# HETEROGENEOUS MULTIHOP WIRELESS NETWORKS BASED ON SRR AND BAR ROUTING PROTOCOLS

[1]DEVDUTTA CHAKRABARTI, [2] SRABANI KUNDU, [3] DEBRAJ ROY

[1] M.Tech Student, Department Of CSE, Gurunanak institute of technology, 157/F, Nilgunj Road, Panihati,Kolkata-700 114,West Bengal, India

[2] Assistant Professor, Department Of CSE, Gurunanak institute of technology, 157/F, Nilgunj Road, Panihati,Kolkata-700 114,West Bengal, India

[3] Assistant Professor, Department Of CSE, Gurunanak institute of technology, 157/F, Nilgunj Road, Panihati,Kolkata-700 114,West Bengal, India

*Abstract— **In multihop wireless networks, once a mobile node needs to communicate with a destination, it depends on the other nodes to advance the packets. This multihop packet transmission will extend the network coverage space victimization restricted power and improve space distance potency. within the planned multihop wireless network E-STAR integrates the payment and hope system with the routing procedure with the purpose of ornamental route dependableness and constancy. The payment system describe to allege the nodes that send packets and recompense those forward packets. The trust system is vital to guage the nodes' trustworthiness and dependableness in forwarding packets in terms of multi-dimensional trust values and therefore the trust values square measure calculated for each node and developed 2 routing protocol is employed to send the packets through extremely trusty nodes having enough energy to minimize the likelihood of breaking the route. To strengthen the trust analysis, recommendation from every node is enclosed in trust calculation by TP (Trusted Party). This protocol is developed over the Manet network and replicated oppression NS2. Performance evaluated from the parameters like packet delivery magnitude relation, decision acceptance magnitude relation and route period.***

## I. INTRODUCTION

The multihop wireless network enforced in several useful applications like information sharing and multimedia system information transmission. It will establish a network to speak, distributed files, and share info. However, the assumption that the nodes are willing to pay their restricted resources, like battery energy and obtainable network bandwidth. Drawbacks within the existing routing protocols such as DSR assume that the network nodes are willing to relay alternative nodes packets. This assumption is cheap in disaster recovery as a result of the nodes pursue a standard goal and belong to 1 authority, however it should not hold for civilian applications wherever the nodes aim to maximise their edges, since their cooperation consumes their valuable resources such as information measure, energy, and computing power while not any edges. In civilian applications, egotistical nodes won't be voluntarily fascinated by cooperation while not enough incentive, and build use of the cooperative nodes to relay their packets, that has negative impact on the network fairness and performance. Fairness issue arises once a selfish node takes advantage from the cooperative nodes without contributory to them, and also the cooperative nodes are unfairly full. The egotistical behavior degrades the network performance considerably leading to failure of the multi-hop communication. additionally, some nodes could break routes as a result of they are doing not have enough energy to relay the supply nodes' packets and keep the routes connected. owing to this uncertainity within the nodes' behavior, every which way choosing the intermediate nodes can degrade the routes' stability. This planned system overcomes these drawbacks by the subsequent techniques, trust and payment system. The payment system uses credits to charge the nodes that send packets and reward those relaying packets . The trust system is important to assess the nodes' trait and dependability in relaying packets. A node's trust worth is outlined because the degree of belief regarding the node's behavior. The trust values are calculated from the nodes' past behaviors and wont to predict their future behavior.

The Fig.1 shows the info is transferred Via extremely Trusted Nodes. In spec from supply to destination the info is transferred through the intermediate nodes (i.e) routes. The route R1, R2 are the low trustworthy nodes and R3, R4 are the extremely trustworthy nodes. For every node it maintains a receipt and it submit to the trustworthy party. The trustworthy party can calculate the trust values. once shrewd the trust price it'll produce a payment receipt for extremely trustworthy nodes.

