VOL. 10, NO. 1, JANUARY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

SEAR: SECURED ENERGY-AWARE ROUTING WITH TRUSTED PAYMENT MODEL FOR WIRELESS NETWORKS

S. P. Manikandan[1], R. Manimegalai[2] and S. Kalimuthu[3]
[1]Department of Computer Science and Engineering, Sri Venkateshwara College of Engineering, Chennai, India
[2]Department of Computer Science and Engineering, Park College of Engineering and Technology, Coimbatore, India
[3]Department of Computer Science and Engineering, SMK Fomra Institute of Technology, Chennai, India
E-Mail: spmanikandan@svce.ac.in

ABSTRACT

In a multi-hop wireless network, a source node that needs to communicate with a destination node relies on other nodes in the network to forward the packets. This multi-hop packet transmission can extend the network coverage area using limited power and improves area spectral efficiency. The proposed Secured Energy-Aware Routing (SEAR) integrates multi-hop wireless network with payment and trust model. The goal of SEAR is to enhance reliable and stable routes. Payment model is used to charge those nodes that send packets and reward those nodes which forward the packet. On the other hand, trust model is used to evaluate nodes trustworthiness and reliability in forwarding packets. Multi-dimensional trust values are calculated for each node to send packets from source to destination. Moreover, trusted nodes with sufficient energy are used for routing and also to minimize the possibility of breaking the route. To evaluate trust, recommendation from each node is included in the process run by Trust Party (TP) and nodes are rewarded according to their status of packet forwarding. The SEAR in multi-hop wireless network is implemented using Network Simulator (NS2). The performance evaluation is done for measuring Quality of Service (QoS) parameters such as Packet Delivery Ratio (PDR), Call Acceptance Ratio (CAR) and Route Lifetime (RL).

Keywords: multi-hop, trust, reliable route, trust party.

1. INTRODUCTION

The multi-hop wireless networks implement useful applications such as data sharing and multimedia data transmission. The multi-hop network can communicate, distribute files, and share information. Nodes in a multi-hop network are willing to spend their limited resources such as battery energy and available network bandwidth [1], whereas in DSR, nodes are willing to relay packets from other nodes [2]. This assumption is reasonable in disaster recovery because the nodes pursue a common goal and belong to one authority, but it may not hold for civilian applications where the nodes aim to maximize their benefits, since their cooperation consumes their valuable resources such as bandwidth, energy, and computing power without any benefits. The selfish behavior degrades the network performance significantly resulting in failure of the multi-hop communication [3]. In addition, some nodes in the network may break routes due to insufficient energy to relay packets of same node and unable to keep the routes connected [4]. Such kind of uncertainty in the nodes behavior, randomly select the intermediate nodes and degrades the route stability [3, 5]. The proposed approach, SEAR, overcomes these drawbacks by implementing the two techniques, called, trust and payment system. The trust system is essential to assess the nodes trustworthiness and reliability in relaying packets [6]. A nodes trust value is defined as the degree of belief about the neighborhood nodes behavior. The trust values are calculated from the nodes past behaviors and used to predict their future behavior. The two standards, namely, the *Shortest Reliable Route* (SRR) and the *Best Available Route* (BAR) are used to identify energy-aware trusted nodes for routing in MANET.

1.1. Shortest reliable route

SRR protocol establishes the shortest route that can satisfy the requirements of the source node which can act as a relay. This protocol, avoids the low-trusted nodes. In this protocol the source node embeds its requirements in the Route REQuest (RREQ) packet, and the nodes that satisfy these requirements broadcast the RREQ packet. The RREQ packet contains the identities of source, destination, maximum number of intermediate nodes, trust, energy requirements, source nodes signature and certificate. Source nodes trust requirements are verified at each intermediate node. If the intermediate node has low trust values, then it is verified at each subsequent intermediate node till it reaches at the highly trusted nodes [7]. Each intermediate node ensures that it can satisfy the source nodes trust/energy requirements. It also verifies the packet signature using the public key extracted from the nodes certificate for generating the receipt. A receipt is a packet which contains all the information about the behavior and status of those nodes that processes the data. The receipt is used by Trust Party (TP) to calculate the trust values of the nodes. These verifications are necessary to ensure that the packet is sent and relayed by genuine nodes and satisfy the trust requirements signed by TP.

