ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 4, Issue 8 , August 2017

Cluster Based Data Centric Trust Management in VANET

[1] S.V.Saboji, [2] Bhagyashree K.L

[1] Department of CSE, Basaveshwar Engineering Collage, Bagalkot

***Abstract*— Vehicular ad hoc networks (VANETs) require the potential to transform the way people travel through the construction, interoperable wireless communications network that comprises cars, buses, traffic indicators mobiles, and other devices. However, VANETs are susceptible to safety threats due to increasing requirement on communication computing and control technologies In this paper an challenges has been made for create new cluster model for efficient communication among the VANET nodes this paper emphases on data centric trust management system to provide consistent communication between the nodes prevents the malicious nodes, RSU aided scheme help to generate the trust values. Simulation shows the effectively analyze data provided in VANET and correctly establish trust on data.**

***Keywords*— VANET; RSU, cluster, Trust management;**

INTRODUCTION

In modern years, the increasing essentials for improved safety and efficiency of road transportation system have promoted automobile constructors in the direction of contribute wireless communications and networking into vehicles. The wirelessly networked vehicles certainly form Vehicular Ad-hoc Networks (VANETs), in which vehicles cooperate to relay various data messages through multi-hop paths, without the need of regional administration. VANETs have the probable to transform the way people travel through the creation of a safe, interoperable wireless communications network. In VANETs, various nodes, such as vehicles and Roadside Units (RSUs), are generally equipped with sensing, processing, and wireless communication capabilities. Both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications enable safety applications that provide cautions regarding road accidents, traffic circumstances (e.g., congestion, emergency decelerating, icy road) and other relevant transportation events. However, VANETs are susceptible to threats due to increasing confidence on communication, computing then control technologies. The distinctive security and privacy challenges posed by VANETs include truthfulness (data trust), privacy, non-repudiation, admission controller, real-time operative limitations demands, accessibility, and privacy safety One typical application of VANETs is the Traffic Estimation and Prophecy Scheme (TrEPS), which normally provides the analytical information required for practical traffic administrator and traveller.

I.I Applications: The goal of VANET remains towards increases driving experience and the safety of transportation.. By frequently broadcasting and receiving messages, vehicles are alert of their surrounding road situations. The drivers can react to events happen on the road by these messages in advance. Even in some urgent cases, the OBU can make the decision (stop or change the lane) automatically. There are many applications used in VANET, which are mainly classified in two parts:

1] safety-related and

2] User application.

Safety-related applications: This type of application can significantly decrease the number of accidents. Normally vehicles travel at very high speed particularly in the high ways. Drivers have very short time to react to the car crashes in front. If an accident occurs, the vehicles overdue often crash before they stop on the road. Safety applications should give warning to drivers in advance, so that they can change the lanes or stop, consequently avoiding accidents. The application should supply driver the road condition and select the best path for driver. This could prevent road blocking, valid people's interval and energy reduction. It can be noticed that the security for this type of application is mandatory even a tiny mistake can cause serious consequences.

User applications: User application provides drivers with information (e.g.Gasstation), online-payment pleasurable and broadcasts. For existence schemes action. For example, TrEPS can provide input to traffic managers who decide where and when to post explicit messages on variable message signs, such as avoid congestion—exit here for alternate route. To help TrEPS more precisely evaluate the current traffic flow conditions and better make calculations, multiple emerging information sources have been taken into consideration, such as real-time situation sensor facts composed and transmitted by driver wants to know the location of cheapest price gas station, he/she can get the information by sending request to the nearby RSU. After getting this request, RSU checks from Internet and much important as in safety-related application.

1.2 VANET Module

Vehicular AdHoc Networks (VANETs) be situated designed by connecting the main principles of portable ad hoc networks (MANETs) the impulsive structure of wireless network for facts conversation - to the domain of vehicles. They are a key component of intelligent transport schemes (ITS).The foundation of vehicular adhoc networks (VANETs) is the discussion of data between entities, and creation a result on received data/event is typically based on information provided by added objects. The entities are permanently connected and are responsible for the traffic or external services. It consists of Manufacturer which is used to uniquely identify the vehicles, Trusted Third Parties (TTP) offer many services like credential management or time stamping, legal authority which is for registration of vehicles and reporting of offenses as dissimilar rules or guidelines of every nation and Service providers offer services like Digital Video Broadcasting (DVB) or Location-Based Services (LBS).

