Reliable Fuzzy Reputation System to enhance the performance of disseminating the information in VANET

P.Uma Maheswari[#1], M.Rajeswari[#2]

Department of CSE,
Info Institute of Engineering, Coimbatore, India
[1]drumasundar@gmail.com

[*] M.Rajeswari

Department of CSE,
Angel College of Engineering and Technology, Tiruppur, India
[2]rajimanickam@gmail.com

Abstract— VANET (Vehicular Adhoc NETwork) is a special type of MANET in which moving vehicles are considered to be nodes. Vehicular nodes are allowed to forward the road related information like traffic condition, congestion in road, accident, weather condition etc to other vehicles. This information is very useful and valuable to nearby vehicles which will increase the road safety and hence it reduces the congestion. Message transmission will not be effective unless it is reliable. This paper demonstrates Reliable Fuzzy Reputation System (RFRS) which is reliable in terms of forwarding the information in vehicular network. Reliability is achieved by introducing RFRS and Universal Generating Function Techniques (UGFT) method in VANET. RFRS is used to find the selfish nodes from non-selfish nodes and gather the information from selfish nodes and finally forward to other ongoing vehicles effectively. Successful transmission of packets from source node to target node is calculated by using node UGF, UGF of FM (Forward Manager) and UGF of FRM (Fuzzy Reputation Manager). Also we projected an EMAP system - trusted authority, which is responsible for sharing secret keys to all OBUs in network that improves the security. Simulation is carried out in Network Simulator (NS-2) to evaluate the performance with respect to Packet Delivery Ratio, Delay, Packet Loss Ratio, Energy Rate and Throughput.

Keyword- RFRS, VANET, UGFT, Reliability

I. INTRODUCTION

VANET is an ephemeral, rapidly changing wireless network formed among vehicles and Road Side Units which are able to communicate with each other. VANET provides a way to collect traffic [2] and road related information from vehicles, and to deliver information including warnings and traffic information to drivers in the vehicles. This type of information is called as road related messages. Due to the broadcasting of reliable and efficient [4] road-related messages, vehicles may aware of this situation. It may improve the safer driving and reduce the traffic congestion. However, these benefits can only be understood clearly if the road-related messages generated by vehicles are reliable. Suppose if the messages may be unreliable, then delay in journey will occur or causes an accident. So the system mainly focuses on ensuring the reliable delivery of messages among the vehicles. There are various ways used to evaluate the reliability of a message such as protocol techniques, based on architecture, reputation system and so on.

Reputation System [14] is one of the most important techniques used to evaluate the reliability of message. A main challenge is to forward the road related messages in such a way that the information can be trusted by the receiving vehicular nodes. Authentication does not solve the problem because it does not concentrate on the quality of messages. One promising solution is given by the reputation system which gathers, forwards, and combines feedback about participants' past behavior. The reliability of a message is evaluated with the help of three different techniques based on reputation system. They are threshold method, networking model and trust based [11 & 13] and reputation based models. They are discussed in the next section. This paper concentrates on collecting the information from both non-selfish nodes and selfish nodes by using Forward Manger (FM) and Fuzzy Reputation Manager (FRM). Reliability is defined by applying Universal Generating Function Techniques (UGFT) from set of nodes to FM and FRM which in turn forwards the information to the desired vehicular nodes. The following sub section focuses on the challenges in VANET environment with respect to trust model.

A. Challenges in VANET environment

- Trust model should be fully decentralized that may be applied to the highly dynamic and distributed environment. To achieve a complete decentralization due to slow approach from different directions, delay in vehicular node status updates, network connections, etc.
- Some VANETs' environments can be explained as dense populations of vehicles restrict with certain limits to relatively tight geographic areas, e.g. peak hours in metropolitan areas. Other environments, like interstate or international highways are characterized by extensive trails with minimal density of vehicles.
- Since the environment of the vehicular nodes in VANET is changing frequently and quickly, a trust model introduce particular but not specified the dynamic measurements.
- In addition, the occurrence of incidents or events on the road could be triggered by many vehicular nodes, as well as single or minor set of vehicles.
- Confidence is to measure the trustworthiness of the vehicles. Some additional measurements require to be applicable, in order to introduce "Quality Assurance"(QA) into VANETs' models.
- Security is a major issue on VANET environment by either centralized or distributed schemes. Security mechanisms allow vehicular nodes to authenticate itself i.e. prove their identity.
- Privacy is an important issue in a VANET environment. In this environment, the appearance of a vehicle owner's identity (e.g. owner's residential address) may allow a possibly malicious party to cause damage to the owner. Some common attacks are Newcomer attack, Sybil attack, Betrayal attack, Inconsistency attack, Collusion attack, Bad-mouthing/Ballot Stuffing attack, Impersonation attack and so on.
- Trust management can effectively improve number of vehicular nodes in VANETs to exchange information about the road conditions and detect malicious nodes.

II. RELATED WORKS

Trust based [5] and reputation based models have several reputation systems. They are Data Intensive Reputation Management Scheme, VARS, On data centric trust establishment, Towards expanded trust management for agent, Fuzzy Reputation System and so on.

