ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficient Stable Routing Protocol for Heterogeneous Multi-Hop Wireless Networks

Dr.Ch.Mukundha
Associate Professor
Department of IT
Sreenidhi Institute of Science and Technology
(Autonomous)
Ghatkesar, Hyderabad, India.

R.Shireesha
M.Tech Student
Department of IT
Sreenidhi Institute of Science and Technology
(Autonomous)
Ghatkesar, Hyderabad, India.

Abstract:

The growth of mobile computing and wireless communication have rapidly increased the mobile users worldwide. This is the reason for the creating new applications of mobile ad-hoc network and also communication is provided with reliability for the users. Due to lack of resource scarcity and dynamic network topology, therefore providing reliable service is difficult. In the proposed multihop wireless network Efficient Stable and Reliable Routing protocol integrates the payment and trust systems with the routing protocols by providing the goal of enhancing route reliability and stability. The payment system allows to charge the nodes that send packets and reward those forwarding packets. The trust system is important to evaluate the nodes' behavior and its trustworthiness, reliability and stability in forwarding packets in terms of multi-dimensional trust values. Hence the trust values are calculated for each node and developed two routing protocols that is to send the packets through highly trusted nodes having required energy to minimize the possibility of breaking the route. To strengthen the trust evaluation, the proposal from each node is included in trust calculation by TP (Trusted Party).

Key words: ***RCRP,AOMDV, MANETS ,QOS, routing bandwidth energy ,delays.***

I.Introduction

In networks, when a mobile node needs to communicate with a remote destination, it relies on the other nodes to relay the packets with the help of multihop wireless networks[1].coverage area using limited power and improve area spectral efficiency network are used for the transmission of multihop packet. In developing and rural areas, the network can be deployed more readily and at low cost.HMWNs can implement many useful applications such as data sharing and multimedia data transmission [2]. Examples that are applicable are, users in one area (residential locality,Academy campus, etc) having different wireless-enabled devices (Personal digital assistants and other wireless devices) can establish a communication network. The multihop wireless network can be implemented in many useful applications such as data sharing and multimedia data transmission. It can establish a network node to communicate, distribute files, and share information. The main assumption is limited resources, such as battery energy and available network bandwidth are willing for the nodes . However the drawbacks in the existing routing protocol such as Dynamic Source Routing(DSR)[6] is assumed that the network nodes are ready to relay other nodes' packets.However this assumption is reasonable in disaster recovery because the nodes pursue a common goal and belong to one command, but it may not support for civilian applications where the nodes aim to maximize their benefits, since their coordination consumes their valuable resources such as bandwidth, vivacity, and computing power without any benefits.

In multihop wireless networks, the big challenge is optimal routing.Quality of Service(QoS) requirements should satisfy a route to ensure that each session is provided by routing protocol(e.g.,ratioband, retard and frazzle). Additionally, the routing protocol should avoid network blockage by balancing the loads optimally between routes to utilize the resources in orderly[4]. The devices that are participating in MANET are likely small devices, with limited processing power, retention and cache capacity. The bandwidth is divided by all devices in the surrounding area in wireless communication.Moreover,an increase in network traffic places extra load on the nodes in the network, which in turn increases energy utilization[5] .Therefore, it is difficult to design a technique that utilizes the energy minimally and uniformly.

In civilian applications, selfish nodes will not be by preference interested in cooperation without sufficient incentive, and cooperative nodes use to make relay their packets, which has negative effect on the network veracity and performance. Impartiality issue occurs when a selfish node takes an advantage from the common nodes without participating among them, and the cooperative nodes are unfairly overloaded.Due to this the selfish behavior regards due to the network performance significantly results in failure of the multi-hop communication. In addition, breakage of nodes takes place due to insufficient energy that results to relay the source nodes' packets and keep the routes connected. Because of the nodes' behaviour an uncertainity occurs,due to this randomly selecting the intermediate nodes will degrade the routes' stability and reliability. This proposed system overcomes these drawbacks by the considering methods, trust values and payment systems[3].

