Review of Various Techniques on Energy Efficient, Congestion Control And Trust Based Routing In MANET

S.Shanthini[1], Dr. D. Devakumari[2]
[1]Dept of Computer Science
[2]Assistant professor, Dept of Computer Science
[1, 2] Government Arts College, Coimbatore, India.

Abstract- *Mobile ad hoc network is un-structured network nodes' are moving any direction and it changes their location very frequently. hence mobile ad hoc network-facing many problems like nodes' energy level, congestion, and secured routing ect., In this paper discussing various energy-efficient techniques, congestion control techniques and trust-based routing techniques are using in MANET.*

Keywords- Mobile ad-hoc network (MANET), energy-efficient, congestion control, trust-based routing techniques.

I. INTRODUCTION

Mobile ad – hoc network (MANET), is a wireless mobile self-organizing network which is also a temporary multi-hop autonomous system composed of a set of mobile nodes with radio transmitters and receivers. Because of the limitation of a node's radio range, any two mobile nodes which can't communicate directly, could forward data packet with the help of the other nodes and so implement data interaction between each other [24]. Compared with other networks, MANET doesn't need any structure to work and has so many characteristics, such as network self-organizing, dynamic network topology, unidirectional wireless links, etc., MANET is mainly used in military operations, emergency communications, co-operating with mobile communication, wireless access, and sensor networks; In MANET, each node is both end system and router, and so for efficient communication, appropriate routes must be constructed between nodes.

A MANET node can perform smoothly and behave co-operatively as the conventional routing protocols were build up with the assumption of a cooperative and trusted environment among the nodes. Attackers can easily attack by compromising some valid internal nodes in the physically hostile environment [15]. These malicious nodes may make up routing information before launching a variety of attacks(such as a black hole or grey hole attack) in order to interrupt the flow of information during data transmission by dropping some number of packets. One of the main principal is network layer attacks and prevention of routing malfunctioning during data transmission is essential for secure routing.

The trust communication route is basically where the information flows from one node to another [8]. For instance, if node A trusts node B, now a route is created form node A to node B in which information can flow from A to B. In this communication sometimes source node may need to discover multi-hop communication routes with destination node in which destination lacks trust information about the source. Conventionally, the destination node develops this trust based on recommendations from the intermediate nodes of the multi-hop route. This trust management is called neighbour-based routing where opinions/recommendations come from. Hence, the integrity and validity of the recommendation are critically important since malicious nodes may be present in a multi-hop route and any misguided recommendation from them may be the result of insecure information flow. A node may also get a contradictory recommendation from different routing for a single node. A trust management system should have a proper mechanism to recognize the valid and correct node by sharing the information.

In MANET energy plays the main role during the broadcasting of data packets [3]. Every node has its own energy level. It reduces partially when the data packet is transmitted and received but when nodes do not have sufficient energy for broadcasting data packets, nodes drop data packets. The major issues regarding security are due to the lack of an infrastructure and the use of the wireless medium, therefore the communication could be easily disturbed or eavesdropped, the nodes could be corrupted by malicious agent and the measures needed to detect the intrusion have to be executed by each node with a distributed approach [1]. The limited power source available to the nodes puts a severe constraint to the operations that a node can execute and this implies that the intrusion detection system should be energy-

efficient, so the node lifetime will not be affected excessively.

II. RELATED WORKS

a) Energy efficiency

Maitir Biphibhai Patel and Manish M. Patel describe the node residual energy and stability of the link in this mode gives a better lifetime of the network [10]. Here analysis various energy-efficient routing protocols SBNRP (stable routing with power) factor, queue-based energy-efficient multipath load balancing in an ad-hoc network, improved AODV using mean energy value, EM_AODV protocol(Energy Matrices _ AODV), adaptive load balancing in AODV, Cost-based power-aware cross-layer AODV, Energy-efficient secured routing protocol. The source node starts to broadcast the request packet. Each intermediated node adds its own residual energy and stability to forward its neighbor nodes. It checking every node's information's finally destination node wait for a predetermined amount of time for all routes calculate cost best on two factors (i) average energy value (ii) stability of node-based selects the path with cost-efficient.