Patwardhan *et al.* [1] discussed the Data Intensive Reputation Management Scheme that implements the reputation management which is determined based on the validation of data. The validation of data is achieved by either trusted source (trivial case) agreement or post validation by trusted source.Dötzer *et al.* [3] proposed the Vehicular Adhoc Reputation System (VARS) that makes use of *direct* and *indirect trust* as well as *opinion piggybacking* to enable confidence decisions based on the road related messages. Decision on the trustworthiness of a road related message is added during message forwarding. Raya *et al.* [6] examined On data centric trust establishment that trust in each individual piece of data calculated, then multiple, related but possibly denied each other, data are combined and finally their validity is concluded by Dempster-Shafer Theory.

Minhas *et al.* [12] discussed and expanded trust management for agents that the system mainly focuses on the trustworthiness of the vehicles. Trustworthiness of the vehicles is calculated by various trust models which includes role based, experience based and majority based trust model. Role-based trust takes advantage of certain predefined roles that are made possible through the identification of vehicles. For example, vehicles may have more trust toward traffic patrol or law enforcement authorities compared with other vehicles. To avoid impersonation attacks, each vehicle is needed to have a certificate that includes its name, role, and public key, issued by a trusted authority for authentication purposes. Majority-based trust [13] is similar to the threshold method. Experience-based trust works based on direct actions on each other: A vehicle decides to whom to trust based on how truthful they have been in their past interactions. However, such a model requires vehicles to establish a long term relationship with each other, which may not be practical in a large VANET environment. Mohammad Jalali *et al.* [7] proposed the Fuzzy Reputation System that source node (vehicular node) sends a road related messages, the counter added the messages to the packet header. Based on these counter values, relay node (vehicular node) can decide whether the road related messages will be forwarded or discarded. In this threshold mechanism, a vehicle accepts a message if it receives messages within the same content that have been broadcasted by a number of different vehicles that exceed a threshold within a time interval. The threshold may be a fixed system-wide parameter or a flexible parameter. Golle *et al.* [8] proposed the evaluation of message reliability by modeling the network. They presented a scheme that allows vehicles to detect and correct malicious messages in VANETs. Vehicles are assumed to maintain a "model" of VANET, which contains all the knowledge that the vehicles possess about the VANET. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

III. RELIABLE FUZZY REPUTATION SYSTEM

The Fuzzy Reputation System considers the following assumptions:

- Vehicular nodes can move at a high average speed.
- No malicious node exists in the network.
- It should be completely decentralized.
- There is no collision between the selfish nodes in the network.

Some vehicular nodes may decide not to work together to exchange their information while still using the network resources. These nodes are called as selfish nodes. Such selfish nodes degrade the overall network performance. The Fuzzy Reputation System checks each source node to determine whether it is selfish or not. If the source node is a selfish node, then that node will be eliminated from the network. Reliable Fuzzy Reputation System is used to increase the overall performance of the Vehicular Adhoc Networks in the presence of selfish nodes. Unlike many techniques that avoid selfish nodes during routing and forwarding road related messages, the Reliable Fuzzy Reputation System of non-selfish nodes allows selfish nodes to work together in routing and forwarding messages and so they can enhance their reputation and join the network again. Fig. 1 represents the Reliable Fuzzy Reputation System which consists of Forward Manager (FM) and Fuzzy Reputation Manager (FRM). Two counters are used in this FRS to find out number of selfish nodes and forwarders or non selfish nodes. Forward Counter (FC) which keeps track of number of forward requests and Discard Counter (DC) are used to hold the number of discarded messages. These counters are maintained by Forward Manager (FM) and Fuzzy Reputation Manger (FRM). FM collects the information from FC and disseminates the road related messages to other ongoing vehicles. FRM gathers the information from DC which denotes the number of vehicles that do not forward the information to other ongoing vehicles and they just utilize the network resources. These nodes are identified as selfish nodes and they are handled by FRM. This FRM extracts the valuable road safety information from selfish nodes and forward it to other vehicles. EMAP, a trusted authority which distributes the secrete key to on board units so that it is possible to verify whether the message is valid or not. Secrete keys are used only by On Board Unit (Trusted Authority).

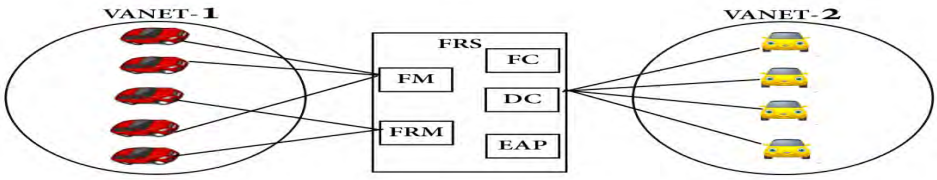

Fig.1. Information dissemination from VANET 1 to VANET 2 via RFRS

So it will not be utilized by unauthorized persons and hence it is used to avoid mal practice. EMAP is used to reduce delay by introducing probabilistic key distribution and H-MAC (Hash Message Authentication Code) code compared to other checking revocation process. EMAP helps to provide security in terms of forwarding information to other vehicles. We survey the number of trust based and reputation based models in VANET and propose the Reliable Fuzzy Reputation System to evaluate the reliability of message. The following table illustrates the performance comparison of different Reputation Systems with respect to different approaches.

