 is compared Reputation Level Table, Reputation value is greater than [1] so the node 2 is justified as trustworthy node.

Algorithm 1: to detect collaborative malicious node attack in MANET's:

Notations:

| | |
|---|---|
| S: Source Node | I: Intermediate Node |
| D: Destination Node RV: Reputation Value | $N_{RREP}$: RREP From Intermediate Node |
| LV: Legitimacy Value | $CH_{IN}$: Cluster Head of Intermediate Node |
| MN: Malicious Node | $CH_S$: Cluster Head of Source Node |
| NNN: Next Hop Node of $N_{RREP}$'s | RLT: Reputation Level Table |

1) Start
2) for (source node)
3) {
4) Broad cast RREQ packet to everyone
5) Receive RREP
6) Based on largest sequence number and minimum hop count and all other RREP buffered at originating node RREP will be selected.
7) Procedure
8) }
9) If (prime product term is fully divisible && replied information is right)
10) {
11) Partially declared node as trustworthy node
12) S sends n number of dummy packets towards NRREP.
13) If ($N_{RREP}$'s CH = S's CH)
14) {
15) CHS enters Promiscuous mode.
16) CHS count RV of NRREP and NNN (if present in the same region) with the following formula.

$$\text{Reputation value} = \frac{(\frac{TDP_S - PSN_{RREP}}{TDP_S})+K(LV)}{K}$$

1) Compare RV with RLT
2) }
3) Else
4) {
5) CHS sends encrypted info from NRREP to CHIN via predefined trusted path. i.e E[number of dummy packets ,S,D,LV1……I, Nonce].
6) CHI enters promiscuous mode after decrypting it.
7) CHI Count RV of NRREP and NNN with the following formula.

$$\text{Reputation value} = \frac{(\frac{TDP_S - PSN_{RREP}}{TDP_S})+K(LV)}{K}$$

1) Compare RV with RLT.
2) }
3) }
4) If(Any node has level 1 or level 2 or reputation >1)
5) Call Removal of Malicious nodes();
6) Else
7) Declare nodes as Trustworthy and start data transmission from S to D.
8) Else
9) {
10) Declare $N_{RREP}$ as MN.
11) Call Removal of Malicious node();
12) }
13) }
14) Stop

Algorithm 2: TO remove malicious nodes from the MANETs

Notations:

CH: Cluster Head MN: Malicious Node(s)

1) Start
2) Respective CH adds MN to malicious list.
3) Transmit this list to the whole network.
4) All nodes of the network after getting the malicious list find the node IDs of the malicious nodes in their table.
5) Each node flushes all the entries related to these node IDs from the respective tables.
6) Stop.

Attack 1: When malicious nodes (MN) does not belong to source S cluster and destination D cluster and same cluster.

Here the malicious nodes (MN) does not belongs to same cluster and not in source and destination clusters. Here node 5 is the source and node 31 is the destination node. Node 5 broadcast RREQ with the neighbour nodes. Suppose node 3 acts as Intermediate node, as it is having larger sequence number & minimum hop count. It replies with RREP & sends its next node 3, cluster head of node 3 is 29 & Prime product number (PPN) is 3,444,441 (31*37*7*3*13*11). Prime product term is fully divisible and considers replied information is reliable.

In Figure 4. Network topology for Malicious Nodes, Now source node 5 sends 170 dummy packets towards $N_{RREP}$ (node 13). As CH of source node 5 and CH of node 13 $N_{RREP}$ is not same, node 11(CHS) sends encrypted information from $N_{RREP}$ to its cluster head 29(CHI) via a pre-defined path (shown in dotted line in figure: ) . The key K is used to encrypt this information which is shared between the two cluster heads & information consists of number of dummy packets, Source node ID & destination node ID ,Legitimacy value of node 13 and node 3 , the unique Identifier N,(One time random number). The encrypted packet is EK [170, 5, 31, 0.2, 0.3, N1] node 29 decrypts the encrypted packet & enters into promiscuous mode. Now source node send 170 dummy packets to node 13(suppose).Node 13 sends 70 packets to the node 3 and node 3 sends 35 packets to the next node . Now node 29 calculates reputation value of node 13 & node 3, Legitimacy value of node 13 & node 3 is 0.2, 0.3, K is 3 (supposed as previously). The reputation value of node 13 is

$$\text{Reputation value of node 13 is} = \frac{(\frac{170-70}{70})+3(0.2)}{3} = 0.6$$

