DATA AGGREGATED E-STAR COMMUNICATION FOR ADVANCED DRIVER SYSTEMS

Vijicaroline.V[1], Vishnupriyaa.P[2], Fincy Mol.F[3]

[1] *Student, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[2] *Student, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[3] *Asst. Prof, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*

ABSTRACT

Vehicular Ad-Hoc Network (VANET) is a self-organized network that can be formed by connecting vehicles aiming to improve driving safety in traffic management with internet access by drivers and programmers. The data aggregation technique is used where data from different nodes are collected. The correlated and redundant data are removed and the difference data is alone transmitted. The main disadvantage of the network correlation data gathering is that each sensor requires global knowledge of the network in terms of distance between all nodes. To overcome this problem E-STAR protocol is proposed. E-STAR is used to provide stable and reliable routes in multi-hop wireless networks, therefore energy consumption is reduced than the existing system. The E-STAR protocol uses Stable Reliable Route (SRR) and Best Available Route (BAR) as routing protocols to establish stable and reliable routes. These protocols include three process Route Request (RREQ) Route Selection, Route Reply (RREP). The energy consumption is reduced by using three modules namely data acquisition, data processing, wireless communication. The E-STAR protocol provides security by detecting the malicious nodes which drops the forwarded packets without forwarding them to save energy. The result shows that the proposed system provides high throughput, high security, reduced energy consumption, reduced packet loss.

Keyword: - *Multi-hop vehicular network, Stable and reliable router, Trust degree and Credit account.*

1. INTRODUCTION

VANET is a self-organized network formed by connecting vehicle thus increasing the convenience and safety of drivers. It improves the traffic management with internet access. The VANET provides two types of communication. The first is purely a wireless ad-hoc network where the communication between vehicles is carried out without any support of infrastructure. The second type of communication is carried out between the vehicles and the Road Side Unit (RSU) which is fixed infrastructure. Each node in VANET consist of two units namely On-Board Unit (OBU) and Application Unit (AU). The major role of all the works towards VANET is to provide road safety information among the nodes. It is achieved by frequent exchange of such type of data on the network. The process of exchange of data is carried out using Advanced Driver Assistance System (ADAS). The process clearly specifies the role of security. The process of providing security in VANET is a crucial one. The security can be achieved by detecting the malicious nodes during data transmission. The malicious nodes actively break router to disrupt data transmission. Thus, these selfish nodes have to be avoided. The selection of poor intermediate nodes may result in invoking time out and reduce packet delivery ratio. The Shortest Reliable Route (SRR) and Best Available Route (BIR) protocols are used to find effective path for data transmission. The SRR protocol provides the available transmission path where the BIR protocol selects the best among those paths. The packet delivery ratio is increased using this method the energy consumption is reduced using three steps namely: data acquisition, data processing and wireless communication.

2. E-STAR PROTOCOL

The E-STAR protocol is used to establish stable and reliable routes is a heterogeneous wireless network. The trust based and energy aware routing protocol are combined in E-STAR. The nodes competence and reliability is determined by the trust system in terms of multi-dimensional trust values. The trust node is encrypted using asymmetric encryption process and is called as public key cryptography. The probability of breaking of nodes is minimized using two routing protocols. The E-STAR stimulates the node and relay packets and also maintains the routes stability without any breaking of the node. The trust values are computed by processing the receipts because imperfection of these values will cause loss of earnings. The E-STAR protocol can secure trust system without any false accusations and also improves router stability.

2.1 DATA TRANSMISSION

The source node NS send messages to the destination node ND through a route with the intermediate nodes A, B, and C. The route is established by the routing protocols, for the i^{th} data packet, S computes the

$$Sig_s(i) = (H(m_i), ts , R , i)K_{(s+)} \quad (1)$$

It sends the packet <*R*, *ts*, *i*, *m*i, *C*S (i)> to the first node in the route. *R*, *ts*, and *m*i are the concatenation of the identities of the nodes in the route (R = IDS, IDA, IDB, IDC, IDD), the route establishment time stamp, and the i^{th} message, respectively. *H*(d) is the hash value resulted from hashing the data d using the has function *H(). The {d}KS+* is the signature of d with the private key of CS.