S. Das and S. Pal havean analysis of various energy-efficient techniques and their pros and cons [20]. The energy-efficient techniques or algorithms are only focused on the results not concentrated on the actual problem. Here analysis some of the major problems to consider to write a new algorithm. This cause for excess energy consumption aspect are - (i) unequal transmission energy due to different path length, (ii) overhearing by nodes, (iii) retransmission or data or control message due to collision or path congestion, (iv) common node / uneven load distribution, (v) route selection through nodes with less residual battery capacity.

Rangaraj Jayavenketesan and Anitha mariappan propose the ACO_FDRPSO algorithm (Ant colony optimization _ fitness distance ratio particle swarm optimization). [16] ACO algorithm to find the energy-efficient routing path based on the higher residual energy value. FDRPSO minimizing the energy consumption to save the network lifetime. Also using one more algorithm called the duty cycle. It collaborated with the ACO_FDRPSO algorithm. It monitors the nodes' activity and nodes have no longer communication between them. It means the nodes no need to active mode put on the sleep mode. This algorithm works on the hybrid method it gives better results of the node lifetime.

Getsy S Sara, Neelavathy Pari. S and D. Sridharan reviewed [6] the various energy-efficient routing protocols, how it works on the network? And what are the techniques used? Here minimizing the active communication of the nodes, energy required for transmitting or receiving or minimizing the inactive energy. There is a comparison table of the various emerging energy-efficient routing protocols. Compared metrics are given a better delivery ratio, lifetime of the nodes, energy dissipation rate, overhead ratio, end-to-end delay, energy reserve, and multipath routing possibilities.

L. Femila and M. Marsaline Beno implementing an efficient power are routing (EPAR) with help of (CCSPR) cooperative cost shortest path routing algorithm and (COSPNR) cooperative over shortest path non-cooperative routing algorithm [9]. The EPAR algorithm to minimizing the variance of energies in all the nodes and prolong the lifetime of the network. it comparatively gives a better throughput ratio in the Future concentrate on the security perspectives.

Razvan Craciunescu, Simona Halunya, and Albena Mihovska analyze the relay selection process in a cooperative communication scenario [18]. The Nash equilibrium algorithm used based on the marriage equation. The marriage equation help to predict the satisfaction ratio between the nodes. It helps to nodes direct communication then select the relay modes.

Xiaozheng Gao, Ping wang, Dusit Niyato, kai yang, and Jianping focused on secondary network performance [25]. So they implemented two auction-based time scheduling structures for fixing the network demand and the variable-demand cases. The nodes act the seller as well as an auctioneer than the bid for time resources. It works very efficiently in the simulation time.

b) Congestion control

Cheten Batra and vishal Arora reviewed on minimizing the packet losses to the help of RED Algorithm [4]. Here also using two differenced techniques Active queue management (AQM) and Virtual output Queue (VOQ). Generally, congested network-facing three types of problems long delay high overhead and many packet losses. Here the red algorithm focused on these three issues. In the traditional drop, tail algorithm wasting a time to buffering but our RED algorithm controls the queueing system scheduler suited for blockage avoidance. The red algorithm prevents the congestion.

P. Dhivya and S. Meenakshi discussed various techniques of congestion control. The problem of the congestion network high date loss, long delay and waste of resources [13]. Drop Tail (DT) algorithm suitable for the

decentralized network environment. Less packet loss at the same time there is some drawback its lack of fairness, less link efficiency and non-responsive flow. The RED algorithm is suitable for long term network not for a short term network. Robust random early detection (RRED), weighted Random Early Detection (WRED), Adaptive Random early detection (ARED) this algorithm maintains a predictable average queue size and reduces RED parameter sensitivity advantage is altering load, low delay, and high link utilization. Disadvantage the choice of the target queue size to network operation. Fair random early drop (FRED), Choke algorithm, BLUE algorithm, adaptive virtual queue (AVQ) algorithm, Dynamic congestion detection and control routing (DCDR) it gives warning message to nodes about congestion.