Now, the reputation value of (NNN) node 3 is calculated as

$$\frac{\frac{70-35}{35}+3(0.3)}{3} = 0.6.$$

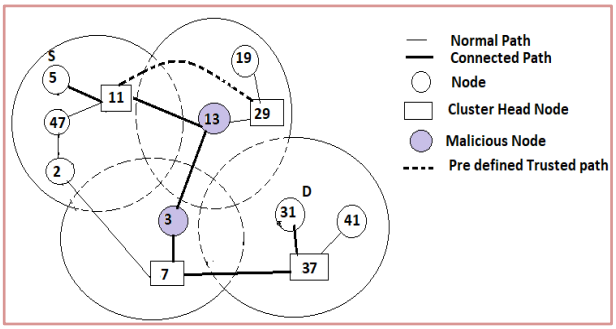


**Fig. 4:** Network topology for Malicious Nodes.

Now, compared reputation value of node 13 & node 3 with reputation level table. As reputation value of node 13 & node 3 are less than 1, declared as malicious nodes.

The reputation value of node 13 & node 3 are compared & nodes has level [2] by the reference with reputation level table. Now the cluster head starts removal of malicious nodes by adding to malicious list, and broadcasts the list of whole network. Now all nodes, with their tables finds the malicious list & each node in network flushes all entries related to malicious nodes from their tables.

## 4. Simulation result

For analysing the functionality of the protocol, we used MATLAB. A total of 20 nodes were simulated. In this simulation 2 to 4 malicious nodes were assorted. Fig .5 ,Here is a graph for packet delivery rate act for the throughput of standard AODV and AODV, CRCMD&R with extension of FALRMD&R scheme. The X-axis of the graph represents network throughput and Y-axis of the graph represents no. of nodes. Compared to standard AODV, AODV based FALRMD&R performs better. Finally, in result network throughput improves from 43% to 82% in the presence of 10-20%malicious nodes in proposed scheme.

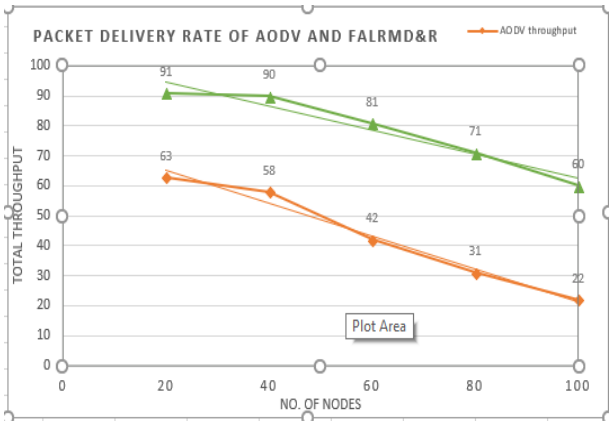


**Fig. 5:** Packet Delivery Rate of AODV and FALRMD&R Scheme.

## 5. Conclusion

For preventing the nodes from visiting through compromised nodes, this paper produces a secure routing protocol without using any special hardware. To know whether the ode is directing from correct routing or not, this paper pivot two tables those are legitimacy value table and reputation level table. Here we used malicious node detection and removal algorithms. For future work, we plan a scheme that may give a solution for an attack i.e., If a malicious node may act as a cluster head to hack data of a whole cluster network.

## References

[1] Saurabh Sharma and Dr.Sapna Gambhir," CRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs", 11 th International Conference on Intelligent Systems and Control (ISCO) in 2017.

[2] Diaa Eldein Mustafa Ahmed, Othman O. Khalifa,"An Overview of MANETs: Applications, Characteristics, Challenges and Recent Issues", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-6 Issue-4, April 2017.

[3] Saurabh Sharma," An ssecure reputation based architecture for MANET Routing" 4th International conference on electronic and communication systems 2017.

[4] Saurabh Gupta, Subrat Kar, S Dharma raja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network," in Proc. iCCCT'j j, 2011, p.468-473.

[5] 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.

[6] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet," in Proc. JJT'll, 2011, p. 226231.

[7] 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.