Table I
Performance comparison of FRS

Approaches	**1**	**2**	**3**	**4**	**5**	**6**
Decentralized	√	√	√	√	√	√
Sparsity	√	-	√	-	√	√
Dynamic	-	√	√	√	√	√
Scalability	-	-	-	-	√	√
Confidence	-	-	-	√	√	√
Security	√	-	√	√	√	√
Privacy	√	√	-	-	√	√
Robustness	√	-	-	-	-	**Partial**

1. Detecting and correcting malicious data in VANETs
2. VARS: A vehicle ad hoc network reputation system
3. A data intensive reputation management scheme for vehicular Adhoc networks
4. On data-centric trust establishment in ephemeral ad hoc networks
5. Towards expanded trust management for agents in vehicular Adhoc networks
6. A Reliable Fuzzy Reputation System in Vehicular Ad hoc Networks

IV. RELIABILITY CALCULATION USING UGFT

Reliability Engineering [11] is the discipline of ensuring that a system will be reliable when operated in a specified manner. Network reliability is an important part of planning, designing and controlling network. Designing, developing and testing real applications for Adhoc network environments still deserves particular attention by VANET community. In VANETs, the information is passed by a flow of transition from node to node to reach the required destination. For a successful packet delivery, reliable routes are necessary. The routes are reliable only in all the connections from source to destination exist. In order to analyse the link reliability, a link UGF is proposed by combining the node UGF of both selfish and non-selfish nodes, UGF of FM, UGF of FRM and link UGF. The UGFT is a common technique because one can use the same procedures for network with different size and different types of node interaction. UGF allows one to assess an output performance for a wide range of networks characterized by different protocol. This can be done by introducing different composition operators over UGF which will predict the happenings of the physical environment. UGF plays an important role in finding out the expected capacity for each transmitting path involved in the VANET and also in the evaluation of link reliability. Then the UGFT approach is based on the definition of a u-function of multistate elements, which are of discrete random variables and composition operators over u-functions.

The first UGFT was proposed for the one-to-many targets acyclic Multi Information Network (MIN) reliability problem by Levitin [15&16], and was improved by Yeh using some simplified techniques [9&10]. The UGFT was proven to be very effective for evaluating the reliability of different types of acyclic multistate networks [17&18], especially for the MIN. In recent years, Yeh extended the UGFT further for general multistate network reliability, which is more practical and reasonable than acyclic multistate networks [9]. So far UGFT is used for reliability calculation of MIN, Multi State System (MSS), Binary State Network (BSN) and Acyclic Binary State Network (ABSN)[19][20][21]. The objective of this paper is to provide an efficient, effective and intuitive technique to manipulate VANET reliability. The reliability of VANET is defined as the successful transmission of information either by selfish or non-selfish nodes via FM or FRM.

A. *Proposed UGF*

UGF allows one to evaluate an output performance distribution for a wide range of systems characterized by different topology, different natures of interaction among system elements, and the different physical nature of elements with its performance measures. This can be done by introducing composition operator over UGF which will predict the happenings of the physical problem.UGF plays an important role in finding out the expected capacity for each traffic-path involved in the VANET and also in the evaluation of system reliability. Then the UGFT approach is based on the definition of a u-function of multistate elements, which are of discrete random variables and composition operators over u-functions.

Definition 4.1

The UGF of non-selfish nodes (Good) is defined as a polynomial in X such that

$$u(i_G) = P_{i_G:FM} X^{FM}, \text{ i=1,2… n-r} \quad (1)$$

where $P_{i_G:FM}$ is the probability of passing the information from node i to FM if there are n-r good nodes in the VANET.

Definition 4.2

The UGF of selfish nodes are defined as

$$u(i_S) = P_{i_s:FRM} X^{FRM}, \text{ i=1,2…r} \quad (2)$$

where $P_{i_s:FRM}$ represents the probability of collecting the information from the selfish nodes by using FRM. Here r denotes the total number of selfish nodes in the VANET.

Definition 4.3

The UGF of Forward Manager (FM) is defined as

$$u\left(FM\right)=\prod_{i=1}^{N_{n-r}} P_{FM:N_i} X^{N_i} \tag{3}$$

where $P_{FM:N_i}$ is the probability that the packets are received by nodes N_i from FM.

Definition 4.4

The UGF of Forward Reputation Manager (FRM) is defined as

$$u\left(FRM\right)=\prod_{i=1}^{N_r} P_{FRM:N_i} X^{N_i} \tag{4}$$

where $P_{FRM:N_i}$ is the probability that the packets are received by nodes N_i from FRM.

Definition 4.5

The reliability of the VANET is defined as the successful transmission of the information by either selfish or non-selfish nodes through FM or FRM to the destination nodes.

$$R_{VAN}=\sum_{i=1}^{N_G} u(i_G)*u(FM)+\sum_{i=1}^{N_S} u(i_S)*u(FRM) \tag{5}$$

B. *Illustration*

Table 2 summarizes all the possible working states and the corresponding transmission probabilities of the VANET. The Reliability calculation proposed in the previous section can be applied to the above network (Fig.1) with the data given in the Table 2 is as follows. A State Dependent Probability (SDP) has been assigned to each working state.