Yeta Mai, Fernando Molina Rodriguez, and Dr. Nan Wang proposed a congestion control_AODV is called (CC_AODV). The techniques work better because the packet delivery ratio bitterly increases [26]. The performance of CC_AODV generates the RREQ, check the congestion counter in the routing table if it is greater than. The request will drop otherwise it reaches the destination. Then destination generates the flag this flag congestion counter flag this flag carries congested route information. It updates the routingtable to find the path (or) route.

S. Leemaroselin analysis the various congestion control algorithm find out the strength and weakness of every algorithm, this algorithm main used in the MANET area [19]. This algorithm gave good packet delivery and decreases the delay packet loss of the network. It also controls the network congestions special on MANET.

Sakshi Sharma and manjot Sidhu implementing based on the RED algorithm [21]. RADNET is a protocol it communicates with the hardware and the electronic Interface can communicate with the nodes. Then the adaptive RAD protocol is working to reduce the congestion of network and improve network performance it gave a better result. RADNET is basically UDI/IP protocol but it can also use to TCP/IP.

Deependar Kumar Jha, Anurag Jain and Susheel Jain [5] developed the AODV protocol and enhance Random early detection algorithm performed for better packet delivery ratio and throughput. The enhanced RED algorithm reduces the parameter sensitivity and helps to calculate the exact packet drop ratio and also fix the maximum and minimum threshold value for the queue length. It calculates the packet drop probability. So it is adaptable for the queue length and easily transmits the packet in the congested network without packet losses.

Neelam Sharma, Shyam Sing Rajput, Amit Kumar Dwivedi, and Manish Shrimali implemented P_RED called probability-based Random early detection algorithm [12]. This algorithm separates the differently behaved nodes to separate it and isolate the nodes because of the preventing propose. Here also fix the maximum and minimum threshold values to give a high throughput value and the same time increase a little bit of delay. In the future, it can reduce the delay and get better performance of the network.

Abinsh Mohan Borah, Bobby Sharma and Manab Mohan Borah [2] analyzed various congestion control algorithms and how it performed to reduce the congestion in the network. It creates a topology by using Random Walk Mobility (RWM) and Lavy Walk Mobility (LWM) models. These models monitor the network performance and if any problems occur in the time of packet transmission this model solves the issue and it maintains the network stability.

c) Trust-based routing techniques

Rashmi Hinge and Jigyasu Dubey evaluated the opinion based trust-based routing protocol in mobile ad hoc networks [17]. Here calculate every nodes` trust value and find the trustworthy nodes in the network. Then find a secure routing path based on the nodes' trust value and the neighbour node opinion. The opinion is calculated by the values 0 and 1. If the value is 1 the neighbours are given positive results otherwise if the value is 0 it is a negative value. Based on this select the trusted routing path in the network.

Suparna Biswa, Tanumoy Nag and Sarmistha Neogy [22] described on the secure routing to avoid the black hole attack. Here a new technique is developed considers some parameters like nodes` stability, pause time, remaining battery level and maximum velocity of the node. Based on these parameters every transmission node adds points. This point of value must increase and not decrease. If the point is going down to 0 that node is considered as a malicious node. In this case, there is a limitation if a new node entered in the network there is no point in that node it’s also considered as a malicious node. In the future,we need to find a solution to this issue.

Vinsh H. Patel, Mukesh A. Zaveri and Hemant Kumar Rath [23] implemented trust-based routing in mobile ad hoc networks. Basically routing process consists of three levels: (i) route discovery (ii) packet forwarding (iii) route maintenance. Most of the attacks happened in the packet transmission and route discovery time. In this paper, trust-based routing techniques focused on the load balancing of every node in the packet forwarding time and it created a

relationship between the nodes so every node knows very well their neighbours. This technique works on two phases: trust formulation and trust usage for routing decisions. It is calculated by the packet drop, packet forwarding, and packet delay.

