# Reliable Trust Computation model in Vehicular ad-hoc Network

Sonam Soni
Department of CSE
ITM University
Gwalior, India
sonamsoni.itm@gmail.com

***Abstract*— This paper concerns about the various implemented work has been studied and analyzed to form a new survey on trust model to VANET. In this paper it is observed that there are lot of new techniques are possible to form a new trust model in VANET to provide better security with trust concern over the entire environment of trust management in VANET. This work concerns of entire trust calculation work which has been done yet over it. Here summarizing the various trust models, various security requirements, issues over it.**

***Keywords—Trust; VANET; Direct and indirect trust computation.***

## I. INTRODUCTION

In VANET communicate is done by sharing information about road condition as traffic jam, accidental alert and for safety by these things while driving, some more effort has been put to develop life critical & road condition related system like traffic visibility system, message sharing, collision detection & avoidance and crash reporting all these activities must be in a safe manner [1]. The main intention of made system is to ensure reliable delivery of entire message among nodes (vehicles). Vehicles should follow traffic rule and road limit to avoid accident, malicious node may send false messages to mislead and to spread spam messages to create problems like false information of traffic jam, accident and robbery. Trust are the main component of security those are used to perform decision making ability in VANETs [2]. Trust is the level of confidence on message those are passed to establish VANET. It is basically depends on the parsuit of the vehicle, the vehicle should free from crime or criminal background [3]. VANET has become a growing area of research. In this field researcher have effort to make strong design and implementation of VANET network environment[4]. It is the technology of building a secure network between vehicles; i.e. vehicles communicate to each other and pass information to another vehicle[5]. Due to the increasing number of the vehicles, roads will likely get rushful. Thus, it is very needful to increase road safety and decrease traffic congestion. In VANET communicate is established between transferring up to date information related to road and traffic conditions, so as to avoid vehicular accidents and fatalities and effectively traffic related decision. VANET is used to give the safety and traffic reports about congestion, earthquake, floods etc. to its user, for reducing the road accidents, fuel wastage and provides secure driving environment.

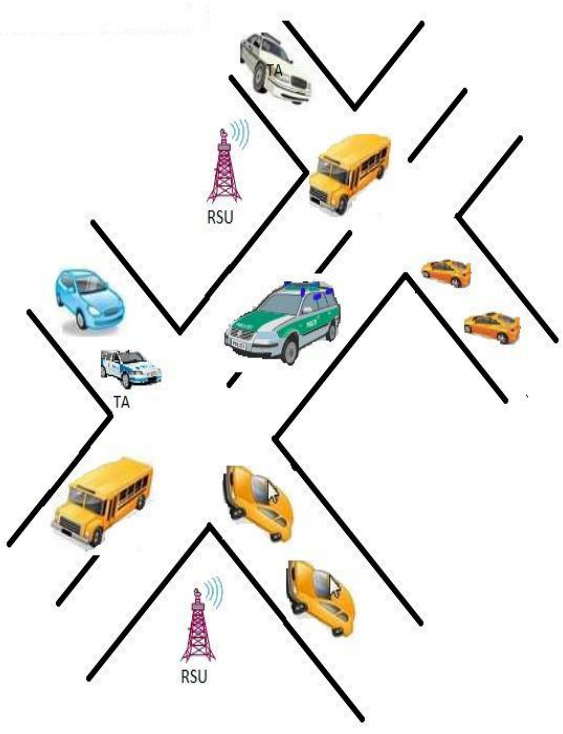

Fig.1. Vehicular ad-hoc Network

In this paper some important section elaborated to build effective trust model which would provide better security with safety from spam spread by an unauthorized node in VANET**.** The important point out of this paper is represented as follows. Section II introduces issues and design requirements for trust management in VANET. Section III, contains security requirements in VANET, section IV, presents trust establishment in VANET and in section V, we describe the existing trust models for VANET. At last, in section VI, we summarize our conclusions.