The purpose of the source node's signature is to ensure the message's authenticity and integrity and secure the payment by enabling Tp to ensure that CS has sent *i* messages. Each intermediate node verifies CS(i) and stores CS(i) and *H*(*m*i) for composing the receipt. It also removes the previous ones (*C*S (i-1) and *H*(*m*i-1)) because *C*S(i) is enough to prove transmitting *i* messages. Signing *H*(*m*i) instead of mi can reduce the receipt size because the smaller-size *H*(*m*i) is attached to the receipt instead of *m*i.

2.2 RECEIPT GENERATION

The destination node generates a one-way hash chain by iteratively hashing a random value hS S times to obtain the has h chain {hS, hS-1,…,h1, h0}, where hi-1= H(hi) for 1 <i<S and h0 is called the root of the hash chain. The node signs *h*0and *R* to authenticate the hash chain and links it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi-1. The underlying idea is that CS(i) and hi are undeniable proofs for sending and receiving *i* messages, respectively.

Each node in the route composes a receipt and submits it to TP on connection to claim the payment and update its trust values. A receipt is a proof for participating in a route and ending, relaying, or receiving a number of messages. A receipt contains R, ts, i, H(mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. *C*m is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay.

The cryptographic token contains the hash value of the last source node's signature and AuthCode. AuthCode is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. More details about *C*m and AuthCode will be given. If i messages are delivered, the format of the receipt is <R, ts, i, H(mi), h0, hi, Cm,H(CS(i), AuthCode)>. CS(i) and AuthCode are hashed to reduced receipt's size.

2.3 UPDATE CREDIT ACCOUNT AND TRUST VALUE

Update Credit Account and Trust Values Phase Once TP receives a receipt, it first checks if the receipt has been processed before using its unique identifier (*R*, *ts*). Then, it verifies the credibility of the receipt by computing the nodes' signatures (CS(i) and AuthCode) and hashing them. The receipt is valid if the resultant hash value is identical to the receipt s cryptographic token. TP verifies the destination hash chain by making sure that hashing hi I times produces h0. TP clears the receipt by rewarding the intermediate nodes and debiting the source and destination nodes. The number of sent messages(*i*) is signed by the source node and the number of delivered messages can be computed from the number of hashing operations to obtain h0 from hi.

The consideration of trust in routing decisions is essential in HMWN that is characterized by uncertainty in the nodes' behavior because they are autonomous and self-interested. A trust relationship is never absolute, but it is context dependent in the sense that a node's trust value depicts its ability to perform as specific action. For example, Alice may trust Bob to repair her computer but she may not trust Bob to repair her car. Trust is also dynamic or time-sensitive, so TP has to periodically evaluate the nodes' trustworthiness, i.e., a trust value at time *t* may be different from its value at another time *t'*. In order to capture the dynamicity of trust, it should be expressed as a continuous value rather than binary or even discrete. Also, a continuous variable can represent uncertainty better than a binary variable.

Payment schemes use credits to encourage the mobile nodes to relay other packets. Since relaying packets utilizes energy and other resources, packet relaying is treated as a service that can be charged. The nodes earn credits for relaying others' packets and pay them to induce their packets delivered. In Sprite, for every message, the supply node signs the identities of the nodes within the route and also the message. Each intermediate node verifies the signature and submits a signed receipt to TP to say the payment. However, the receipts overwhelm the network as a result of one receipt consists for each message. To scale back the receipts' range, PIS generates a hard and fast size receipt per route in spite of the number of messages. In ESIP, the payment Technique uses a communication protocol which will transfer messages from the source node to the destination with restricted use of the general public key cryptography operations.

2.4 ROUTE ESTABLISHMENT

The route establishment phase involves the use of SRR and BAR routing protocols. The routing protocols includes three processes: Route Request Packet (RREQ) delivery, Route Selection and Route Reply Packet (RREP) delivery. The SRR protocol establishes the shortest route that satisfies the source nodes energy and trust requirement, but the destination node selects the destination node selects the best available route in BAR.

SRR protocol: The SRR protocol establishes the shortest route that satisfies the source nodes requirements is trusted enough to act as a relay. This protocol avoids the low-trusted nodes. The Data is transferred Via Highly Trusted Nodes. In network architecture from source (node S) to destination (node D) the data is transferred through the intermediate nodes (i.e.) routes. The route i.e. A, B through which data transmission is carried out are the highly trusted nodes. For each node a receipt is maintained and is submit to the trusted party. The trusted party will calculate the trust values. After calculating the trust value it will produce a payment receipt for highly trusted nodes. To establish a route to the destination node, the source node broadcasts RREQ packet and waits for RREP packet. The source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the packet. The destination node establishes the shortest route that can satisfy the source nodes requirements. The SRR protocol believe that the node that satisfies the source nodes requirements is trusted enough to act as a relay.