Poonam Gera, Kumkum Garg and Manoj Misra [14] focused on end-to-end delay secure data delivery in MANET using trust-based multipath routing. There are many attackers attacked in the time of transmission but here using self-encryption techniques. There is no need can cryptographic key in this technique to help secure packet transmission from source to destination. First find the path trust value route discovery at the source node, RREQ processing at intermediate nodes, RREP at the destination node and proceeding the intermediate node. Finally path decision at the source node.

Nagisetty. Rachana, Kandi. Sreeja, et al. implemented trust embedded ad-hoc on-demand vector (T_AODV) it extended in eT_AODV [11]. In AODV routing the protocol is facing some of the attacks. The attacks created by malicious nodes like (i) Routing loop attacks: this attack modified the routing information the packets do not reach the destination. (ii) Packet drop: malicious nodes or queue status having this type of issue. (iii) Gray-hole attack: dropping random packets and it can forward a routing packet not the data packet and receive the packets without information. (iv)Packet modification: this type of attack can change the packet information and packets are going to the wrong destination. These four types of attacks are overcome on this trust-based routing algorithm. It gives a better packet delivery ratio, trusted path distance, hop by hop cost and trusted path hops.

Hala Mustafa and Noureldien A. Noureldien analyzed selfishness behaviour and misbehaviour nodes [7]. These types of nodes are non-trustable nodes there are many classified methods available to detect the misbehaved nodes and selfishness node. This technique is processed on first control of the packets based on the detected method, trust-based detection method analysing various methods, sequence number based detection method finally method based on control packets and sequence number.

III. CONCLUSION

Here discussed various energy-efficient techniques, congestion control techniques and trust-based routing techniques are using in MANET. These techniques are handling and solving various issues and it helps to improvise the network performance and lifetime.

REFERENCE

[1] A. Lupia and F. De Rango, “A probabilistic energy-efficient approach for monitoring and detecting malicious/selfish nodes in mobile ad-hoc networks,” in Wireless Communications and Networking Conference (WCNC), 2016 IEEE. IEEE, 2016, pp. 1–6.

[2] Abinasha Mohan Borah, Bobby Sharma, and Manab Mohan Borah, “A congestion control algorithm for mobility model in mobile ad-hoc networks”, International Journal of Computer Applications, Volume 118, issue 23, May 2015.

[3] Anshu Chaturvedi, D.N. Goswami and Shivjay Singh, “Energy Aware Route Selection Algorithm for Cross-Layer Design over MANET” 2015 IEEE, Issue No -978-1-4673-7231-2.

[4] Cheten Batra and vishal Arora, “Red strategy for improving performance in MANET: A Review”, Journal of information science and Computing Technologies (JISCT), ISSN: 2394-9066, Volume: 3, Issue 2, Aril 30.2015.

[5] Deependar Kumar Jha, Anurag Jain, and Susheel Jain: Network performance optimization based on AODV routing in MANET: International Journal of science and research (IJSR),: ISSN. 2319-7064, Vol. 3, Issue. 5, PP. 1128-1132, May 2014.

[6] Getsy S Sara, S. Neelavathy Pari, D. Sridharan, “Evaluation and Comparison of emerging energy-efficient routing protocols in MANET”, ICTACT – Journal of communication Technology, ISSN 2229-6948, Issue 01, Volume 01, March-2010, PP 37-47.

[7] Hala Mustafa and Noureldien A.Noureldien: Detection of routing discovery misbehaving nodes in AODV MANETs a survey: International journal of networks and communication, Vol. 8, Issue. 4, PP. 115-122, 2018.

[8] K. Bijon, M. Haque, and R. Hasan, “A trust-based information-sharing model (truism) in manet in the presence of uncertainty,” in Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, July 2014, pp. 347–354.

[9] L. Femila and M. Marsaline Beno, “Optimizing Transmission Power and energy-efficient routing protocol in MANETs”, spring – 2019.