Table 2
State Dependent Probabilities of Fig.1.

Working States					
VAN 1	**SDP**	**VAN 2**	**SDP**	**VAN 2**	**SDP**
1-FM	0.75	FM-6	0.8	FRM-6	0.6
2-FM	0.7	FM-7	0.7	FRM-7	0.3
3-FRM	0.8	FM-8	0.6	FRM-8	0.5
4-FM	0.9	FM-9	0.9	FRM-9	0.4
5-FRM	0.6				

The above table describes the link connectivity between vehicular nodes and FM or FRM. State Dependent Probability (SDP) is assigned to each connectivity. Next subsection describes the reliability calculation of VANET.

C. *Reliability calculation of VANET*

The link reliability of a VANET can be calculated as follows:

$$R_{L_1}=U(1)=u(1)*u(\text{FM})=0.75*[0.8*0.7*0.6*0.9]=0.2268$$

$$R_{L_1}=U(1)=u(1)*u(\text{FM})=0.7*[0.8*0.7*0.6*0.9]=0.21168$$

$$R_{L_1}=U(1)=u(1)*u(\text{FM})=0.8*[0.6*0.3*0.5*0.4]=0.0288$$

$$R_{L_1}=U(1)=u(1)*u(\text{FM})=0.9*[0.8*0.7*0.6*0.9]=0.27216$$

$$R_{L_1}=U(1)=u(1)*u(\text{FM})=0.6*[0.6*0.3*0.5*0.4]=0.0216$$

$$R_{VAN} = \sum_{i=1}^{3} u(i_G) * u(FM) + \sum_{i=1}^{2} u(i_S) * u(FRM)$$

$$=0.2268+0.21168+0.0288+0.27216+0.0216$$

$$=0.761 = 0.8$$

The proposed UGFT in this work is the first scheme that calculates the VANET reliability that consists of FRS (Forward Reputation System). In this pilot study, the proposed UGFs are totally different from other existing known UGFT based algorithm. SDPs are built for each link in the VANET. The UGF is used to mathematically represent the reliability of each link and combine their SDPs through a formally introduced multiplication operator to find the final VANET reliability.

V. RESULTS AND DISCUSSIONS

Fig.2 shows the effect of good put of the network based on the percentage of selfish nodes. Here there are five different packets received with the mean receive ratio and percentage of selfish nodes. This diagram shows the percentage of selfish packets received among the available number of packets received. This clearly states that some of the nodes are not forwarding traffic information to other nodes which in turn just utilizes the network resources. So FRM takes the responsibility to collect the valuable information from selfish nodes and forward to other ongoing vehicles.

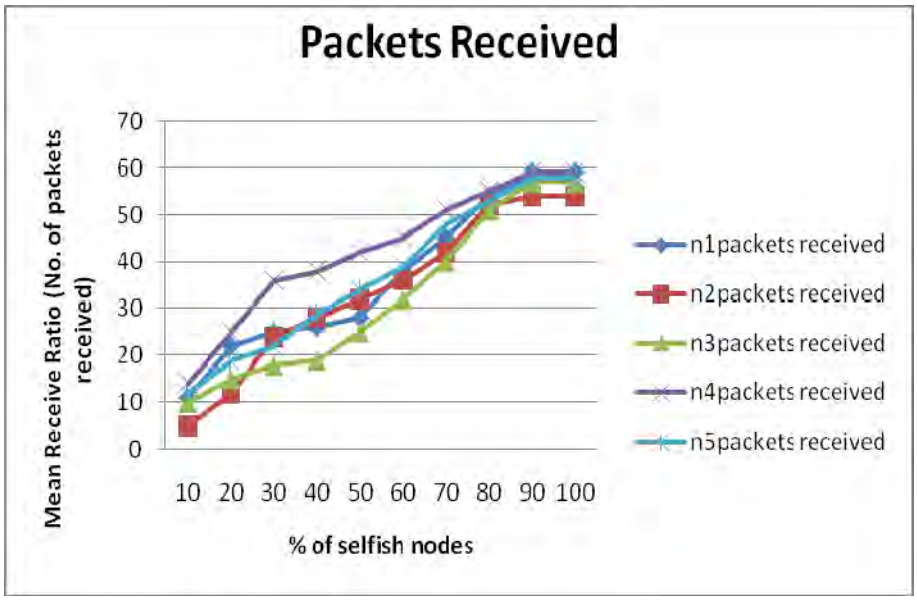

Fig. 2. Goodput expressed as the ratio of received to send packets

Delay is one of the most important performance measurements for any wireless network system. In general, it represents the average time difference of a packet transmitting from a source node to the destination. In order to reduce the delay, the optimal situation is, all nodes along the route can forward the packet immediately until it reaches the destination. In our scheme, each packet needs to be checked to find whether the node is a selfish node or non-selfish nodes by using FC and DC. This reduces the delay in packet transmission. From Fig.3, it is shown that the imposed delay by our solution is negligible in comparison with defenceless scheme. X-axis represents the percentage of selfish nodes and Y-axis represents the total number of packets that are delayed.

