PERFORMANCE IMPROVEMENT OF SECURITY IN VANET

Mrs.V.Sutha Jebakumari

Assistant Professor of CSE

T.Shanmathi , T.Thirupathi Murugeswari , T.Nithiya

UG students

Kamaraj college of engineering and Technology, Virudhunagar.

Abstract-**The faster development of intelligent transportation provides a new way for solving the road congestion, travel comfort and road safety. Many existing system provides information to the vehicular user which may be wrong information that are dangerous to other vehicles followed by poor network performance. In the proposed system, a reliable trust based head service recommendation scheme for helping the other vehicles. Here header node provides emergency information to the other vehicles on the network. A new reputation system is designed for collecting and modeling the feedback from other vehicles. Our experimental procedures provide effective results when compared with existing systems.**

Indexterms-VANET,Trust,Robustness, Scalability.

I.INTRODUCTION

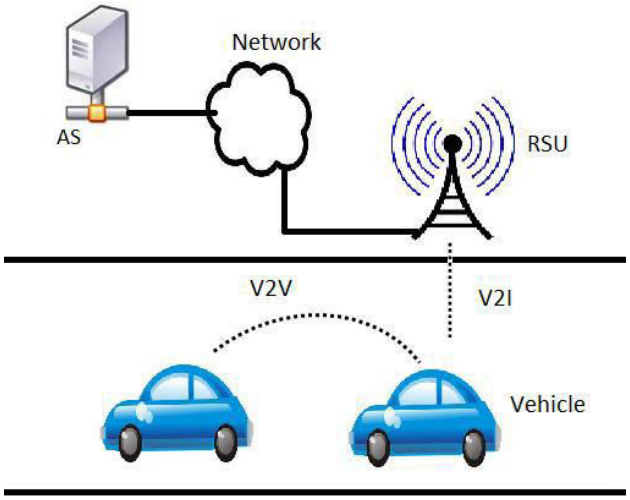
Automobile reaches its advanced technology in vehicle manufacturing. There are more innovative benefits to achieve. This aims at enabling road safety and self organizing agents.

The estimated number of deaths increases about 1.2 million every year. VANET's, security and privacy are identified as major challenges.

The National Highway Traffic Safety Administration(NHTSA) promotes in reducing road victims and save billions of gallons of fuel by reducing the congestion with the help of *self-driving cars*. At the same time, the driver error is a major key factor in 90% of car crashes, and
technologies could help in preventing many crashes. This NHTSA emerges as the new field for the technology which provides as **wireless** communication**.** This NHTSA completely aims at deploying two things:

i. Vehicle-to-vehicle(V2V)
ii. Vehicle-to-infrastructure(V2I)

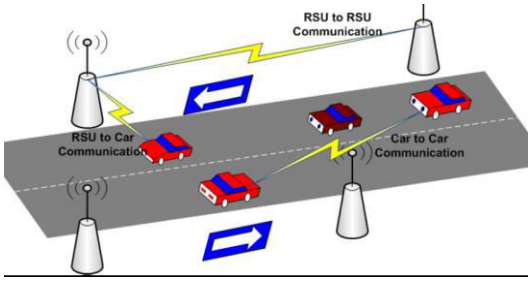
This NHTSA helps us for both safety and non-safety applications. It provides ability to communicate nearby vehicles **via header node**. The header node is taken in the basis of trust. There are few security issues confidentiality, authenticity, integrity, availability and non-repudiation aim to secure communication between V2Vand V2I.