The intermediate node signs the packets signature forming a chain of signed nodes that broadcast the packet. This signature authenticates the intermediate node and proves that the node is the certificate holder and thus the attached trust values belong to the node.

The destination node composes the RREP packet for the route traversed by the first received RREQ packet, and sends it to the source node. This route is the shortest

one that satisfy the source nodes requirement. The source node requirements cannot be achieved if it does not receive the RREP packet within a time period [3]. The source can initiate a second RREQ packet with more flexible requirements. The destination node verifies the hash message and certificate of intermediate nodes to make sure that it satisfies with trust requirements. The destination node responses with RREP packet through the best route among all possible routes as shown in Figure-1.

The source node (N1) broadcasts the RREQ packet through all possible routes i.e. via route1 (N2-N3-N4) and route2 (N6-N7-N8) to reach destination node (N5). The destination node (N5) responses with RREP packet through the best route i.e. via nodes N8-N7-N6 having good energy level values 8.1, 9.2 and 8.2, respectively.

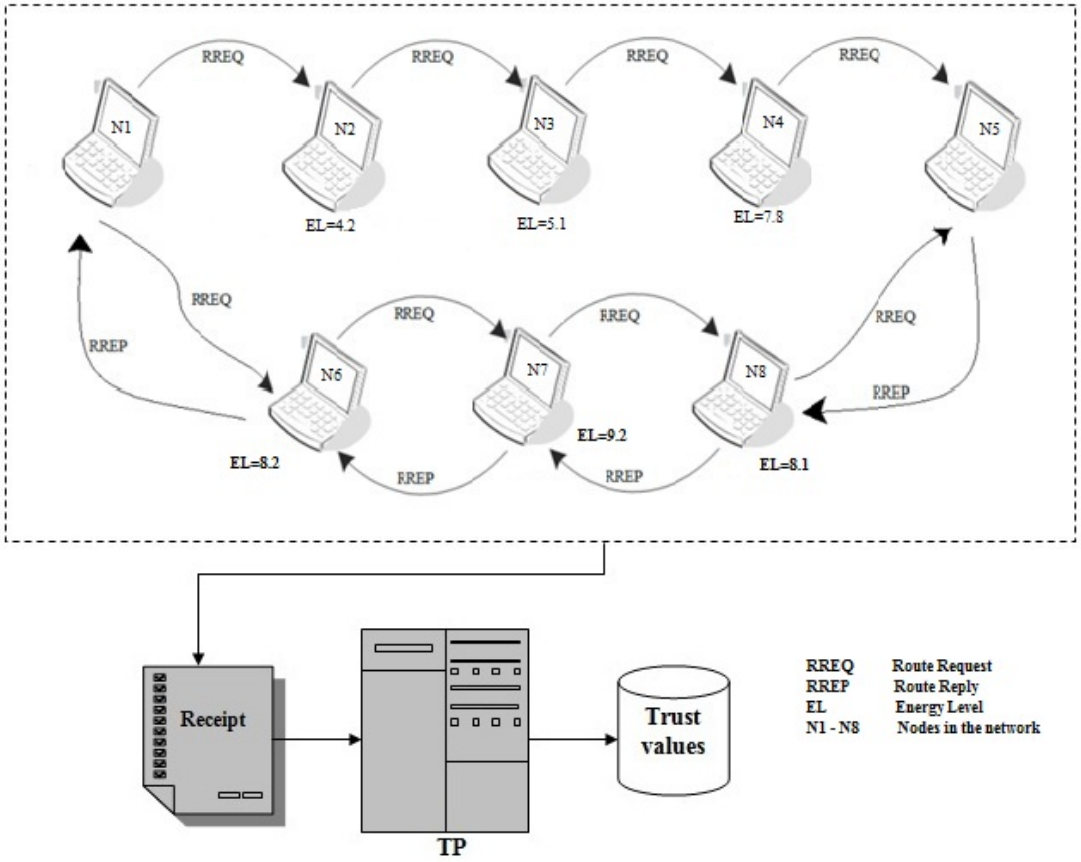

Figure-1. Trust evaluation in SEAR.