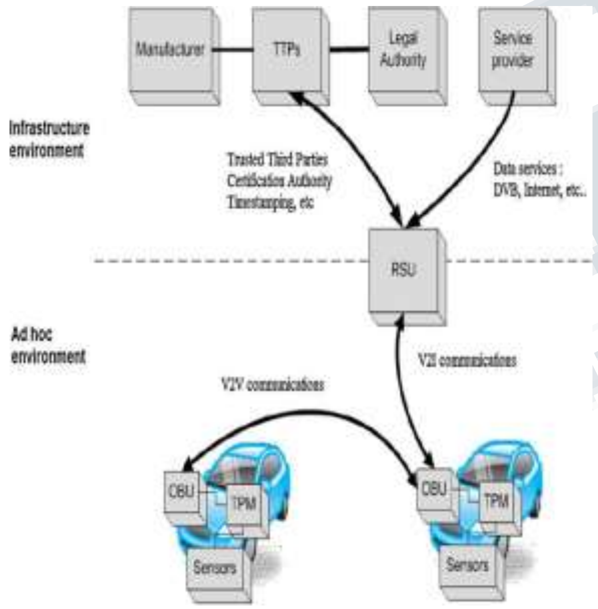


Figure 1.Vanet module

In this environment, vehicles are interactive. There are three devices such as OBU, which enables communication among V2V, V2I and I2I, Sensors which is used to intelligence the environment and improve the road safety and TPM (Trusted Platform Module).

1.3 Trust in VANETs

The belief that an entity has about other entities, from past experiences, on knowledge about the entity's nature, in addition/or on recommendations from trusted entities. Trust mechanisms not only help in node routine discovery, but also improve network performance because honest nodes can avoid working with untrustworthy nodes.

1.4 Trust management in VANET

Trust management is to determine whether the traffic event reported by a warning message is really occurring and to prevent false traffic warning messages from being spread on VANET. Trust and reputation management has been proposed in the last years as an accurate alternative to deal with some security threats in highly spread and self-motivated scenarios.

In common, based on the main object in model (facts or entity), the trust models in VANETs can be considered into three main groups as follows: (i) entity-centric, (ii) data-centric, and (iii) combined.

Entity-centric: The entity is the prime objective in this cluster, and the trust model focuses on the constancy of vehicles. To achieve this, the trust model needs appropriate information about the neighbours and sender of the message. But the high mobility of vehicles leads to failure to collect enough information about the neighbours/sender. When an entity received data from a trustworthy sender, according to the presence of attackers as well as limitation of sensors, data correctness still remains obscure.

Data-centric: The data/event message is the main object in this group, and the trust model focuses on the trustworthiness of data. In this group, the trust model needs to assess the level of trust for each received event message. Therefore, the large number of data as well as replicated data in heavy traffic density leads to increased latency and lost data. In contrast, in the sparse traffic density, this model would not perform well.

Combined: Both entity and data are the main objects in this group. The trust model uses vehicle trust to evaluate the trustworthiness of data.

1.5 Data-based trust management

The data-based trust model determinations to approve whether the described authorization is reliable or not. Created on the trust value, the prototypical decides how to react on the reported event. A few models of trust based on data have been proposed such as the data-centric, intrusion-aware trust model, reputation-based trust model, event-based repute structure (ERS), and roadside-unit aided data centric trust formation .Raya et al. proposed a framework for data-centric trust establishment where trust in respectively individual piece of data is computed. They proposed the collection of multiple reports related to the same event and of their weights and their arrangement into a robust decision scheme.

II LITERATURE SURVEY

In this paper [1] author proposed about present trust based models .It has developed a stimulating task due towards the nonexistence of infrastructure, trustworthiness of wireless associations and the frequently extremely active system topology. Trust-based methods have been mainly applied to provide reliable direction-finding in computer networks So far, trust consumes existed used to manage with packet dropping attacks or to excellent trusted pathways among the source and the destination.

In this paper [2] author proposed an RSU assisted beacon-based trust organization scheme called RaBTM that targets to rapidly create assessments and internal malicious attackers more precisely in location privacy-enhanced VANETs. In this system, a vehicle cannot only utilize beacon messages and event messages to determine the trustworthiness of event messages from VANETs but also get assistance from RSUs'reliable opinions. Another significant maintenance of projected configuration is that it can make assessments rapidly and give estimations over a small delay.

In this paper [3] author presented a RSU-aided scheme for data-centric trust establishment in VANET. In contrast to entity-centric trust establishment approaches, our scheme is purely data centric due to its decoupling the trust relations between the data-reporting vehicles and the data-consuming vehicles. RSU plays the role of intermediate that collects data from data reporting vehicles, transforms data into evidences, calculates other hand, our scheme combines observation factor and feedback factor with the assistance of fundamental ant colony optimization (ACO) ACO algorithm recognized issues that affect the presentation of Roadside-unit Aided Trust Establishment scheme (RATE) RATE, including observing condition, event evolving status and malicious data proportion trust establishment.

