International Journal of Grid and Distributed Computing
Vol. 9, No. 5 (2016), pp.313-320
http://dx.doi.org/10.14257/ijgdc.2016.9.5.27

Token Based Trust Computation in VANET

Kapil Sharma[1],Brijesh Kumar Chaurasia [2] Shekhar Verma[3], and Geetam Singh Tomar[4]

[1,2]ITM University Gwalior, (M.P.), India, IIIT Allahabad, India and
[4]MIR Labs, (M.P.), India
[1]kapil.sharma.cse@ itmuniversity.ac.in, [2]bkchaurasia@ gmail.com

Abstract

In vehicular ad hoc network or VANET, the safety related messages broadcast by vehicles is used by other vehicles to make critical decisions. This may trap a vehicle taking wrong decision with dire consequences and authenticated vehicles or malicious vehicles may also broadcast wrong messages. This necessitates those messages of vehicles to be trusted after authentication process of vehicles, especially in the absence of centralized authority. In this paper, token based trust computation based on network connectivity duration of vehicles in VANET is proposed. The proposed technique is based on travelling time association among vehicles or network connectivity of vehicle at the time of driving on the road. We present simulations of the proposed technique that verify its correctness and reliability in the presence of infrastructure and absence of infrastructure. Results show that the efficacy of the proposed scheme and makes it viable for secure and lightweight trusted communication in a VANET.

Keywords: *VANET, Trust computation, Tokens and RSU*

1. Introduction

VANET is a network of vehicles, road side unit and a trusted authority. So, it is a hybrid ad hoc network. It is a branch of mobile ad hoc network (MANET). VANET has many prominent characteristics from other ad hoc networks i.e. vehicles moving at high speeds on the road, dynamic topology, predictable and short interaction time between vehicle with limited transmission range of the network [1]. In VANET, vehicles can communicate with nearby vehicles known as a vehicle-to-vehicle (V2V) communication and also with road side infrastructure also known as vehicle-to-infrastructure (V2I) through dedicated short range communications (DSRC). The road side infrastructure is known as RSU may be situated at a fixed optimal place like road intersections *etc* [2]. The vehicles are equipped with wireless communication component known as on board units (OBUs), event data recorder (EDR), global positioning system (GPS) *etc* [3]. The DSRC [4] based on IEEE 802.11p recommends a transmission range for vehicles 300 meters and 1000 meters for RSUs, signal bandwidth of 10 MHz and data rate from 3-27 Mbps. In VANET, trusted authority (TA) is responsible for the authentication process of vehicles and messages. The most important goal of this network is to enable public safety applications that can potentially save lives and improve traffic conditions. Non-safety services are also envisaged to provide toll tax collection [5], comfort, convenience and infotainment to road users, such as geo-location information, weather reports and online gaming *etc*. In VANET, information is exchanged over the shared wireless medium within limited communication range. The safety related messages broadcast by vehicles are used by other vehicles to make critical decisions. This may trap a vehicle taking wrong decision with dire consequences. Moreover, authenticated vehicles or malicious vehicles may also broadcast wrong messages. This necessitates that messages and vehicles to be trusted after authentication process, especially in the absence of centralized authority. In VANET communication the trust management system should be quickly compute the trust, simple (not complex), accurate, scalable and resilient to threats. In this paper, we have

ISSN: 2005-4262 IJGDC

proposed a token based mechanism for evaluating trust of vehicles based on nature of vehicles. Nature of vehicle will depends upon daily meet vehicle on the road and stay time associated with among vehicles or network connectivity of vehicles during driving time on the road.

The remainder of the paper is organized as follows. State of art on trust management in VANET is presented in Section 2. Section 3 describes the problem formulation. In Section 4, proposed methodology is presented. Simulation and results are discussed in section 5. And finally, Section 6 briefly concludes the contribution.