II .HOW VANET WORKS

Vanet System contains nodes in large number, it is approximately believed that the number of vehicles are exceeding 750 million all around the world, these vehicles requires an authority to govern, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), the range can reach 1 KM, the kind of communication is an Ad Hoc communication that actually means each and every connected node can move freely, here no wires required, here the routers are used and it is called Road Side Unit (RSU),the RSU works as a router between the vehicles on the road and connected to other network devices for the purpose of communication.
Each vehicle has its own OBU (on board unit), the OBU connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device). The TPD device holds the vehicle secrets. It contains all the information about the vehicle like

i. Driver's identity
ii. Details of the trip
iii. Speed
iv. Rout
v. Has its own battery



III.VANET SECURITY CONCERNS

There are different kinds of attacks in vanet. They are discussed in the following subsections:

1) Denial of Service attack:

The attack happens when the attacker takes the full control over vehicle's resources or jams the entire communication channel used by the Vehicular Network. It is believed that it prevents critical information from arriving and also increases the possibility of danger to the driver.

2) *Sybil Attack:*

The attack happens when an attacker claims multiple identities illegally and also creates large number of pseudonymous, and it can increaseing false information.

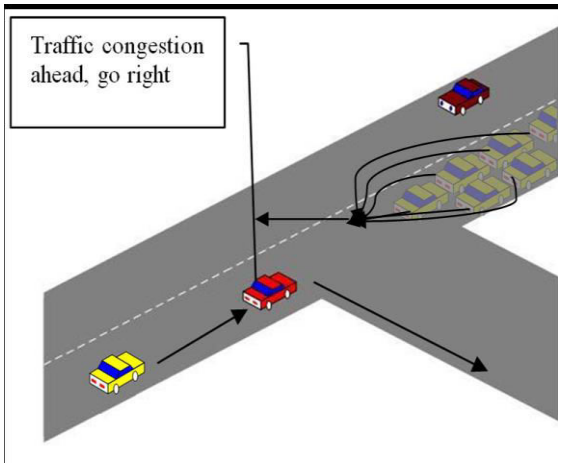


Fig 2

Sybil attack corrupts the entire network.
For instance ,

An attacker can pretend to clear the road and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another route, so the road will be clear.

3) Fabrication Attack

The attack transmits the false information into the network. The information could be false or the transmitter could claim that it is somebody else. This attack includes fabricating messages, warnings, certificates, identities etc.

4) Alteration Attack

The attack happens when attacker alters the existing data
For instance:

i. Delaying the transmission of the information
ii. Replaying earlier transmission
iii. Altering the actual entry of the data transmitted.

5) *Message Suppression Attack:*

An attacker selectively dropping packets from the network and these packets may hold critical information for the receiver. The attacker suppresses these packets and can use them again in other time. The goal of such an attacker is to learn about collisions.

IV. *SYSTEM MODEL*

A. *System Model*

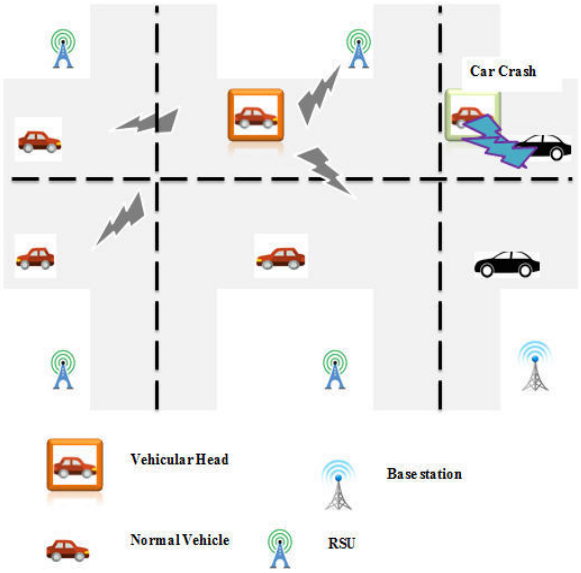


Fig 3

It introduces reliable trust based head service recommendation scheme for helping the other vehicles. Here header node provides emergency information to the other vehicles on the network.

A new reputation system is designed for collecting and modeling the feedback from other vehicles. Our experimental procedures provide effective results

IV. VEHICULAR NETWORKS CHALENGES

1) Mobility

The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection throw their way with another vehicles that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is hard problem.

i. Dos Attack
ii. Selfish Driver
iii. Sybil Attack.