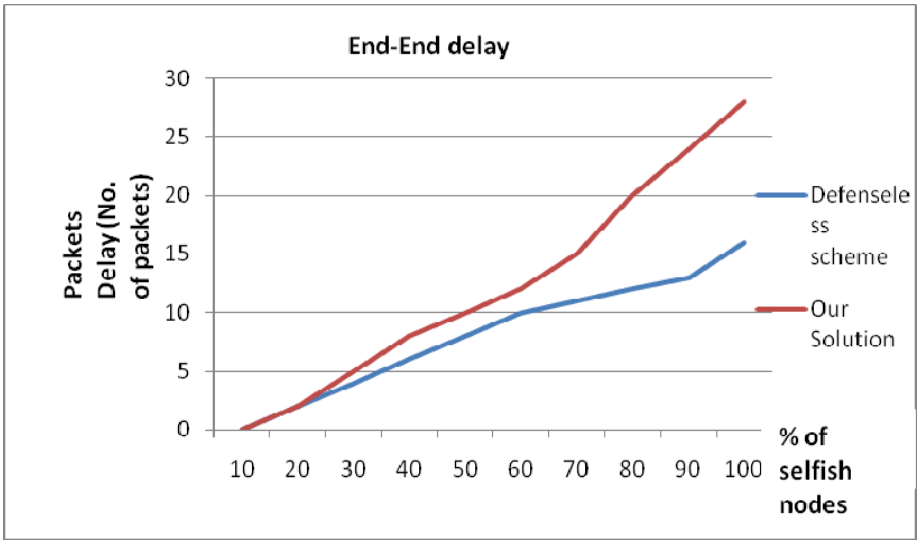

Fig. 3. End to end delay comparison between our solution and defenceless scheme

Fig. 4 shows the throughput against the number of nodes, i.e., the actual scale of the network which means that the system should retain in the same state if the size of network also increases. In this figure, it is assured that RFRS system outperforms the standard in terms of system throughput for different network scales. Performance of the entire network does not get degraded when the packet size gets increased.

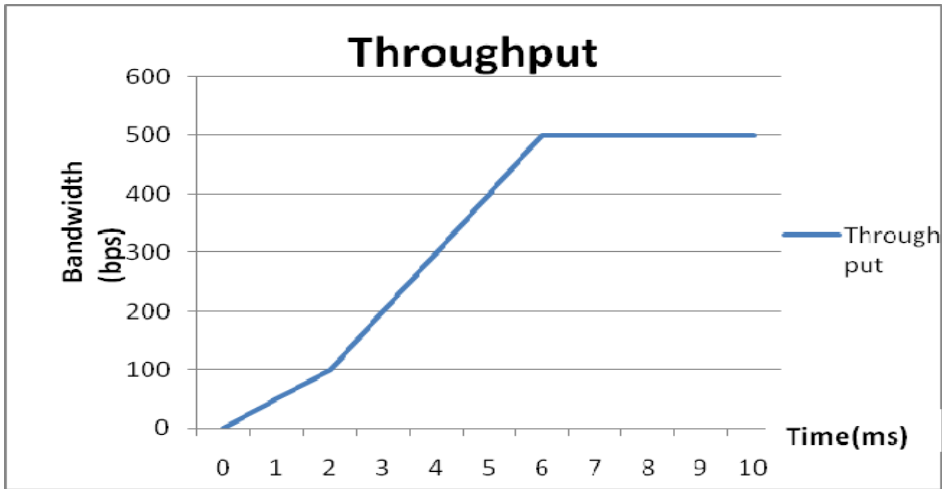

Fig. 4. Throughput

Fig.5 shows the packet delivery ratio compared to the selfish delivery ratio as a function of the vehicular nodes. It defines the ratio of the number of delivered data packet to the destination. Packet Delivery Ratio is represented as

$$\text{Packet Delivery Ratio} = \sum \text{Number of packet receive} / \sum \text{Number of packet send}$$

X-axis represents the time taken to receive the packets in milliseconds whereas Y-axis denotes the total number of packets that are sent or delivered. This clearly defines that the network consists of both non-selfish nodes and selfish nodes and packet delivery is better comparatively by both the nodes. FM delivers the packet much higher rate than selfish nodes.