The payment system uses credits to charge the nodes for relaying packets to send packets and rewards for those relaying packets[7] . The trust system is required to evaluate the nature of the nodes' trustworthiness,stability and reliability in relaying packets. A node's value is trusted based on the degree of belief about the node's behavior. The calculation is made to trust from the nodes' past behaviors and used to predict their future behaviour.

We propose a trust system like multidimensional trust values on each node to evaluate the node's behavior from various perspectives. Multidimensional trust values predict the node's future behavior, to help in making smarter routing decisions. In trust systems, the nodes behaves such a way that frequently drop packets, breakage of routes, or are unactive in relaying packets to have a low trust values.The implementation of the trust system are efficient,because TP computes the trust values by processing the payment receipts. The node's trust values are attached to its public-key certificate for making routing decisions.

The paper is organized as follows. Section II Related work III gives an overview ESRP. Section IV Overview of Route establishment phase. In Section V Performance Evolution Section VI Conclusion.

II RELATED WORK

Reputation-based schemes[3] experience the ill effects of false allegations where some fair nodes are erroneously distinguished as malicious. This is on account of the nodes that drop bundles incidentally, e.g., because of blockage, dishonestly distinguished as malicious by its neighbors. With a specific end goal to decrease the false allegations, the plans trust to utilize progressive limits to ensure that a node's bundle dropping rate can just achieve the limit if the node is malevolent.

Be that as it may, this increases the missed discoveries where a few pernicious nodes are not recognized. Additionally, tolerant edge empowers the nodes with high bundle dropping rate to take an interest in courses, and empowers the malignant nodes to dodge the plan by dropping bundles at a rate lower than the plan's edge. At the point when a node's notoriety quality is over the threshold,it does not have impetus to hand-off bundles since it doesn't bring more utility. The framework proposed the idea that enhance throughput in an specially appointed system within the sight of nodes that consent to forward bundles however neglect to do as such. To moderate this issue to classifying the nodes based upon their powerfully measured conduct. So in this segment the two expansions are acquainted with the Dynamic Source Routing calculation[4] to moderate the impacts of directing rowdiness, for example, watch dog and path router. The watchdog recognizes acting up nodes, while the way rater abstains from directing bundles through these nodes.

In ESIP[5],secure incentive protocol the payment scheme uses a communication protocol transfer messages from the source node with limited operations to the destination node in the public key cryptography. For a single packet Public key cryptography is used and in the next packets efficient hashing operations are used.Secure incentive protocol aims to transfer messages efficiently, it aims to establish stable and reliable routes in multihop wireless networks.The payment[6] through the rational packet-dropping attacks, where the attackers drop packets due to non-benefit from relaying packets.A reputation system to identifies the irrational packet-dropping attackers which packet-dropping rates exceed a threshold.

In[8] Velloso et al. have proposed a human-based model which builds a trust relationship between nodes in ad hoc network. Without the necessity for global trust knowledge, they have presented a protocol that scales efficiently for large networks. In a secure and reliable routing protocol with quality of service support has been proposed. The routing metrics are by combing the nodes based on requirements on the trustworthiness and the quality of service of the links along a route.

III Efficient Stable Routing protocol (ESRP)

The heterogeneous Multihop Wireless Networks has public key certificates is used to all the nodes with mobile nodes and offline Trusted Party (TP).The mobile nodes have different hardware and energy capabilities. Each node has its unique identity and with a limited time certificate issued by TP by public/private key pair.The node cannot communicate nor act as an intermediate node without a valid certificate,. TP maintains the node’s credit accounts and trust values. Each node submit the payment reports by contacting TP and TP updates the involved node’s payment accounts and trust values.