2. State of Art

Trust in general is the level of confidence [6] of a person or a thing or it is a relationship between two entities as vehicles in VANET such that one vehicle believes and accepts that the other trusted vehicle will act or intend to act beneficially [7]. However, reputation is the opinion of one entity about another. Essentially it signifies the trustworthiness of an entity [8]. In VANET, trust is context dependent, dynamic and non-monotonic. In general, trust establishment is categorized into two categories first is infrastructure aided trust establishment and other is self-organizing. Infrastructure aided trust establishment is further sub classified into centralized and distributed. It may be based upon certificates from central authority in the presence of RSU. Similarly, self organizing trust establishment is further categorized into direct, hybrid and indirect. It may be based upon entity oriented trust, data oriented trust and combined trust.

Existing literature has very few approaches of trust computation in VANET. The trust computation method is based on Perron–Frobenius theorem [9] 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.

A reputation assisted trust management mechanism for VANET using privacy preserving trusted group formation is presented in [10]. In this scheme, pre-trusted vehicles are police vans/cars, ambulances and other government vehicles which can be trusted a priori. It will act as a group manager and initiates the formation of a group of vehicles moving on the road. It is also provided anonymity and traceability of group member vehicles in VANET. In [12], pre-authenticated anchor node is used to provide trustworthiness and identified malicious node. Another trust based message propagation model is proposed in [12]. Combined trust evaluation technique evaluates trustworthiness of data and maintains vehicle trust at the same time. Distribution reputation system is proposed in [13] using piggybacking approach. Survey of trust management approaches is presented in [17]. In the next section, problem formulation is presented.

3. Problem Formulation

In this section problem formulation is discussed with system and model assumption.

3.1. System and Model Assumption

VANET consists of vehicles (OBUs), RSUs along with the roads and TA. In this work, we focus on the token based trust computation for inter-vehicle communications over the wireless channel because in absence of infrastructure trust evaluation for vehicle moving on the road is a major security issue in VANET. We assume the followings:

Once the identity of vehicles in VANET is authenticated, the behaviours of the vehicles will not be monitored any more even though they might do something harmful. Vehicles have some initial trusted value assigned by RSU or TA as per nature depicted by Table 1. The TA is always online and trusted. Under TA there are so many RSUs. RSUs and TA communicate through a secure fixed wired network.

The RSUs have higher computation power than OBUs and communication range of RSU is 1000 meter and communication range of vehicle is 500 meter respectively *i.e.* RSU communication range is twice range of vehicle. The real identity of any vehicle is only known by the TA and itself but not by others. Vehicle can communicate certificate assigned and certified by RSU.
Trust evaluation of vehicle will calculated dynamically by vehicle itself on the basis of vehicle categories and time limit as shown in Table 1.

3.2. Problem Description

The main problem of security in VANET is trust computation, privacy and authentication. Here, we addressed trust computation problem of VANET. Hence, the safety related messages broadcast by vehicles are used by other vehicles to make critical decisions. Authenticated vehicles may also send wrong messages. This may trap a vehicle taking wrong decision with dire consequences. Moreover, VANET is high density network and every vehicle may communicate with each other vehicle and RSU within its communication range. Verification of each messages may overloaded the network. So, trust evaluation of messages at the time of driving is required for safe journey. Trust computation time and it's vaildation time are also major challenges in VANET [16], [18].

Our aim in this paper is to present a short certificate or token based trust computation technique and the value of trust based upon network connectivity of vehicles.

4. Proposed Methodology

The proposed trust evaluation methodology consists two cases in the presence of infrastructure and absence of infrastructure. The trust value will depend upon the network connectivity of vehicles with communication range during driving is shown in Table1. In this proposed technique, vehicle will request to authenticate itself from RSU and at the same time RSU will also authenticate to vehicle from TA via sameRSU. At this time vehicle also send the request for token or certificate on the basis journey time covered on the road. RSU assigns the initial trust value and token or certificate for trust value evaluation and extend privacy preserved mutual authentication. The mechanism is able to achieve privacy preservation of vehicle and authenticate to each other at the same time vehicle to RSU and RSU to vehicle along with the trust evaluation of messages using journey duration based tokens. The trust evaluation technique is simple and light weight. Format of token or certificate is shown by Figure 1.