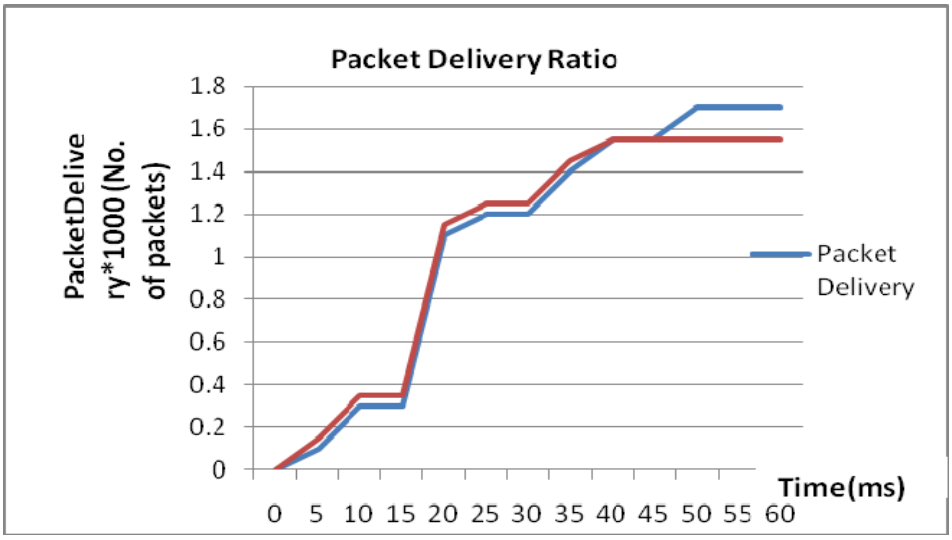

Fig. 5. Packet Delivery ratio

Fig.6 shows the packet loss based on the number of packets received within the time in the various vehicular nodes. Packet Loss is the total number of packets dropped during the simulation. X-axis represents the time in milliseconds and Y-axis represents the number of dropped packets in numbers. Packet Loss Ratio is this scheme is getting decreased when time increases.

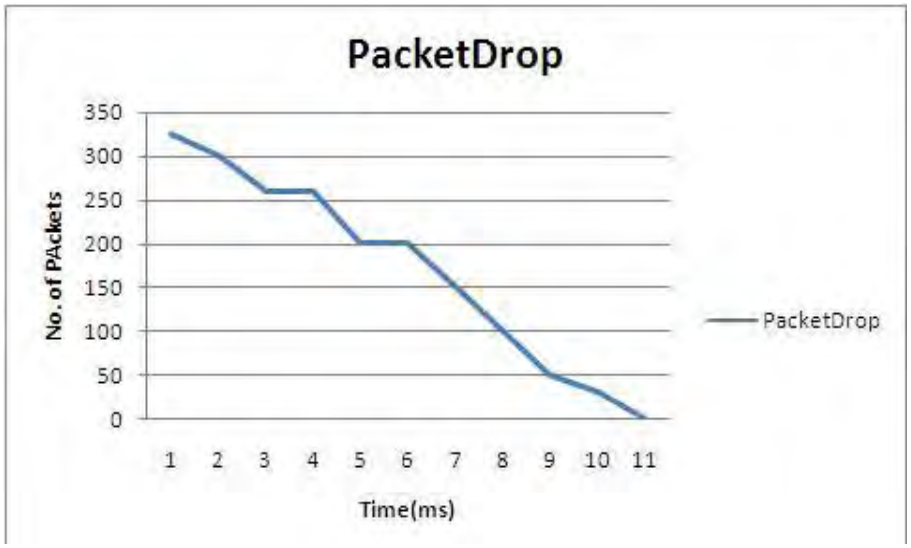

Fig. 6. Packet Drop ratio

Fig.7 shows the energy rate between the residual energy and the time. In this figure the energy rate derived from the fuzzy reputation system. Energy rate is the level of energy performance based on the network criteria like traffic condition, congestion, weather conditions and so on.

Comparison of Existing Reputation System

In this section, the packet delivery ratio of VARS, TETMA, Defenseless network and RFRS have been compared based on the performance. The Fig.8 shows the Packet Delivery Ratio (PDR) and performance of various reputation system based on different vehicle densities. Simulation results demonstrate that a directly proportionate relationship between vehicle density and PDR. The PDR is high for FRS when compared to VARS, TETMA and Defenseless network.

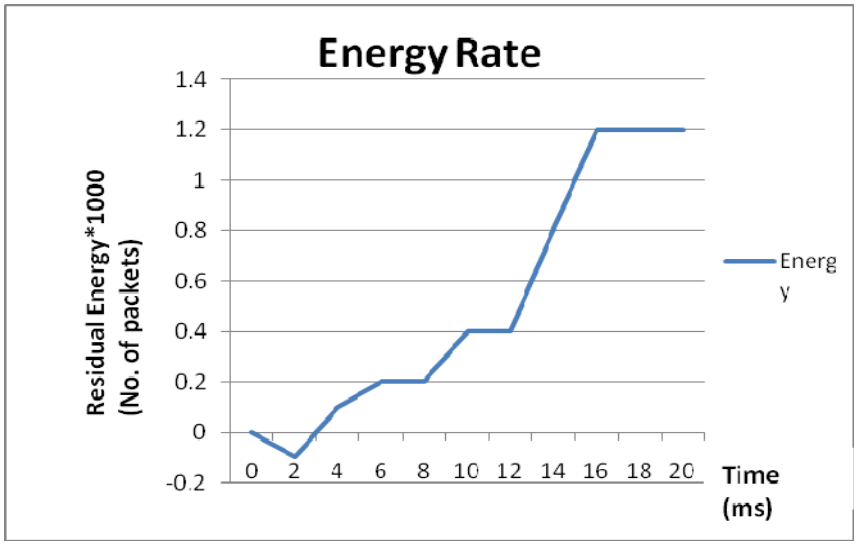

Fig. 7. Energy rate

In FRS, the data packets are transmitted, which gives maximum possibility to meet neighbor vehicle to forward the packet.FRS assures packet delivery even from selfish nodes also. In this situation, RFRS provides better packet delivery ratio when compared to other reputation systems.

