International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

Multipath Congestion Control and Predication and Detection of Attacks in MANET

M. Tech. Scholar Vinita Kashid, Asst. Prof. Dr. Mukesh Patidar, Hod. Mr. K. K. Sharma
Department of Elctronics & Communication Engineering
Patel College of Science and Technology, Indore,MP,India
Kksharma18685@ gmail.com

***Abstract*- Manet is self-configuring and self-organizing network; it doesn't rely on pre-existing infrastructure. Manet or mobile ad-hoc network is capable of forming proxy network without the necessity of a central administration or any standard support devices. It is a wireless network that can communicate to each other. Since it's a wireless network therefore its biggest problem is Congestion. This congestion occurs due to the presence of heavy traffic (packets) in the network. The controlling of the congestion is important within the manet, the quality congestion control mechanism isn't ready to handle the complex or any hardcore congestion, if this congestion couldn't be control it will collapse the whole network. We have proposed the congestion control by performing the default network nodes using Network Simulator NS2.35 with the Routing Technique of AODV and DSR, along with them we perform our routing technique called CCAODV (Congestion Control AODV) thus after final result one can see the workability and enhanced performance in packet delivery ratio and throughput from our proposed work.**

***Keywords*- Load Balancing, Congestion, CCAODV, Multipath Routing; MANET, AODV, TCP, PDR.**

I. INTRODUCTION

Manet stands for Mobile ad-hoc Network also called as wireless ad-hoc network or ad-hoc wireless network that usually has a routable networking environment. It is a set of wireless mobile nodes that can communicate without any centralized administration, many applications like disaster management and defence services comes under it [1].

It consists of set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. Manet3 nodes are free to move randomly as the network topology changes frequently [2].

Each node behaves as a router as they forwarded towards the traffic of other specified node in the network. Manet can operate as single network or it can be the part of larger internet. It forms a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes [3].

MANETs are generally utilized in scenarios like disaster areas, war zones and transportation sites. In most cases, the infrastructure isn't fixed while the communication happens. Cars, soldiers, ships, buses, airplanes and model wireless devices, can represent MANETs as shown in Fig 1. At an equivalent time, nodes are often removed of range at any time, thus, the network must be reconfigured [4].

There are several MANET types, including VANETs (vehicular unplanned networks), SPANs (smart phone unplanned networks), IMANETs (Internet based mobile unplanned networks), and military or tactical MANETs [5].

The main challenge for the Manet is to equip each device to continuously maintain the information required to properly route traffic. There are several ways to study Manets for instance the use of simulation tools like OpNet. NetSim. or NS2 [6].

It consists of a peer-to-peer, self-forming, self-healing network. It can be used in road safety, ranging from sensors for environment, home, health, rescue operations during natural disaster, defence services, weapons, robotics, etc [7]. The remaining a part of this paper are often described as follows: Section two consists of work associated with this article which published by different authors in past [8].

Section three describes the suggested method for safe and Quality of Service process. Section fourth showing some analysis and results for the advantage of suggested method on 2 different methods in sort of necessary metrics within the end conclusion of this whole analysis.

II. ROUTING PROTOCOLS

1. AAd-hoc On-demand Distance Vector (AODV):
Ad-hoc On-Demand Distance Vector (AODV) may be a routing protocol which is capable of both unicast and multicast routing. Being an on-demand algorithm, it generates routes among nodes only source node desires and maintains them as long as they're required by source. It uses the concept of sequence numbers so as to ensure

that the routes are fresh its self- starting and loop free. Also, it is often used for giant number of mobile nodes. AODV generates routes employing a route request / route reply cycle.

A route request is broadcasted over the network when source node wishes to line a route to destination for which it doesn't possess a route already. Every node receiving this packet updates the knowledge of source node then set backward tips that could it within the routing table. The RREQ contains the IP address of the source node, its current sequence number, broadcast ID and therefore the latest sequence number of destination that source node is conscious of A node receiving the RREQ sends route reply (RREP) in two cases.