3.1 NETWORK ARCHITECTURE

The heterogeneous Multihop Wireless Networks has public key certificates is used to all the nodes with mobile nodes and offline Trusted Party (TP).The mobile nodes have different hardware and energy capabilities.The nodes have long relation with the network and its lifetime is long in civilian applications.The heterogeneous Multihop Wireless Networks has public key certificates is used to all the nodes with mobile nodes and offline Trusted Party (TP). Different hardware and energy capabilities the have mobile nodes.The network that used for civilian applications, and its lifetime is long, and the nodes have the network with long relation.Thus,every interaction will always have an expectation of future reaction. Each node has a unique identity and limited-time certificate issued by TP with a public/private key pair.A valid certificate is provided for the node that cannot communicate nor act as an intermediate node. Trusted party maintains the nodes’ credit accounts and trust values. Each node submit the payment reports by contacting TP and payment accounts and trust values are involved node to updates the TP . The adversaries have full control on their nodes.The cryptographic identification can be obtained by changing the normal operation of nodes. Attempts can be made to attack the payment system like steal credits, pay less, or communicate for free.

3.2 DATA TRANSMISSION PHASE

The source node sends messages with the intermediate node through a route to the destination node. Source node computes the signature with hash message for transferring the data packets and in the route first node sends the packet.Source node has sent messages to ensure the TP.The node verifies source node signature from each intermediate node and for composing the report signature can be stored with the hash messages. Hash messages for the destination node is to generate acknowledgement for the received message and ACK packet is sent by the destination node for each intermediate node.For composing the report the hash messages verifies the each intermediate nodes. A report composes a route for each node and the payment and update its trust values are claimed by the TP to submit when it has connection.

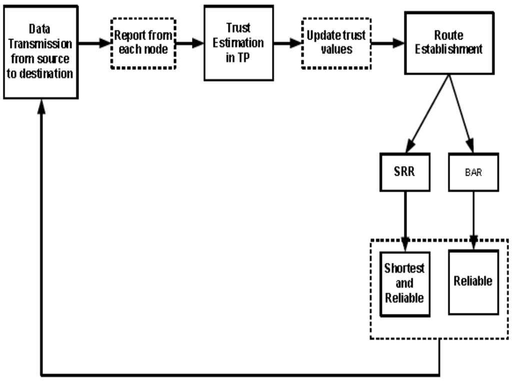

Fig 1: ESRP in Multihop WSN

3.3 TRUST ESTIMATION PHASE

A report is received by trust party and the unique identifier before processing it checks the report first. Computing the node signatures with hash message can be verified by the authority of the reports. If the report is valid, if hash message can be verified by trust party at destination node. TP clears the report by rewarding the intermediate nodes and debiting the source and destination nodes.From the source node the number of messages sent are signed and from the hashing operations number of hashing operations can be computed.In nodes trust values are calculated based in relaying packets based on node's trustworthiness and reliability.In the proposed system node's future behaviour can be predicted based on multidimensional trust instead of single trust.In routing node selection is made based on the trust values.

IV. ROUTE ESTABLISHMENT PHASE

4.1 SRR Protocol

The SRR routing protocol establishes the shortest route that can satisfies the source nodes requirements is trusted enough to act as a relay. This protocol avoids the lowtrusted nodes. In this protocol the source node fix its requirements in the RREQ packet, and these requirements should satisfy the nodes that broadcast the RREQ packet, RREQ packet broadcasts the source node.The identities of the source and destination nodes contains the RREQ packets,which has the maximum number of in-between nodes, requirements like energy and trust values and signature and certificate of the source node's.The trust requirements of source nodes are verified at each intermediate node will have low trust values,it then verified at each ensuing intermediate nodes until it reaches at the eminently trusted nodes.

Source node's trust/energy requirements can satisfy by ensuring each intermediate node.The public keys extracted from the node's certificates verifies the packets signature using intermediate nodes. These verifications are necessary to ensure that the packet is sent and received by genuine nodes and the nodes can satisfy the trust requirements because their trust values are signed by TP. The packet's signature forming a chain that signs the intermediate node of signatures that broadcast the packet.The intermediate node authenticates the signature node and proves that the node is the certificate holder and the node belong to the attached trust values.The trust system enables the signature to make the intermediate nodes that had surely participated in the route which hold them responsible for the route breakage. Finally, the packet after connecting the signature chain, its identity and certificate it broadcasts the intermediate node.