1.2. Best available route

The BAR routing protocol enables the destination node to select the best reliable route in the network. The source node sends RREQ packet to the intermediate nodes, an intermediate node broadcasts the RREQ packet after attaching its identity and certificate, the number of messages it commits to relay. The intermediate nodes are motivated to report correct energy commitments to avoid breaking the route. The RREQ packets are flooded to generate few routes. The source cannot find better routes because each node broadcasts the packet only once. So the BAR protocol allows each node to broadcast the RREQ more than once if the route reliability or lifetime of the recently received packet is greater than the last broadcasted packet. Destination node selects the route with high reliability for broadcasting the packet.

The destination node receives the first RREQ packet and waits for a while to receive more RREQ packets if any. Then, it selects the best available route from a set of feasible routes. If there are multiple reliable routes to send packets, the destination node selects the most reliable route, otherwise, it establishes multiple routes to send messages such a way that reduces the routes and maximizes the reliability. Then the destination node composes the RREP packet through the reliable route to the source node.

2. RELATED WORK

Marti et al., have proposed a watchdog mechanism implemented using DSR by categorizing nodes in the network based on their dynamic behavior [1]. The proposed method complements DSR by having watchdog and path-rater incorporated in it. The watchdog

is used for detection of malicious behavior. It runs on each node listening to all transmissions of neighboring nodes. On the other hand, path-rater is used for trust management and routing policy. Each possible path is rated by path-rater. A buffer is maintained by the watchdog which contains details of recently sent packets. When a packet is forwarded to the next hop, its details are removed from the buffer. If a packet remains in the buffer for a long time, watchdog isolates the corresponding node as misbehaving node. The misbehaving nodes identified by the watchdog are avoided for packet transmission. On simulation, the proposed method (Marti et al 2000) performed efficiently, increasing the throughput by 17% in the presence of 40% misbehaving nodes. Further investigation needs to be carried out on conducting tests using watchdog and path-rater to determine optimal values to increase throughput in different situations. In addition to throughput, evaluation of watchdog and path-rater need to be done with respect to latency.

Velloso *et al.*, implements the concepts of human trust applied in ad hoc network [4]. This model builds a trust relationship between each node and its neighbor nodes in the network. The trust is based on previous individual experiences of the node and recommendations of its neighbors. The ability of assessing the trust level of its neighbors brings several advantages. First, a node can detect and isolate malicious behaviors and avoiding relaying packets to malicious neighbors. The cooperation is stimulated by selecting the neighbors with higher trust levels. The recommendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link breakage.

The Recommendation Exchange Protocol (REP) in [4] allows nodes to exchange recommendations about their neighbors. The trust information is not disseminated over the entire network. Instead, nodes only need to keep and exchange trust information about nodes within the transmission range. Recommendation Exchange Protocol introduces a relationship maturity model, which improves the efficiency of the trust evaluation process in the presence of mobile nodes for multi-hop networks. Keeping neighborhood information implies significant lower energy consumption, less processing for trust level calculation, and less memory space.

Gunasekaran *et al.*, have proposed a payment scheme for multi-hop networks called Report-based pAyment sChemE (RACE) [10]. RACE used to stimulate node cooperation, regulate packet transmission, and enforce fairness. Nodes in the network submit lightweight payment reports to the Accounting Center (AC) and temporarily store undeniable security tokens called Evidences. The report contains the charges and rewards without security proofs. The AC can verify the payment by investigating the reliability of the reports, and clear the payment of the fair reports with almost no processing overhead. For cheating reports, the evidences are requested to identify and remove the cheating nodes that submit incorrect reports. RACE can identify the cheating nodes with requesting few evidences. Moreover, evidence aggregation technique is used to reduce the evidences storage area. RACE can secure the payment and precisely identify the cheating nodes without false accusations. If RACE fails to manage a broken route, a new route is established with a new receipt, and thus multiple receipts may be generated per session. Simulation results shows that RACE can significantly reduce the communication and processing overhead when compared to the existing receipt-based payment schemes.