## II. ISSUES AND DESIGN REQUIREMENTS FOR TRUST MANAGEMENT IN VANET

Trust is a process by which relationships develop [6]. Philosophical view Management of trust is the today's wonder word we could not trust easily because node (vehicle) in VANET or other component may harm any time through any way like spam or warm attack with lots of faith to break, corrupt and destroy the entire system of VANET [7]. Various issues occur to create a faithful environment in VANET. Some of the issues and design requirements of trust computation are described below.

- *Accuracy*

Evidently, a trust and reputation computation in VANETs is always expected to be accurate. Due to detect false information of vehicles.

- *Decentralized*

Decentralized is one of the main issues of trust and reputation computation in VANETs. It should also be applicable to highly dynamic and distributed environment.

- *Simple, light and fast*

Trust and reputation technique should be light weighted, fast in terms of computing and not complex or simple.

- *Scalable*

Hence, VANET is variable density and vehicular density depends on traffic conditions and locations such as traffic jam conditions, city centre, rural roads or highways. So, scalability is also an important issue of trust and reputation computation in VANETs.

## III. SECURITY REQUIREMENTS

There are essential and significant in order to maintain a reliable and secure VANET environment.

These are the security requirements [8].

- *Authentication*

Authentication [9] is required to check whether the message sender is not a fake vehicle or attacker that could gain unauthorized access to resource & critical information that may negatively affect the resources & node information.

- *Availability*

Data must be available at any time [10]. Network service unavailability would be possible by a DOS attack. So it is required to make sure for availability of network services despite of various attacks.

- *Confidentially*

protection & safety of vital information from being subjected to unauthorized users or entities of the entire network area make confidences[11].

- *Privacy*

privacy and secrecy formed in case of sensitive and critical information, the identity of the driver, location of the vehicle, location details of the destination route would be used as private information etc.

- *Integrity*

The originality of data from the adversary and /or harsh environment ensured to avoid inconsistence. Integrity means information should be protected to prevent malicious attackers from modification or altering them, and message contents to be trusted.

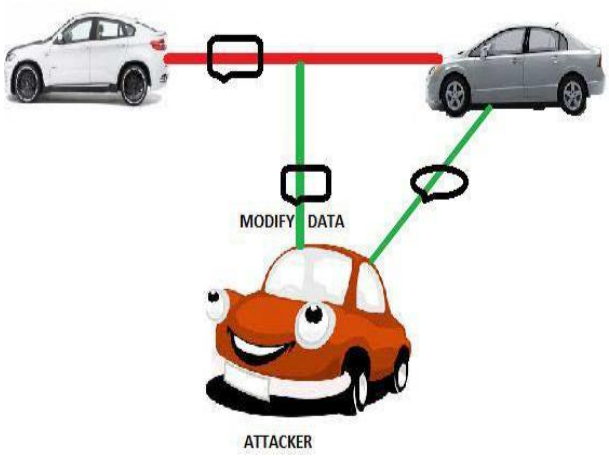


Figure 2 - Loss of integrity

IV. TRUST ESTABLISHMENT IN VANET There are two basic options for trust establishment:

A. *Self organizing trust establishment-*

- *Direct*

Direct trust computation[12] means direct interaction between them based on past experience etc. it is calculated for find out the trustworthy information. Perron- Frobenius theorem calculate trust in VANET environment is based on message strength[13].

- *Indirect*

Indirect trust[12] means second hand information given by nodes. It is calculated according to based on evaluating the several authentication certificate exchange at certain time of vehicles within communication range [14]. If three messages are right out of five messages then source vehicle will increase 1 rank of trust value otherwise indirect rank will decrease 1 rank.

- *Hybrid*

It is the combination of both direct and indirect trust mechanisms.