2) Volatility

The connectivity among nodes can be highly ephemeral, and maybe will not happen again, vehicles travelling throw coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction.

Vehicular networks lacks the relatively long life context, so personal contact of user's device to a hot spot will require long life password and this will be impractical for securing VC.

3) Privacy VS Authentication

The importance of authentication in Vehicular Ad Hoc Networks is to prevent Sybil Attack that been discussed earlier. To avoid this problem we can give a specific identity for every vehicle, but this solution will not be appropriate for the most of the drivers who wish to keep their information protected and private.

4) Privacy VS Liability

Liability will give a good opportunity for legal investigation and this data can't be denied (in case of accidents), in other hand the privacy mustn't be violated and each driver must have the ability to keep
his personal information from others (Identity, Driving Path, Account Number for toll Collector etc.).

5) Network Scalability

The scale of this network in the world approximately exceeding the 750 million nodes , and this number is growing, another problem arise when we must know that there is no a global authority govern the standards for this network for example: the standards for DSRC in North America is deferent from the DSRC standards in Europe, the standards for the GM Vehicles is deferent from the BMW one.

6) Bootstrap

At this moment only few number of cars will be have the equipment required for the DSRC radios, so if we make a communication we have to assume that there is a limited number of cars that will receive the communication, in the future we must concentrate on getting the number higher, to get a financial benefit that will courage the commercial firms to invest in this technology .

V.NETWORK SIMULATOR 3

The ns-3 simulator is a discrete-event network simulator targeted primarily for research and educational use.

The goal of the ns-3 project is to create an open simulation environment for computer networking research that will be preferred inside the research community.

- It should be aligned with the simulation needs of modern networking research.
- It should encourage community contribution, peer review, and validation of the software.

Since the process of creation of a network simulator that contains a sufficient number of high-quality validated, tested and actively maintained models requires a lot of work, ns-3 project spreads this workload over a large community of users and developers.ns-3 is built using **C++** and **Python** with scripting capability. These automatically-generated C++ files are finally compiled into the ns-3 Python module to allow users to interact with the C++ ns-3 models and core through Python scripts. The ns-3 simulator features an integrated attribute-based system to manage default and per-instance values for simulation parameters.

SIMULATION WORKFLOW

***1. Topology definition*:** To ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process.

***2. Model development*:** Models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.

***3.Node and link configuration*:** Models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.

***4.Execution*:** Simulation facilities generate events, data requested by the user is logged.

***5.Performance analysis*:** After the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analyzed with tools like R to draw conclusions.

6.***Graphical Visualization*:** Raw or processed data collected in a simulation can be graphed using tools like Gnuplot matplotlib or XGRAPH.

VI.Modules:

- Network Formation
- Feedback process
- TH Selection
- Performance

Modules Description:

Network Formation:

In our proposed network formation process is a system arrangement;it is apart of network knowledge that seeks to copy how a network evolves by identifying which factors affect its structure and how these mechanisms operate. Network formation hypotheses are tested by using either a dynamic model with an increasing network size or by making an agent based model to determine which network structure is the equilibrium in a fixed size network.

Feedback process:

The feedbacks of user vehicles and trip information updates of head vehicles will be forwarded through RSUs to TA or server. From this point of view, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, we assume that RSUs are widely deployed along the roads to cover the whole area which ensures that the vehicles are able to update the information timely when driving on the roads.

In some areas where RSUs are sparsely deployed, the update of the feedbacks and traveling information of trust head vehicles are delayed, the accuracy of our proposed scheme will be decreased. But in the long run, the scheme is still efficient.