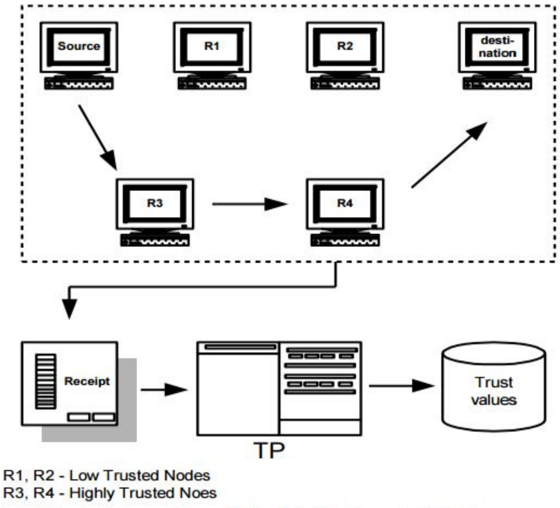


**Fig. 1 Data is transferred Via Highly Trusted Nodes**

## II. RELATED WORK

### 2.1. ROUTING MISBEHAVIOUR IN MOBILE AD HOC NETWORKS

The system planned the thought that improve throughput in a commercial hoc network within the presence of nodes that conform to forward packets however fail to try and do thus. To mitigate this drawback to categorizing the nodes based mostly upon their dynamically measured behavior. thus during this section the two extensions square measure introduced to the Dynamic supply Routing rule to mitigate the consequences of routing misbehavior, like watchdog and path rater. The watchdog identifies misbehaving nodes, whereas the trail rater avoids routing packets through these nodes.

### 2.2. ESIP FOR MULTIHOP WIRELESS NETWORKS

In multi-hop wireless networks, egoistic nodes do not relay different nodes' packets and build use of the cooperative nodes to relay their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the egoistic nodes' cooperation, however the prevailing protocols sometimes believe on the heavy-weight public-key operations to secure the payment. The planned technique concerned within the secure cooperation incentive protocol that uses the publickey operations just for the primary packet during a series and uses the light-weight hashing operations within the next

packets, in order that the overhead of the packet series converges thereto of the hashing operations. Hash chains and keyed hash values square measure wont to attain payment non repudiation and forestall free riding attacks.

### 2.3. TRUST MANAGEMENT IN MOBILE AD HOC NETWORKS MATURITY- BASED MODE

In mobile unexpected network trust management supported he thought of human trust and applies this model to ad hoc networks. This model builds for a trust relationship to any or all neighbors for every node. The trust is based on previous individual experiences of the node and on the recommendations of its neighbors. The recommendations improve the trust analysis process for nodes that don't achieve perceptive their neighbors because of resource constraints or link breakage. The Recommendation Exchange Protocol (REP) that allows nodes to exchange recommendations concerning their neighbors. The proposal doesn't need publicize the trust data over the whole network. Instead, nodesonly have to be compelled to keep and exchange trust data concerning nodes among the radio vary while not the requirement for a worldwide trust data.

### 2.4. TRUST MODEL FOR SECURE AND QOS ROUTING IN MANET

MANET is liable to varied forms of attacks because of open infrastructure, dynamic network topology, lack of central administration and restricted battery-based energy of mobile nodes. Most unexpected network routing protocols becomes inefficient and shows born performance whereas coping with massive number of misbehaving nodes. Such misbehaving nodes support the flow of route discovery traffic however interrupt the info flow, inflicting the routing protocol to restart the route-discovery method or to pick associate degree alternative route if one is obtainable. The new chosen routes should embrace a number of misbehaving nodes, and hence the new route also will fail. This method can continue till the supply concludes that knowledge can not be further transferred. The routing management messages square measure secured by mistreatment each public and shared keys, which can be generated on-demand and maintained dynamically.