First, if it itself is that the destination. Second, if itpossesses a route to the destination. But in second case, the condition is that the corresponding sequence number of the node must be either greater than or adequate to the sequence number contained in RREQ. In both cases, it unicasts RREP back to the source. If not, RREQ is rebroadcasted by it. Each node keeps track of source IP address and broadcast ID of RREQ. If a RREQ is received which is already processed by node, RREQ is discarded.

Nodes then set forward tips that could destination because the RREP propagate back to the source. When RREP is received by the source node, it begins forwarding data packets to the destination. Later, if the source receives RREP which contains greater sequence number or same sequence number with a smaller hop count; it updates its routing information for that destination and begins using the better route.

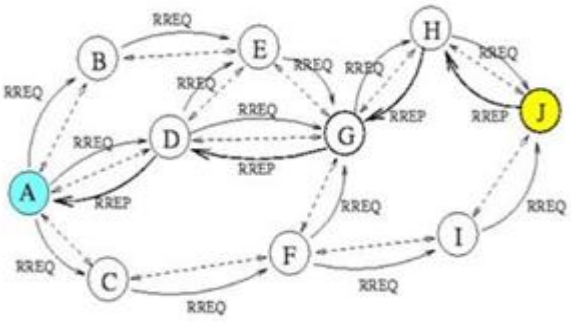

Fig 1. AODV Routing Protocol.

The routes are maintained as long as they're active, i.e., the info packets moving to the destination from the source along that very same path periodically. When the sending of knowledge packets stops, the links will be outing and eventually deleted from the intermediate node routing tables. just in case there's a link break during transmission, the node which is simply before the node where link break occur generates a route error (RERR) message and sends it to source so as to tell it that the destination is not reachable. On receiving RERR, if the source node still wants the route, it can reinitiate route discovery [9].

2. Dynamic Source Routing (DSR):

In DSR, when a node features a packet to send to some destination and doesn't currently have a route thereto destination in its Route Cache, the node initiates Route Discovery to seek out a route; this node is understood because the initiator of the Route Discovery, and therefore the destination of the packet is understood because the Discovery's target. The initiator transmits a Route Request (RREQ) 802.11; queuing type is Drop-tail. The Simulation Parameter are listed in Table 1.

Packet as an area broadcast, specifying the target and a singular identifier from the initiator. Each node receiving the Route Request, if it's recently seen this request identifier from the initiator, discards the Request. Otherwise, it appends its own node address to an inventory within the Request and rebroadcasts the Request. When the Route Request reaches its target node, the target sends a Route Replay (RREP) back to the initiator of the Request, including a replica of the accumulated list of addresses from the Request. When the Replay reaches the initiator of the Request, it caches the new route in its Route Cache.

Route Maintenance is that the mechanism by which a node sending a packet along a specified route to some destination detects if that route has broken, for instance because two nodes in it have moved too apart. DSR is predicated on source routing: when sending a packet, the originator lists within the header of the packet the entire sequence of nodes through which the packet is forwarded.

Each node along the route forwards the packet to subsequent hop indicated within the packet's header, and attempts to verify this by means of a link-layer acknowledgment or network layer acknowledgment. If, after a limited number of local retransmissions of the packet, a node within the route are unable to form this confirmation, it returns a Route Error to the first source of packet, identifying the link from itself to subsequent node was broken.

The sender then removes this broken link from its Route Cache; for subsequent packets to its destination, the sender may use the other route to its destination in its Cash, or it's going to attempt a replacement Route Discovery for that focus on if necessary [10].

3. Congestion Control Ad-hoc on-demand Distance Vector:

Congestion Control AODV (CCAODV) routing protocol has three main steps: Route Discovery, Route Monitoring and Route Recovery. In route discovery, stable path is found by using received signal strength information. The route stability involves both forward and reverse path. In

route monitoring, stable and unstable paths are decided by checking received power is usually greater than threshold. If link is weak, it's unstable path. In route rediscovery process, moving node is found and route recovery is completed by finding new intermediatenode [11].