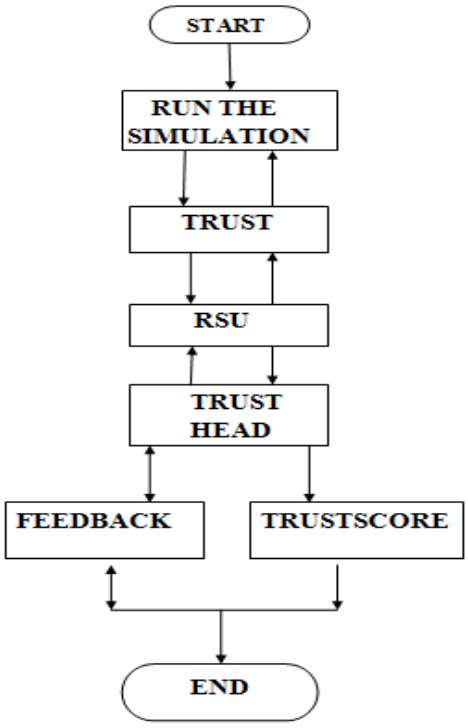
Trust head (TH) Selection:

Trust authority plays a significant role in the whole system, which takes charge of registration of the server, all RSUs and vehicles.Trust is defined as a particular level of subjective probability with which an agent assesses another agent or a group of agents who will perform a particular action before it can monitor such action and in a context in which it affects its own action. When we say someone is trustworthy, we implicitly mean that it will perform an action within our expectation so that we can cooperate with it. It can be represented as a particular expectation regarding the behaviors.

Performance:

On car crash incidents, the information is updated to RSU by specific trust head. The RSU sends information to all trust heads. In the performance of our proposed scheme process are, The performance metrics used in the evaluation aretrust scores in terms of the round for different user vehicles; reputation scores' variations with round for PH vehicles with different performances likedetection rate variations.

DATA FLOW DIAGRAM



VII.METHODOLOGY

Iterative Filtering algorithm is used for excluding the feedback from the trusted nodes in the network.

- The server uses the feedbacks collected from user vehicles to compute the reputation scores of platoon head vehicles.
- As a result of responsibility the well-behaved and badly-behaved head vehicles are clearly distinguished according to their reputation scores
- Then the server will recommend a reliable platoon head vehicle to the user vehicle.

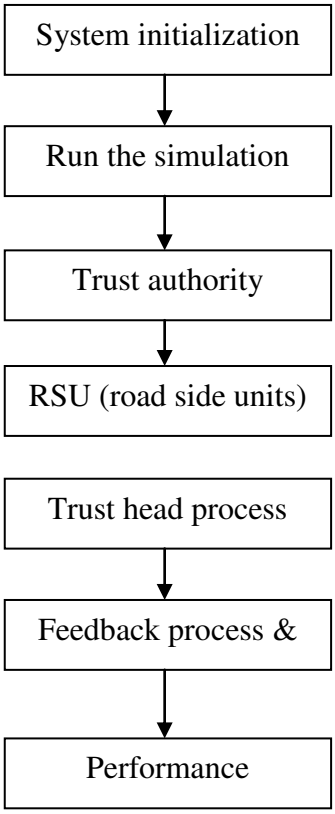
E-R DIAGRAM

An entity-relationship diagram (ERD) is a data modeling technique that graphically illustrates an information system's entities and the relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure.

The three main components of an ERD are:

- The *entity* is a person, object, place or event for which data is collected. For example, if you consider the information system for a business, entities would include not only customers, but the customer's address, and orders as well. The entity is represented by a rectangle and labelled with a singular noun.

- The *relationship* is the interaction between the entities. In the example above, the customer *places* an order, so the word "places" defines the relationship between that instance of a customer and the order or orders that they place. A relationship may be represented by a diamond shape, or more simply, by the line connecting the entities. In either case, verbs are used to label the relationships.



Feasibility Study:

Nowadays, the faster development of intelligent transportation provides a new way for solving the road congestion, travel comfort and road safety. Many existing system provides information to the vehicular user which may be wrong information that are dangerous to other vehicles and follow as a result of network performance. In our proposed system, we introduce a reliable trust based head service recommendation scheme for helping the other vehicles. Here header node which provides emergency information to the other vehicles on the network. A new reputation system is designed for collecting and modeling the feedback from other vehicles. A comprehensive security analysis is given to show that our proposed REPLACE scheme is secure and robust against badmouth, ballot-stuffing, newcomer and on-off attacks existing in VANETs. In adding up, we perform extensive experiments to demonstrate the correctness, accuracy and robustness of our proposed scheme.