### 2.5. RELIABLE ROUTING AGAINST SELECTIVE PACKET DROP ATTACK IN DSR BASED MANET

A mobile ad hoc network (MANET) might be a self self-configuring & organizing wireless system. Mobile nodes communicate exploitation wireless interfaces without a hard and fast network infrastructure. In these environments every node might act as supply or as a router. Nodes that can't communicate directly depend upon their neighbors so as to forward their messages to the suitable destination. The active topologies, mobile connections structure, localised management, and secrecy creates several challenges to the safety of systems and network infrastructure during a Edouard Manet environment. Consequently, this extreme variety of dynamic and distributed model needs a review of conventional approaches to security enforcements. This system proposes a brand new routing mechanism to conflict the common selective packet dropping. A selective packet drop could be a quite denial of service wherever a malicious node attracts packets and drops them by selection while not forwarding them to the destination.

## III. FRAME WORK

### 3.1. NETWORK ARCHITECTURE

The heterogeneous Multihop Wireless Networks has mobile nodes and offline sure Party (TP) whose public key is well-known to any or all the nodes. The mobile nodes have different hardware and energy capabilities. The network is used for civilian applications, its life is long, and the nodes have long relation with the network. Thus, with every interaction, there's invariably an expectation of future reaction. every node incorporates a distinctive identity and public/private key try with a limited-time certificate issued by TP. while not a sound certificate, the node cannot communicate nor act as an intermediate node. TP maintains the nodes' credit accounts and trust values. Each node contacts TP to submit the payment reports and TP updates the concerned nodes' payment accounts and trust values. The adversaries have full management on their nodes. they will amendment the nodes' traditional operation and obtain the scientific discipline identification. they will try to attack the payment system to steal credits, pay less, or communicate at no cost.

### 3.2. Attack Scenario

Some adversaries might report incorrect energy capability to extend their likelihood to be elite by the routing protocol, e.g., to earn a lot of credits. The adversaries can also conceive to attack the trust system to falsely augment their trust values to extend their likelihood to participate in routes. they will try and insult different nodes' trust values. Attackers might launch denial-ofservice attacks by breaking the communication routes intentionally. once a node B receives packets from node A to forward to ensuing node within the route, node B drops the packets and keeps silent to let node A believe that node B is out of transmission vary and also the link between them is broken. These attacks is also launched by compromised, malfunctioned, or low-resource nodes.

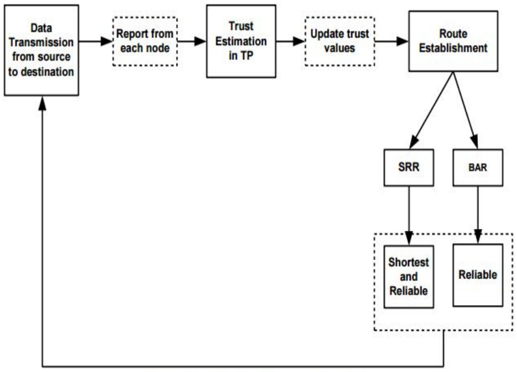


Fig. 2 E-STAR in Multihop Wireless Network

E-STAR in multihop wireless network. In wireless network knowledge transmission from supply to destination and each node can have a singular identity and report back to the trusted party. The trusty party can assess a trust price for each node with their nodes' past behaviour. After updating the trust values the routing institution process square measure done through by SRR and BAR. Whereas SRR can realize a shortest and reliable path and it avoids the low trusty nodes. BAR can realize the foremost reliable one.

### 3.3. DATA TRANSMISSION PHASE

The supply node sends messages to the destination node through a route with the intermediate nodes. For transferred information packets supply node computes the signature with hash message and sends the packet to the first node within the route. the aim of the supply node's signature is to confirm the message's legitimacy and integrity. TP ensures that supply node has sent messages. Each intermediate node verifies supply node signature and stores signatures with hash message for composing the report. A report may be a proof for collaborating in an exceedingly route and causation, forwarding, or receiving variety of messages. It additionally removes the previous ones as a result of node signature is enough to prove transmittal messages and then destination node generates a hash messages to acknowledge the received message and therefore the destination node sends ACK packet to every intermediate node. Each intermediate node verifies the hash messages for composing the report. every node within the route composes a report and submits it once it's a affiliation to TP to claim the payment and update its trust values.