3. TRUSTED SECURE ROUTING

3.1. Data transmission phase

Figure-2 depicts the architecture of the proposed SEAR protocol.

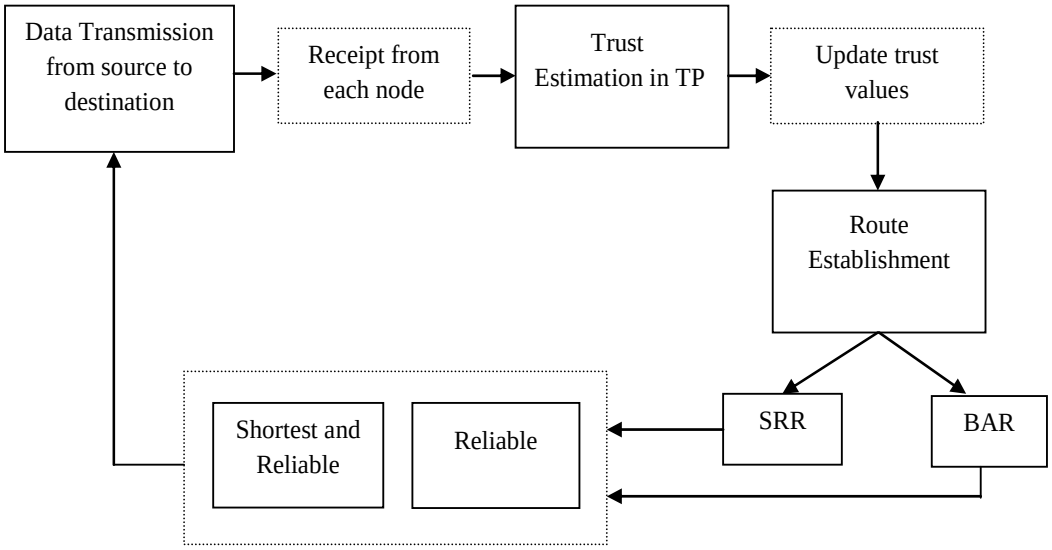

Figure-2. The architecture of SEAR.

In this work, the source node sends messages to the destination node through the best route. While transferring data packets source node computes the signature with hash message and sends the packet to the first node in the route. The source nodes signature ensures the authenticity and integrity of the message. Trust Party (TP) ensures that source node has sent messages. Each intermediate node verifies the signature of source node and stores signatures with hash message for composing the receipt. A receipt is a proof for participating in a route i.e. for sending, forwarding, or receiving a number of messages. Destination node generates a hash message to acknowledge the received message and sends ACK packet to each intermediate node. Each intermediate node verifies the hash message for composing the receipt [8]. Every node along the route composes a receipt and submits it with TP to claim the payment and updates its trust value [9].

3.2. Trust estimation phase

Trust Party (TP) receives a receipt, it first checks if the receipt has been processed before using its unique identifier. Then, it verifies the authority of the receipt by, computing the node's signature with hash message. If the receipt is valid, trust party verifies the destination nodes hash message. TP clears the receipt by rewarding the intermediate nodes and debiting the source and destination nodes. The number of message sent is signed by the source node and the number of message delivered can be computed from the number of hashing operations.

The trust values are calculated from each node based on nodes trustworthiness and reliability in relaying packets [10]. It is fair to increase the trust values of the nodes that are not in broken links, because they relayed packets truthfully. On the other hand, the trust system decreases the trust values of those nodes in a broken link. Trust is also dynamic or time-sensitive. So trust party has to periodically evaluate the nodes trustworthiness, i.e., a trust value at time t may be different from its value at another time. So the proposed system relies on the multi-dimensional trust values instead of single trust value to predict the nodes future behavior. Trust values are used to decide which nodes to be selected or avoided during routing [3, 11]. Since a trust value depicts the probability that the node conducts an action. Further the route reliability can be computed using the nodes trust values to give probabilistic information about the route stability and lifetime.