Token ID	Vehicle Pseudo Identity	Journey Time	Initial Trust Value by RSU	Time Stamp
2 Byte	2 Byte	1 Byte	1 Byte	4 Byte

Figure 1 Structure of Token or Certificate

Table 1 Category of Vehicles on the basis on Time Association on the Road

S. No.	Types of Vehicles	Trust Value
1	Regular travelling vehicle on the specific road	7
2	Vehicle association time on the road more than 5 Hrs. to 10 Hrs.	5
3	Vehicle association time on the road more than 3 Hrs. to 5 Hrs.	3
4	Vehicle association time on the road more than 1 Hrs. to 3 Hrs.	2
5	Vehicle association time on the road less than 1 Hrs.	1

Algorithm for Tokens of Initial Trust Value()

Vehicle sends the request for authentication to RSU ($v \rightarrow RSU_i$) along with initial travel plan in terms of hours.

Step1. At the time of vehicle's authentication process. When vehicle enters in the communication range of RSU, it receives identity of RSU ID_{RSU} and public key of RSU $PK^{+}_{RSU_i}$ for sending authentication request and journey of time of vehicle.

Step2: Vehicle sends time of journey and MAC value.

$$v_i \rightarrow RSU_i: PE_{ID_{RSU}}\{PE_{K_{CTS}}(ID_v, t_0, ID_{RSU_i}), ps_0, T\}$$

Here, T is the journey time value of vehicle. The MAC value is the hash value of time stamp of vehicle and identity of vehicle.

$$ps_0 = h(ID_v, t_0)$$

The use of time stamp t_0 for freshness is to prevent message by replay attack / Sybil attack. Vehicle uses self generated pseudo identity ID_v from its storage pool to preserve the privacy. Encryption technique is used to maintain the confidentiality. The proposed technique is used two times encryption to prevent the forgery by RSU.

Step3: RSU forwards vehicle's authentication request to TA. And i^{th} RSU_i decrypt received request and store ps_0 and T, for the time duration until the TA does not send the response to the RSU of vehicle authentication.

$$RSU_i \rightarrow TA: \{PE_{K_{CTA}}(ID_v, t_0, ID_{RSU_i})\}$$

After receiving authentication report of vehicle by TA, RSU will generate the initial trust value on the basis of the request and send to the vehicle.

$$TA \rightarrow RSU_i: PE_{ID_{RSU}}[PE_{K_{CTs}}(ID_{RSU}, cert[Sig_{TA}, t_1], ID_v)\ ps_0, T]$$

The certificate is valid for a time period determined by the approximate duration of journey time.

Step4: $RSU_i \rightarrow v$: i^{th} RSU_i sends the initial trust value and authentication report to the vehicle.

$$RSU_i \rightarrow v: \{PE_{K_{CTA}}(ID_{RSU}, cert[Sig_{TA}, t_1], ID_v, T, S)\}$$

Here, t_1 is the time stamp of TA, journey time of vehicle T, initial trust value assigned by RSU is S_i.

Vehicle receives the initial trust value authentication certificate and at the same time vehicle will authenticate theRSU_i.

Table 2 Notation used for this Algorithm

Notation	Description
v_i	i^{th} Vehicle
RSU_i	i^{th} Road Side Infrastructure / Unit
$PK^{+}_{RSU_i}$	The Public key of i^{th} RSU_i
PE_{RSU_i}	A public-key encryption function using the i^{th} RSU_i's public key
TA	The trusted authority
ID_v	Unique identity of vehicle, issued by CTA
ID_{RSU}	Unique identity of i^{th} road side infrastructure, issued by CTA
Sig_{TA}	Signature of TA
$cert[Sig_{TA},t_1]$	The certificate signed by TA along with time- stamp

Algorithm for Evaluation of Trust Value for Vehicle

The algorithm is divided in two cases in the presence of RSU and absence of RSU.

Case 1: In the absence of RSU

Source vehicle receives the messages from vehicles with in transmission range. Vehicle receives initial trust value S. If message information is true then receiver vehicle will increase trust value as per nature of vehicle journey time. If message is false then receiver vehicle will decrease the trust value of neighbouring vehicle.

$$Final\ Trust\ Vlaue\ (S_F) = S_i \pm assigned\ S_i$$

Case 2: In the presence of RSU.