### 3.4. TRUST ESTIMATION PHASE

Trust Party receives a report, it initial checks if the report has been processed before mistreatment its distinctive symbol. Then, it verifies the authority of the report by computing the node signatures with hash message. If the report is valid, trust party verifies the destination node's hash message. TP clears the report by rewardable the intermediate nodes and debiting the supply and destination nodes. the amount of sent message is signed by the supply node and therefore the range of delivered messages can be computed from the amount of hashing operations done. The trust values ar calculated from every node based mostly on nodes' trait and responsibility in relaying packets. it's honest to extend the trust values of the nodes that aren't in broken links, as a result of they relayed packets truthfully. On the opposite hand, the trust system decreases the trust values of the 2 nodes in an exceedingly broken link. Trust is also dynamic or time-sensitive. thus trust party must periodically valuate the nodes' trait, i.e., a trust worth at time t could also be completely different from its worth at another time. that the planned system depends on the multidimensional trust worths rather than single trust value to precisely predict the nodes' future behavior. Trust values are wont to decide that nodes to pick out or avoid in routing. Since a trust price depicts the chance that the node conducts AN action, route responsibleness are often computed victimization its nodes' trust values to relinquish probabilistic info concerning the route stability and lifetime. The trust values ar calculated from the subsequent Formula:

T (1) = (No of packets that are forwarded in last t sessions) / (Total no of incoming packets in last t sessions)

T (2) =1-((No of sessions broken by node in the last t sessions)/t))

T (3) = No of session that node at least f packets/t

T (4) = No of session node participated in the period t/m

$T\ xyz_{(i)} = Tx_{(i)}\ x\ Ty_{(i)}\ x\ Tz_{(i)}$

$Txyz_{(i)}$ = Trust value denotes the Route reliability

x, y, z = Intermediate node

i = 1,2,3,4(dimensions)

## 3.5. ROUTE ESTABLISHMENT PHASE

### A. SRR Protocol

SRR protocol establishes the shortest route that may satisfies the supply nodes needs is trusty enough to act as a relay. This protocol avoids the low-trusted nodes. during this protocol the supply node embeds its requirements within the RREQ packet, and also the nodes that may satisfy these needs broadcast the RREQ packet, the supply node broadcasts RREQ packet .The RREQ packet contains the identities of the supply and destination nodes, the utmost variety of intermediate nodes , trust and energy needs and also the supply node's signature and certificate then the supply node is trust needs square measure verified at every intermediate node can have low trust values, then verified at every subsequent intermediate nodes until it reaches at the extremely trusted nodes. every intermediate node ensures that it will satisfy the supply node's trust/energy needs. It also verifies the packet's signature victimization the general public keys extracted from the nodes' certificates. These verifications are necessary to confirm that the packet is distributed and relayed by real nodes and also the nodes will satisfy the trust requirements as a result of their trust values square measure signed by TP. The intermediate node signs the packet's signature forming a series of signatures of the nodes that broadcast the packet. This signature authenticates the intermediate node and proves that the node is that the certificate holder and thus the connected trust values belong to the node. The signature additionally allows the trust system to create positive that the intermediate nodes have so participated within the route to carry them chargeable for breaking the route. Finally, the intermediate node broadcasts the packet once adding the signature chain and its identity and certificate.