The trust values are calculated from the following:

$$T(1) = \frac{\text{(No of packets that are forwarded in last t sessions)}}{\text{(Total no of incoming packets in last t sessions)}}$$

$$T(2) = 1 - \frac{\text{(No of sessions broken by node in the last t sessions)}}{t}$$

$$T(3) = \frac{\text{(No of session that a node at least forward packets)}}{}$$

$$T(4) = \frac{\text{No of session that a node participated in the period t/m}}{}$$

$T_{xyz\,(i)} = T_{x\,(i)} \times T_{y\,(i)} \times T_{z\,(i)}$
T_{xyz} (i) = Trust value denotes the route reliability
Total Route Reliability = [T(1) x T(2) x T(3) x T(4)]
x, y, z = Intermediate nodes
i = 1, 2, 3, 4 (dimensions)

Trust values are used to decide which nodes to select/avoid in routing. Reliable route is selected to route the packet based on the probability of route stability and lifetime. If *i* = 1, then the packets will be transferred through the intermediate nodes x, y, z, and if i = 2 then it uses the route 2 to transfer the data and similar for other route selection.

4. PERFORMANCE EVALUATION

To analyze the effectiveness of the proposed SEAR protocol it is compared with existing Dynamic Source Routing (DSR) protocol. Performance is analyzed using the following metrics.

4.1. Performance metrics

The Packet Delivery Ratio (PDR) is the total number of packets received by the destination node over the total number of packets sent by the source nodes.

$$PDR = \frac{\text{Total Number of packet received}}{\text{Total Number of packet sent}}$$

In Figure-3, it can be seen that the PDR of SRR and BAR is higher than that of DSR. Because, the SRR and BAR protocol selects the highly trusted nodes and the nodes having sufficient energy to deliver the packets from source to destination. But DSR protocol randomly selects the intermediate nodes. So it contains low trusted nodes and with low energy for packet delivery.

The packet delivery ratio in DSR is at the range of 70% when there are 40 to 50 random nodes and it drops to around 65% when there are 60 nodes in the network. Moreover, the energy levels for the nodes using DSR are less compare to SRR and BAR protocols. The packet delivery ratio in SRR is seem to be above 70% which is comparatively higher than the DSR. By comparing BAR with DSR and SRR, BAR gives the best result i.e. 80 % of PDR is achieved.

The Call Acceptance Ratio (CAR) is the ratio of the number of times a route is established after sending a RREQ packet. As shown in Figure-4, the acceptance ratio of BAR is higher when the number of nodes in the wireless network is more whereas the number of nodes is less than 50 SEAR protocol chooses SRR to route the packet over the network. When more number of nodes

present in the network there exist a chance of presence of more malicious nodes in the network, so SEAR prefers BAR to route the packet.

The call acceptance ratio is achieved at the time when a route is established after sending a RREQ packet, whereas in BAR this is not based on number of nodes. In SRR the call acceptance ratio is decreased when numbers of nodes are getting increased.

The route lifetime is the number of packets sent in one route before it is broken.

Route Lifetime is high→Energy consumption is low.

Route Lifetime is low→Energy consumption is high.

In SEAR energy consumption is higher in all the cases, so amount of time taken to deliver all the packets to the destination node very less in BAR.

The Figure 5 shows the normalized route lifetime which is the average route lifetime in SEAR. The normalized route lifetime is always more in SEAR.

Performance of the proposed protocol establishes more stable routes by selecting reliable intermediate nodes and therefore it delivers packets more successfully compared with DSR in terms of total number of packets generated, received, forwarded and packet delivery ratio, call acceptance ratio, route lifetime.