III. PROPOSED TECHNIQUE

In this section we have to explain about proposed steps and flowchart of our techniques

1. **Input:** Network with Random Nodes
2. **Output:** Preventive Routing on Network Procedure:

- We have a network consisting of random nodes; nodes are 25, 50, and 75,100,125,150.
- A packet requires from source to destination; it generate route request (RREQ) and waits for reply (RREP). As soon as it receives reply it will decide the best route.

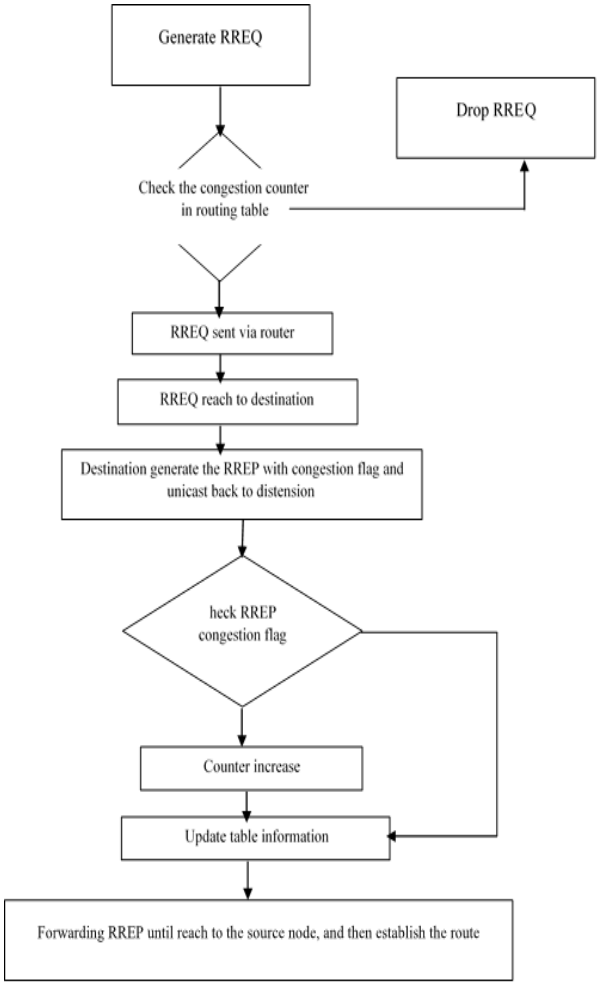

Fig 2. Process of CCAODV Flow Chart.

For the monitoring of this performance the residual energy, throughput and packet delivery fraction graph table is maintained. The procedure can be understood from the flow chart given below. Based on the routing mechanism a node could be untrusted, in-between untrusted and trusted and trusted. The CCAODV may avoid the congestion or tackle them via load balancing them to another route, depending on situation.

IV. SIMULATION PARAMETER

The simulation performance of CCAODV is done by using Network Simulator-2 (NS-2.35). The operating system is Windows 10, it done taking nodes as 25, 50, and 75,100,125,150 within the simulation area of 2000*800. Mac Type is IEEE.

1. Performance Metrics:

Performance of the proposed EMAODV protocol was simulated and compared to the 2-existing reactive protocols, AODV and DSR supported four performance metrics.

1.1 Packet Delivery Ratio (PDR): the ratio of the number of packets received by the destination to the number of packets sent by the source.

1.2 Throughput: the ratio of number of packets received by the destination to the time taken for simulation.

1.3 Power consumption: the facility consumption from which sink nodes receiving packets

Table 1. Simulation Parameters.