B. *establishment based on infrastructure-*

- *Zero knowledge/nizkp*

It can be used for the anonymity establishment [15] one node proves the other node the trust of an assertion (its certified statement) with knowledge of hidden information (its ID) without revealing it. The concept of NIZK proofs is the prover's and verifier's access to a common random string (public randomness). That is the reason why NIZK proofs are a sparingly promising concept for the establishment of trust in VANETs. We found only the problem is its still questionable applicability.

- *Group signature*

Group signature is calculated by five phases [16]. setup, join sign, verify and open. Group manager issue a private key that could be used to generate signatures. Outside member cannot identify the actual signer. Outside member can only verify that a signature which generated by members of the group but cannot get member information. This approach maintained by a central authority, and it is able to provide anonymity.

## V. EXISTING TRUST COMPUTING MODEL

There are some existing schemes for establishing the trust model for Vehicular ad-hoc network. This table shows the various research papers according to their different-2 technique for finding of trust in VANET environment.

| Paper Title | Proposed methodology |
|---|---|
| Trust computation in VANET [13] | The trust computation method is based on Perron–Frobenius theorem [66] in the VANET environment based on types of messages, direct interaction with vehicles, aggregated recommendation from other vehicles and content of the messages are used. |
| AHP Based Trust Model in VANETs [14] | To established the trust, we introduce the analytical hierarchy process based technique constitutes the combination of direct, reputation and indirect trust technique. |
| Forming Vehicular Web of Trust in VANET [17] | In this paper used TPM for proposed a new model for chain of trust within vehicular to handle all types of attacks and maintain the integrity of messages. |
| A trusted neighbor table based | In this paper presents a trusted neighbor table |

| | |
|---|---|
| location verification for VANET Routing [18] | (TNT) based location verification technique to identify and prevent position-spoofing attack. |
| TRIP, a trust and reputation infrastructure aided approach for VANETs is presented in [19]. | In this work, trust is calculated using reputation score assigned by other vehicles. Trust computation is further categorized in three different trust levels with fuzzy sets. However, in the presence of malicious nodes more than fifty percent the scheme is unrealistic. |
| TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks [20] | This paper represents the decentralized lightweight authentication scheme called Trust-Extended Authentication Mechanism for vehicular ad hoc network.<br>It gives the theory of transitive trust relationship which accelerates the function of an authentication procedure. However TEAM gives the some security requirements which are anonymity, location privacy, mutual authentication which prevent some attacks such as- spoofing attack, forgery attack, modification attack and replay attacks, also no clock synchronization problem, quick error detection and session key agreement. |
| A Similarity based Trust and Reputation Management Framework for VANETs [21] | This trust management framework is based on similarity mining technique and reputation evaluation algorithm for estimating the trustworthiness of a message. |
| Chains of Trust inVehicular Networks:a Secure Points of Interest Dissemination Strategy [22] | This paper presents user signatures to share information about Points of Interest in Vehicular Ad hoc Networks. |

## VI. CONCLUSION

The conclusion of the entire study is that here lot of ways of pointing the research interest, here free file of same domain has been defined and briefly described. Our proposed work should be in this area to perform an effective job in trust modeling, issues and achieved all desired properties of trust model in VANET. This paper helps to increase researchers to put their effort in a new direction of the trust model building we are highly inspired through current work to made new trust model. After this review study it is observed that new model a new precaution from the attract & new approach to security & safety in vehicular ad-hoc network.

## REFERENCES


[1] Y. Toor, P. Muhlethaler, A. Laouti and A. De La Fortelle, *"Vehicle Ad hoc Networks: Applications and Related Technical Issues," IEEE Communications Surveys and Tutorials*, Vol. 10, No. 3, pp. 74–88, 2008.

[2] Qing Ding and Xi Li, *"Reputation Management in Vehicular Ad-Hoc Networks"*, Multimedia Technology (ICMT), International Conference, pp. 1-5, Oct 2010.

[3] Wenjun Jiang, Guojun Wang and Jie Wu, *"Generating trusted graphs for trust evaluation in online social networks,"* In future generation computer systems, Elsevier, Vol. 31, pp. 48–58, 2014.