Vehicle receives the messages from vehicles and RSU with in transmission range. Vehicle receives initial trust value S. If information in messages is true then vehicle will increase trust value as per nature of vehicle journey time and compare the message sent by RSU. If both message are correct then increase trust value in addition with 10. If message is false of anyone vehicle with in transmission range of receiver vehicle and RSU will decrease the trust value of neighboring vehicles along with decrease 10 value of trust. If message of RSU is false then vehicle will inform through another adjacent RSU to TA.

$$Final\ Trust\ Vlaue\ (S_F) = S_i \pm assigned\ S_i \pm 10$$

If message from RSU is wrong in comparision of sufficient number of vehicles then vehicle may report TA through adjacent RSU or other infrascructure as petrol pumps, spot areas *etc* for malicious or misbehaviour nature or wrong message. So that, TA can notify to all vehicles in the network. Switch off same RSU or may be replaced along with new security credentials.

The proposed scheme is able to trace / revoke the malicious vehicles along with SUs, privacy preserved extended mutual authentication, confidentiality and simple light weighted trust evaluation scheme. Source vehicle can evaluate trusted message at the time of driving on the road, not only in the presence of RSU, but also in the absence of infrastructure. The approach can be applicable for safety, non-safety messages and VANET applications like location finding, toll collection, collision warning *etc*.

5. Simulation and Results

In this section, simulation setup and results are presented. Simulation is conducted to verify the efficiency of the proposed secure protocol for VANET communication with NCTUns [14]. For cryptographic delay we install Multi-precision Integer and rational arithmetic C/C++ library [15].

5.1. Simulation Set up

So for these cryptographic delays computation we run a program that contains computational time of all standard hash function and encryption / decryption algorithms. In trust computation process, delays are divided in two types of delays, communication delay and computational delay in both the algorithms.

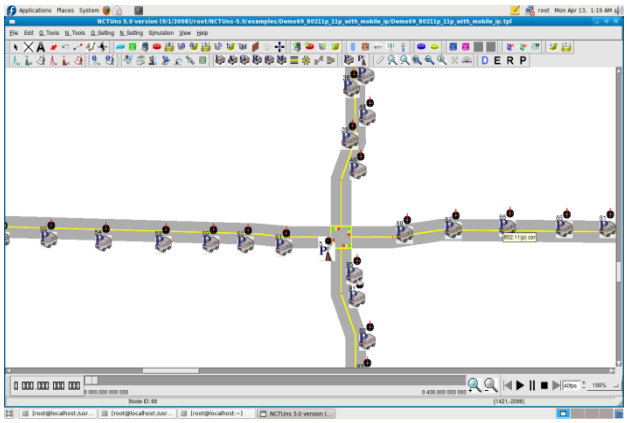

Figure 2. Simulation Setup in NCTUns

The communication delay is estimated by running the simulation experiment for different density of vehicles (5-40) and by varying the speed (10 - 30 ms^{-1}) and acceleration (3 ms^{-2}) of the vehicles. The computation platform was a desktop (CPU speed - 2.50 GHz, RAM - 2 GB RAM). We assumed token size is 10 Byte.

5.2. Results

Data packets were generated at a constant bit rate at *RSU* and the vehicle. Figure 3 shows the average and maximum communication delay when number of vehicles in the *RSU* region varies from 5-40 (DSRC).

The communication delay between vehicle to *RSU* is considered as per DSRC recommendation and also presented in [3], [4]. Packet length, communication range and vehicle density is considered in authentication as already presented in [16]. Figure 3 is showing the communication delay 105 ms maximum value at the speed of 10 ms^{-1} and 224 ms at the speed of 30 ms^{-1} respectively.