A. Simulation Tool	B. NS-2.35
C. IEEE Scenario	D. 802.11
E. Propagation	F. Two Ray Ground
G.	H. 25, 50, 75, 100,
I. Network Scenario	J. 125, 150 nodes
K. Traffic Type	L. TCP
M. Antenna	N. Omnidirectional antenna
O. MAC Type	P. IEEE 802.11
Q. Routing Protocol	R. AODV, DSR, CCAODV
S. Queue limit	T. 50 Packets
U. Simulation area (in meter)	V. 2000*800
W. Queue type Channel	X. Drop-tail Wireless Channel
Y. Simulation time	Z. 100 Seconds

V. RESULT ANALYSIS

1. Packet Delivery Ratio:

Packet Delivery Ratio of CCAODV (Congestion Control AODV) is better than the DSR (Dynamic Source Routing) along with comparing with traditional AODV. As the Node Density increases the PDR decreases but is still performing better than DSR and AODV. When the node density is 25 the AODV shows result of almost 88% and DSR showing result of more than 88% (less than 90%) while CCAODV shows more than 92% of packet delivery fraction. When the node density is highest with 150 the AODV perform almost 84% of PDF, DSR shows more

than 86% and less than 88% and CCAODV shows result of more than 90%. This satisfies the packet delivery potential of our routing method is far better than AODV and DSR.

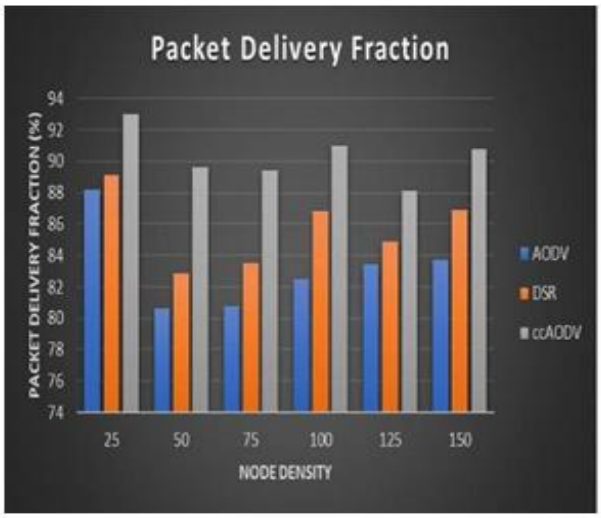

Fig 3. Packet Delivery Fraction Analysis.

2. Throughput Result:
It is one of the dimensional parameters of the network which provides the fraction of the info rate used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations. Throughput of CCAODV is better than AODV and DSR, so the performance of our network rise.

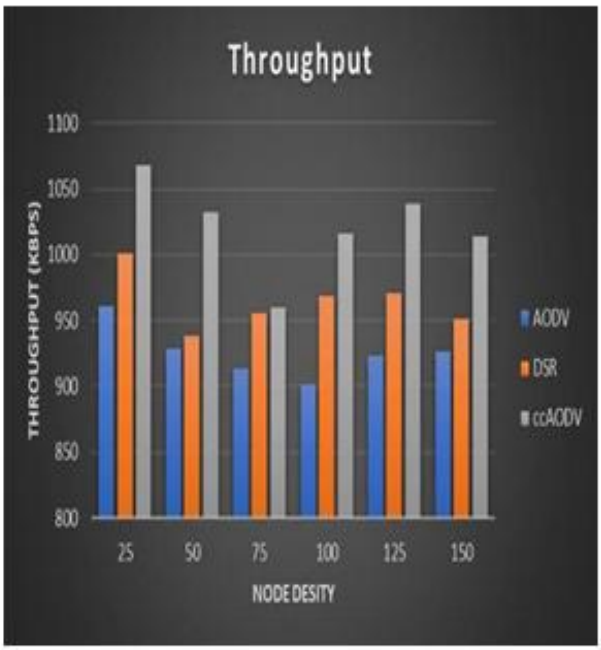

Fig 4. Throughput Analysis.

3. Residual Energy:
The Energy of CCAODV is better than DSR and AODV at every node density. From the graph one can clearly understood the results.