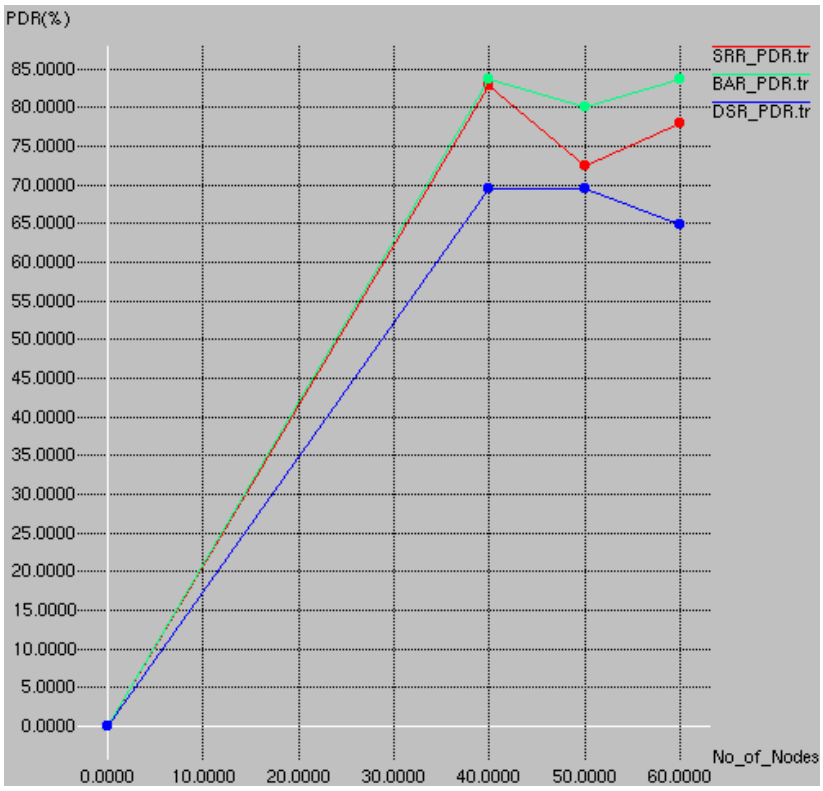

Figure-3. % of Packet Delivery Ratio.

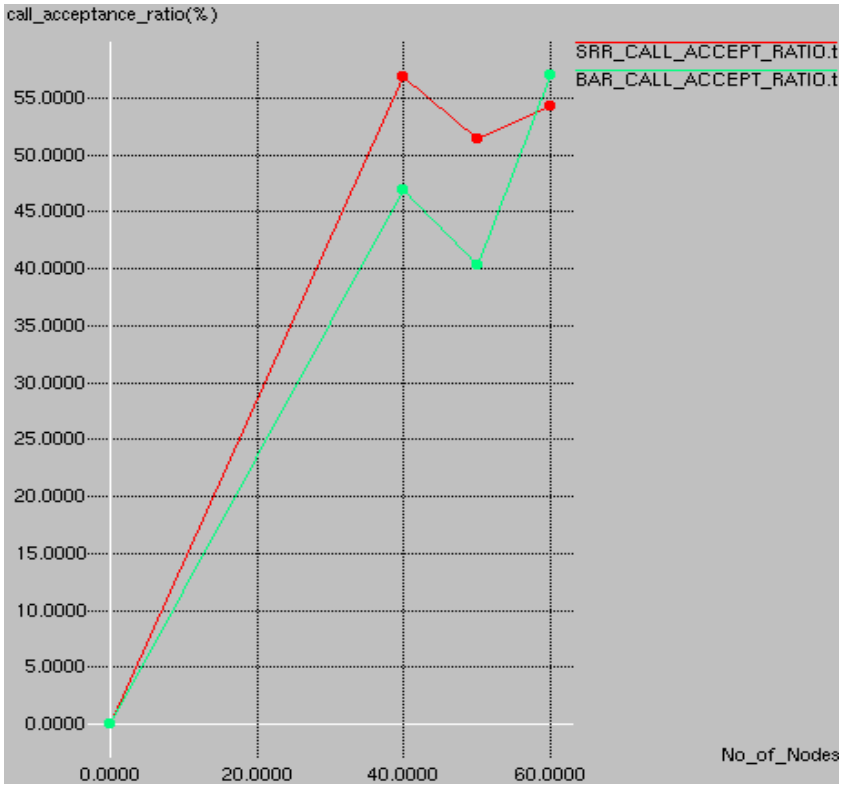

Figure-4. Ratio of route establishment.