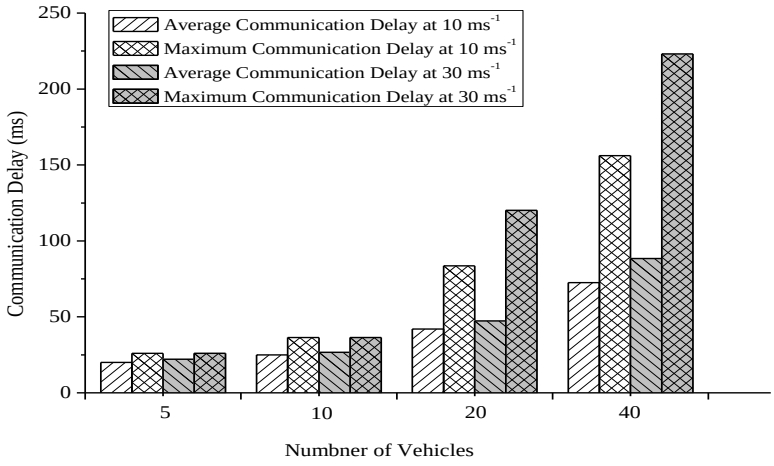

Figure 3. Communication Delay at Speed of 10 – 30 ms^{-1}

Delays for Algorithms of Tokens or Initial Trust Value ()

Communication delay in between *RSU* and vehicle is not considered because *RSU* will broadcast message with dedicated allocated channel, so if vehicle will within communication

range in *RSU* then vehicle will receive response for trust request association without delay like radio broadcast (DSRC).

Communication delay t_1 in step 1 is 224 ms at high speed and maximum delay as shown in Figure 3. Computational delay t_2 in step 2 is combination of two times encryption and one time hashing computation delay. So, computational delay t_2 in step 2 is 3.6 ms. Computational delay t_3 in step 3 is the decryption delay. So, the computational delay t_3 in step 3 is 3.32 ms. Similarly, computational delay t_4 in step 4 is also 3.32 ms. Total computational delay of initial trust value along with authentication vehicle is approximate 235 ms.

Evaluation of Token Based Trust Value ()

Case 1: When vehicle is moving on the road and infrastructure *RSU* is absent. If vehicle is received critical safety message from type 1 and type 2 vehicle or regular vehicle and vehicle association time on the road more than 5 Hrs. to 10 Hrs. than source vehicle will trust / priority high on type 1. Vehicle will assign trust value for both the vehicles if message information is correct.

$$S_{F_1} = 7 + 7 = 14$$
$$S_{F_2} = 5 + 5 = 10$$

If vehicle receives same messages from more than one vehicle i.e. vehicle will evaluate trust taking average information, example vehicle receives 10 messages from different vehicles and 7 are true 3 are false then vehicle assign trust value on the basis of average information. If vehicle found any critical situation or doubt than vehicle may use the case 2 or may take decision on the basis of previous record / on priority basis given in Table 1.

Case 2: When vehicle is moving on the road and infrastructure is present. If vehicle is received critical safety messages from type1, type2 and type4 vehicles along with message from *RSU*. In this case, vehicle found that message is false then vehicle will assign trust values to vehicles.

$$S_{F_1} = 14 - 10 = 4$$
$$S_{F_2} = 10 - 10 = 0 = \text{Malicious Vehicle}$$
$$S_{F_2} = 2 - 10 = Negative\ Value = Malicious\ vehicle$$

In this case, all vehicles having trusted value less than 2 are malicious vehicle. They may be re-authenticated and will take all security credentials means keys or pseudonyms and tokens from trusted authority. The un-trusted or malicious vehicle's list announced by *RSU*. The list of un-trusted vehicles may be downloaded at the time of connectivity from any infrastructural resources as petrol pumps, hot spot area and *RSU etc*.

In this proposed trust evaluation technique vehicle is not only to assign trust value but also may be able to find the malicious vehicles. These are authenticated vehicles but at some time if such vehicles send wrong messages then it should be traced. The proposed approach is distributed because VANET is high density and high mobility networks. Moreover, the proposed scheme is also simple and based on network connectivity time of vehicles moving on the road or driving duration time of vehicle in VANET.