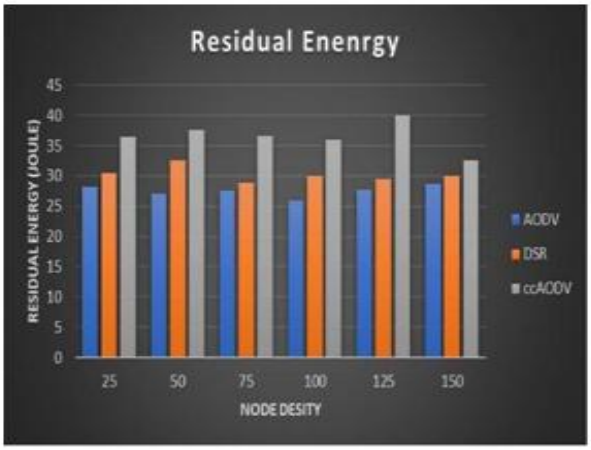

Fig 5. Residual Energy Analysis

VI. CONCLUSION

An improved AODV routing algorithm, named CC-AODV is proposed in this paper. Simulations are administered and results are compared between the AODV and therefore the proposed CCAODV based on five different parameters. From the simulation results, CC-AODV has higher end-to-end delay than the AODV when the network has more nodes the major problem which led to make a situation which will collapse the entire network is congestion and it's vital to require a step to avoid it.

This paper shows the performance of our proposed work via graphical representation of Packet Delivery Fractions, Throughput and increase in Residual Energy. The node doesn't ensure us that the present route is usually fine for its use many packets are dropped in its way but due to network malfunctions and for this retransmission has been assigned to them which is additionally a common divisor in Manet.

By comparing the results of AODV and DSG technique with our proposed procedure, we can easily observe the increase in the Packet Delivery Ratio, Throughput and Residual Energy. The congestion counter implementation in the routing table will be a keystone to achieve multiple routing paths while increasing the wireless performance. The future implementation of CCAODV will be improved by optimizing the predefined counter threshold module.

REFERENCES

[1] Hasan Abdulwahid, Bin Dai, Benxiong Huang and Zijing Chen, Optimal Energy and Load Balance Routing for MANETs, International Conference on

ComputerScience and Network Technology (ICCSNT 2015).

[2] S. Santhosh baboo and B. Narasimha, A Hop-by-Hop Congestion Aware Routing Protocol for Heterogenous Mobile Ad hocNetwork, International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No. 1, 2009.

[3] G. Vijaya Lakshmi, Dr. C. Sobha Bindhu, Congestion Control Avoidance in ad hocnet work using queuing model, international journal of computer technology and Application, pp 750-760, vol2, issue 4, 2011.

[4] Vishnu Kumar Sharma and Dr. Sarita Singh Bhadauria, Performance Analysis on Mobile Agent Based Congestion Control Using AODV Routing Protocol Technique with Hop-by-Hop Algorithm for Mobile Ad hoc Network, International journal of Ad Hoc sensor & Ubiquitous Computing (IJASUC), April, 2012.

[5] Mehran Abolhasen, Tadevsz Wysocki and Eryk Dutkiewicz, A Review of Routing Protocol for Mobile Ad-Hoc Network, Elsevier, pp 1-22, 2003.

[6] Lakshit Prashar and Raj Kamal Kapur"Performance Analysis of Routing Protocol under Different Types of Attacks in MANETs" IEEE International Conference on Reliability Infocom Technologies and Optimization (ICRITO)" December 2016.

[7] Drake Xavier Dzurovcak; Shuhui Yang, "Performance Analysis of Routing Protocols in Delay Tolerant Networks", IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2017, pp.1-7.

[8] Ravi Parihar, Ashish Jain, Upendra Singh, "Support Vector Machine Through Detecting Packet Dropping Mis behaving Nodes In MANET", Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE, 20-22 April 2017, pp.1-6.

[9] Daichen Zhang & Dan Zhou, Load Balancing Algorithm Based on History Information In MANET, Institute of Electrical and Electronics Engineers, 2017.

[10] P. Sambasivam, A. Murthy and E.M.Belding-Royer, Dynamic Adaptive Multipath Routing based on AODV, 2004.

[11] Y. Mai, F. M. Rodriguez and N. Wang, "CC-ADOV: An effective multiple paths congestion control AODV," 2018 IEEE 8th.