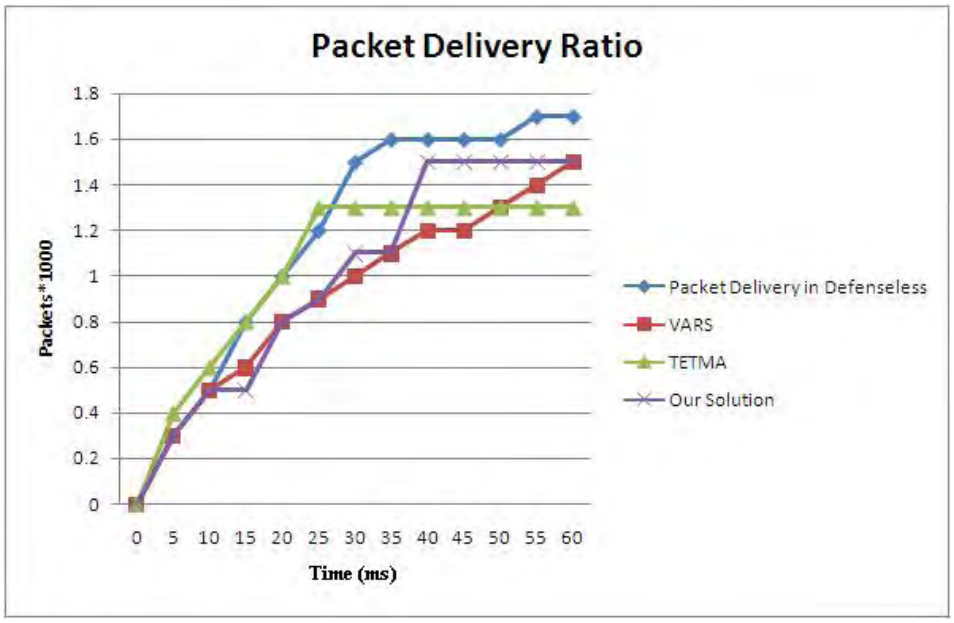

Fig. 8. Packet Delivery Ratio –Comparison

The Packet Loss Ratio of various reputation systems like VARS, TETMA, Defenseless scheme, FRS, etc have also been compared based on their performance. Fig.9 shows the Packet Loss based on the various reputation systems. The Packet Loss Ratio is low for RFRS when compared to VARS, TETMA and Defenseless scheme.

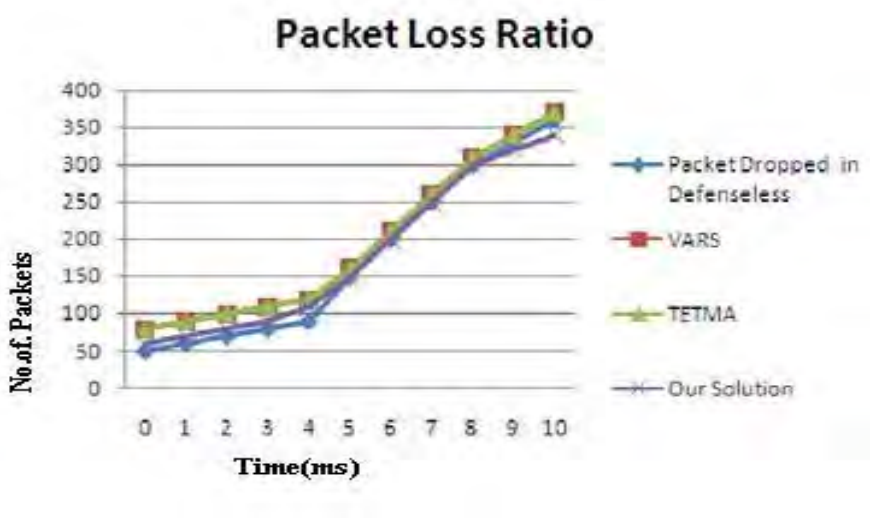

Fig. 9. Packet Loss Ratio –Comparison

Performance Comparison table states that Reliable Fuzzy Reputation System works well in the presence of selfish nodes also.

VI. CONCLUSION

Reputation System is one of the most important techniques used to control the packet transmission from a vehicular node to other vehicular node. There are many Reputation Systems have been proposed for disseminating the information from a vehicle to other vehicle in VANET. The main challenge here is to provide reliable and efficient data delivery in a highly dynamic environment. Reliable Fuzzy Reputation System is proposed to forward the data packets from both non-selfish and selfish nodes by using FM (Forward Manager) and FRM (Forward Reputation Manger). Existing Reputation Systems do not consider selfish nodes for the reliable data delivery. But selfish nodes will also have valuable information which will be forwarded to other ongoing vehicles efficiently by using FRM. Reliability is defined as the successful transmission of packets from both non-selfish and selfish nodes through FM and FRM. Behavior of each node is calculated by using FC (Forward Counter) and DC (Discard Counter). This method increases the network performance in the presence of selfish nodes also. Performance comparison table and simulation results show that the information is delivered efficiently and reliably with respect to different parameters.