RREQ: RREQ packet contains the packet identifier (RREQ), the identities of the source and destination nodes (ID_S and ID_D), the maximum no. of intermediate nodes (H_{max}), the time stamp of route establishment (t_s), trust and energy requirements (Tr = [T(1), T(2), T(3), T(4)] and E_r), and source nodes signature and certificate. Each intermediate node ensures that it can satisfy the source nodes energy and trust requirements. It also verifies the packets signature using public key extracted from the nodes certificates. The intermediate node signs the packets signature forming a chain of signatures of the 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 intermediate node broadcasts the packet after adding the signature chain and its identity and certificate. If a node receives the same request packet from different nodes, it processes only the first packet and discards the subsequent packets.

Route Selection: If there is a route that can satisfy the source nodes requirements, the destination node receives at least one RREQ packet. 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 is the shortest route that can satisfy the source nodes requirements. The source nodes requirements cannot be achieved if it does not receive the RREP packet within a specific time period. It can initiate a second RREQ packet but with more flexible requirements.

RREP: RREP packet contains packet type identifier (RREP), the identities of the nodes in the route (R), root of the hash chain created by destination node by iteratively hashing a random value h_s S times (h0), the destination nodes certificate, and the nodes authentication code. i.e. (Sig, h0) K_{D+}, where

$$Sig = (((D)K_{S+}) K_{A+}) K_{B+} \quad (2)$$

The destination nodes signature authenticates the hash chain and links it to the session. It also authenticates the destination node and proves to TP that ND has indeed participated in the session. Each intermediate node can authenticate the source node and the in-between intermediate nodes from the RREQ packet, and each intermediate

node can authenticate the destination node and the in-between Nodes from the RREP packet. The source node verifies the Auth Code and the nodes certificates to make sure that the nodes satisfy its trust requirements and the intended destination node was reached, then it starts data transmission.

BAR Routing Protocol: RREQ: RREQ packet contains IDS, IDD, H_{max}, t_s, the source nodes certificate and signature (Sig_s) and the number of messages it needs to send ($E_r(S)$).

The first received RREQ packet, an intermediate node A broadcasts the packet after attaching its identity and certificate, the number of messages it commits to relay (Er(A)). Unlike the SRR protocol, $E_r(A)$ can be fewer than $E_r(S)$. The A also signs the concatenation of $E_r(A)$ and the signature received in the RREQ packet. $E_r(A)$ not only depends on the available battery energy in A, but also on other factors such as the cooperation strategy and the link quality and stability. The nodes are motivated to report correct energy commitments to avoid breaking the route and thus degrading their trust values. BAR 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. The route lifetime is the minimum number of packets the intermediate nodes commit to relay.

Route Selection: After receiving the first RREQ packet, the destination node waits for a while to receive more RREQ packets if there are. Then, it selects the best available route if a set of feasible routes are found. If there are multiple routes with lifetimes at least Er(S), the destination node selects the most reliable route, otherwise, it establishes multiple routes with at least total lifetime of Er(S) in such a way that reduces the routes number and maximizes the reliability. The destination node should not select multiple routes with common node(s) (if possible) to disallow one node to break the routes RREP : This packet is identical to that of SRR protocol, but Sig is the signature chain in the RREQ packet and nodes energy commitments (Er(S),Er(A),Er(B)) are attached.

3. RESULT AND ANALYSIS

The corresponding simulation represents initialisation of vehicle as a wireless router or node as shown in fig.1. It allows vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range**.**