Different nodes receives the same request packet, it processes only the first packet and discards the later packets. The RREP packet composes the destination packet for the route go across the first received RREQ packet, and the source node receives it. This source node's requirements satisfy this as one of the shortest route. The RREP packet within a time period cannot be received then the source node's requirements does not achieve.With more flexible requirements second RREQ packet can be intiated. The source node verifies the hash message and the node's certificates to make the nodes satisfy its trust requirements and its the future destination node was reached, then it starts data transmission.

4.2 BAR Routing Protocol

The BAR routing protocol it enables, the destination node to select the best reliable route in the network. The RREQ packet sends source node to the intermediate nodes, the RREQ packet broadcasts an intermediate node after attaching its identity and certificate, it commits to relay the number of messages. The intermediate nodes are moved to report correct energy fidelities to avoid breaking the route and thus degrading their trust values. The RREQ packet flooding generates few routes, because the packet boardcasts each node once, it cannot find the better routes. So the BAR protocol allows the RREQ to broadcast each node more than once if the route reliability or lifetime of the recently received packet is more than the last broadcasted packet.

RREQ packet at first it sends to destination node and waits for a period to receive another RREQ packets if there are. It selects the best available and shortest route are arranged if a set of feasible routes are found. If there are multiple routes with lifetimes, atleast to send messages, the destination node selects the reliable route, otherwise, it establishes numerous routes to send messages in such a way that it reduces the routes and maximizes the reliability and stability. Then the destination node composes the RREP packet sends that packets to the route.

Establish stable route based on trust value Initialize N number of nodes in the network i=1,….N S broadcast RREQ packet to all the nodes TP compute the trust value of each node in the network If (nodes that relay messages more successfully) Highest trust value Else Lowest trust value End if Select the highest trust nodes Based on the highest trust value select the route and update the trust values S select the stable route D composes RREP packet for the first received RREQ packet and reply to S.

V.PERFORMANCE EVALUATION:

We investigate the performance of proposed ESRP protocol using the ns-2 simulator with the necessary extension and compare it with AODV In our simulations, we use a fixed transmission range of 250 meters, most of real time and current network interface cards are supported by this.We used the “random waypoint” with speed of nodes is uniformly distributed between 0 to maximum speed of 20 m/s with pause time value of 60 sec. All mobile nodes to be equipped with IEEE 802.11network interface card and data rates of 2.5Mbps. The initial energy of all the nodes is 10J. The transmission power is600mW and the receiving power is 300mW. Finally, source nodes generate CBR (constant bit rate) traffic. Traffic sessions are generated randomly on selected different source-destinations with a packet size of 512 bytes.

Every node in a network has to run our algorithm whenever it becomes an intermediate node to forward the information of source nodes. Each simulation was run for the duration of 200 seconds and sampled data we collected from simulation is average of 4 times.

Our aim is mainly to improve the reliability and packet delivery ration.

This Fig.2 clearly shows ESRP can significantly that the first node failure occurs in a network due to exhausting of battery. Delay in the failure of first node impacts on other node to be delayed.

In Fig.3 shows the important characteristic of ESRP is finding reliable route .In fig.3 shows the finding packet delivery ratio compare to other, where less amount of energy consumed to route a packet.