[4] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia and Lihong Zheng, " Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges," Journal of Wireless Networking and Communications, vol. 3(3), pp. 29-38, 2013.

[5] Md Mahbubul Haque, Jelena Misic, Vojislav Misic, Subir Biswas, and Saeed Rashwand, "Vehicular Network Security," Encyclopedia of Wireless and Mobile Communications second edition, 2013.

[6] D. Warne, C. P. Holland, *"Exploring trust in flexible working using a new model," BT Technology Journal*, vol. 17, No.1, pp.111-119, 1999.

[7] Jie Zhang, *"A Survey on Trust Management for VANETs",* 2011 International Conference on Advanced Information Networking and Applications (AINA), pp. 105-112, 2011.

[8] Ghassan samara, Wafaa A.H.Al-Salihy, R.Sures*,"Security Analysis of Vehicular Ad-hoc Networks (VANET),"* Second International Conference on Network Applications,Protocols and Services, pp. 55-60, 2010.

[9] M Raya, P Papadimitratos and JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol. 13, pp. 1-10, Oct. 2006.

[10] B. Parno and A. Perrig, "Challenges in securing vehicular networks," In Proc. of the Int. Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[11] Jose Maria de Fuentes, Ana Isabel González-Tablas and Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks," Handbook of Research on Mobility and Computing, IGI Global, 2010.

[12] Mayuri Pophali and T.S.Yengantiwar, “Trusted Opportunistic Forwarding Model in VANET,” International Journal of Computer Applications (0975 – 8887),pp 8-13, 2013.

[13] B. K. Chaurasia, S. Verma and G. S. Tomar, *“Trust Computation in VANETs”*, In the International Conference on Communication Systems and Network Technologies (CSNT-2013), Organized by IEEE, pp. 468-471, April 2013.

[14] Brijesh K. Chaurasia, *“AHP based Trust model in VANETs”*, 5th International Conference on Computational Intelligence and Communication Networks, pp. 391-393, 2013.

*[15]* Philipp Wex, Jochen Breuer, Albert Held, Tim Leinm¨uller and Luca Delgrossi *“Trust Issues for Vehicular Ad Hoc Networks”*, VTC Spring, pp.2800-2804, 2008.

[16] Brijesh K. Chaurasia and Shekhar Verma *“Trust Based Group formation in VANETs”,* Modern Traffic and Transportation Engineering Research (MTTER) Volume 2,Issue 2, pp.121-125, April 2013.

[17] Irshad Ahmed Sumra, Halabi Hasbullah and Iftikhar Ahmad, “Forming Vehicular Web of Trust in VANET,” Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, Riyadh, pp. 1-6, April 2011.

[18] Xiaoping XUE, Nizhong LIN, Jia DING and Yiwen JI, “A trusted neighbor table based location verification for VANET Routing,” Wireless, Mobile and Multimedia Networks (ICWMNN), IET 3rd International Conference, Beijing, pp. 1-5, Sept. 2010.

[19] F. G. Marmol and G. M. Perez, “TRIP, a trust and reputation infrastructure based proposal for vehicular ad hoc networks,” In journal of network and computer applications, Vol. 35, issue 3, pp. 934-941, May 2012.

[20] Ming-Chin Chuang and Jeng-Farn Lee, “TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks,” IEEE SYSTEMS JOURNAL, pp.1-10.

[21] Nianhua Yang, “A Similarity based Trust and Reputation Management Framework for VANETs,” International Journal of Future Generation Communication and Networking Vol. 6, No. 2, , pp. 25-34, April, 2013.

[22] David Antolino Rivas, Manel Guerrero Zapata, “Chains of Trust in Vehicular Networks: a Secure Points of Interest Dissemination Strategy,” Journal of Network and Computer Application Vol. 10, Issue 6, pp. 1115-1133, Aug. 2012.