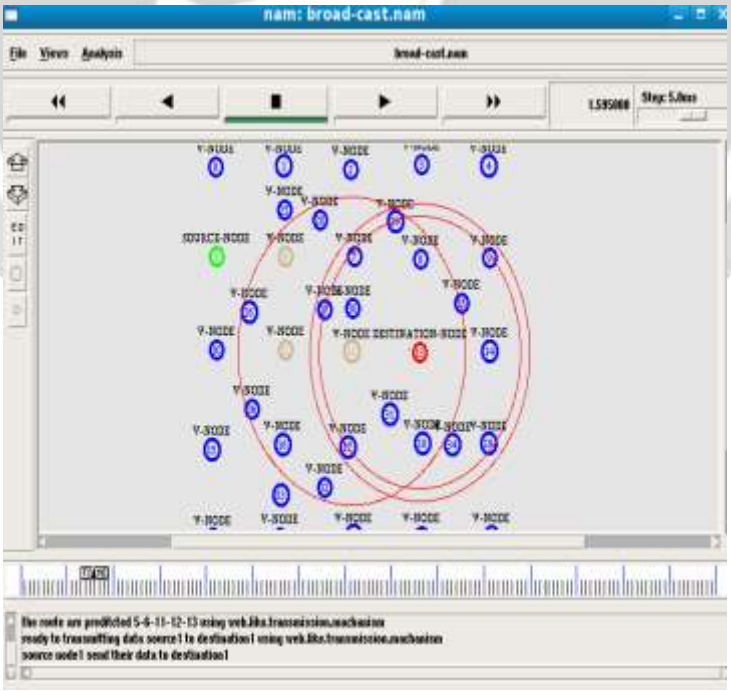

Fig.1 Node creation

The simulation output for node identification is shown in fig.2. It provides a routing mechanism which gives the valid route between two vehicles. The effective path between source and destination is identified by

calculating the trust degree for the intermediate nodes. The node with high trust degree is always taken for routing using Shortest Reliable Route (SRR) and Best Available Route (BAR) protocols.

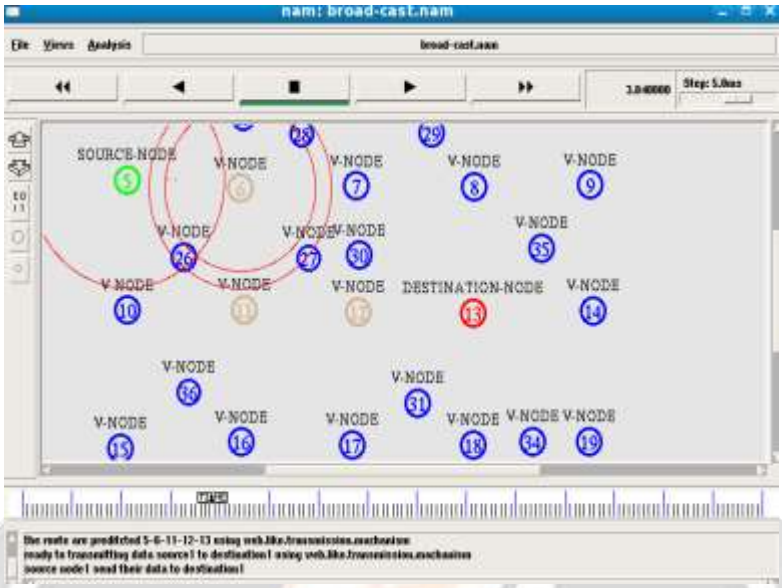

Fig.2 Node identification

The simulation output for data transmission is shown in the fig.3. It is the process of sending data between vehicles in multi-hop pattern. During transmission from source to destination the signatures are calculated along the intermediate nodes. The intermediate nodes form the receipts by combining the signature and hashed value of the message signal and submit it to the trusted party on connection. The destination computes the hash chain and sends its last element as acknowledgement to source.