In this paper [4] author proposed VANET becomes useless if a vehicle cannot accept the accuracy of message and act on a message broadcast in the network. The acceptance of VANET is, therefore, relies on the implementation of a successful trust evaluation system. The sparsity on direct interactions, availability of forwarded messages, trustworthiness of the level is generated by RSU network architecture is being established to enhance the effectiveness and safety of the conveyance system.

In this paper [5] author proposed from the study of Reputation-based Global Trust Establishment RGTE scheme we can draw a conclusion that RGTE scheme has advantage in confidence-building, security assurance and high adaptability in rapid changing environment of VANET. In our future work we will focus on improving the algorithms to get a more reasonable dynamic threshold and complete the strategy of distinguishing malicious nodes.

III. PROPOSED METHODOLOGY

We projected "Road side unit" assisted as data centric trust management system that goal is to provide the successful message transmission among the nodes so that avoids the problem of road traffic hazard road side unit have two main properties first one is based on data centric and second one is infrastructure for information centric, cluster are formed one of the node is chosen as the cluster head it will broadcast the message to all its cluster member and node in infrastructure communication takes place vehicle will communicate to RSU then trust values are generated by using some technique "Bayesian Interface ,DST "BI says that trust values between [0,1] threshold value is taken as 0.5 DST of proof is implemented by combine honesty of events messages from the several vehicles.

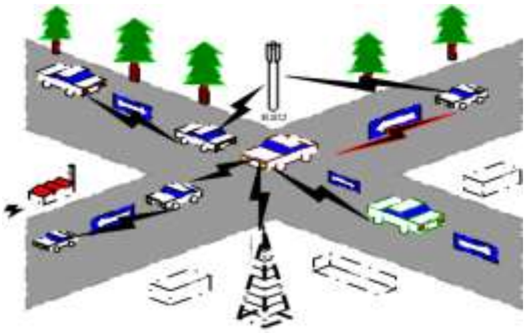


Figure 2: vehicular network architecture

The proposed model of the architecture is shown in the diagram trustworthiness of the level is generated by RSU network architecture is being established to enhance the effectiveness and safety of the conveyance system providing for example road condition alternative reduce speed jamming from the networking fact of assessment nodes are vehicles and road side infrastructure are RSU

Proposed Methodology

Cluster Creation Algorithm

```
Step 1: [Pi, Qi] =find position (node);
Step 2: [Ai, Bi] = subclass (Pi, Qi);
Step 3: for (i=0; i<count (Ai) i++)
Step 4: {for association speed N (i)}
Step 5: if (all the nodes sum of movement speed is slow)
Step 6: then smaller size group of nodes created
Step 7: end if
Step 8: else larger cluster formed
Step 9: end if
Step 10: function discovery position (int n)
Step 11: for (k=0 k<n; k++)
Step 12: treasure position PQ (i)
Step 13: return PQ
```

From this algorithm total number of nodes belong to 'n , node i is the i th node verifying from 0 to n-1 if n=3 values becomes P0Q0,P1Q1,P2Q2 so on then algorithm determine the position of the nodes cluster area ; x y position of the node of specific cluster area (Ai,Bi) is the subgroup of (Pi,Qi).from the above algorithm we can determine the movement speed of N(i)that is the subset of(Ai,Bi) smaller size is found by if the average of cluster is less otherwise cluster size larger .

Algorithm 2

Cluster head selection

```
Step 1: count the number of nodes that are available in the cluster For i=0 to node count
Step 2:  x location of node i at the interval Ti= Ti(x)
         Y position of node i at the period Pi =Pi(y)
Step 3: Vi (x) =  x place of node i at the v
         Vi (y) = y point of node i at the v
Step 4: Least distance diff (X) =determine the difference among the X place of node i between the time T &V
         Minimum distance diff (y) = find the difference between the y location of node i among the time at T (time), V (vehicle)
Step 5: locate the path of the node association if slow moving node at left end
         Then all additional nodes in the bunch then node are moving slowly near in the right place
Step 6: then {choice that node as cluster head}
Step 7: end
```

Algorithm 3:

Technique for trust of slow moving vehicles

```
Step 1: determine the total trust values on slow moving by using equation
Step 2: if (trust of slow moving > threshold values of n th vehicles) & its communicates to RSU then
Step 3: slow moving is trust worthy node
Step 4: else
Step 5: malicious node
```