6. Conclusion

This paper presents, the token based trust computation technique using travelling time association on the road in VANET. The proposed technique is able to work in the presence of infrastructure as well as absence of infrastructure. The proposed technique is simple, light

weight and viable for secure communication among vehicles in a VANET. This technique allows the vehicle assess the behaviour of the authenticated vehicle and take decisions quickly in critical situations without further confirmation from infrastructure. This trust mechanism also dissuades vehicles and RSUs malicious or selfish behaviour. This makes the scheme viable for implementation in VANET environment. However, further research is required to formation of trusted vehicle's group on demand for secure and safe communication along with comfort driving over when pre-trusted vehicles are absent in a region.

References

[1] Vinel, C. Campolo, J. Petit and Y. Koucheryavy, "Trustworthy Broadcasting in IEEE 802.11p/WAVE Vehicular Networks: Delay Analysis", IEEE Communications Letters, vol. 15, no. 9, **(2011)**, pp. 1010-1012.
[2] D. Jiang and Luca Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments", IEEE Vehicular Technology Conference (VTC Spring-08), **(2008)**, pp. 2036-2040.
[3] B. K. Chaurasia, S. Verma and G. S. Tomar, "Mechanism for Privacy Preservation in VANETs", In the International Journal of Grid and High Performance Computing (*IJGHPC*), Special Issue on: Grid computing and Security, IGI, vol. 2, no. 2, **(2010)**, pp. 12-22.
[4] Y. L. Morgan, "Notes on DSRC & WAVE Standards Suite: Its Architecture, Design, and Characteristics", IEEE Communications Surveys and Tutorials, vol. 12, no. 4, **(2010)**, pp. 504-518.
[5] B. K. Chaurasia and S. Verma, "Secure Pay While On Move Toll Collection through VANET", International of Computer Standards & Interfaces, Elsevier, vol. 36, no. 2, **(2014)**, pp. 403-411.
[6] L. J. Hoffman, K. L. Jenkins and J. Blum, "Trust beyond Security: An Expanded Trust Model", Comm. ACM, vol. 49, no. 7, **(2006)**, pp. 95-101.
[7] Q. Ding and Xi Li, "Reputation Management in Vehicular Ad-Hoc Networks", International Conference on Multimedia Technology (ICMT), **(2010)**, pp. 1-5.
[8] S. Ganeriwal and M. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SAN '04), **(2004)**, pp. 66-77.
[9] B. K. Chaurasia, S. Verma and G. S. Tomar, "Trust Computation in VANETs", The International Conference on Communication Systems and Network Technologies (CSNT-2013), **(2013)**, pp. 468-471.
[10] B. K. Chaurasia and S. Verma, "Trust Based Group Formation in VANET", International Journal of Modern Traffic and Transportation Engineering Research (MTTER), vol. 2, no. 2, **(2013)**, pp. 121-125.
[11] A. Patwardhan, A. Joshi, T. Finin and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks", Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems - Workshops, Mobiquitous, **(2006)**, pp. 1-8.
[12] C. Chen, J. Zhang, R. Cohen and P. H. Ho, "A trust-based message propagation and evaluation framework in vanets", Proceedings of the Int. Conf. on Information Technology Convergence and Services, **(2010)**.
[13] F. Dotzer, L. Fischer and P. Magiera, "Vars: A vehicle ad-hoc network reputation system", Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, **(2005)**, pp. 454-456.
[14] NCTUns, online available at: http://nsl.csie.nctu.edu.tw/nctuns.html.
[15] Shamus Software Ltd, MIRACL, Multiprecision Integer and Rational Arithmetic C/C++ Library, Available at http://indigo.ie/~mscott.
[16] B. K. Chaurasia and S. Verma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering, vol. 6, no. 2, **(2011)**, pp. 41-54.
[17] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. Ali Rezazadeh Baee and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review", EURASIP Journal onWireless Communications and Networking, vol. 146, **(2015)**, pp. 1-22.
[18] P. Rani, B. K. Chaurasia and G. S. Tomar, "ID- Based Authentication for WiMAX", International Journal of Future Generation Communication and Networking", vol. 9, no. 2, **(2016)**, pp. 211-218.