[10] Maitri Bipinbhai Patel and Manish M. Patel: Energy Efficient Routing using Residual energy and stability in mobile ad-hoc network: Processeedings of the International conference on inventive research in computer application (ICIRCA 2018). PP. 857-861.

[11] Nagisetty. Rachana, Kandi. Sreeja, Nagisetty Abhinaya and BKSP. Kumar Raj Alluri: Enhanced T_AODV routing protocol in wireless networks: Asian Journal of

Convergence in Technology, Vol. 6, Issue. 3, ISSN: 2350-1146, PP. 1-7.

[12] Neelam Sharma, Shyam Sing Rajput, Amit Kumar Dwivedi, and Manish Shrimali: P-RED probability based random early detection algorithm for queue management in MANET,: Advances in computer and computational science – Springer,: Vol. 554, PP. 637-643.

[13] P. Dhivya and S. Meenakshi, "Review of congestion control techniques in mobile Ad-hoc network", International journal of computer science and Engineering (IJCSE), E-ISSN: 2347-2693, Sep-2015, PP 44-49, Volume 3, and Issue 9.

[14] Poonam Gera, Kumkum Garg and monoj misra,: Trust based Multi path routing for end-to-end secure data delivery in MANETs,: Proceedings of the 3rdinternational conference on security of information and networks,: SIN 2010, Rostov-on-Don, Russian Federation, Sep-2010.

[15] R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," International Journal of Communication Systems, 2016.

[16] Rangaraj Jayavenketesan, Anitha Mariappan, "Energy efficient multipath Routing for MANET based on Hybrid ACO-FDRPSO", International Journal of Pure and Applied Mathematics, ISSN 1311-8080 Volume 115, No. 6, 2017, PP 185-191.

[17] Rashmi Hinge and Jigyasu Dubey.: Opinion based trusted AODV routing protocol for MANET,: ICTCS`16 proceeding of the second international conference on information and communication technology for competitive strategies, Article No:126, March 2016.

[18] Razvan Craciunescu, simona halunga and Albena Mihovska, "Analysis of Relay Selection Game in a Cooperative Communication scenario", 2018, PP 89-94.

[19] S. Leemaroselin, "A Review on Congestion Control Algorithms in MANET", International Journal of Computer Science and Engineering Technology (IJCSET), ISSN 2229-3345, Vol 6, Issue 04, Apr 2015.

[20] S.Das, S. Pal, "Analysis of energy-efficient routing protocol in mobile Ad-hoc Network", Springer – 2019.

[21] Sakshi Sharma and manjot sidhu,"RADNET Routing Enhancement by RED algorithm", International journal of Science and Research (IJSR). ISSN: 2319 – 7064, Volume – 3 Issue 10 Oct 2014, PP 2007-2011.

[22] Suparna Biswa, Tanumoy Nag and Sarmistha Neogy,: Trust based Energy Efficient Detection and Avoidance of Black hole attack to ensure secure routing in MANET,: 2014 Application and Innovations in mobile computing (AIMOC) IEEE.: PP. 157-164.

[23] Vinesh H.Parel, Mukesh A. Zaveri and Hemant Kumar Rath,: Trust based routing in mobile Ad-Hoc network,: Lecture node on software engineering,: Vol. 3, No.4, November 2015.

[24] Xiaozheng Geo, Ping Wang, Dusit Niyato, Kai Yang and Jianping An, "Auction Based Time Scheduling for Backscatter – aided RF-Powered Cognitive ration Networks", IEEE Transactions on wireless communications, ISSN 1536-1276, Volume 18, No 3, March 2019, PP 1684- .

[25] Xiaozong Yang, Renfa Li, Kenli Li, Yanyan Liu, "A New On-demand Routing Algorithm Based on Nodes' Locations for MANET", 2005 IEEE, Issue No- 0-7803-9335-X, PP- 776-782.

[26] Yeta Mai, Fernando Molina Rodriguez and Dr. Nan Wang, "CC-AODV: An Effective Multiple paths congestion control AODV", PP 1001-1004.