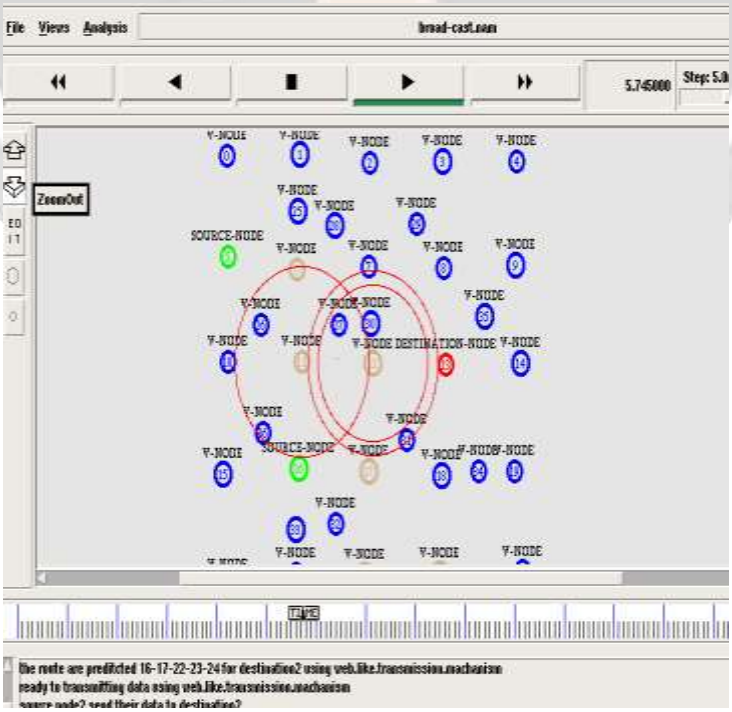

Fig.3 Data transmission

4. SIMULATION

The fig.4 shows the energy consumption for varying no of nodes. The energy consumption has been reduced by 40% with respect to the existing system. This is done using three steps which includes data acquisition, data processing, wireless communication.

The fig.5 illustrates the performance of a network in terms of delay by varying no of nodes. The delay has been reduced by 26% with respect for existing system.

The energy consumption is the total energy used by the entire human civilization. Typically measured per year, it involves all energy harnessed energy consumption from every energy source applied towards humanity's endeavors across every single industrial and technological sector, across every country. It does not include energy from food, and the extent to which direct biomass burning has been accounted for is poorly documented. Being the power source metric of civilization, World Energy Consumption has deep implications for humanity's socio-economic-political sphere.

The fig.6 shows the relationship between packet speed and packet delivery. The packet delivery ratio has been increased by 50% with respect to existing system.

The fig.7 shows the relationship between packet speed and routing overhead. The number of bits needed to do the synchronisation for routing purpose has be reduced using E-STAR. The routing overhead has been reduced by 30% with respect to the existing system. The routing over head should me maintained as low as possible.