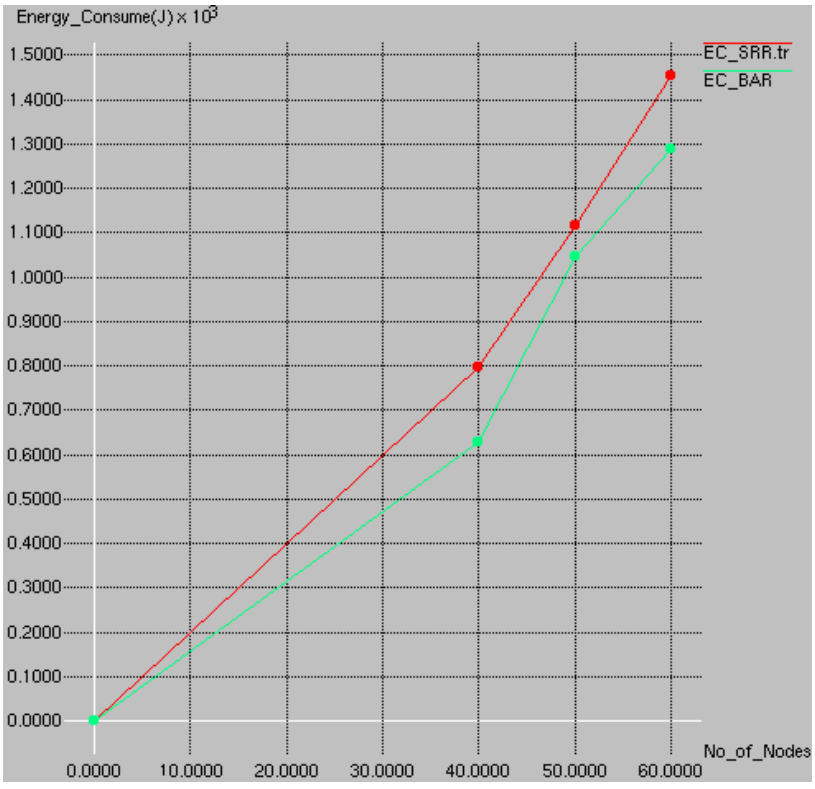

Figure-5. The route life time in SEAR.

5. CONCLUSIONS

The proposed SEAR algorithm uses trust and payment systems with trust-based-energy-aware routing protocol to establish stable and reliable routes in wireless networks. SEAR stimulates the nodes not only to relay other packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. The proposed SRR and BAR routing protocols is evaluated in terms of overhead and route stability. These protocols can make routing decisions by considering multiple factors, including the route length, route reliability based on nodes past behavior, and route lifetime based on the nodes energy capability. Performance evaluation and simulation is done using Network Simulator (NS2). From the results it is proved that the route reliability and packet delivery ratio has been improved using the proposed SEAR protocol.

REFERENCES

[1] S. Marti, T. Giuli, K. Lai and M. Baker. 2000. Mitigating routing misbehavior in mobile ad hoc networks. 'Proc. of IEEE/ACM MobiCom. pp. 255-265.

[2] D. Johnson, D. Maltz and J. Broch. 2001. 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.

[3] M. Mahmoud and X. Shen. 2011. ESIP: Secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks. IEEE Transactions on Mobile Computing. 10(7): 997-1010.

[4] P. Velloso, R. Laufer, D. Cunha, O. Duarte and G. Pujolle. 2010. Trust management in mobile ad hoc networks using a scalable maturity-based model. IEEE Transactions on Network and Service Management. 7(3): 172-185.

[5] M. Mahmoud and X. Shen. 2011. An integrated stimulation and punishment mechanism for thwarting packet drop in multihop wireless networks. IEEE Transactions on Vehicular Technology. 60(8): 3947-3962.

[6] S. Dhanalakshmi and M. Rajaram. 2008. A Reliable and Secure Framework or Detection and Isolation of Malicious Nodes in MANET. International Journal of Computer Science and Network Security. 8(10).

[7] S.G Shilpa, N.R. Sunitha and B.B. Amberker. 2011. A Trust Model for Secure and QoS Routing in MANETS. International Journal of Innovative Technology and Creative Engineering. 1: 2045-8711.