If a node receives identical request packet from completely different nodes, it processes solely the primary packet and discards the subsequent packets. The destination node composes the RREP packet for the route traversed by the primary received RREQ packet, and sends it to the supply node. This route is the shortest one that may satisfy the supply node's requirements. The supply node's needs can not be achieved if it doesn't receive the RREP packet at intervals a time amount. It will initiate a second RREQ packet however with additional versatile needs. The supply node verifies the hash message and also the nodes' certificates to create positive that the nodes satisfy its trust needs and also the future destination node was reached, then it starts knowledge transmission.

### B. BAR Routing Protocol

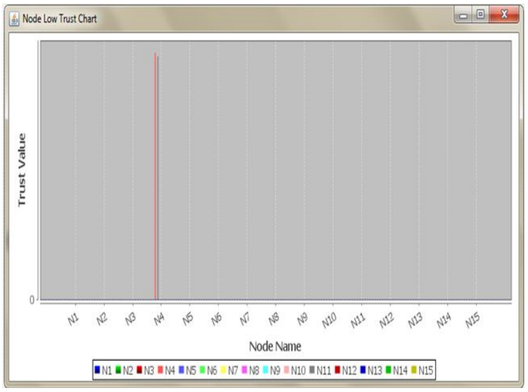
The The BAR routing protocol permits, the destination node to choose out the foremost effective reliable route at intervals the network. The supply node sends RREQ packet to the intermediate nodes, Associate in Nursing intermediate node broadcasts the RREQ packet once attaching its identity and certificate, the number of messages it commits to relay. The intermediate nodes unit of measurement impelled to report correct energy commitments to avoid breaking the route and so degrading their trust values. The RREQ packet flooding generates few routes, as a result of every node broadcasts the packet once, it cannot notice the higher routes. that the BAR protocol permits each node to broadcast the RREQ quite once if the route dependableness or period of the recently received packet is larger than the last broadcasted packet. Destination selects the route with high responsibility that is calculated by the formula given below. therefore it thought-about the route path with high responsibility for broadcasting the packet. The route responsibility calculated for the first trust worth is simplicity, but the alternative trust values may additionally be thought of victimization weight factors. the provision node can attach the load vector (w1, w2, w3, w4) to the RREQ packet. The Destination node calculates the whole route responsibility as follows:

Total route dependableness = (((w1 x T (1)) + (w2 x T (2)) + (w3 x T (3)) + (w4 x T (4)))

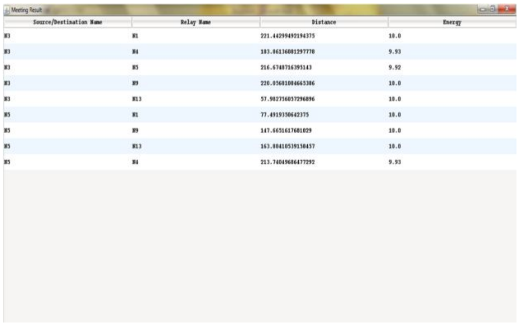
wherever w1+ w2+ w3+ w4 = 1

## IV. EXPERIMENTAL RESULTS

Below diagram will shows us the node which is acting as relay node. This relay node will have low trust value because of this relay node only communicated with the both source and destination nodes. Here as per below graph N4 will be the relay node.



When we try to see the instance of nodes. We can find the below table. Below table will represents complete info about the source/destination nodes and it shows us the relay for particular sources/destinations. It also shows the distance between source/destination node to relays. We can also find energy levels of nodes.



| Source/Destination Name | Relay Name | Distance | Energy |
|---|---|---|---|
| N3 | N1 | 221.44299492194375 | 10.0 |
| N3 | N4 | 183.06136081297778 | 9.93 |
| N3 | N5 | 216.6748716395143 | 9.92 |
| N3 | N9 | 220.05681084665306 | 10.0 |
| N3 | N13 | 57.982756057296896 | 10.0 |
| N5 | N1 | 77.4919350642375 | 10.0 |
| N5 | N9 | 147.6651617681029 | 10.0 |
| N5 | N13 | 163.08410539158457 | 10.0 |
| N5 | N4 | 213.74049686477292 | 9.93 |