REFERENCES

[1] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst., 2006, pp. 1–8.
[2] C2CC, The Car-to-Car Communication Consortium, 2011. [Online].Available: http://www.car-to-car.org
[3] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad hoc network reputation system," in Proc. 6th IEEE Int. Symp. World Wireless Mobile Multimedia Netw., 2005, vol. 1, pp. 454–456.
[4] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Reliable and efficient broadcasting in vehicular ad hoc networks," IEEE the 69th Vehicular Technology Conference (VTC'09), Barcelona, Spain, April 26-29, 2009.
[5] L. Mui, M. Mohtashemi, and A. Halberstadt ,"A Computational Model of Trust and Reputation" In Proceedings of the 35th Hawaii International Conference on System Science (HICSS), 2002.
[6] M. Raya, P. Papadimitratos, V. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in Proc. IEEE INFOCOM, 2008, pp. 1238–1246.
[7] Mohammad Jalali and Nasser Ghasem Aghaee "A Fuzzy Reputation System in Vehicular Ad hoc Networks ", Science direct., 2011.
[8] P. Golle, D. H. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw., 2004, pp. 29–37.
[9] Wei-Chang Yeh, IEEE, and Yuan-Ming Yeh, "A Novel Label Universal Generating Function Method for Evaluating the One-to-all-Subsets General Multistate Information Network Reliability," IEEE Transactions on Reliability, vol. 60, no. 2, pp. 470-477, 2011.
[10] W. C. Yeh, "The K Out Of N Acyclic Multistate Node Networks Reliability Evaluation Using The Universal Generating Function Method," Reliability Engineering & System Safety, vol. 91, no. 7,pp. 800808, 2006.
[11] P. Wex, J. Breuer, A. Held, T. Leinmüller, and L. Delgrossi, "Trust issues for vehicular ad hoc networks," in Proc. IEEE VTC Spring, 2008, pp. 2800–2804.
[12] U. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad hoc networks," Int. J. Comput. Intell. Theory Pract., vol. 5, no. 1, pp. 3–15, Jun. 2010.
[13] Q.Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEETrans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.
[14] Qin Li, Amizah Malip, Keith M. Martin, Siaw-Lynn Ng, and Jie Zhang," A Reputation-Based Announcement Scheme for VANETs", IEEE Transactions on Vehicular Technology, vol. 61, no. 9, November 2012.
[15] Levitin.G, "Universal Generating Function in Reliability Analysis and Optimization", Springer-Verlag, 2005.
[16] Lisnianski.A and G. Levitin, "Multi-State System Reliability, Assessment,Optimization and Applications," New York: World Scientific,2003.

[17] Malinowski.J and W. Preuss, "Reliability evaluation for treestructured systems with multistate components," Microelectronics Reliability, vol. 36, pp. 917, 1996.
[18] Ushakov.I, "Universal generating function," Sov. Journal of Computing System Science, vol. 24, no. 5, pp. 118129, 1986.
[19] W. C. Yeh, "A Simple Universal Generating Function Method For Estimating General Multistate-Node Networks Reliability," IIE Trans.,vol. 41, no. 1, pp. 311, 2009.
[20] W. C. Yeh and X. He, "A New Universal Generating Function Method for Estimating the Novel Multi-Resource Multistate Information Network Reliability," IEEE Transactions on Reliability, 2007.
[21] Meena K.S. and T.Vasanthi, "Reliability evaluation of a flow network through m number of minimal paths with time and cost," European journal of scientific research, Vol. 5,2012.

AUTHOR PROFILE

Dr.P.UmaMaheswari M.E., M.B.A. Ph.D She is presently being a Professor and Head of the department of Computer Science &Engg., at INFO Institute of Engineering, Coimbatore. She completed her B.E. Degree (Computer Science & Engineering) at Thiagarajar College of Engineering, Madurai in the year 1997, M.E. Degree (Software Engineering) at Government Periyar Maniammai College of Technology for Women, in 2004, M.B.A from Madurai Kamaraj University, Madurai and PhD (Data Mining) at Anna University, Chennai in 2009. Being one among the senior Professors and, having completed 16 years of Teaching in Engineering Colleges in Computer Science & Engineering discipline, her research interests are in the field of Data Mining, Intelligent Computing and Image processing. 15 candidates are pursuing PhD under her guidance at present. From her record, she has published her Research findings in 11 International Journals/National Journals, 21 International Conferences and 10 National Conferences. She has also authored 8 Text Books, in which the Engineering students find informative and useful. She has rendered unblemished services in various categories as Coordinator of various programs relating to Services to Community, conducted many workshops and conferences. She is a life time member of ISTE, IEEE, CSI, IAENG and ICTACT.

Ms. M. Rajeswari She received M.E degree in Computer Science and Engineering from Anna University, Chennai and pursuing her PhD in Ad Hoc Network in Anna University, Chennai. She is currently working as an Assistant Professor in the Department of Computer Science and Engineering in Angel College of Engineering and Technology, Tirupur. She has published more than 15 papers in both International conferences and National conferences and published 4 papers in International Journal. She has given a Guest Lecturer in various subjects and acted as a jury in a National level project fair, Symposium and Conferences. She has been awarded a best faculty in the year 2010-2011.She has attended various Seminars, guest lecture, Workshops and Faculty Development Programs to enhance the knowledge of student's community. She is also an active life time member in Indian Society of Technical Education.