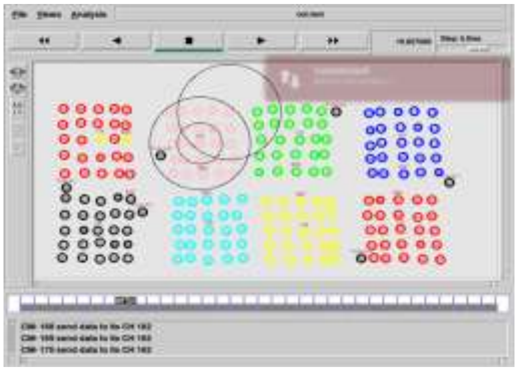
The above two algorithm represents the cluster head selection and to identify the trust worthiness of node if the vehicles communicates to RSU then trust values are incremented then RSU broadcast to that messages to CH cluster head will send to its cluster members.

IV. EXPERMENTAL RESULTS AND ANALYSIS

Simulation parameter setting table

Number of nodes	210
Number of cluster	8(each of contain 22nodes)
Number of cluster head	8
Packet size	512
Simulation time	5ms
Antenna	Omni antenna

The below figure demonstrate the NAM window and deployment of node we are deploying the maximum possible nodes in NAM window and some nodes are static , dynamic in nature in static nodes ,centric node is chosen as cluster head and it will broadcast message to all its neighbor dynamic nodes are communicating through the road side unit if vehicle communicate to RSU trust level is incremented to identify the trustworthiness of node threshold values are set to be 0.5 according to Bayesian inference Dempster shafer theory to evaluate the logic model these methods focus on data they do not importance on trustworthiness of sender or forwarder of event messages therefore in order to improve the proposed system RSU aided hybrid trust is implemented .trust values range from [0,1] in the proposed system



CM- 168 send data to its CH 182
CM- 169 send data to its CH 183
CM- 170 send data to its CH 182

Figure 3: Simulation topology

No of cluster	Cluster creation time
2	2.0500ms
4	2.1500ms
6	2.5000ms
8	2.6000ms

Table 1: cluster creation time

The table and graph represents cluster creation in X axis number of cluster in Y axis time taken to form the cluster active for the time cluster creation is shown in table and same number of cluster increses the time time also increses .

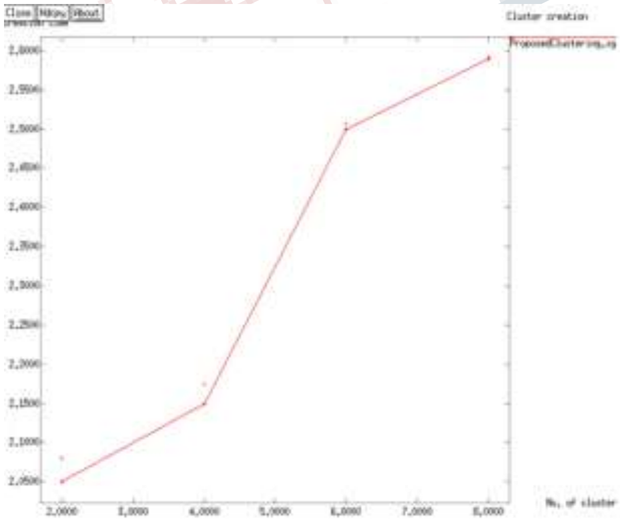


Figure 4: Cluster creation

No of cluster	Cluster head selection time
2	3.5000ms
4	2.8000ms
6	1.5000ms
8	1.4000ms

Table 2: Cluster Head Selection

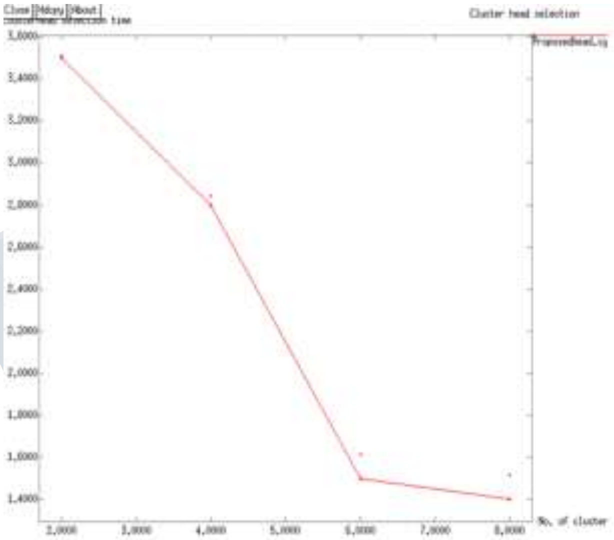


Figure : Cluster Head Selecetion

Cluster head selection table and graph represents to form the cluster head intial it consums more time because first need to form all cluster and need to chose cluster head among the nodes so time required is more to create two CH it take more time once all cluster are designed to elect the next CH it takes less time compared to previous one so graph is plotted in decreasing order.