A reliable trust based recommendation service is used to the proposed system. The trust is introduced for different vehicles based on establishing a trust and reputation system. The server uses the feedback which is collected from other vehicles for computing the reputation scores on the head vehicles. Based on these procedures, the well-behaved vehicles head and badly behaved vehicle heads are clearly identified based on the repute scores of every node. An iterative filtering algorithm is introduced for excluding the feedback from the trusted nodes in the network.

In our proposed network formation process is a system arrangement; it is a part of network knowledge that seeks to copy how a network evolves by identifying which factors affect its structure and how these mechanisms operate. Network formation hypotheses are tested by using either a dynamic model with an increasing network size or by making an agent based model to determine which network structure is the equilibrium in a fixed size network.

The feedbacks of user vehicles and trip information updates of head vehicles will be forwarded through RSUs to TA or server. From this point of view, RSUs can be regarded as relays of data between vehicles and TA or between vehicles and server. In our system model, we assume that RSUs are widely deployed along the roads to cover the whole area which ensures that the vehicles are able to update the information timely when driving on the roads.

In some areas where RSUs are sparsely deployed, the update of the feedbacks and traveling

information of trust head vehicles are delayed, the accuracy of our proposed scheme will be decreased. But in the long run, the scheme is still efficient.

Trust authority plays a significant role in the whole system, which takes charge of registration of the server, all RSUs and vehicles. Trust is defined as a particular level of subjective probability with which an agent assesses another agent or a group of agents who will perform a particular action before it can monitor such action and in a context in which it affects its own action. When we say someone is trustworthy, we implicitly mean that it will perform an action within our expectation so that we can cooperate with it. It can be represented as a particular expectation regarding the behaviors.

On car crash incidents, the information is updated to RSU by specific trust head. The RSU sends information to all trust heads. In the performance of our proposed scheme process are, The performance metrics used in the evaluation are trust scores in terms of the round for different user vehicles; reputation scores' variations with round for PH vehicles with different performances like detection rate variations.

SYSTEM DESIGN

System design is the process of defining the elements of a system such as the architecture, modules and components, the different interfaces of those components and the data that goes through that system. It is meant to satisfy specific needs and requirements of a business or organization through the engineering of a coherent and well-running system.

OUTPUT DESIGN

The term output necessarily implies to information printed or displayed by an information system. Following are the activities that are carried out in the output design stage:

•Identification of the specific outputs required to meet the information requirements.

•Selection of methods required for presenting information.

•Designing of reports, formats or other documents that acts as carrier of information.

Output design objectives

The output design of an information system must meet the following objectives:

1.) The output design should provide information about the past, present or future events. The operational control level outputs provide information of the past and present events. On the other hand, required at the strategic planning level provide information of the future events.

2.) The output design should indicate the important events, opportunities and problems.

3.) The output design should be designed keeping in mind that an action must be triggered in response to some event. A set of rules is pre-defined for such trigger.

4.) The output design should produce some action to the transaction. For example, when the telephone bill is received, a receipt is printed.

Presentation of output

The next consideration in the output design is the presentation involved with an information system. The presentation of an output is regarded as an important feature of output design. The presentation of an output represented either in tabular or graphical form or in both forms. A tabular format is preferred in the following conditions:

•When the details dominate the content of the output

•When the contents of the output are classified in groups.

•When the output design are to be compared.

A tabular format is also preferred for the detailed reports. Graphical representation is used to improve the effectiveness of the output because some users prefer to view information in graphic form rather than in rows and columns of the tables. The tabular and graphical formats may be combined together to enhance the presentation of the output.

INPUT DESIGN

Similar to the output design, input design is equally important for a system designer. This is because output from a system is regarded as the foremost determinant for defining the performance of a system. The output of the system greatly affects the input design of the system.