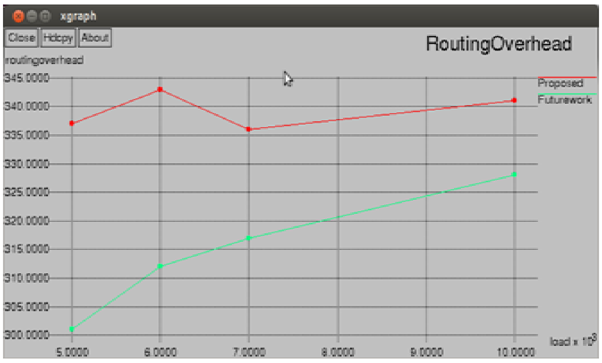

Fig 2.network routingoverhead when load varies

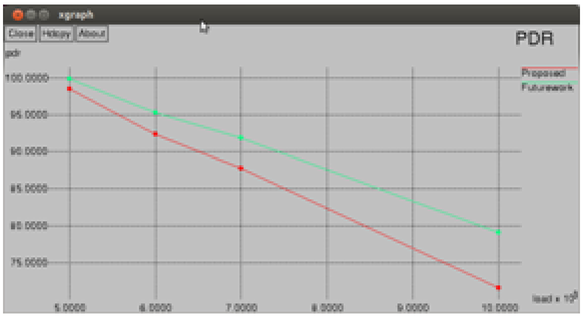

Fig: 3 packet delivery ratio vs when load varies

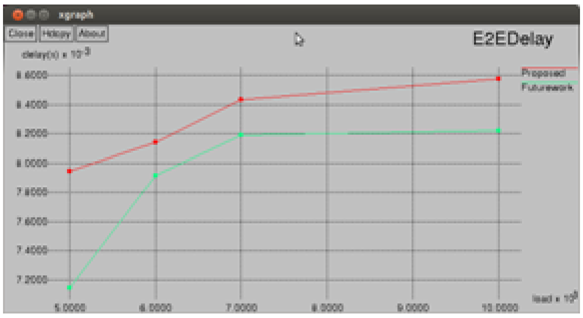

Fig: 4 Average end to end delay, when load varies

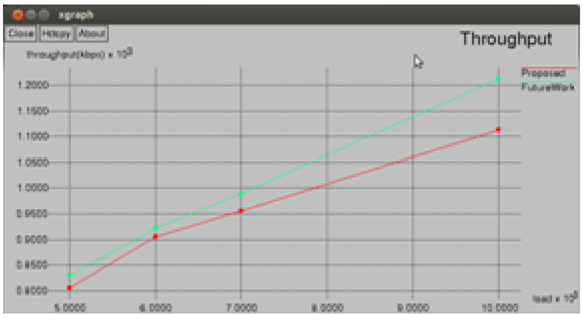

Fig:: 5 Average throughput, when load varies

VI. CONCLUSION:

The proposed ESTAR uses payment and trust systems with trust-based and energy-aware routing protocol to establish stable and reliable routes in wireless networks. ESTAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also penalizes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. The proposed routing protocols like SRR and BAR is evaluated them in terms of overhead,stable and route stability. These routing protocols can be informed by considering multifactors, including the route length, the route reliability and stability based on the node's past behavior, and the route lifetime based on the node's energy capability. Performance evaluation is done based on the results of the simulation done using ns2. It is proved from the results that the route reliability and packet delivery ratio has been improved using this protocol. The packet security is decreased with untrusted nodes. In future it provides security for each packet, so that the intruders can't able to get or damage the packets.

VII.REFERENCE

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J.,vol. 13, no. 4, pp. 175-193, 2009.

[2] Sevil Sen, and John A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks", Proceedings of the second ACM conference on Wireless network security (WiSec '09).

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACMMobiCom'00,pp. 255-265, Aug. 2000.

[4] Johnson, D. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", In C. Perkins, editor, Ad Hoc Networking, chapter 5, pp. 139-172. Addison-Wesley, 2001.

[5] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop WirelessNetworks ," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[6] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in MultihopWireless Networks,"IEEETrans.VehicularTechnology, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[7] G. Theodorakopoulos and J.S. Baras, “On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[8] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, “Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model,” IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[9] M. Yu and K. Leung, “A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks,” IEEE Trans. Wireless Comm.,vol. 8, no. 4, pp. 1888-1898, Apr. 2009.

[10] Kartik Kumar Srivastava et al ,”Secure Data Transmission in MANET Routing Protocol”,Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921.