Dynamic Trust Matrix level.

Vehicles	RSU	RSU	RSU	RSU
V1 trust	0.6	0.6	0.6	0.4
V1 trust1	0.6	0.6	0.6	0.6
V1 trust 2	0.6	0.4	0.6	0.4
V1 t3	0.4	0.4	0.6	0.4
V1 t4	0.6	0.4	0.4	0.6
V2 t0	0.4	0.4	0.4	0.6
V2 t1	0.4	0.6	0.4	0.6
V3 t2	0.6	0.4	0.4	0.6

V3 t3	0.6	0.4	0.6	0.6
V4 t4	0.6	0.4	0.6	0.4
V3 t	0.4	0.6		
V3 t1	0.6	0.4		
V3 t2	0.4	0.6		
V3 t3	0.4	0.6		
V3 t4	0.6	0.6		
V4 t	0.4	0.4		

Table 3:Dynamic trust matrix

V1 represents the vehicles and t0 represents the trust values the table shows the dynamic trust values these values will be changes according to the simulation .

CONCLUSION

In our paper we developed data centric trust management in vanet using cluster and RSU plays important role to provide reliable communication among the nodes and provide less or zero packet dropping less overhead RSU aided trust management system aims to quickly make decision and prevent internal malicious attackers RSU collect the data from the vehicles and broadcast to CH cluster head will transform to cluster members in the group RSU plays the role of intermediate that collect data from data reporting vehicles transforms data into evidence computes trust and provides trust to data consuming vehicles.

REFERENCES

[1] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, “Towards expanded trust management for agents in vehicular adhoc networks,” International Journal of Computational Intelligence: Theory and Practice, vol. 5, no. 1, pp. 3–15, 2010.

[2] Y.-C. Wei, “A beacon-based trust management system for enhancing user centric location privacy in vanets,” Communications and Networks, Journal of, vol. 15, no. 2, pp. 153–163, 2013..

[3] A. Wu, J. Ma, and S. Zhang, “Rate: a rsu-aided scheme for data-centric trust establishment in vanets,” in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, 2011, pp. 1 –6.

[4] J. Zhang, C. Chen, and R. Cohen, “Trust modelling for message relay control and local action decision making in vanets,” Security and Communication Networks, vol.6, no. 1, pp. 1 –14, 2013..

[5] Dhurandher, Sanjay K., Mohammad S. Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi, "Securing vehicular networks: a reputation and plausibility checks-based approach", In GLOBECOM Workshops (GC Wkshps), IEEE, pp- 1550-1554, IEEE, 2010.

[6] Yu Yanli, Li Keqiu, Zhou Wanlei and Li Ping, “Trust Mechanisms Wireless Senor Networks: Attack Analysis and Countermeasures”, In Journal of Network and Computer Applications, pp. 1-14, 2011.

[7] Huang, Zhen, Sushmita Ruj, Marcos Cavenaghi, and Amiya Nayak, "Limitations of trust management schemes in VANET and countermeasures", In Personal Indoor and Mobile Radio Communications (PIMRC), IEEE 22nd International Symposium on, pp- 1228- 1232. IEEE, 2011.

[8] Wang, Jian Yanheng Liu, Xiaomin Liu, and Jing Zhang,"A trust propagation scheme in VANETs", In Intelligent Vehicles Symposium, IEEE, pp- 1067-1071, IEEE, 2009

[9] Wang, Zhou,and Chunxiao Chigan, "Countermeasure uncooperative behaviors with dynamic trust token in VANETs", In Communications, ICC'07, IEEE International Conference on, pp- 3959-3964, IEEE, 2007.

[10] Gazdar, Tahani, Abderrahim Benslimane, and Abdelfettah Belghith, "Secure clustering scheme based keys management in VANETs", In Vehicular Technology Conference (VTC Spring), IEEE 73rd, pp- 1-5. IEEE, 2011.

[11] M.-C. Chuang and J.-F. Lee, “TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks,” in International Conference on Consumer Electronics, Communications and Networks (CECNet), Apr. 2011, pp. 1758–1761
.

[12] Hong, Xiaoyan, Dijiang Huang, Mario Gerla, and Zhen Cao, "SAT: situation-aware trust architecture for vehicular networks", In Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture, pp-31-36, ACM, 2008.