Input Design Objectives

The input design of an information system must the following objectives:

•The input design of the system must attempt and try reducing the data requirements. It should also avoid capturing unnecessary data such as constant and system-computable data.

•The input design must avoid processing delays during data entry. Capturing automatic data can reduce this kind of delay.

- he input design must avoid data entry errors. This can be achieved by checking the errors in data entry program. This technique of checking

data entry program programs for errors is known as input validation technique.

- he input design must keep the process simple and easy to use.

Conclusion:

In our proposed system a reliable trust based recommendation service is used. The trust is introduced for different vehicles based on establishing a trust and reputation system. The server uses the feedback which is collected from other vehicles for computing the reputation scores on the head vehicles. Based on these procedures, the well-behaved vehicles head and badly behaved vehicle heads are clearly identified based on the repute scores of every node. On car crash incidents, the information is updated to RSU by specific trust head. The RSU sends information to all trust heads. In the performance of our proposed scheme process are, The performance metrics used in the evaluation are trust scores in terms of the round for different user vehicles; reputation scores' variations with round for PH vehicles with different performances like detection rate variations. An iterative filtering algorithm is introduced for excluding the feedback from the trusted nodes in the network.

Future Work:

In the future work, we will target on preserving the privacy of feedback data and trust data that are stored and computed in the server.

REFERENCES

1. *A. A. Alam, A. Gattami, and K. H. Johansson, "An experimental study on the fuel reduction potential of heavy duty vehicle platooning," in 13th International IEEE Conference on Intelligent Transportation Systems (ITSC), 2010. IEEE, 2010.*

2. R. Du, C. Chen, B. Yang, N. Lu, X. Guan, and X. Shen, "Effective urban traffic monitoring by vehicular sensor networks," IEEE Trans. Vehicular Technology, 2015.

3. H. Hu, R. Lu, and Z. Zhang, "Tpsq: Trust-based platoon service query via vehicular communications," Peer-to-Peer Networking and Applications, 2015.

4. Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," IEEE Trans. Vehicular Technology, to appear.

5. H. Hu, R. Lu, and Z. Zhang, "Vtrust: A robust trust framework forrelay selection in hybrid vehicular communications," in 2015 IEEEGlobal Communications Conference, GLOBECOM 2015, San Diego,CA, USA, December 6-10, 2015, 2015.

6. A. *Jøsang and J. Haller, "Dirichlete reputation systems," in The Second International Conference on Availability, Reliability and Security, 2007.ARES 2007.IEEE, 2007.*

7. *E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," IEEE Trans. Mob.Comput., , 2012.*

8**.** *J. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," IEEE Trans. Network and Service Management ,vol. 8, no. 2, 2011.*

9**.***Y.L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation frame working distributed networks: Vulnerability analysis and defence against attacks," in INFOCOM 2006. 25th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies23-April2009*

10. J. Quain, "Social Networking for Cars," 2012. [Online]. Available http://wheels.blogs.nytimes.com/2010/07/20/socialnetworking-for-cars

11. W. Sha, D. Kwak, B. Nath, and L. Iftode, "Social vehicle navigation: Integrating shared driving experience into vehicle navigation," in Proc. 14th HotMobile Workshop, New York, NY, USA, 2013, pp. 161–166.

12. S. Stephen, L. Han, P. Shankar, and L. Iftode, "Roadspeak: Enabling voice chat on roadways using vehicular social networks," in Proc. 1st Workshop SocialNets, Glasgow, Scotland, 2008, pp. 43–48.

13. G. Karagiannis et al., "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 584–616, 4th Quart. 2011.

14. M. Conti and M. Kumar, "Opportunities in opportunistic computing,"Computer, vol. 43, no. 1, pp. 42–50, Jan. 2010.

[15] A. M. Vegni, M. Biagi, and R. Cusani, "Smart vehicles, technologies andmain applications in vehicular Ad Hoc networks," InTech, Princeton, NJ, USA, Feb. 2013.