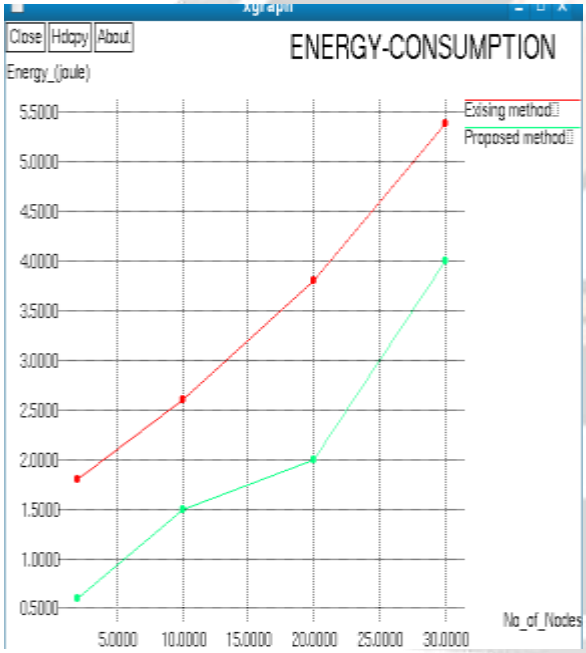

Fig.4 No of nodes Vs Energy consumption

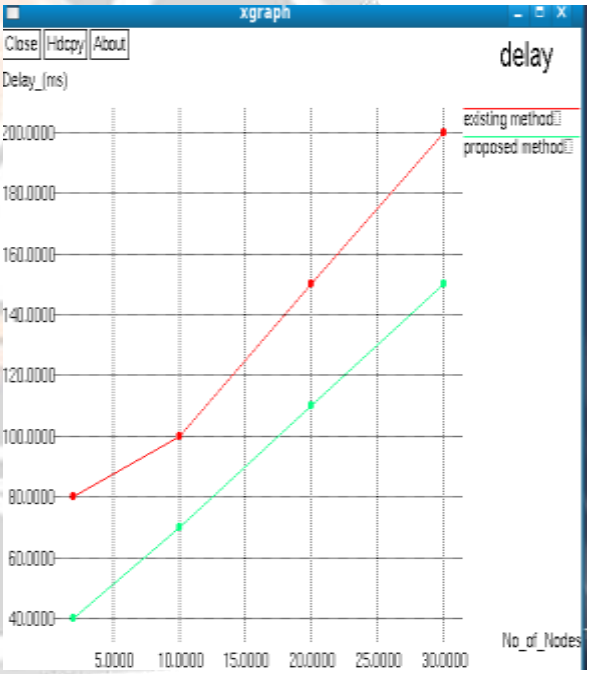

Fig.5 No of nodes Vs Delay

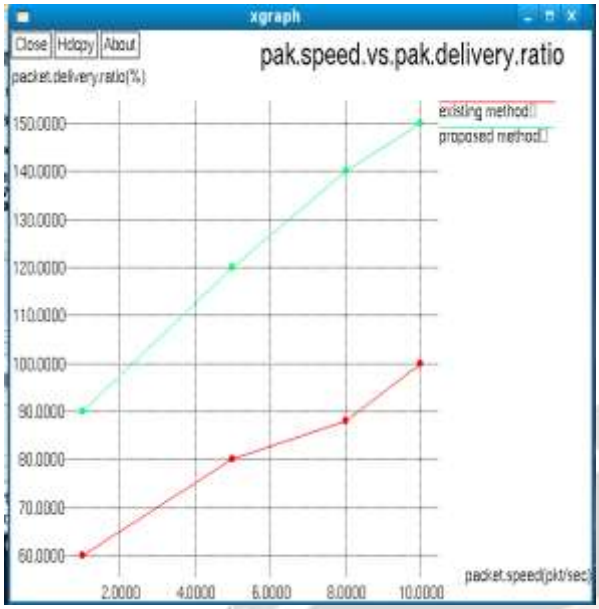

Fig.6 Packet speed Vs Packet delivery ratio

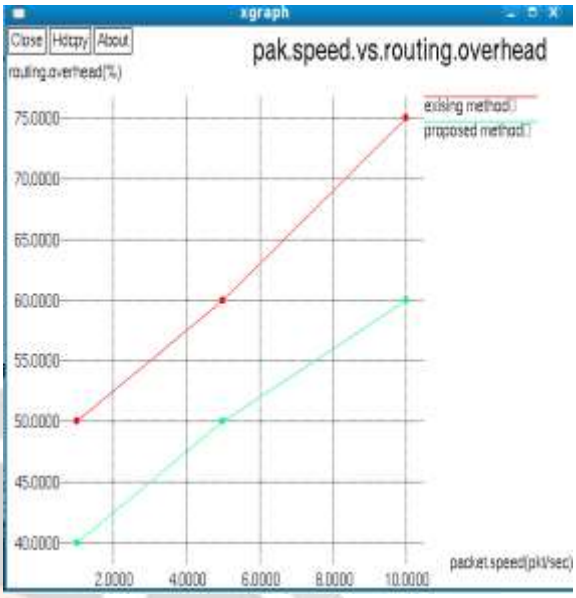

Fig.7 Packet speed Vs Routing overhead

5. CONCLUSION

The proposed E-STAR that uses payment/trust systems with trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. E-STAR stimulates the nodes not only to relay others' 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 routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behaviour, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. The analytical results have demonstrated that E-STAR can secure the payment and trust calculation without false accusations. Moreover, the simulation results have demonstrated that E-STAR can improve packet delivery ratio due to establishing stable routes.

6. REFERENCES

[1]. Abduljalil, F. M. (2012) 'A framework for vehicular accident management using wireless networks,' in Information Reuse and Integration (IRI), IEEE 13th International Conference on, pp. 727–729.

[2]. Chang, I. C. Tai, H. T. Yeh, F. H. Hsieh, D. L. and Chang, S. H. (2013) 'A VANET-Based Route Planning Algorithm for Travelling Time- and Energy Efficient GPS Navigation App,' Int. J. Distrib. Sens. Netw., vol., pp. 1–14.

[3]. Goel, A. Ray, S. and Chandra, N. (2012) 'Intelligent Traffic Light System to Prioritized Emergency Purpose Vehicles based on Wireless Sensor Network,' Int. J. Comput. Appl., vol. 40, no. 12, pp. 36–39.

[4]. Li, Y. J. (2012) 'An overview of the DSRC/WAVE technology,' in Quality, Reliability, Security and Robustness in Heterogeneous Networks, Springer, pp. 544–558.

[5]. Mitropoulos, G. K. Karanasiou, I. S. Hinsberger, A. Aguado-Agelet, F. Wieker, H. Hilt, H. J. Mammar, S. and Noecker, G. (2010) 'Wireless Local Danger Warning: Cooperative Foresighted Driving Using Intervehicle Communication,' IEEE Trans. Intell. Transp. Syst., vol. 11, no. 3, pp. 539– 553.