## V. CONCLUSION

The continued analysis within the field of mobile wireless communication can continuously offer North American country alternatives on a way to remain connected continuously. though most of the architectures have shown a way to increase network capability and increase turnout and how to cut back delay still there's a lot of work to be done. As the future are going to be heterogeneous therefore the quality protocol being selected ought to be ready to adapt to totally different network topologies and varied potential eventualities. a lot of incentives have to be compelled to be to the top user on why he ought to be wiling to assist a client located outside the cellular coverage. a lot of security protocols additionally need to be introduced to boost the effectiveness against any kind of attack by a user.

## References:

[1] Lee K.H, Han K Y, Song Y J ,1997, ―Capacity Enhancement of Uplink Channel Through spatial reuse in multihop cellular networks

[2] Carbone, B., 2006, ―Routing Protocols for Interconnecting Cellular and Ad Hoc Networks., Universite Libre De Bruxeles , Faculte des Sciences, Department ‗d Informatique,2006‖ Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Perkins E C. and Bhagwat P ,2001 , ―DSDV Routing over a Multihop Wireless Network of Mobile Computers‖, , in Ad hoc Networking Addison Wesley Chapter 3 ,pages 53-74.

[4] Clausen T. and Jacquet P, 2003, ‖Optimized link state routing protocol (OLSR). In RFC3626, October.

[5] Johnson B D. and Maltz A D., and Hu C Y,1996 , ―The Dynamic Source Routing Protocol for Mobile Ad Hoc

Networks (DSR)‖. In Tomasz imielinski and Hank Korth , Mobile Computing Volume 353, pages 153-181. Kluwer Academic Publishers,Chapter 5.

[6] Park D V. and Corson S M,1997, ‖A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks‖, at IEEE Conference on Computer Communications, INFOCOM 97, April 7-11, Kobe Japan

[7] Perkins E C. and Royer Belding M E., Das S., 2003, ―On Demand Distance Vector Routing Protocol‖ in draft – ietfmanet-aodv-13.

[8] Cavalcanti D and Agarwal D ,2005, ―Issues in Integrating Cellular Networks WLAN‗s & MANET‗s‖, IEEE Wireless communications.

[9] H. Wu, C. Qiao, S. De, O. Tonguz,. 2001, ― Integrated cellular and ad hoc relaying systems: iCAR, ―, IEEE Journal on Selected Areas in Communications 19 (10) (2001) 2105–2115. IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010 66

[10] S. Dixit, E. Yanmaz, O.K. Tonguz, 2005, ―On the design of self-organized cellular wireless networks‖ , IEEE Communications Magazine 43 (7) (2005) 86–93.

[11] Li J X, Seet C B, Chong Joo H P, 2008 ―Multihop Cellular networks Technology and Economics‖, Computer Networks 52 (2008) 1825–1837 www.elsevier.com/locate/comnet.

[12] Y.-D. Lin, Y.-C. Hsu 2000, ― Multihop cellular: a new architecture for wireless communications‖, in: Proceedings of IEEE INFOCOM‗00, Tel Aviv, Israel, 26–30 March, 2000, pp. 1273–1282.

[13] H. Luo, R. Ramjee, P. Sinha, L.E. Li, S. Lu,2003 ‖ UCAN: a unified cellular and ad-hoc network architecture ―, in: Proceedings of ACM MOBICOM‗03, San Diego, CA, USA, 14–19 September 2003, pp. 353–367.

[14] IEEE Computer Society, Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band: IEEE Standard 802.11b, 1999.

[15] L.M. Feeney, B. Cetin, D. Hollos, M. Kubisch, S. Mengesha, H. Karl, 2007 , ―Multi-rate relaying for performance improvement in IEEE 802.11 WLANs‖, in: Proceedings of WWIC‗07, Coimbra, Portugal, 23–25 May,2007, pp. 201– 212.